060967-00 Rev. A

OmniVista Terra 10.5.1 Documentation

OmniVista Terra 10.5.1 Documentation

24 October, 2025

Table of Contents

1 Introducing OmniVista® Terra 5
2 Getting Started 6
2.1 Network and Device Prerequisites 8
2.2 Onboarding Devices for OmniVista Terra Management 13
2.3 Configure Your User Profile 20
2.4 User Interface 29
3 Configure Organizations for Network Management 60
3.1 Configure and Manage an Organization 61
3.2 Configure and Manage a Site 72
3.3 Configure and Manage a Building 83
3.4 Configure and Manage a Floor (Floorplans) 92
3.5 Configure and Manage Walls 101
3.6 Configure and Manage Users 109
3.7 Configure and Manage Organization Settings 126
3.8 License Management in OmniVista Terra 139
4 Configure and Manage Device Inventory 168
4.1 Device Catalog 169
4.2 NaaS Device Licenses 262
4.3 Locate a Device on a Floorplan 271
4.4 Schedule a Device Software Update 276
4.5 Managing Switch Configuration Backups 290
5 Configure WLAN Network Management 306
5.1 Profile 308
5.2 SSIDs 347
5.3 Wireless Intrusion Protection System (WIPS) 375
5.4 Advanced 387
5.5 Data VPN Settings 414
6 Configure and Manage LANs 418
6.1 Configure and Manage Layer 2 VLANs 419

6.2 Configure and Manage Layer 3 VLANs 443
6.3 CLI Based Provisioning 451
7 Configure Network Access Control 479
7.1 Unified Access 481
7.2 Authentication Servers 588
7.3 Groups 604
7.4 UPAM - NAC 619
7.5 Accounts 707
7.6 Application Visibility Signature Profiles 766
8 Monitoring Network Device Activity 773
8.1 Network Analytics 774
8.2 Location 943
8.3 Alerts 948
8.4 Diagnostic Tools 969
9 Automation with APIs 1022
9.1 What you'll find here 1022
9.2 Quick links 1022
9.3 Quick Start Guide 1023
9.4 Authentication 1035
9.5 API Reference 1042
10 Troubleshooting 1043
10.1 Troubleshooting Switch Management Problems (Management Connectivity, Configuration/ Statistics Updates, Configuration Not Delivered) 1043
10.2 I signed up for a new account (or an invited account), but I can't find the verification email to activate my account 1045
10.3 My account has been successfully created but I don’t see any data in OmniVista Terra 1045
10.4 From the OmniVista Terra UI, how do I know if my Access Points are connected to the platform? 1045
10.5 One of the three open browser tabs running OmniVista Terra is not responding 1045
10.6 I want to update a configuration object, but I can't click on the Save button. It is disabled (grayed out) 1045
10.7 When I edit a configuration and click on “Launch … in a new browser tab” to open another screen to edit a related configuration, when I return to the main screen, the Save button is disabled (grayed out) 1046

10.8 I open an SSH Terminal session after entering login credentials, but there is no message in the Terminal window console 1046

10.9 The Access Point Health Threshold data doesn’t reflect the changes done even after saving the changes and getting the success notification message..... 1046

10.10 The Device Health color and counter aren't updated after the threshold was saved and getting the success notification message. 1046

10.11 I am not able to customize the WiFi4EU captive portal template for SSID and got error 500 when deploy changes to Access Point with layout type WiFi4EU. 1047

10.12 In Configuration Backup table, I got timeout message after waiting for 1 minute "Can not connect to the server, the request has been timeout. Please try again later." 1047

10.13 When I click on Full screen mode to put table in full screen mode, the top toolbar buttons disappear. 1047

10.14 When I open an OmniVista Terra page, I wait for more than 15 seconds for the Loading the screen. 1047

10.15 For the Guest Access code or Guest Account screen, I cannot find the Service level or Registration Profile selection when creating or updating a Guest Account or Guest Access code. 1047

10.16 When I access the Wi-Fi Heatmap screen, the Device icon disappears upon selecting the Channel utilization option from the Device Layers drop-down list. 1047

10.17 When I try to copy the Golden Configuration content to the clipboard in the ‘Device Detail’ section on the left side of the screen (Monitor > Network > Analytics > Network Analytics), it does not work..... 1048

11 OmniVista Terra Installation 1049

11.1 Installation Introduction 1050

11.2 Prerequisites 1051

11.3 Deploying OmniVista Terra on VMware ESXi..... 1052

11.4 Deploying OmniVista Terra from vSphere Client 1059

11.5 OmniVista Admin Center 1064

11.6 Configuring DNS for OmniVista Terra 1075

11.7 How to Onboard an AP and Switch..... 1076

11.8 License Management Overview..... 1078

11.9 Uploading AOS/AWOS Images 1080

11.10 Guidelines and FAQs 1082

12 OmniVista Terra Release Notes..... 1085

12.1 OmniVista Terra Release Notes (October 2025) 1086

1 Introducing OmniVista® Terra

OmniVista Terra is an on-premise Network Management System that simplifies the monitoring and managing of Stellar Access Points and AOS Switches from an easy-to-read dashboard display. A free trial version is offered that extends for 90 days and can be used to manage up to 20 devices (additional time and number of devices can be requested).

This release of OmniVista Terra provides a licensed-based solution that enables a Network Administrator to set up a Management Portal for their Organization. Once an Organization is created, the Network Administrator invites users to access the Organization's Management Portal. These are known as Organization Users.

When an OmniVista Terra account is created, a default Organization Management Portal is created. The Network Administrator can then create different physical sites under that Organization. Or, create additional Organization Management Portals. For example, in a university system the Administrator could set up an Organization for each campus (e.g., Northridge, Channel Islands) and invite users to access each Organization.

Refer to the following documentation for more information about using OmniVista Terra:

- Getting Started (see page 6) - Details information you need to know to get up and running with OmniVista Terra, including creating an OmniVista Terra Account and creating and managing Organizations (creating sites, adding devices, creating users). It also provides an overview of the OmniVista Terra User Interface to help you navigate the application.
- OmniVista Terra Installation Guide (see page 1049) - Details the OmniVista Terra 10.5.1 installation procedure. OmniVista Terra 10.5.1 can be installed as a fresh installation from a downloaded file available on the Customer Support website. OmniVista Terra is distributed and installed only as a VMware Appliance. There are no other standalone installers (e.g., Windows/Linux). The "Prerequisites" section in this guide defines the system and hypervisors to use for OmniVista Terra deployment.
- OmniVista Terra 10.5.1 Release Notes (see page 1086) - Details features and functions, network/device configuration prerequisites, supported devices, and known issues/workarounds in OmniVista Terra 10.5.1.

21 Oct 2025

2 Getting Started

This section details information you need to know to get up and running with OmniVista Terra, including creating an OmniVista Terra Account and creating and managing Organizations (creating sites, adding devices, creating users). It also provides an overview of the OmniVista Terra User Interface to help you navigate the application.

Use the information provided in the following sections to get started with OmniVista Terra:

- Network and Device Prerequisites (see page 8) - There are certain prerequisites that you **must verify/configure** on your local network and devices **before getting started**. For example:
  - Network DHCP Server, Firewall, and NTP Server requirements.
  - Minimum AWOS software release requirements for Access Points.
  - Minimum AOS software release requirements for Switches.
  - Upload AWOS and AOS image files to the OmniVista Image Server to support the upgrade of device images through OmniVista Terra 10.5.1. This procedure is required and is covered in the OmniVista Terra 10.5.1 Installation Guide (see page 1049).
- Create an Account/Access Management Portal (see page 1049) - OmniVista Terra is installed from download files available on the Customer Support website. When the installation is complete, you will have an initial Network Administrator login and an Organization that was created based on the information you provided during the installation process. Use this login to create additional Organizations and invite users to access the Organization(s).

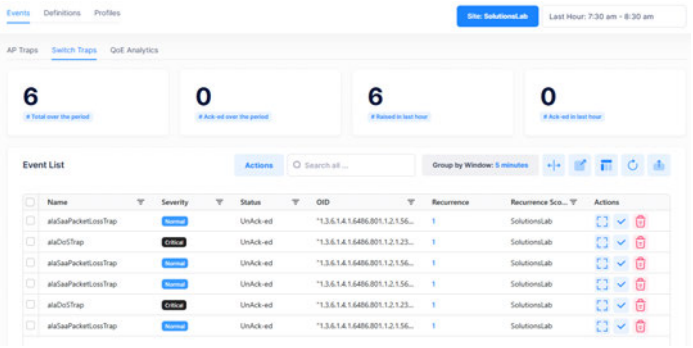
> When you initially login to OmniVista Terra, the default password for your account is “changeme”. You are then required to change the password at that time.

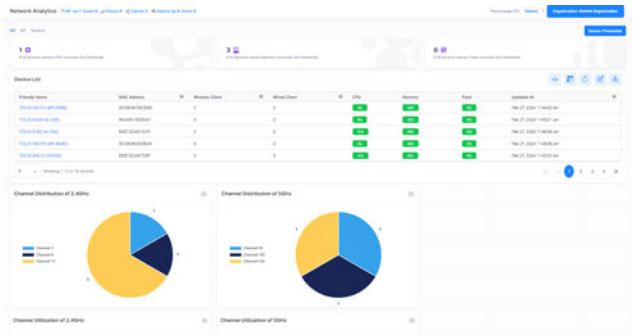
- Onboarding Devices Workflow (see page 13) - The basic steps involved to onboard Access Points and Switches for management in OmniVista.
- Declare your Devices in OmniVista (see page 169) - Learn how to declare your devices (Access Points and switches) using the Device Catalog application. When you add an Access Point or switch to the Device Catalog, the device serial number is sent to the OmniVista Server for validation.
- Start the Device Activation Process (see page 195) - A device must connect to the OmniVista Server to complete the activation process. After a device is added to the Device Catalog, connect the device to the network and power it on. The device will automatically call home to the OmniVista Server to register and complete the activation process, if the Network and Device Prerequisites (see page 8) have been met.

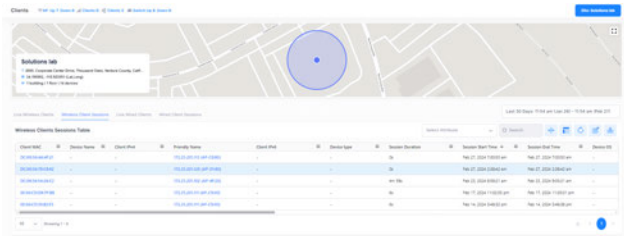
Once the above requirements are met and the devices are declared, you can start to manage and monitor your network devices using OmniVista Terra.

Additionally, you may want to:

- Configure Your User Profile (see page 20) - Edit your basic User Profile, including user information, password, login security, and user preferences (for example, UI appearance, display color scheme).
- Discover the User Interface (see page 29) - Provides an overview of the OmniVista Terra User Interface for the the Organization Dashboard, including common tools used for working with tables and graphical displays, as well as the OmniVista Menu, which is used to access OmniVista functions and applications.







21 Oct 2025

2.1 Network and Device Prerequisites

To ensure the necessary communication between network devices and OmniVista Terra, verify/configure the following prerequisites on your local network:

- Network DHCP Server, Firewall, and NTP Server requirements (see page 9)
- Minimum software release requirements for network devices (see page 12)

21 Oct 2025

2.1.1 Network Prerequisites

2.1.1.1 OmniVista Terra Internet Access

OmniVista Terra (OV Terra) is installed as an on-premise Network Management System that may or may not have access to the Internet. If the OV Terra installation does not have Internet access, then some of the features may not function. For example:

- IoT Categorization default list
- IoT Category & Manufacturer details about each client
- OpenStreetMap
- Rainbow integration
- SMS gateway
- Email integration, if Gmail Enterprise (or other email applications) are used.
    - The email server specified in the SMS Settings of the OmniVista Admin Center must be reachable from OV Terra. If the server is internal to the network, then the email server is reachable. However, if an external email server is used for the network, then access to the server is mandatory to support several critical functions, such as Invite User, Forgot Password, and receiving emails for Reports and Alerts.

The OV Terra installation is connected to a gateway in the network. To provide selective Internet access for specific features, you can define rules either on the gateway or on a firewall within the network to allow traffic from OV Terra to specific IP addresses and ports.

> If you decide to not open access, then the features that require Internet access will not function.

2.1.1.2 Device Connectivity to OmniVista Terra

To ensure the necessary communication between devices (Access Point/Switch) and OmniVista Terra 10.5.1, verify/configure the following Network Deployment (see page 9), Bandwidth (see page 10), Proxy (see page 10), Firewall (see page 11), and NTP Servers (see page 11) configurations must be verified/configured on your local network before using OmniVista Terra.

2.1.1.2.1 Network Deployment

Verify the following DHCP deployment requirements are met:

Standard Requirements

- **IP Address -** DHCP Server IP address.
- **Option 1 -** Subnet Mask.
- **Option 2 -** Gateway.
- **Option 6 -** Domain Name Servers - Required for FQDN resolution of OmniVista Terra connection points.

- **Option 28 -** Broadcast Address. This option is only recommended, **not** required.
- **Option 42 -** NTP Server(s) - Required for Certificate validation (start date and duration), and all related encryption functions. This option is **not** required; however, it is recommended.

ALE Specific Requirements

- **Option 43**
  - **Sub-Option 1** - Vendor ID. Validate the DHCP response (**must** be set with the value **alenterprise**). This sub-option is **only** required if you specify any of the sub-options listed below.

Refer to Access Point Onboarding Workflow (see page 13) for information about configuring Option 43 to onboard Stellar Access Points for OmniVista Terra to manage.

The following Sub-Options are **only** required if you are **using a Proxy** to connect to the Internet.

- **Sub-Option 129 -** Proxy URL. It can be either an IP address or a URL (e.g., "IP-address=4.4.4.4", "URL=http://server.name").
- **Sub-Option 130 -** Proxy Port.
- **Sub-Option 131 -** Proxy User Name. If the customer proxy access requires authentication, both 131 and 132 can be supplied via these sub-options.
- **Sub-Option 132 -** Proxy Password.
- **Sub-Option 133 -** Network ID.
- **Option 138 -** Remove any existing configuration (required for all ALE Devices).

2.1.1.2.2 Bandwidth Requirements

Onboarding
For basic onboarding of devices and connection to the OmniVista Terra Server, a minimum of 10 kbps end-to-end network throughput is required between the device and OmniVista Terra.

Advanced Management
To enable statistics data transfer, status queries, configuration commands, and other requests/ responses between devices and OmniVista Terra, a minimum of 64 kbps end-to-end network throughput is required between the device and OmniVista Terra. APs must be running the latest AWOS software version specified in Device Prerequisites (see page 12).

2.1.1.2.3 Proxy Requirements

If a device is accessing the Internet via an HTTP/HTTPs proxy, the proxy server must be specified in DHCP Option 43, Sub-option 129 (Server) and Sub-Option 130 (Port). The server may be specified in 1 of 2 formats: 1) “URL=http://server.domain”, or 2) “IP-address=x.x.x.x”. The port is specified as a number (8080).

2.1.1.2.4 Firewall Requirements

The following ports must be configured to allow outbound traffic from your local network:

- **443 -** If you are not using a Proxy to connect to the Internet, your firewall must allow outbound access to this port; if you are using a Proxy, you need to be able to access this port via your local proxy.
- **123 -** Relevant if you are using an NTP Server that is outside of your network. You must ensure that your firewall allows outbound access to port 123 UDP. This access cannot be mediated by a proxy, it must be direct (NAT is allowed). In addition, open this port for the following:
  - clock1.ovcirrus.com
  - clock2.ovcirrus.com
  - clock0.ovcirrus.com
  - clock3.ovcirrus.com.
- **53 -** Relevant if you are using a DNS Server that is outside of your network. You must ensure that your firewall allows outbound access to both port 53 TCP and port 53 UDP. This access cannot be mediated by a proxy, it must be direct (NAT is allowed).

2.1.1.2.5 NTP Server Requirements

An NTP Server(s) is required for Certificate validation (start date and duration), and all related encryption functions. Devices must have access to at least one NTP Server, whether local or external. Note that if a device's System Time is not correct, it may take several attempts to synchronize with the NTP Server before the device connects to the OmniVista Terra Server.

21 Oct 2025

2.1.2 Device Prerequisites

The device prerequisites provided in this section apply to the following devices:

- Access Points that are fully managed by OmniVista Terra.
- AOS Switches that are fully managed by OmniVista Terra.

The minimum device software versions for onboarding and management are detailed below.

2.1.2.1 Onboarding

For onboarding (call home and connection to OmniVista Terra), devices must be running the following **minimum** software versions:

- **AOS 8.9R4** - If the AOS device is running a software version less than 8.9R4, you must manually upgrade the device to 8.9R4 (or higher) when the device is added to the Device Catalog.
- **AWOS 5.0.3** - If the AWOS device is running a software version less than 5.0.3, you must manually upgrade the device to 5.0.3 when the device is added to the Device Catalog.

Notes:

- There are configuration steps that must be completed to onboard devices. See the OmniVista Terra Installation Guide and the Onboarding Devices for OmniVista Terra Management (see page 13) online help for more information.
- When a switch running AOS 8.10.R1 GA boots up without a vcboot.cfg file for auto-configuration, the SSH is disabled by default causing provisioning to fail. Only the console is enabled. This is not limited to a particular platform and can be seen on any switch running AOS 8.10.R1. To workaround this issue, you can do one of the following:
  - Enable AAA authentication SSH on the 8.10R1 GA switch via the CLI.
  - Upgrade to AOS 8.10R1 MR1 or AOS 8.10R2 (or higher) release, which include a fix for this problem.

2.1.2.2 Management

Click here for a list of supported Stellar Access Points and AOS Switch models, which includes the minimum supported releases and the license information based on the licensing model.

Devices must be running the software versions specified to support all of the features available in OmniVista Terra.

21 Oct 2025

2.2 Onboarding Devices for OmniVista Terra Management

This section describes the required prerequisites and general workflow to onboard OmniSwitch and Access Point devices for OmniVista Terra Management, as well as troubleshooting information.

- Switch Onboarding Workflow (see page 13)
- Access Point Onboarding Workflow (see page 17)
- Troubleshooting (see page 18)

2.2.1 Switch Onboarding Workflow

The process to onboard AOS Switches for OmniVista management is described in this section. It is important to verify and configure the required prerequisites (see page 13) before attempting to onboard and provision a switch.

When a switch powers on, it contacts the DHCP Server and gets the location of the OmniVista Activation Server. The Cloud Agent on the switch then makes an HTTPS call to the OmniVista Activation Server and is matched to a Device Catalog entry containing the Management User and Provisioning Templates for that switch/switch model. OmniVista then uses SSH to log into the switch using the credentials specified in the Management User Template and configures/provisions the switch. Once provisioning is complete, the switch is manageable by OmniVista.

2.2.1.1 Verify the Required Prerequisites for Onboarding Switches

The prerequisite configurations below must be completed to ensure a successful onboarding process. Once the prerequisites are met, switches can be deployed as described in the Basic Deployment Workflow (see page 14) section.

- Verify Network Prerequisites (see page 9) are configured. For example: DHCP, Firewall, DNS settings.
- Verify Device Prerequisites (see page 12) for the switch are configured. For example: Minimum AOS software supported; license info; models supported
- CLI-Based Provisioning (see page 451)
  - At a minimum, the Management User Template (see page 472) is pushed to the switch. This template provides the login credentials that OmniVista will use to communicate with the switch. A Default Management User template is used, unless you select another template. The Default Management User Template uses the “admin/switch” login credentials to connect with the Switch.
  - Configure any additional configuration to append to the switch configuration through CLI commands in a Provisioning Template (see page 313).
  - Configure CLI-Based Provisioning Settings (see page 478) to specify the onboarding process for switches with no initial configuration (no initial template, no value mapping).
- To implement a global redirect configuration for Captive Portal authentication on an OmniSwitch, you have to manually configure the redirect settings through the switch CLI. This step is required until OmniVista supports Global Configuration in a future release. To configure a redirect for Captive Portal authentication, use one of the following methods:

- Configure the redirect on the switch using the redirect server IP address (use nslookup to find the IP address). For example:

```
nslookup <server domain name>
unp redirect pause-timer 60
unp redirect proxy-server-port 1024
unp redirect server <server IP>
```

- Configure the redirect on the switch with the redirect server domain name (no need to use nslookup). For example:

```
unp redirect pause-timer 60
unp redirect proxy-server-port 1024
unp redirect server us.manage.ovcirrus.com
```

  - Note that the server domain name should match the FQDN for the OmniVista cluster. Refer to the Creating a Guest Access Strategy (see page 633) screen to obtain the cluster FQDN.

2.2.1.2 Basic Deployment Workflow

The basic deployment workflow is slightly different for new "out-of-the-box" (see page 14) switches or currently-deployed switches (see page 15).

2.2.1.2.1 New Switches

1. OmniVista Terra uses SSH to log into the switch using the credentials specified in the Default Management User Template and configures/provisions the switch. It is recommended that you change the login credentials contained in this template or create a new Management User Template (see page 472).
   Note: After switches are successfully onboarded and provisioned, it is highly recommended that you change the default "admin" password on the switches.
2. Make sure the switch has Internet access and is running from the Working directory.
3. Declare the switch(es) in the Device Catalog List and specify the Management User Template and the required Provisioning Template (see Prerequisites (see page 13) above) to assign to the switch.
4. Connect the switch(es) to the network.
5. New “out-of-the-box” switches automatically call the OmniVista Activation Server when first connected to the network. OmniVista verifies the call home request is from an AOS switch, then checks if the switch serial number is already declared in the Device Catalog List for an Organization. If found, OmniVista returns the required certificates that the switch needs to initiate a VPN connection to OmniVista.

6. The switch initiates the VPN connection. Once the connection is made, OmniVista downloads, installs, and starts the OmniVista Terra Agent (see page 232) on the switch. The OmniVista Terra Agent package consists of a monitoring and configuration agent that interacts on a push-pull, on demand basis with OmniVista to manage switches.
7. OmniVista then delivers the provisioning configuration (Management User Template and Provisioning Template) assigned to the switch when you added the switch to the Device Catalog List. When the provisioning configuration is sent, OmniVista applies the following CLI commands to the switch to set up Event Configuration (see page 1004):

Provisioning Config (OV_provisioning_vcboot.cfg)

```
1 user ovngv3_sha_aes password "  password  " read-only all SHA384+AES allow-ssh disable
2 aaa authentication snmp local
3 snmp authentication-trap enable
4 snmp station 143.209.0.2 31162 ovngv3_sha_aes v3 enable
5 snmp-trap filter-ip 143.209.0.2 5 6 7 8 9 10 11 12 13 14 16 17 18 19 20 21 22 23 24 25 26 27 28 29 32 33 34 35 36 37 38 39 40 41
6 snmp-trap filter-ip 143.209.0.2 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132
7 snmp-trap filter-ip 143.209.0.2 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233
8
```

8. Once the switch is onboarded in OmniVista, the switch running configuration will become unsaved. OmniVista will automatically save the configuration if "Certify" (see page 208) was enabled (the default) when you added the switch to the Device Catalog List. If the “Certify” option was disabled, then the switch configuration remains unsaved and you should perform a "Save to Running" (see page 227)action from the Device Catalog.
9. When the switch is successfully onboarded and managed, the Activation Status and Management Connectivity (see page 170) for the switch is updated in the Device Catalog.

2.2.1.2.2 Currently Deployed Switches

A switch should be running from the Working Directory for provisioning. If a switch is running from the Certified Directory, reload the switch from the Working Directory before beginning the steps below.

> Note that a switch running from the Certified Directory can be provisioned, however, the configuration is temporary and will not be persisted. The switch will lose its configuration if it reboots. If a switch is provisioned from the Certified Directory, reload the switch from the Working Directory and "Force Provision" the configuration to the switch from the Results screen. When you "Force Provision" a switch, the configuration is pushed to the switch the next time the switch contacts OmniVista Terra. See the Results Screen online help (see page 453) for more information on manually pushing ("Force Provisioning") a configuration to a provisioned switch.

1. If the switch is currently managed by OmniVista Cirrus 10 or OmniVista Cirrus 4, you must remove certificates from the switch before adding the switch to OmniVista Terra. Otherwise, go to Step 2. Use the following CLI command to remove the listed certificates:

```
-> cd switch/cloud
```

```
-> rm -f client.crt cloudCAchain.pem csr.crt private.key public.key
```

2. Go to the CLI-Based Provisioning Management User Templates (see page 472) screen to view/configure the Default Management User Template or the template you want to assign to the switch when the switch is added to the Device Catalog List. The Management User Template is initially applied to a switch that is successfully provisioned and enables OmniVista management of the switch.
   a. Select "Use existing credentials" and enter the current CLI/FTP Username and Password for the switch. OmniVista will expect these credentials to already exist on the switch. See the Management User Templates online help (see page 472) for more information on configuring the Management User Template.
   Note: If the switch username/password is different than the one defined in the Management User Template, OmniVista will be unable to connect to the switch and provisioning will fail. The switch will be displayed on the Results screen with a Provisioning Status of "Failed". If this happens, configure the "Use existing credentials" option on the Management User Template, and "Force Provision" the switch. See the Results (see page 453) screen online help for more information on "Force Provisioning".
3. Declare the switch(es) in the Device Catalog List and specify the Management User Template and the required Provisioning Template (see Prerequisites (see page 13) above) to assign to the switch. When the switch(es) contacts OmniVista, it will be matched to a corresponding Device Catalog List entry and the configuration in the templates will be pushed to the switch(es). The CLI-based configuration in the Provisioning Template is appended to the existing switch configuration file.
4. To enable a currently-deployed switch to contact the OmniVista Server, you must telnet to the switch and modify the cloudagent.cfg file and enable the Cloud Agent:
   a. **Modify the cloudagent.cfg file** - Configure the "Activation Server URL" field in the cloudagent.cfg file and enter the FQDN - ***activation.myovterra.com***.
   b. **Enable the Cloud Agent -** Telnet to the switch and issue the following command: **cloud-agent admin-state enable**.
5. Once the connection is made, OmniVista downloads, installs, and starts the OmniVista Terra Agent (see page 232) on the switch. The OmniVista Terra Agent package consists of a monitoring and configuration agent that interacts on a push-pull, on demand basis with OmniVista to manage switches.
6. OmniVista delivers the provisioning configuration (Management User Template and Provisioning Template) assigned to the switch when you added the switch to the Device Catalog List.
7. When the switch is successfully onboarded and managed, the Activation Status and Management Connectivity (see page 170) for the switch is updated in the Device Catalog.

When a Provisioning Template is pushed to the switch, the configuration in the template is appended to the existing switch configuration file. If the Provisioning Template configuration conflicts with the current switch configuration, provisioning will fail and the device will not be manageable by OmniVista. If provisioning fails, go to the Results (see page 453) screen and check the "Last Provision Message" column for more information. If the Provisioning Template is the problem, make any

necessary updates to the Provisioning Template then “Force Provision” the configuration to the switch from the Results screen. The next time the switch contacts OmniVista, provisioning should be successful. See the Results (see page 453) screen online help for more information on manually pushing ("Force Provisioning") a Rule to a switch.

2.2.2 Access Point Onboarding Workflow

The process to onboard Stellar AP devices for OmniVista management is described below. It is important to verify and configure the required prerequisites (see page 9)before attempting to onboard and provision Access Points.

The following is the basic deployment workflow for onboarding Stellar AP Series devices for OmniVista Terra management.

1. If the AP is currently managed by OmniVista Cirrus 10 or OmniVista Cirrus 4, you must remove certificates from the AP before adding the AP to OmniVista Terra. Otherwise, go to Step 2. Use the following commands to remove the listed certificates:

```
rm -rf /.ocloud/callhome_hash.json /.ocloud/certificateFile.cert
/.ocloud/cloudCaChain.pem /.ocloud/privateKey.key /.ocloud/csr.csr
/.ocloud/publicKey.key ./privateKey.key.dec
```

2. Configure ***option 43*** for the AP in your DHCP server:

```
option 43
[010C616C656E7465727072697365801F687474703A2F2F6163746976174696F6E2E6D796F7674657
272612E636F6D];
```

   - For example, if you want to configure the **dhcpd.conf** file in the core switch to which the AP is connected: (*Note that the following is a sample configuration only. Use IP addresses, domain name server, and NTP server information specific to your deployment*.).

```
manual-dhcp dc:08:56:3c:2f:20 10.95.171.178 {
option subnet-mask 255.255.255.0;
option routers 10.95.171.1;
option domain-name "myovterra.com";
option domain-name-servers 10.95.163.213;
option ntp-servers 112.111.111.108;
option 43
[010C616C656E7465727072697365801F687474703A2F2F6163746976174696F6E2E6D796F76
74657272612E636F6D]
;
option 43 activation.myovterra.com;
}
```

- The option 43 hexadecimal string is equivalent to the following: **alenterprisehttp://activation.myovterra.com**.

3. Enter the **dhcp-server restart** command on the switch.
4. Enter **first boot** and **reboot** commands on the AP.
5. Declare the AP device(s) in the Device Catalog List (see page 170).
6. Make sure the AP has Internet access.
7. Connect the AP to the network and power it on.
8. The AP will automatically call the OmniVista Activation Server.
9. OmniVista verifies the call home request is from an AWOS AP device, then checks if the AP serial number is already declared in the Device Catalog List for an Organization. If found, OmniVista returns the required certificates that the AP needs to initiate a VPN connection to OmniVista Cirrus.
10. The AP will then connect with OmniVista Terra.
11. If the AP is unable to connect with OmniVista Terra, the AP will operate in Express Mode and periodically call home until the AP is able to connect with OmniVista Terra.
12. The AP is registered and licensed once it successfully connects with OmniVista Terra.
13. When the AP is successfully onboarded and managed, the Activation Status and Management Connectivity (see page 170) for the AP is updated in the Device Catalog.

2.2.3 Troubleshooting the Onboarding Process

2.2.3.1 Provisioning Fails

- If provisioning fails, go to the Results screen (see page 453) and check the "Last Provisioning Message" column for the reason. The most common cause of failure is that OmniVista does not know the correct credentials to SSH/SFTP the switch. The credentials that OmniVista uses to connect to the switch are specified in the Default Management User Template (see page 472) or in a Custom Management Template. If the Provisioning Template (see page 459) is the problem, make any necessary updates to the Provisioning Template, and save it. The next time the switch contacts OmniVista, provisioning should be successful.
- For additional troubleshooting information, refer to the Device Onboarding - FAQs/Troubleshooting (see page 210) online help page.

2.2.3.2 Verify the OmniVista Terra Agent Installation On the Switch

In addition to the OmniVista Terra Agent options (see page 232) available through the OmniVista Cirrus UI, you can also perform the following CLI commands on the switch.

To verify the Agent was successfully downloaded and installed on the switch, use the **show pkgmgr** CLI command:

```
OS6465--> show pkgmgr
Legend: (+) indicates package is not saved across reboot
        (*) indicates packages will be installed or removed after reload
 Name               Version           Status             Install Script
---------------+--------------------+-----------------+--------------------------------
  ams           default               installed          default
  ams-apps      default               installed          default
  ovng-agent    1.11                  installed          /flash/working/pkg/ovng-agent/install.sh
```

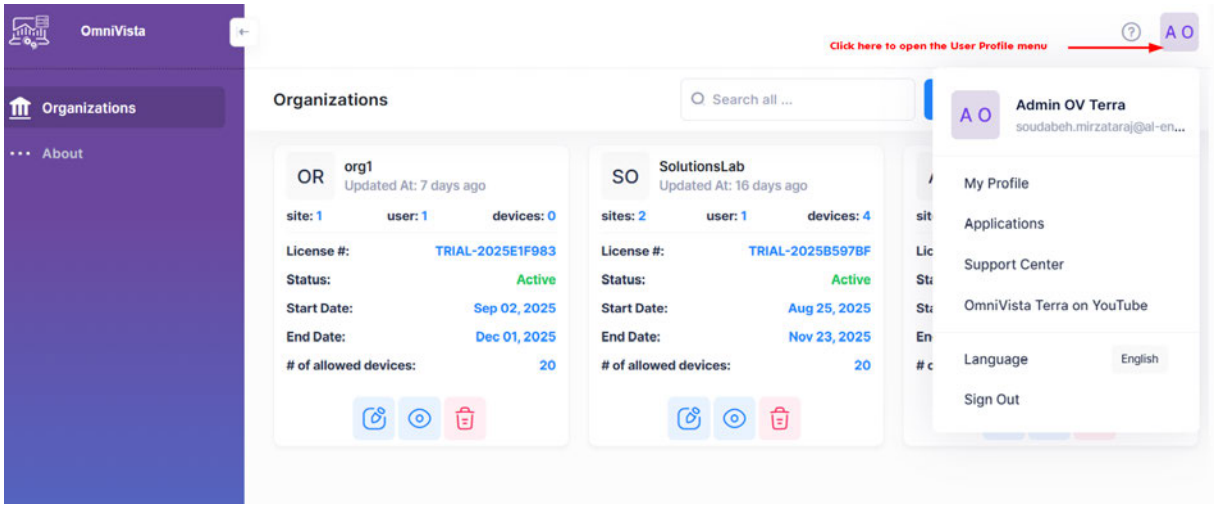
To verify that the two components of the OmniVista Terra Agent package (Config Agent and Monitoring Agent) were started, use the **show appmgr** CLI command:

```
OS6465--> show appmgr
Legend: (+) indicates application is not saved across reboot
  Application    Status    Package Name        User                  Status Time Stamp
---------------+---------+------------------+---------------------+---------------------
  config-agent  started   ovng-agent          admin                Fri Feb  2 19:23:47 2024
  monitoring-agent started   ovng-agent          admin                Fri Feb  2 19:23:51 2024
```

23 Sep 2025

2.3 Configure Your User Profile

Your basic User Profile is created from the information you enter when you create your OmniVista Account (e.g., Name, Company Name, Password). However, you can edit your User Profile at any time. Click on your login initials in the upper-right corner of any screen to open the User Profile drop-down menu. Updates are made to your User Profile only.



The following options are available:

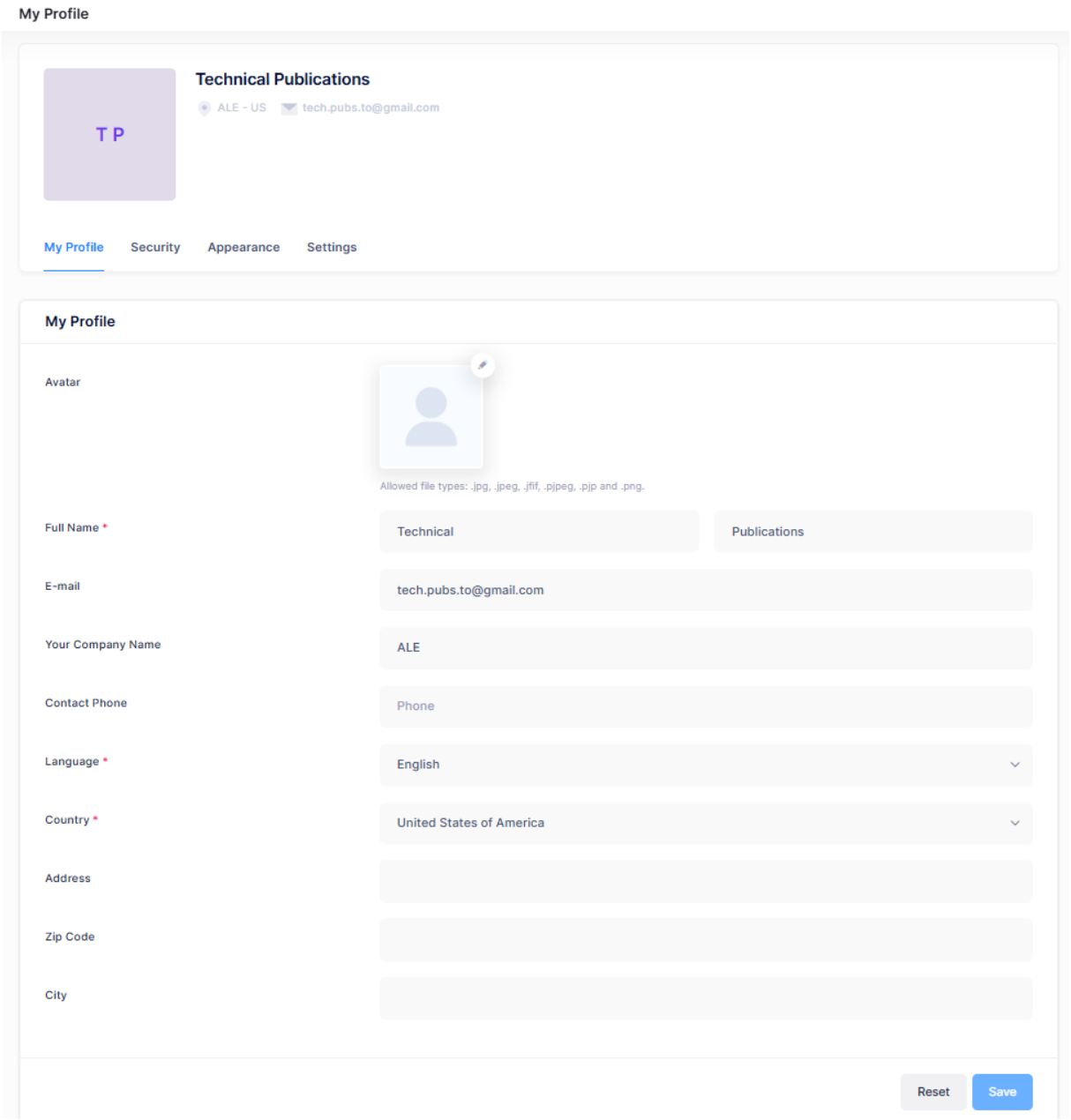
- **My Profile -** Edit your Account Information (see page 21), Login Security (see page 23), configure user preferences (see page 26) for the UI look and feel, and enable login history.
- **Applications -** Create custom APIs for OmniVista. Click here (see page 1022)for more information.
- **Support Center -** View OmniVista On-Line Help.
- **OmniVista Terra on Youtube** - View OmniVista tutorial videos on YouTube.
- **Language -** Select the language to display in the UI (English, French).

21 Oct 2025

2.3.1 My Profile - Account Information

Your basic User Profile is created from the information you enter when you create your OmniVista Account (e.g., Name, Company Name, Password). However, you can edit your account information at any time.

Open your User Profile Menu by clicking on your login initials in the upper-right corner of any screen, then select **My Profile.** The My Profile account information tab opens. Edit any field as described below, then click on **Save**.



- **Avatar -** Click on the Camera icon and upload a .png, .jpg, or jpeg file.
- **Full Name -** You can edit your name.
- **E-mail -** Filled in when your account was created. Cannot be edited.

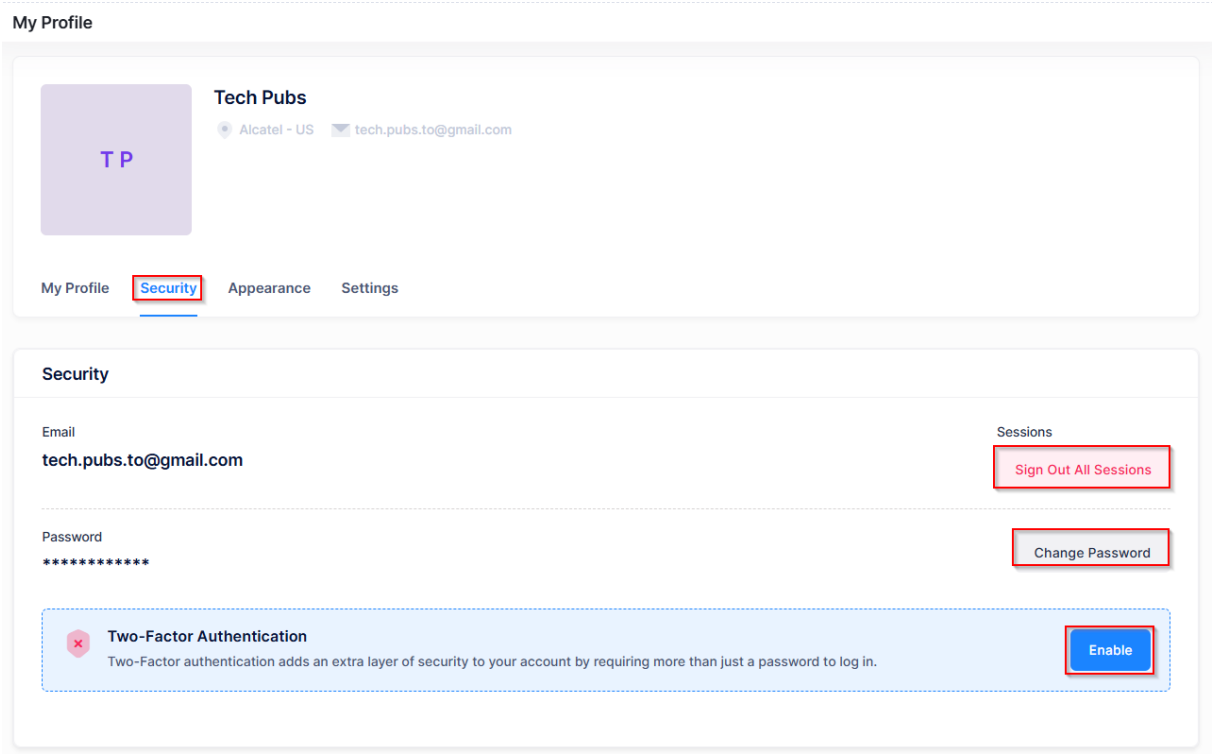
- **Your Company Name -** Filled in when your account was created. Cannot be edited.
- **Contact Phone -** Enter a contact phone number.
- **Language -** Select the language to display in the UI (English, French).
- **Country -** You can edit your country by selecting a country from the drop-down menu.
- **Address -** Enter your company street address.
- **Zip Code -** Enter your company Zip Code.
- **City -** Enter your company city.

21 Oct 2025

2.3.2 Login Security

Your OmniVista login password is created when you create your account. You can change it at any time on the Security menu.

Open the Security tab by clicking on your login initials in the upper-right corner of any screen. Select **My Profile**, then click on the **Security** tab. Edit any of the login security attributes as described below.

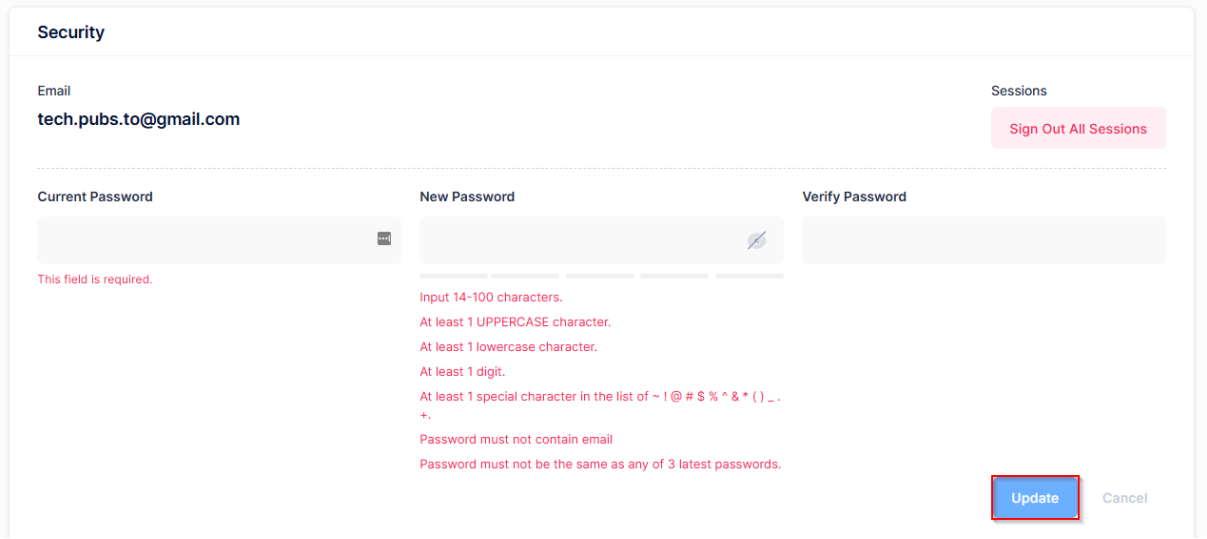


2.3.2.1 Sign Out All Sessions

The “Sign Out All Sessions” option allows you to log out of all active sessions by disabling all current authentication tokens, including both your current web session and any other web or external application sessions. When you sign out, all authenticated sessions will require you to log in again. You will be redirected to the login page.

2.3.2.2 Change Password

Click on **Change Password** to update your login password settings. You are prompted to enter the following:



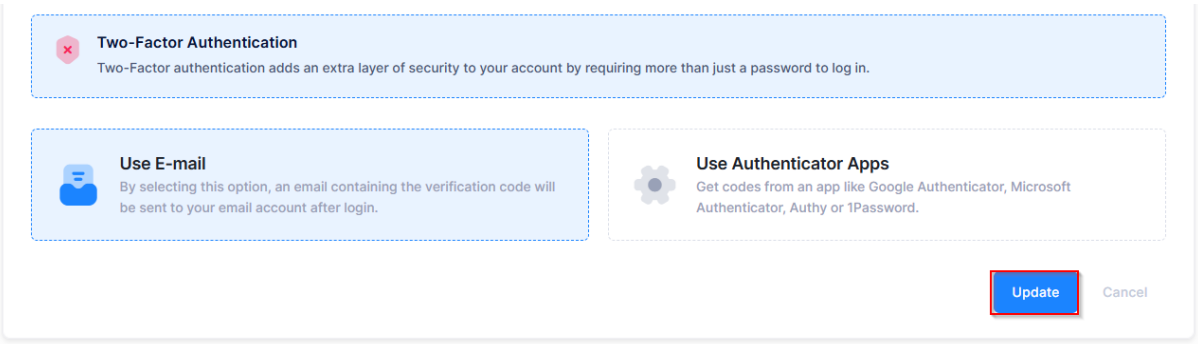
- **Current Password** - Enter your current password.
- **New Password** - Enter a new password following the guidelines shown below this field.
- **Very Password** - Enter the new password again to confirm the password change.

Once you have entered the required password information, click on **Update** to change the current password to the new one. Note that after the password is changed, all active sessions are disabled and required to authenticate again.

> To reset the password, you should follow the Enforcement password policy (EPP) guidelines. For more information, see the Basic Settings (see page 127) online help page.

2.3.2.3 Two-Factor Authentication

You can also use the Two-Factor Authentication method to enhance the security of your account. Click on **Enable** to configure Two-Factor Authentication. You are prompted to select the following options:



- **Use E-mail** - Select this option to have an email containing a verification code sent to your email account after you login. To log into OmniVista, enter your username/password, then the verification code provided in the email.

- **Use Authenticator Apps** - Select this option to use a verification code obtained from an authenticator application (such as Google Authenticator, Microsoft Authenticator, Authy or 1Password). To log into OmniVista, enter your username/password, open the authenticator application, and enter the code for your account.

21 Oct 2025

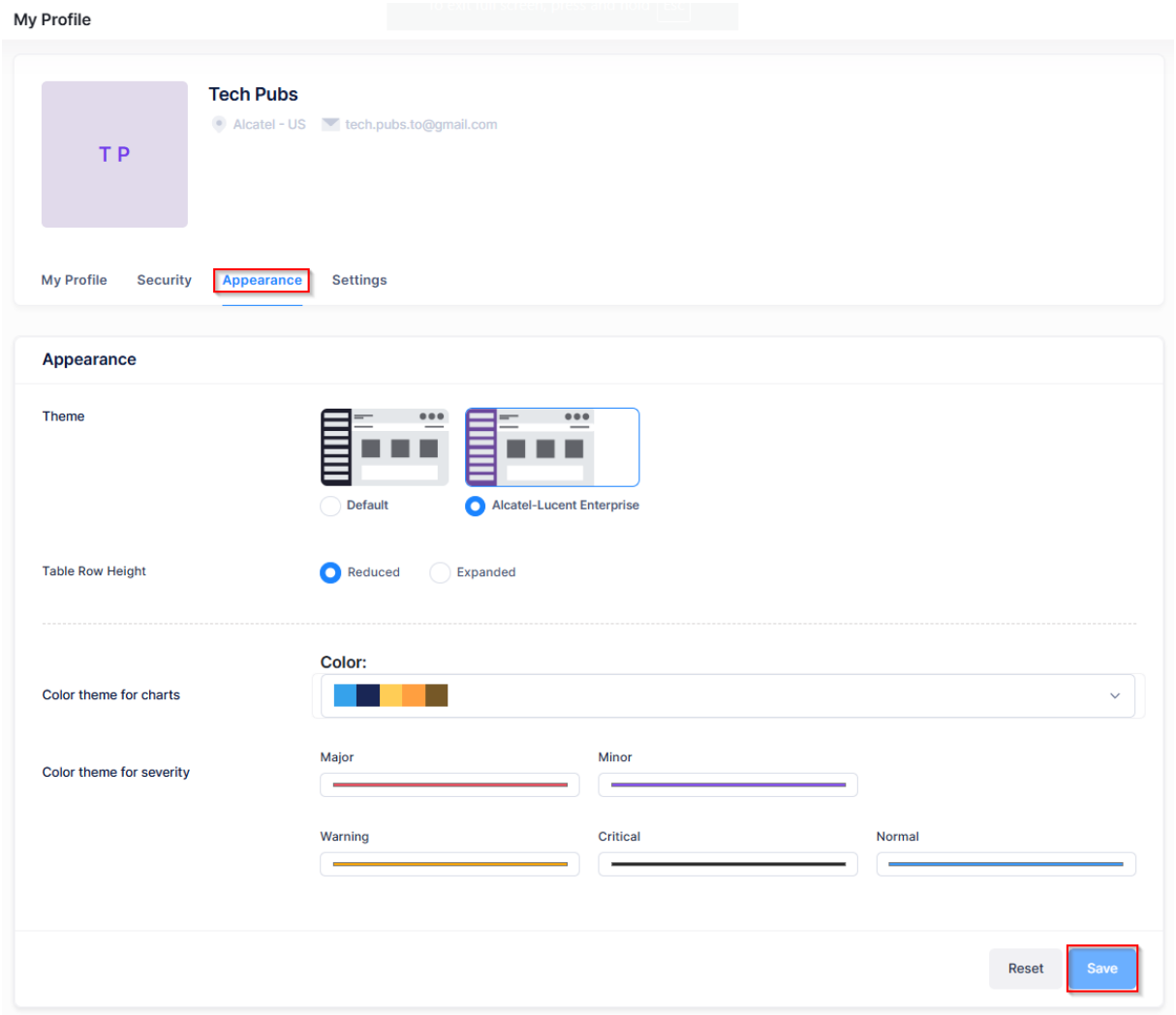
2.3.3 User Preferences

You can change the following user preferences to change the look and feel of the OmniVista Terra User Interface:

- Appearance (see page 26) - Specify color schemes for the UI screens, charts, and severity levels.
- Settings (see page 27)- Enable/disable login history storage for your account and specify the preferred naming convention to use for displaying the device Friendly Name.

2.3.3.1 Appearance

Open the Appearance tab by clicking on your login initials in the upper-right corner of any screen. Select **My Profile** from the drop-down menu, then click on the **Appearance** tab.



2.3.3.1.1 Theme

By default, the OmniVista Terra User Interface colors are set to an Alcatel-Lucent Enterprise look (purple and grey). You can change the basic colors to your preference by selecting this option and clicking **Save**. The change takes effect immediately. You can revert back at any time.

2.3.3.1.2 Table Row Height

Tables in OmniVista provide an overview of information that can be sorted and filtered. For example, the Device Catalog (see page 169) displays a list of network devices. You can change the height of table rows by selecting **Reduced** (the default) or **Expanded** and clicking **Save**. The change takes effect immediately. You can revert back at any time.

2.3.3.1.3 Color Theme for Charts

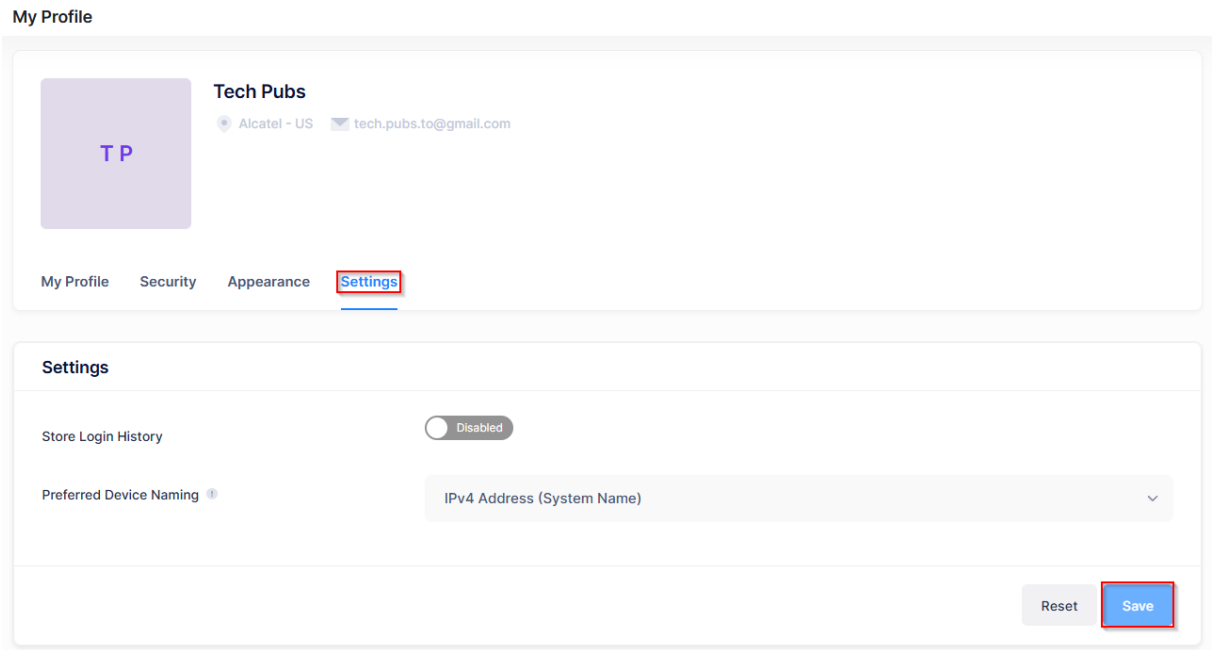
By default, a primary color theme is applied. Pie, Line, and Bar Charts will take this theme for their display. You can also select another color theme based on a purple gradient.

2.3.3.1.4 Color Theme for Severity

The color theme for severity specifies the colors to use to highlight the different severity levels. For example, the color to use for Major, Minor, Warning, Critical, and Normal. Severity levels are indicated in certain tables, such as the Events List (see page 981) table. You can change the color theme for severity by selecting a color for one or more of the severity levels and clicking **Save**. The change takes effect immediately. You can revert back at any time.

2.3.3.2 Settings

Open the Settings tab by clicking on your login initials in the upper-right corner of any screen. Select **My Profile** from the drop-down menu, then click on the **Settings** tab.



2.3.3.2.1 Store Login History

By default, login history information for your account is not stored. Click on the **Store Login History** slider to enable storage of login history information. Click **Save** to save the change.

2.3.3.2.2 Preferred Device Naming

You can change the network device naming convention to suit your preference. By default, IP Address (System Name) is the convention used in OmniVista Terra. The other naming conventions you can use are:

- IPv4 Address
- IPv4 Address (System Name) (Default)
- IPv6 Address
- IPv6 Address (System Name)
- MAC Address
- Mesh Level: IPv4 Address (System Name)
- Mesh Level: IPv6 Address (System Name)
- System Name
- System Name (IPv6 Address)
- System (Mesh Level: IPv4 Address (System Name))

21 Oct 2025

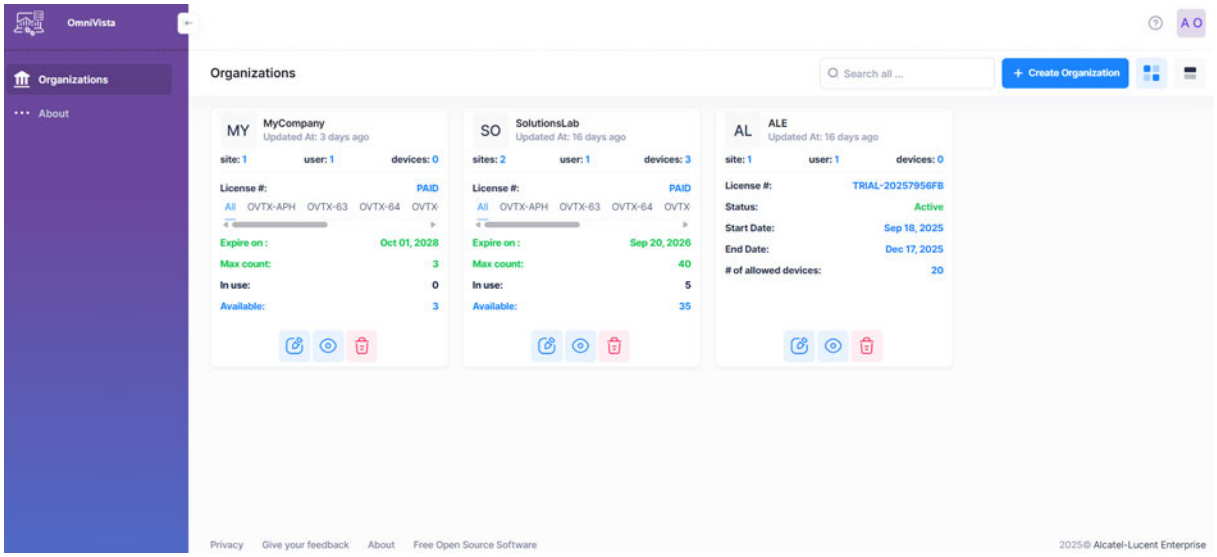
2.4 User Interface

There are two dashboards in OmniVista - the OmniVista Main Dashboard (see page 31), and the Organization Dashboard (see page 33).

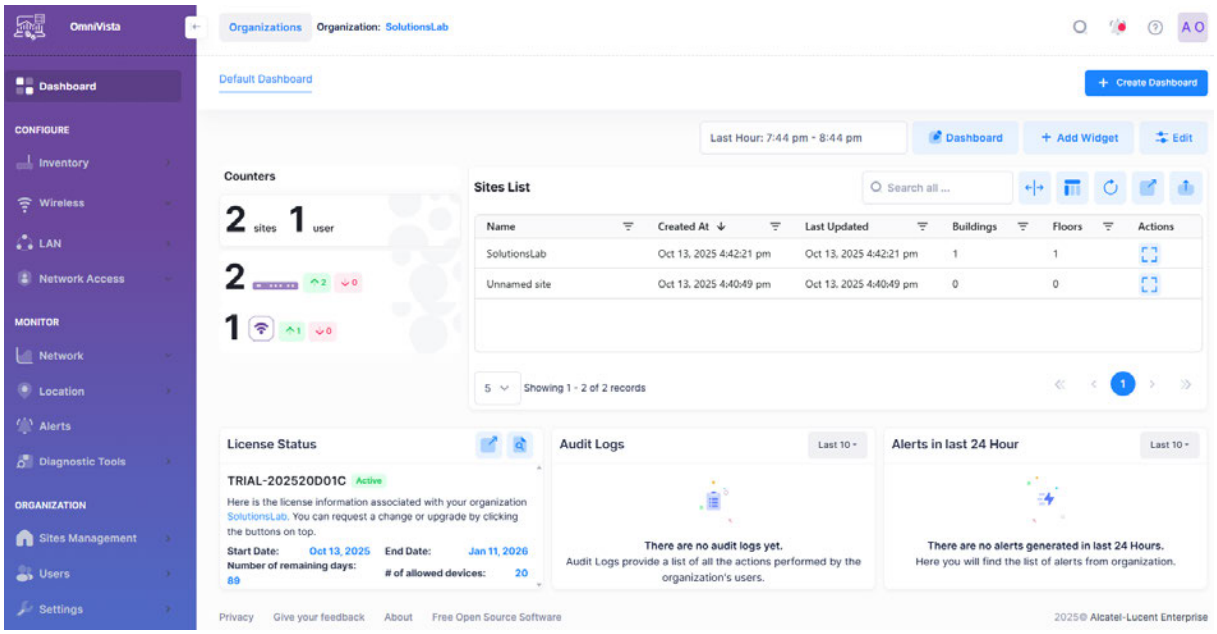
The OmniVista Main Dashboard is initially presented to a user at login. The dashboard displays widgets for any organizations the user is managing and is used to access the Organization Dashboard for an organization.

The Organization Dashboard is presented to an organization user at login. The Organization Dashboard is used to manage an organization (create sites, buildings, floors) and monitor an organization's network (e.g., create devices, monitor devices).

This section provides an overview of the OmniVista user interface for both dashboards, including common tools used for working with tables and graphical displays (see page 49), as well as the OmniVista Terra Menu (see page 45), which is used to access OmniVista Terra functions and applications.



OmniVista Main Dashboard



Organization Dashboard

21 Oct 2025

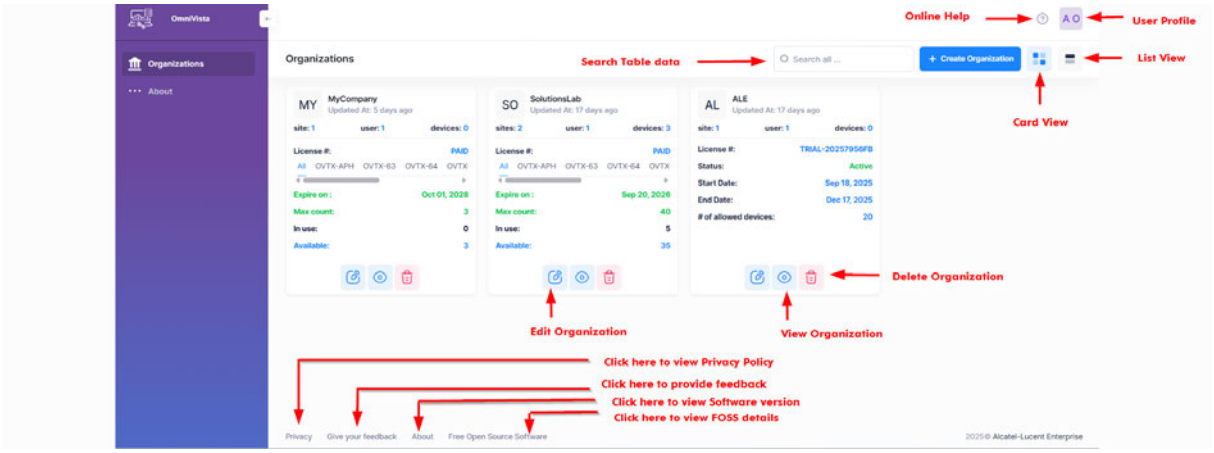
2.4.1 OmniVista Main Dashboard

The OmniVista Main Dashboard is initially presented to a user at login. The Dashboard is used to create and manage Organizations, and displays widgets for any Organizations the user has created.

This is where the process of managing an Organization's network begins. Once a user creates an Organization, the administrator can access that Organization to create sites (including the site's physical location, buildings, and floors), and add network devices to those sites.

To manage any Organization network, simply click on the **View Organization** button at the bottom of the Organization Widget to bring up the Organization Administrator Dashboard (see page 33) for that Organization.

The basic functions that can be performed from this screen are described below (see page 31). For detailed procedures on the functions available from the OmniVista Main Dashboard, see Configure and Manage an Organization (see page 61).



2.4.1.1 UI Functions

The following functions are available on this Dashboard:

- **Create an Organization -** Click on the **Create Organization** button to bring up the Organization Information Form. Once you complete the form, you will be returned to the Main Dashboard and the new Organization widget will be displayed on the left side of the Dashboard.
- **View an Organization -** Networks are managed from an Organization's Dashboard. Once you are approved to access an Organization, click on the **View Organization** button at the bottom of the Organization's widget to access the Organization Administrator Dashboard. For an overview of this Dashboard, see the Organization Administrator Dashboard (see page 33).
- **Edit/Delete an Organization -** To edit an Organization's name/image, or delete an Organization, click on the buttons at the bottom of the Organization's widget.
  - Select **Edit** to change an Organization's name, image, persistency values, password policy, or the audit configuration schedule.
  - Select **Delete** to delete the Organization. Deleting an Organization will delete the associated users, licenses, sites, buildings, floors, devices, reports, walls declared, and all device configurations in this organization.

- **Search for an Organization -** If you are managing a large number of Organizations, you can type the Organization name into the Search Bar at the top of the screen to filter the Dashboard view to only display specific Organization(s).
- **Privacy -** ALE Privacy and Data Protection Policy.
- **Give Your Feedback -** Provide feedback about OmniVista.
- **About -** It provides details of the software version being used for various Applications.
- **Free and Open Source Software -** Free and Open Source Software (FOSS) used in OmniVista.

21 Oct 2025

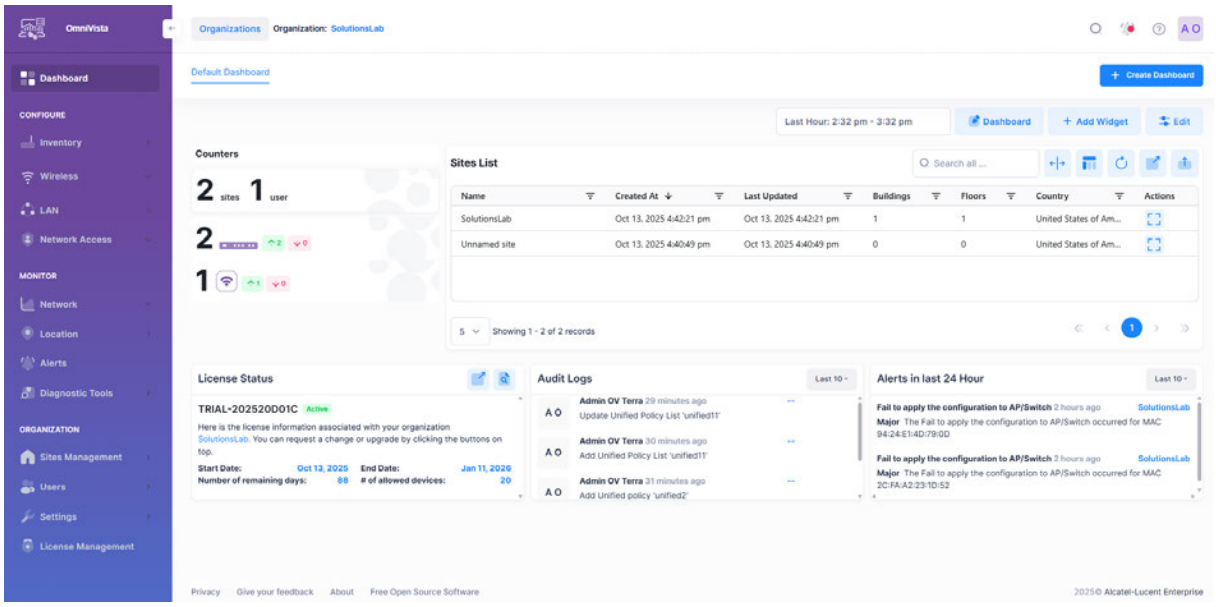
2.4.2 Organization Dashboard

The Organization Administrator Dashboard is presented to an Organization Administrator at login. The Organization Administrator Dashboard is used to create and manage an Organization's network. From this Dashboard, an Organization Administrator can create sites for the Organization (including the site's physical location, buildings, and floors), add network devices to those sites, and monitor and manage those devices.

The Dashboard provides an overview of the number of sites, users, and devices being managed by the Organization, including a list of sites being managed. The Dashboard also provides an overview of the OmniVista License and a list of any Audit logs created for the Organization.

The OmniVista Terra Menu on the left-hand side provides links to all of the OmniVista applications used to configure and monitor the Organization's network, as well as manage the Organization.

The basic functions that can be performed from this screen are described below (see page 33).



2.4.2.1 UI Functions

The Organization Administrator Dashboard provides the following information and functions:

- **Organization Overview -** The fields at the top of the Dashboard display the number of Sites, Users, and Devices for the Organization.
- **Sites List -** Displays all of the physical sites configured for the Organization. Click on Site Name to bring up the Site Information Screen and edit site details.
- **License Status -** Displays the OmniVista Terra license information associated with the Organization, including the start and end dates for the license, the number of days remaining in the license period, and the number of devices that can be managed with the current license.
  - Click on the **More details** button to navigate to the License Management page to view the license information.
  - Click on the **Import Licenses** button to import device management Licenses from Orders.

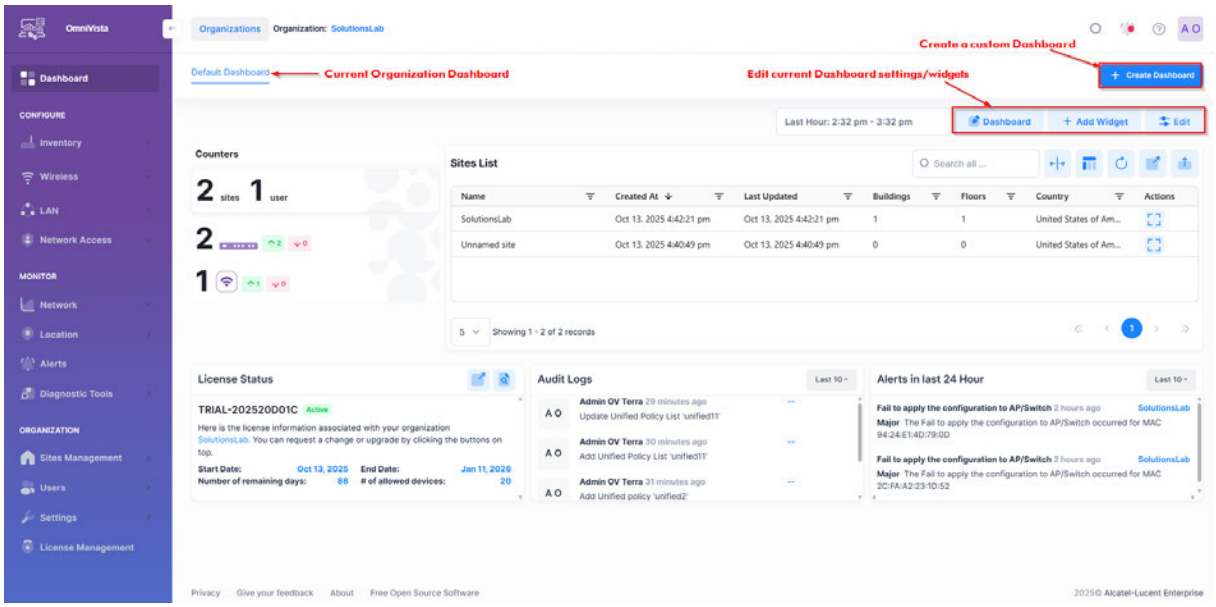
- **Audit Logs -** Displays the Audit Log, which provides a list of all the actions performed by the Organization's users.
- **Alerts and Traps -** Displays a list of alerts and traps received from network devices managed by the Organization.
- **OmniVista Terra Menu -** Provides links to all of the OmniVista Terra applications used to configure and monitor the Organization’s network, as well as manage the Organization. Click here (see page 45)for an overview of OmniVista Terra applications.

21 Oct 2025

2.4.3 Custom Dashboards

OmniVista Terra provides focused dashboards to support common use-cases and enables you to display a specific set of metrics and data points on one screen. You can use custom dashboards to view selected metrics and a relatively narrow or focused view of the data.

When an Organization is created, a “Default Dashboard” is provided.



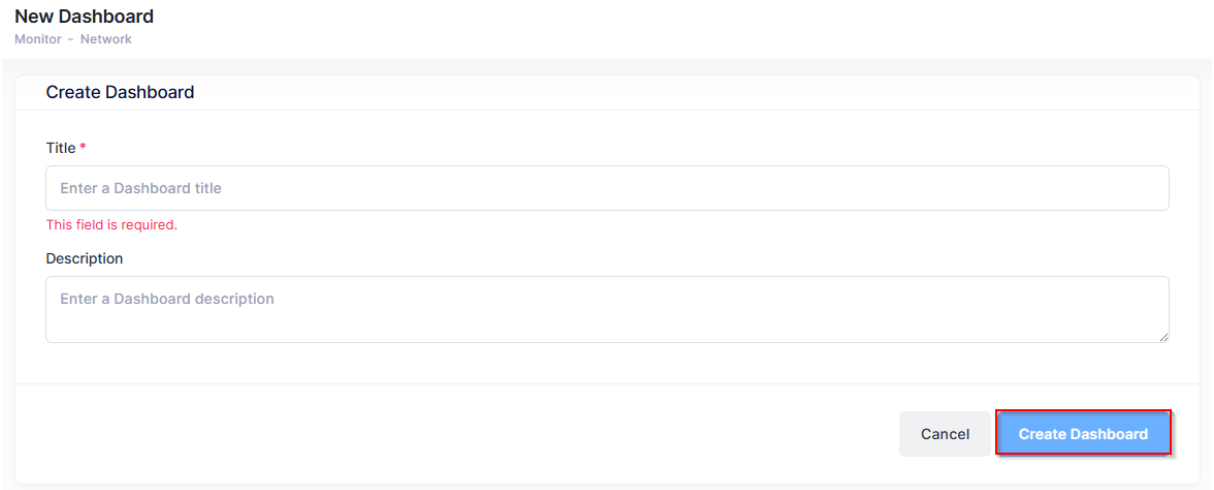
To customize the Organization Dashboard, you can complete any of the following tasks:

- Create a Custom Dashboard (see page 36) - Create a new dashboard with a custom name, and widgets to the dashboard, and customize the dashboard layout.
- Edit Dashboard Widgets (see page 40) - Change widget settings and location on the Custom Dashboard.
- Application Widgets (see page 44) - List of application metrics that you can monitor in a widget.

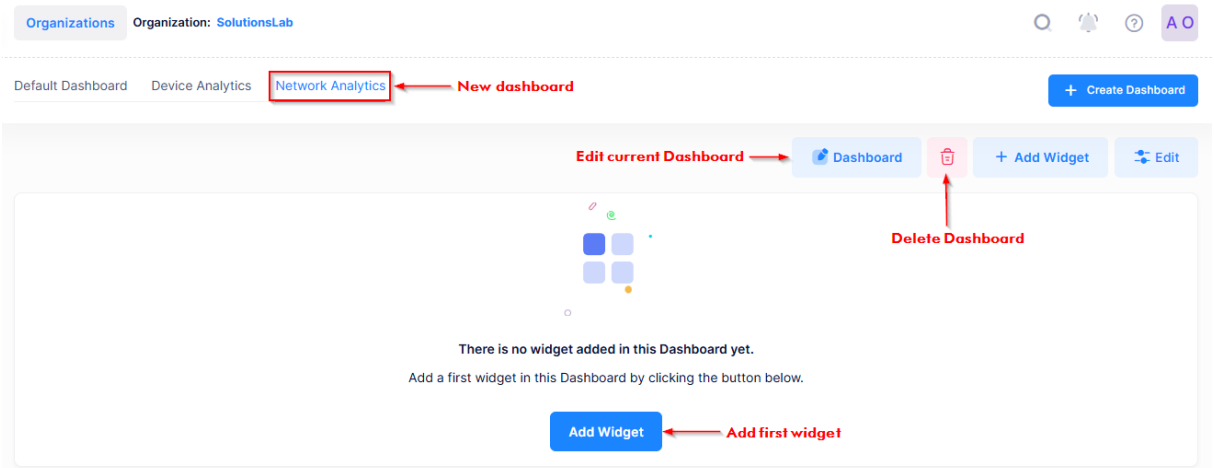
21 Oct 2025

2.4.3.1 Create a Custom Dashboard

To create a custom dashboard, click on **Create Dashboard** in the right corner of the Organization Dashboard (see page 35) screen. The New Dashboard window opens.



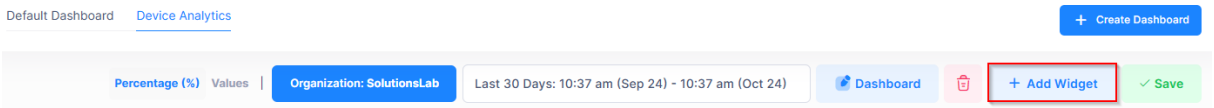
Enter a title and optional description for the custom dashboard, then click on **Create Dashboard**. A dashboard is created and displayed as the current dashboard on the Organization Dashboard screen.



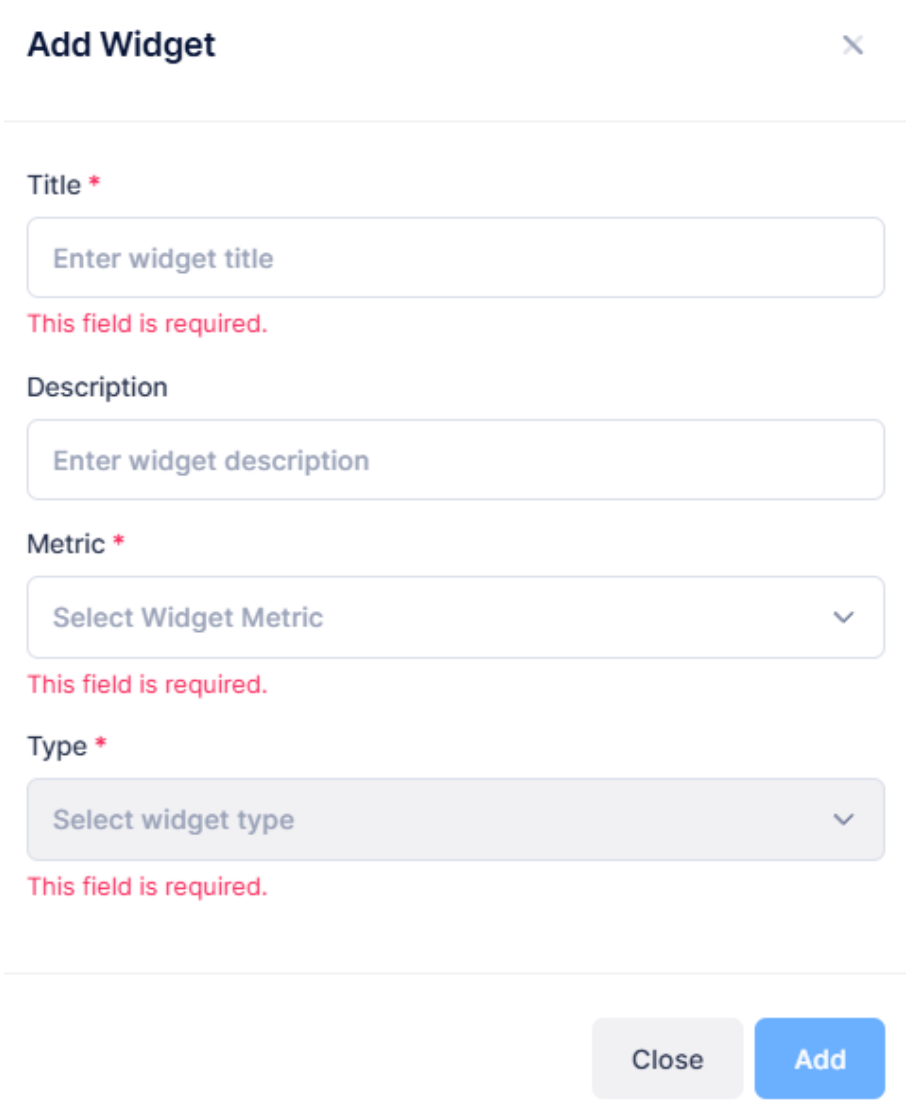
Click on **Add Widget** at the bottom of the Dashboard to add the first widget to your new Dashboard. You can then continue to add more widgets to the Dashboard.

2.4.3.1.1 Adding Widgets to a Custom Dashboard

To add application widgets to a Custom Dashboard, click on **+Add Widget** at the top of the Dashboard.

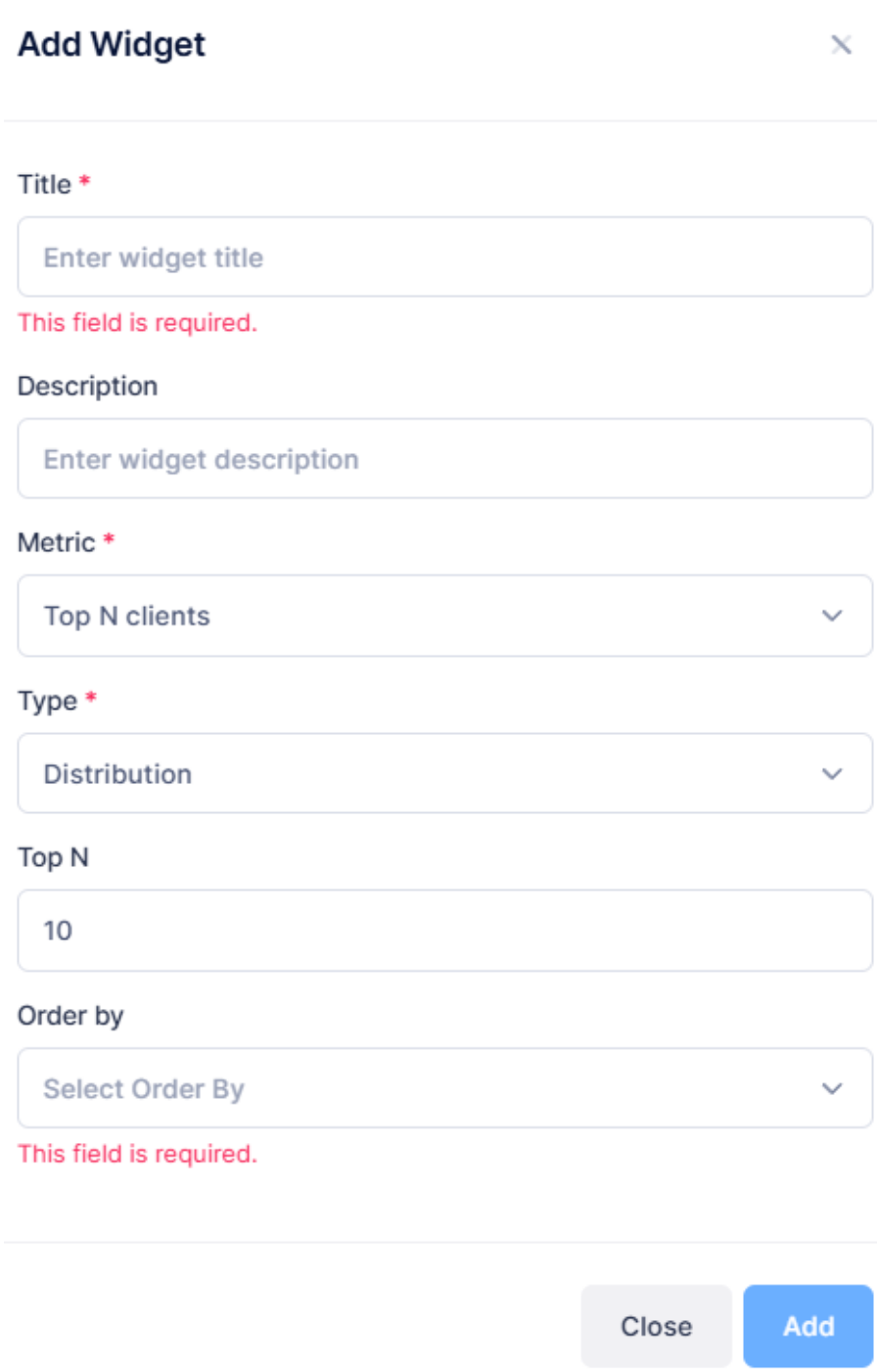


The Add Widget form appears. Enter the required details as described below, then click on **Add**.

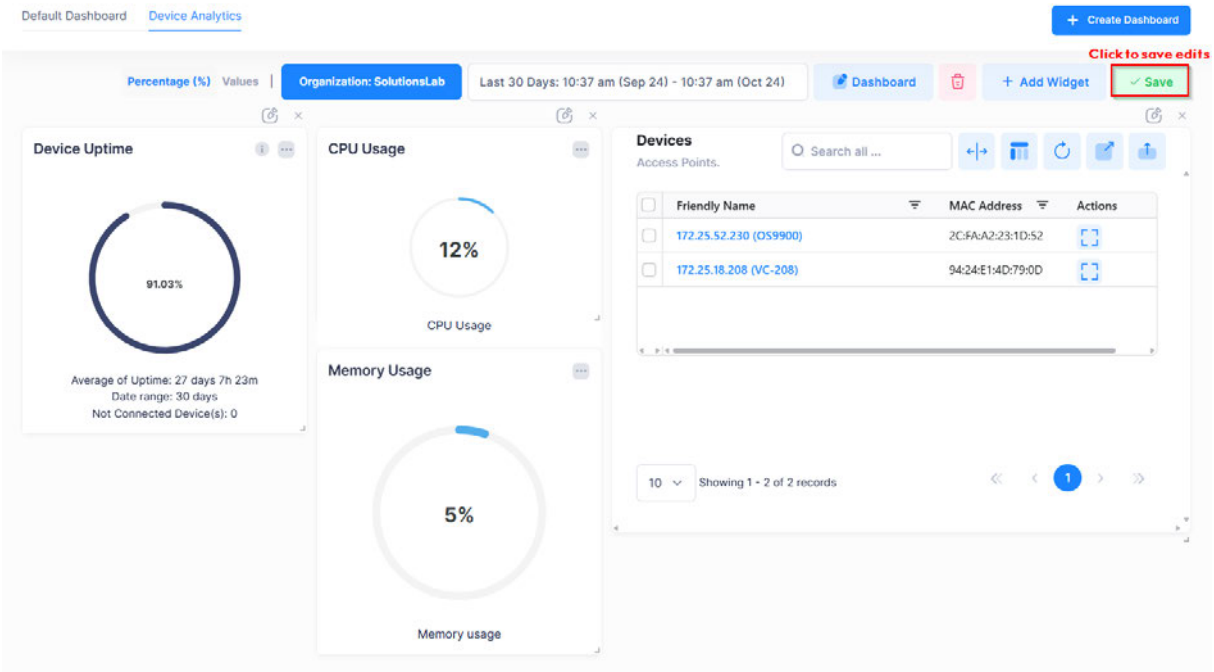


- **Title** - Enter a title for the widget.
- **Description** - Enter a short description for the widget.
- **Metric** - Select the Widget metric that you want to monitor. For a list of application metrics that you can monitor in a widget, see Application Widgets (see page 44).
- **Type**- Select the type of data that you want to monitor with the widget. Note that the available options for this field are based on the Metric selected.

Note that the selection made for the “Metric” and “Type” fields may require you to select options for additional fields. For example, if “Top N Clients” is selected for the Metric, the “Top N” and “Order by” fields are displayed:



Each time you add a widget, it is immediately displayed on the Custom Dashboard. When you are done adding widgets, click on **Save**.

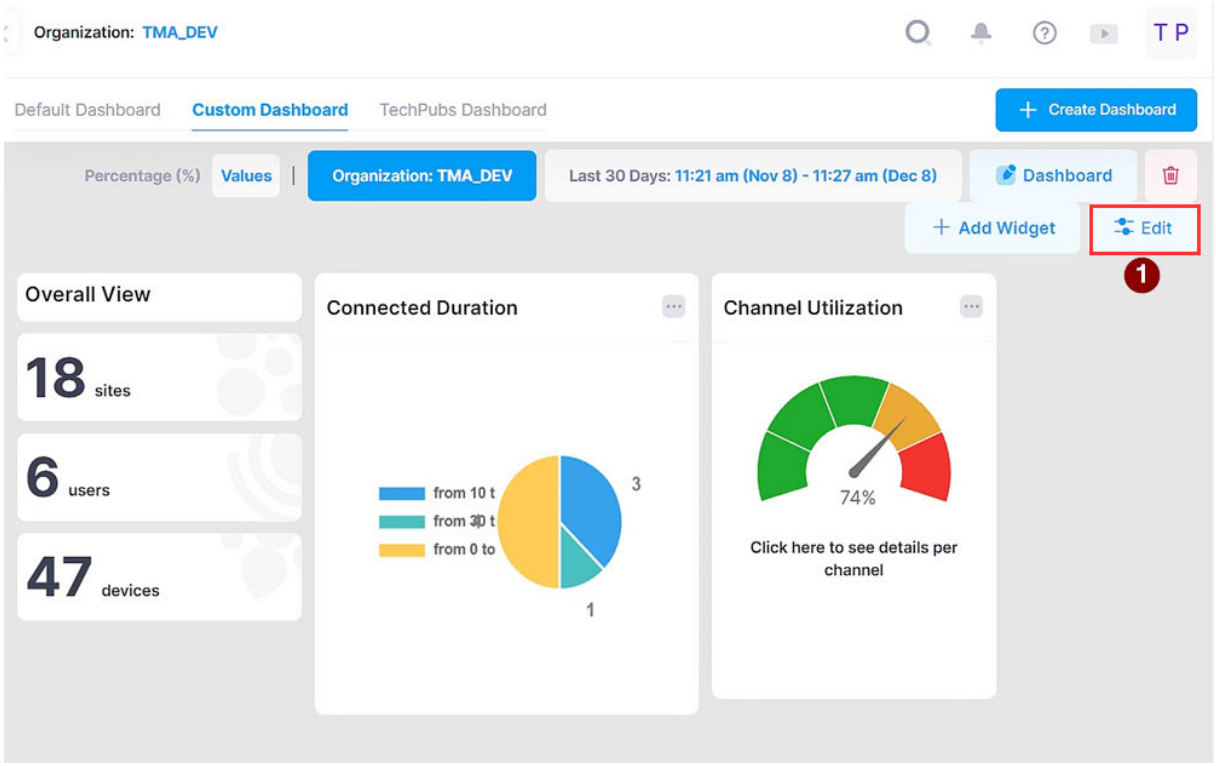


To edit widget settings and location on the Custom Dashboard, see Editing Widgets (see page 40)

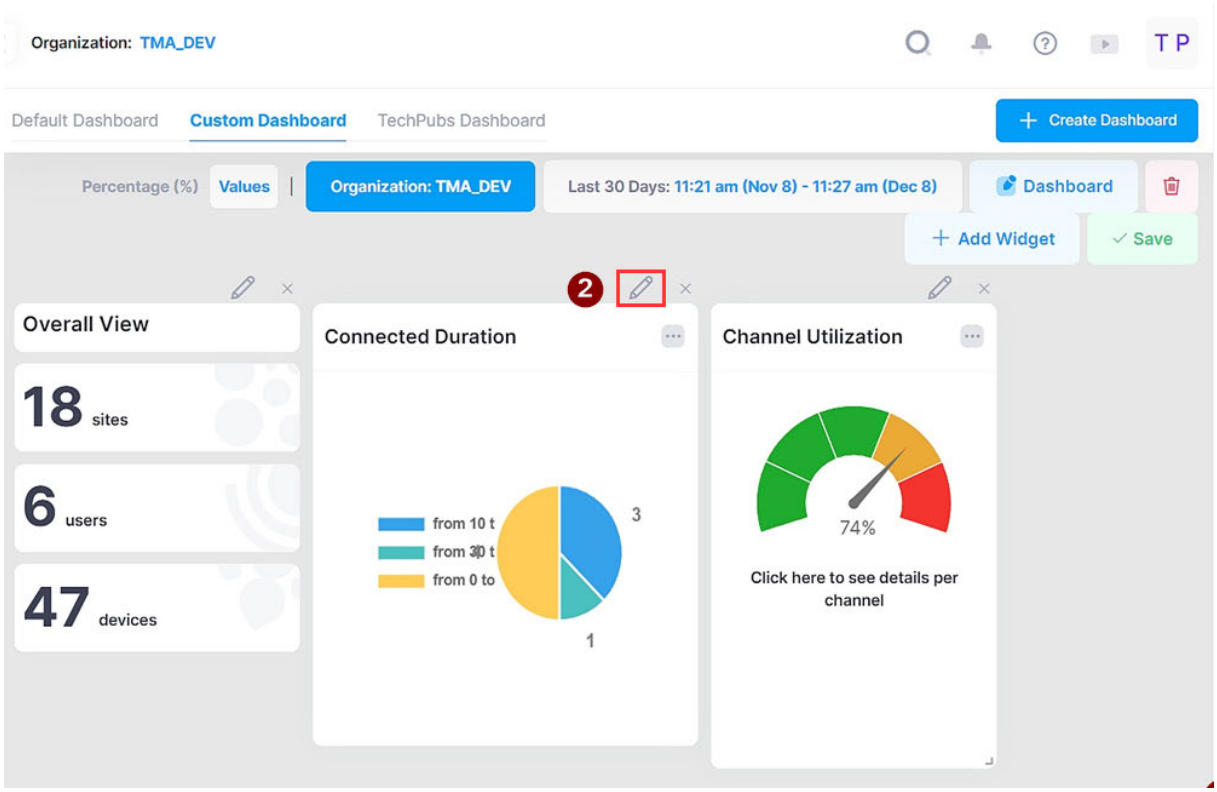
21 Oct 2025

2.4.3.2 Editing a Widget

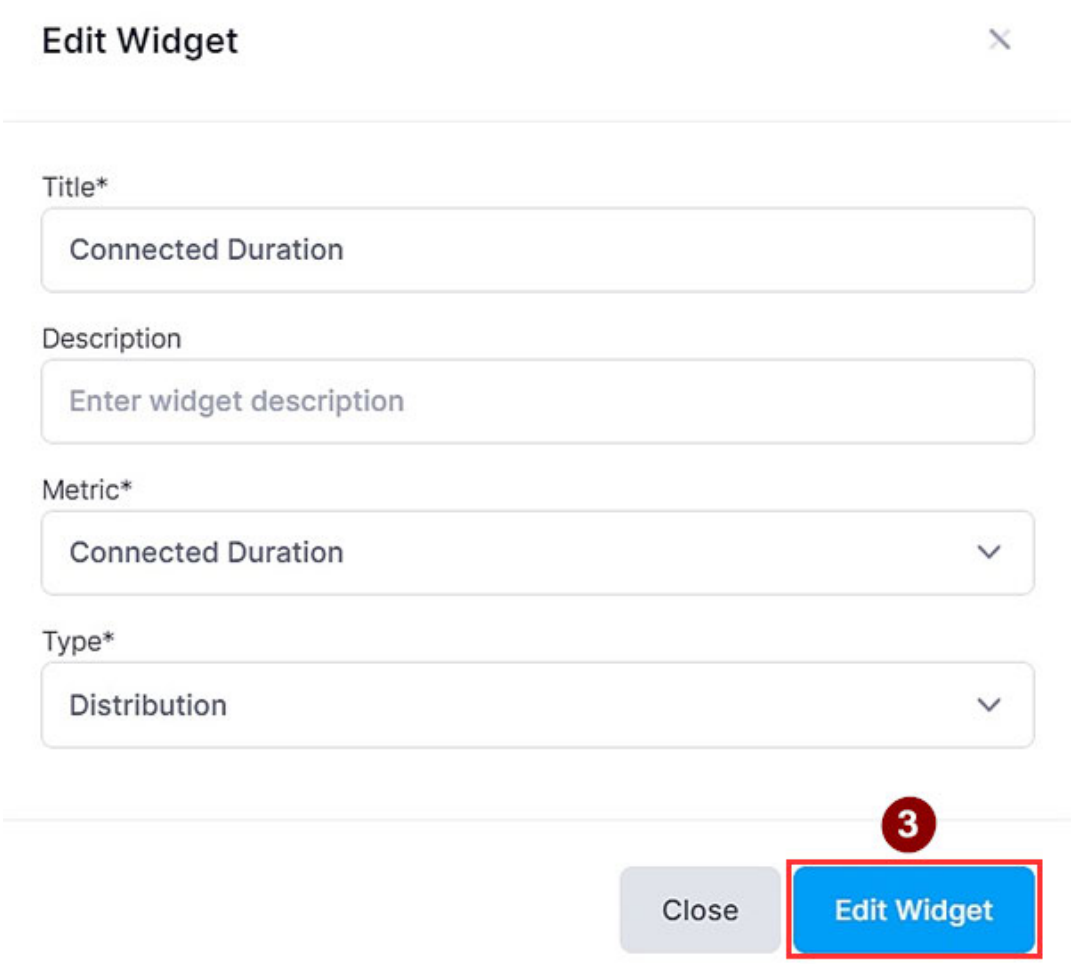
To edit an existing widget, click on **Edit** on the Custom Dashboard home page.



Click on the pencil icon to open the **Edit Widget** screen.



A new Edit Widget window appears.

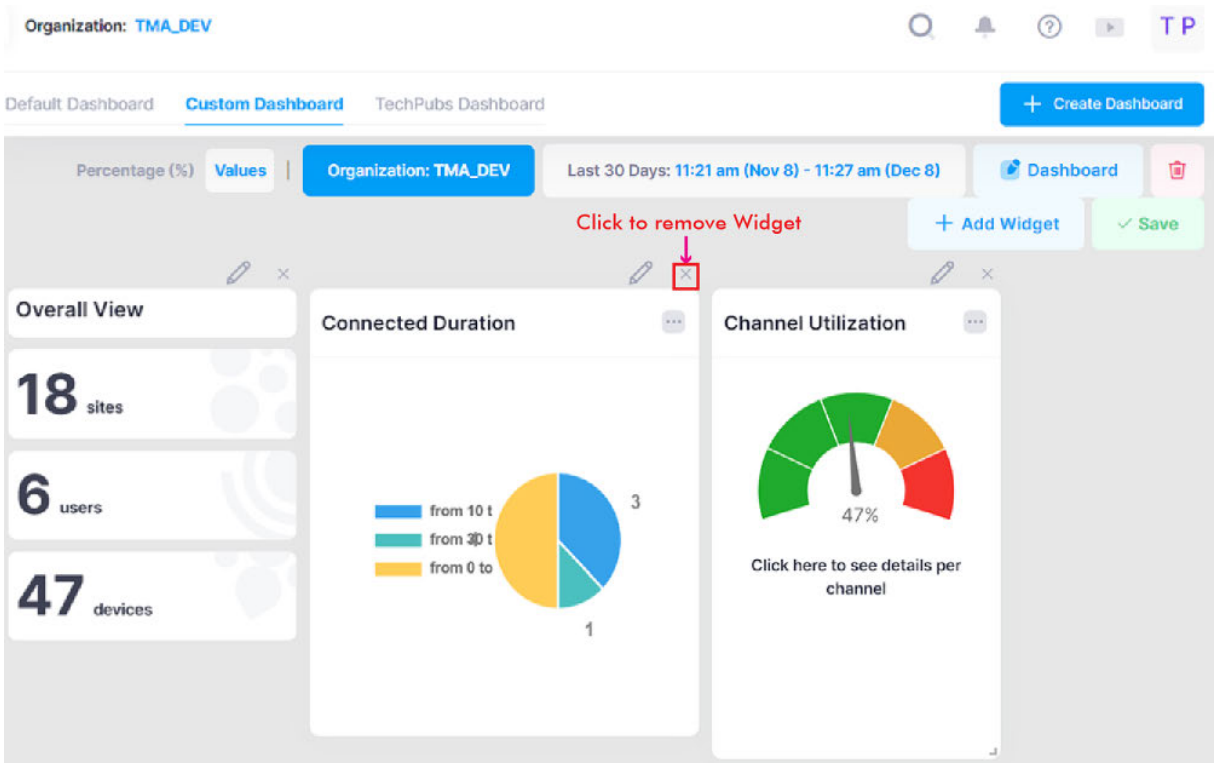


Enter the new details that you want to modify for the widget and click on **Edit Widget** to save the changes. Click on **Save** when you are done editing widgets for the custom dashboard.

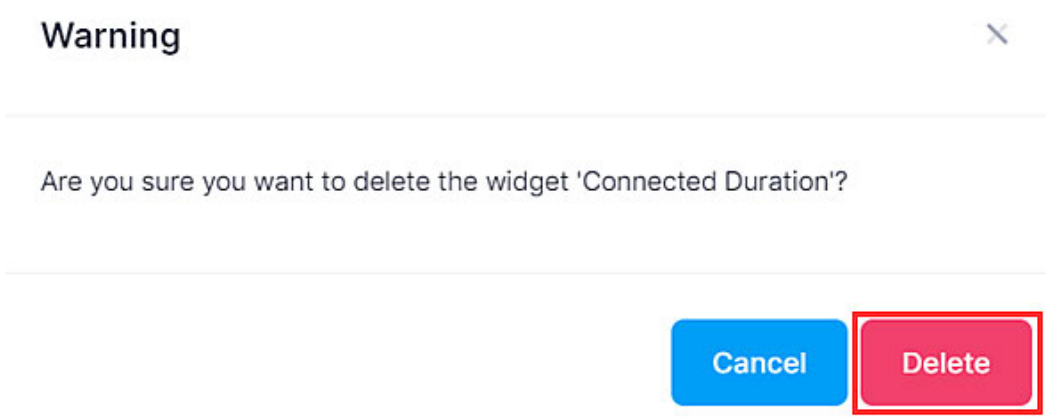
For a list of application metrics that you can monitor in a widget, see Application Widgets (see page 44)

2.4.3.2.1 Removing a Widget from Dashboard

To remove a widget from the custom dashboard, select the widget and click on **"X"** on the widget. A confirmation screen opens.

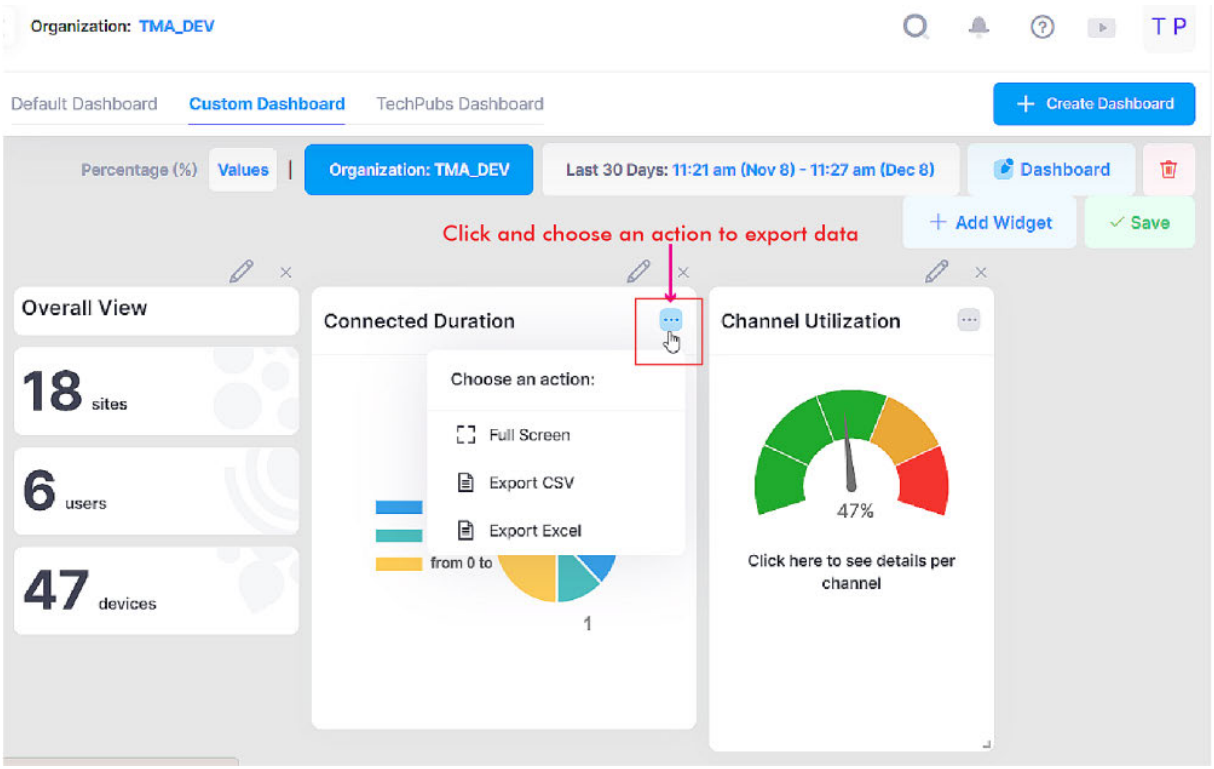


Click on **Delete** to remove the widget.



2.4.3.2.2 Export Widget Data

To export the data in the widget, click on **Export** to choose export data options. Choose an action to export the widget data to an Excel or .csv or PDF file format.



Full Screen - Click to view information displayed on a full screen in your monitor.

Export CSV - Click to download information displayed in custom dashboard to a CSV file.

Export Excel - Click to download information displayed in custom dashboard to a excel (spreadsheet) file.

To create a Custom Dashboard and add a new widget to the Custom Dashboard, see Create a Custom Dashboard (see page 36)

21 Oct 2025

2.4.3.3 Application Widgets

The following Global application widgets are available to be configured on custom dashboards . Some widgets (e.g., Network Availability, Licenses) collect and display information automatically. Others (e.g., Alarms) require configuration in an application (e.g., Notifications, Application Visibility/ Analytics) to display information.

Entities

- Default Dashboard Widgets
- Wireless Client sessions
- Top Categories
- Top Applications
- Top Users
- Wired Client sessions
- Sites
- Client over time
- Organization Users
- Channel
- Devices

Measures

- Channel Utilization
- Categorization of clients
- Top N clients
- Time to connect
- Device Up Time
- Available Capacity
- Device Analytics
- Roaming
- Memory Usage
- Flash Usage
- Coverage
- Successful connects
- CPU usage
- Throughput consumption
- Connected Duration
- Wireless connected duration
- Wired connected duration

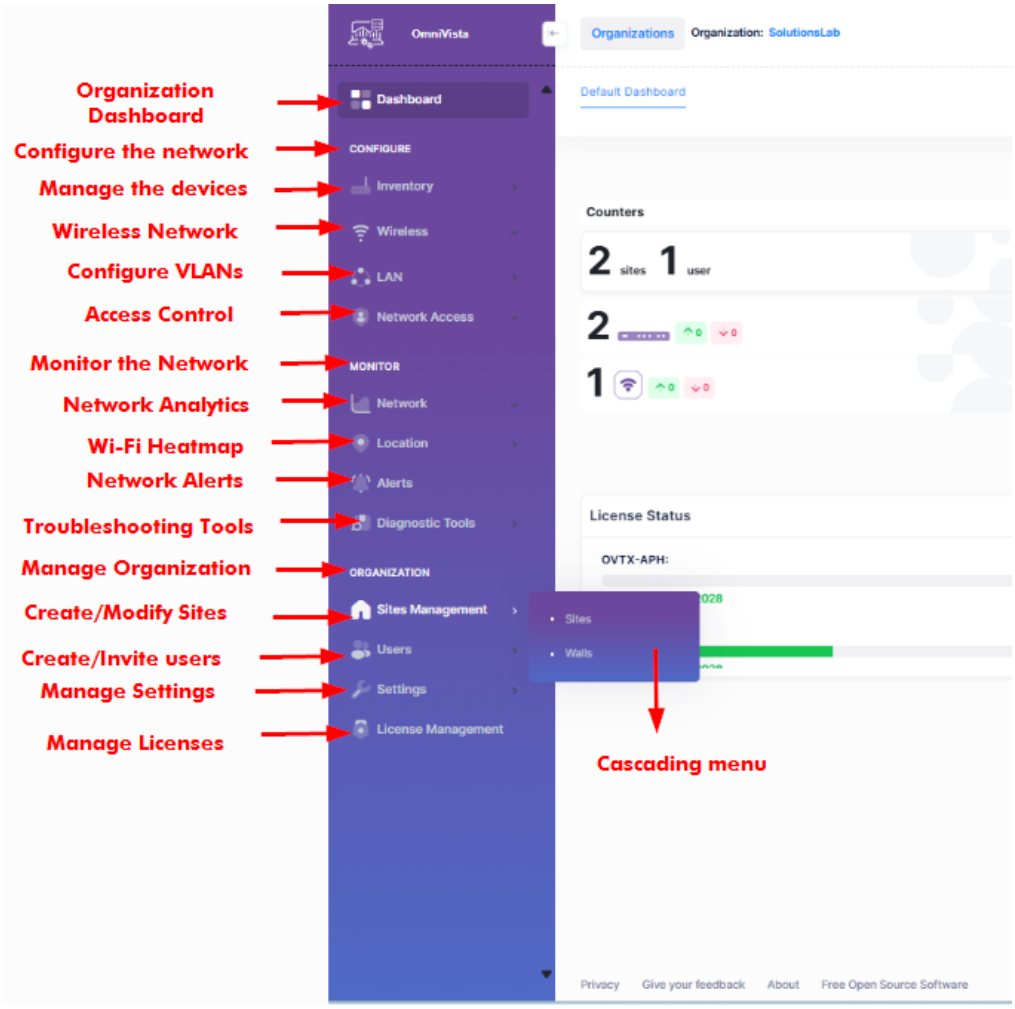
2.4.4 OmniVista Terra Menu

The OmniVista Terra Menu is displayed on the left-hand side of any Organization Administrator screen. The menu provides links to all of the OmniVista applications used to configure and monitor the Organization's network, as well as manage the Organization.

The menu is divided into three (3) areas: Configure (see page 45), Monitor (see page 46), and Organization (see page 47). The section below (see page 45)provides an overview of each application/ function by section.

2.4.4.1 OmniVista Applications and Functions

The OmniVista Terra Menu is divided into three (3) areas: Configure (see page 45), Monitor (see page 46), and Organization (see page 47).



2.4.4.1.1 Configure

This section is used to configure the Organization's network, which includes operations that can be applied to wireless devices (e.g., adding/deleting devices).

- **Inventory -** The following Inventory applications are used to manage OmniVista device inventory:
  - **Device Catalog -** Display the Devices List and create/edit/delete network devices. You can view/configure all devices in an Organization or view/configure devices by Site.
  - **NaaS Device Licenses** - Display the NaaS Device Licensing information for managed devices. Use this screen to determine and monitor the status of the Device License for each device.
  - **Device Location -** Place devices on a Site Map. Devices can be placed in specific buildings/ floors/locations in a Site. You can also edit and delete existing devices that have been placed into a Site Map.
  - **Backup/ Upgrade** - Display all configured schedules used to upgrade the software version of the devices. You can schedule automatic upgrades for specific network devices that will take place during specific time windows (e.g., non-business hours) to ensure minimal network disruption. It lists all existing switch configuration backups in OmniVista.
- **Wireless -** The Wireless applications are used to configure wireless networks, Radio Frequency (RF) profiles for devices, and policies to prevent attacks on Stellar AP Series Wireless Devices. It is also used to configure External Engines, UPAM server certificates, an external Captive Portal server configuration, and VPN settings for remote access points.
- **LAN -** VLANs are used to segment network traffic so that VLAN configuration and port assignment is handled through software. This eliminates the need to physically change a network device connection or location when adding or removing devices from the VLAN broadcast domain.
- **Network Access** - The Network Access applications are used to provide unified device configuration of security functions for Access Points (APs) devices. In addition to device authentication and classification, you can create Access Role Profiles (similar to User Network Profiles) to configure network access controls for one or more user devices. Network Access applications work together with the Authentication Servers to seamlessly authenticate and configure QoS for network devices.

2.4.4.1.2 Monitor

This section is used to monitor the Organization's network. This includes monitoring capabilities for wireless devices (e.g., Analytics and Location information).

- **Network**
  - **Analytics** - Displays advanced analytics data that provides a comprehensive view of QoE, network resource utilization, client statistics (current clients, session history, client distribution and throughput), and a list of clients blocked from accessing the network.
  - **Access Records** - Displays information for all devices authenticated through UPAM.
  - **Reports** - Used to create and review reports containing information about your Organization.
  - **Topology** - Used to view the topology of all managed devices in the network, view information about a specific device and perform certain actions on those devices.
- **Location**

    - **Wi-Fi Heatmap** - Displays Heat Maps to provide a comprehensive view of Wi-Fi coverage that is used as a design, verification, and troubleshooting tool for Stellar Access Points.
    - **Current Client Density** - Displays the density of connected clients in the floor plan.
    - **Client Density History** - Displays the density of connected clients in the floor plan over a specified time period.
- **Alerts** - Displays a list of alerts received from network devices managed by the Organization.
- **Diagnostic Tools** - Provides tools for monitoring network events, initiating a terminal session with a device, and collecting log information from devices to send to Alcatel-Lucent Enterprise (ALE) Technical Support to troubleshoot problems.

2.4.4.1.3 Organization

This section is used to configure/modify the Organization (e.g., creating/modifying sites, creating users, requesting a subscription update, viewing Audit Logs).

- **Sites Management**
    - **Sites -** Configure physical sites for the Organization, including buildings and floors.
    - **Walls -** Configure walls in a building at the site.
- **Users**
    - **User Accounts & Roles -** Displays a list of current users for the Organization. You can also create users and specify user permissions for the Organization (e.g., Admin, Viewer).
    - **Login Attempts -** Displays login information for the Organization by time and user.
    - **Two-Factor Authentication** - Displays the two-factor authentication configuration status for Organization users. You can also impose a two-factor authentication requirement on Organization users.
    - **Audit Logs** - Displays a list of all the actions performed by Organization users (such as inviting a user to join the Organization or updating building information for an Organization Site).
- **Settings**
    - **Basic Settings** - Modify the name for the Organization, Region and Timezone, upload an optional Organization Image from your computer, set the timeout value for user sessions, and the amount of time user data/analytics is retained.
    - **Email Templates** - Customize the content of email notifications sent to the user from OmniVista.
    - **Notifications** - Select which SMS Service to use (Plivo or Twillio) to send SMS notifications. Use the Rainbow configuration to send notifications from OmniVista to an existing and/or new Rainbow Bubble. For each Organization, Admin users can enable the sending of alerts to the specified Rainbow Bubble.
    - **Pii Requests** - Monitor the request to delete Personally Identifiable Information requests (PII data) in the Organization.
- **License Management -** Displays information about the Organization's OmniVista License, such as the license type (free trial or paid subscription). A user is allowed to manage up to the

maximum number of devices allowed for that license for the length of the trial or paid subscription contract.

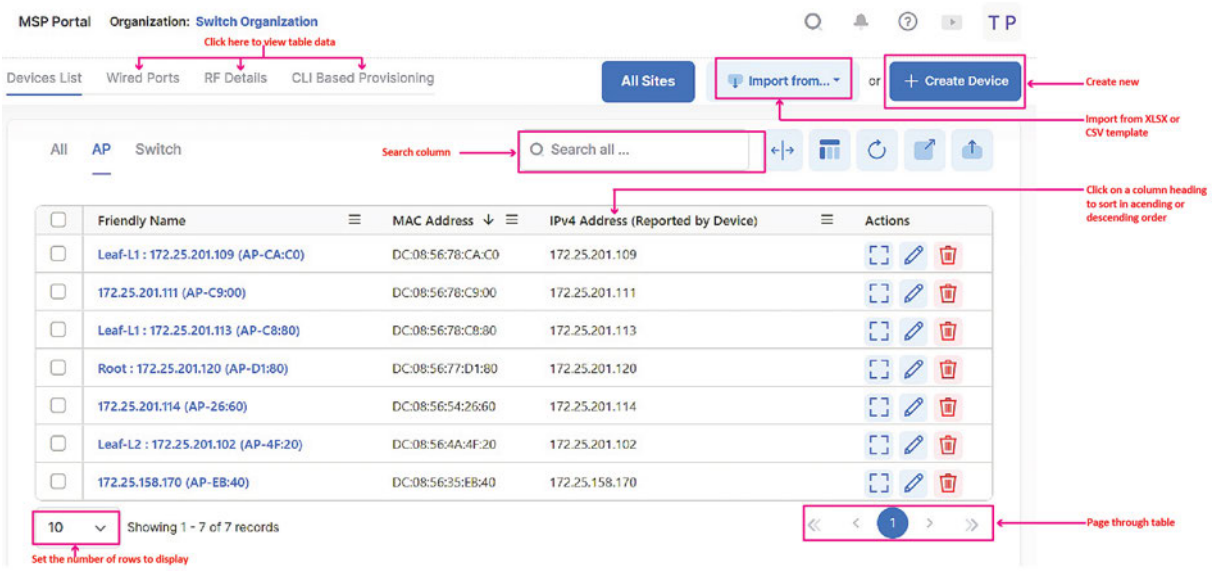
21 Oct 2025

2.4.5 Working with Tables and Graphical Displays

Information in OmniVista is presented in table (e.g., Device Catalog) and graphical form (e.g., Analytics). This section provides an overview of the common tools/operations found in tables (see page 49)and graphical displays (see page 50) in OmniVista.

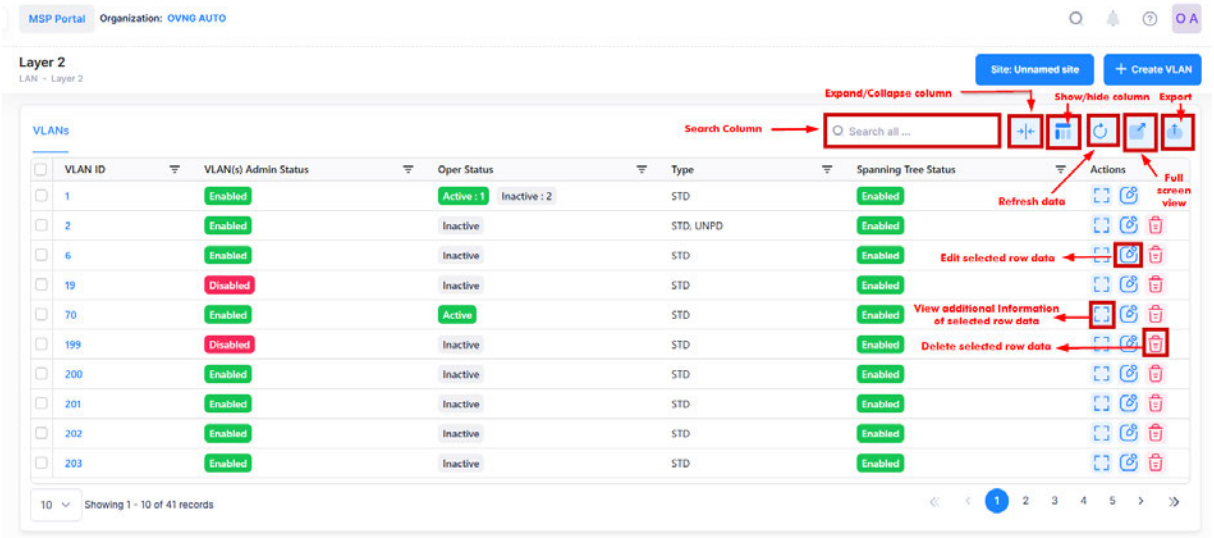
2.4.5.1 Tables

Tables in OmniVista provide an overview of information that can be sorted and filtered and are used for configuration. For example, the Device Catalog displays a list of network devices and can be used to add, edit, and delete devices. Common table tools and operations are detailed below (see page 49).



2.4.5.2 Table Tools and Operations

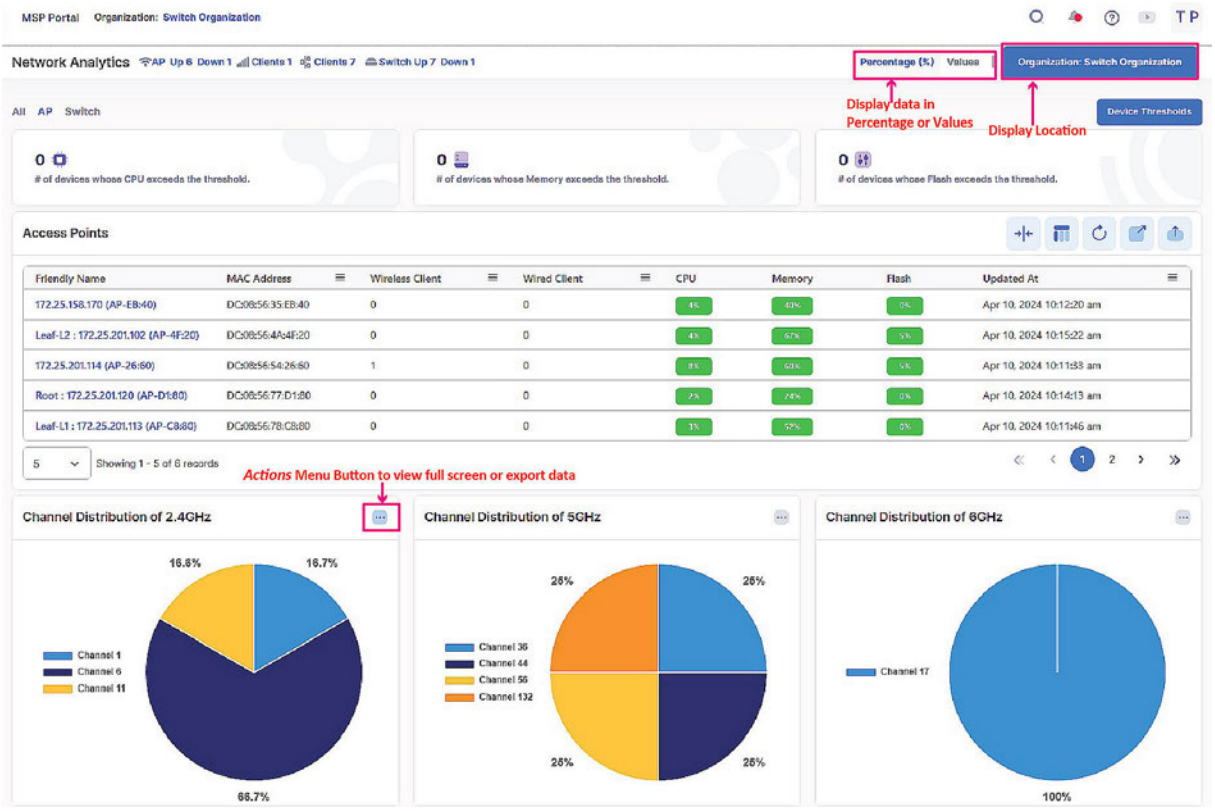
- **Sorting and Filtering** - By default, tables are sorted in ascending order based on the first column. You can sort a table by one or more columns in ascending or descending order by clicking on any column heading. To filter data for one or more columns, click on the magnifying glass in the top-right corner of a column and select the filtering data. See Sorting and Filtering Tables (see page 53) for more information.
- **Search -** Enter search criteria in the Search Bar at the top of the table to search for specific information in a table. The table will be filtered as you enter search criteria. Delete the search criteria from the Search Bar to return to the previous display. You can also search for information in a specific column by clicking on the Search icon at the top of the column and entering search criteria. Delete the search criteria to return to the previous display.
- **Configure Display -** You can change the display using the icons at the top of the table.



- ***Search all*** **-** By default, information from all sites is displayed. Enter a name of the site to select a site to display information from a specific site.
- ***Expand/ Collapse*** - By default, the display is set to Collapse View, which automatically sizes tables (limiting the columns displayed) based on the display area available. Click on the icon to toggle to Full View and display all columns in a table. Click on the icon again to return to Collapse View.
- ***Show/Hide Columns*** **-** By default, all columns in a table are displayed. Click on the icon to select specific columns you want to display. This selection will remain in place until it is changed. You can change the columns displayed at any time. You can also choose to 'Select All' and 'Deselect All' option to select or unselect all columns. In addition, you can pin a specific column to the left side of the table (see Pin a Column to the Left (see page 51) for more information).
- ***Refresh Data*** **-** Click on the refresh button to retrieve the most recent data from the OmniVista database.
- ***Full Screen View*** **-** Click on the icon to display the table in Full View (the table will expand to cover the entire screen. Click on the **Quit full screen mode button**, or press **Esc** to return to the default view.
- **Export -** Click on the **Export** button to export the table to an Excel, .csv, or PDF file.
- **Configuration -** Click on an icon in the Actions column next to an entry to view detailed information, edit, or delete an entry.
- **Set Number of Lines to Display** - By default, 10 lines of a table are displayed. Click on the drop-down to change the number of lines displayed.
- **Page Through Table** - Click on the Forward and Back arrows or select a page number to page through a table.

2.4.5.3 Graphical Displays

Graphical displays in OmniVista provide an overview of information that can be filtered by location and time range. You can also change the display format (percentage/values), and export information to and Excel or .csv file. Common graphical display tools and operations are detailed below (see page 51).

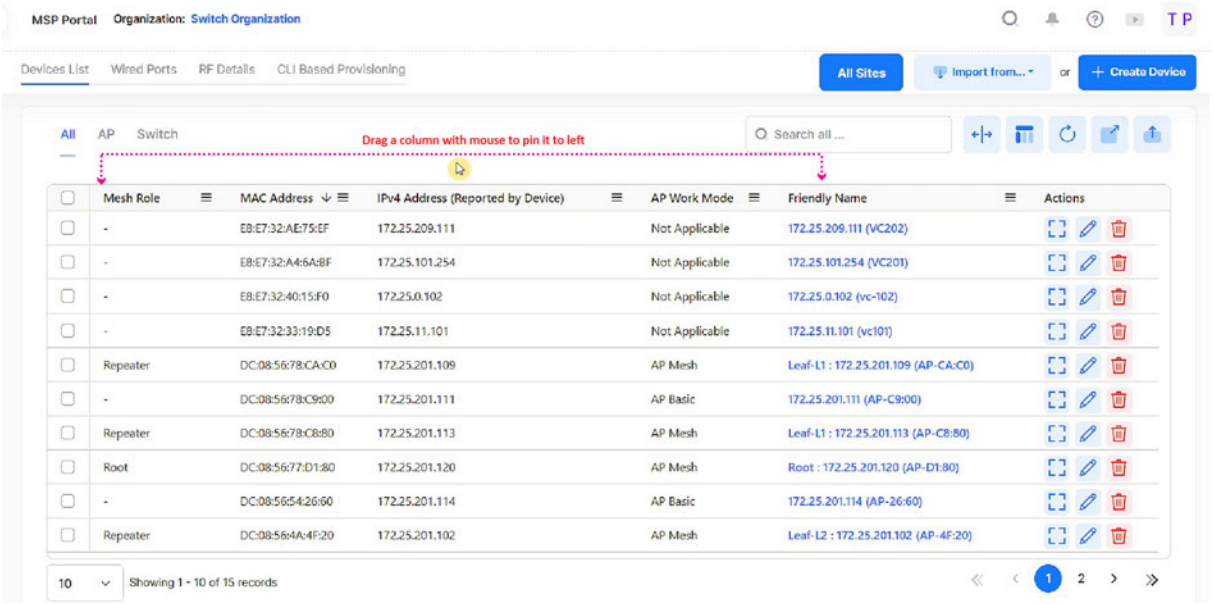


2.4.5.4 Graphical Display Tools and Operations

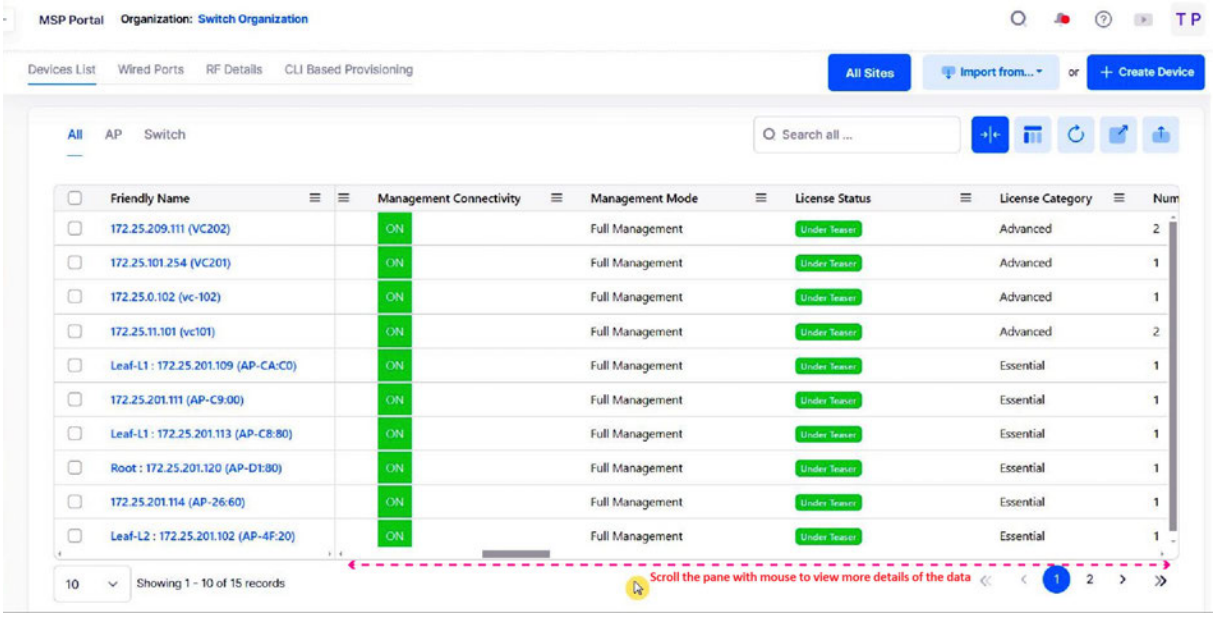
- **Display Format -** By default, data is displayed in percentages. Click on the button to display data in numerical (Values) format. Click again to toggle the display back to percentage format.
- **Display Location -** By default, data for all sites in an Organization are displayed. Click on the button to display the data for a specific Site, Building, Floor, or AP.
- **Display Time Range -** By default, data for the last hour is displayed. Click on the button to display data for the last 6 Hours, 12 Hours, 24 Hours, Week, Month, or a Custom Range. Data is stored in OmniVista Terra for one year, so a Custom Range can go back one year.
- **Actions -** Click to enlarge a widget to full screen view, or to export the data in the widget to am Excel or .csv file in tabular format.

2.4.5.5 Pin a Column to the Left

Pinned or frozen columns are columns that remain visible at all times while you scroll horizontally through a data grid. These columns can be affixed to the left side of the grid to ensure they remain visible.



To pin a column, select the desired column and drag it to the left side of the data grid. This will lock the column data to the left-hand side of the data grid.



To view additional details of the pinned data, scroll through the pane on the right-hand side of the grid.

To unpin a column, select the pinned column on the left and drag it to the right-hand side of the data grid, then release the column. This will release the column data from being pinned to the grid.

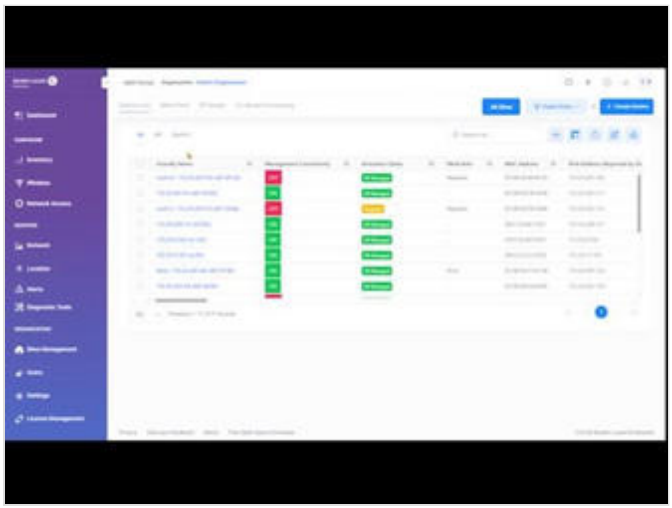
21 Oct 2025

2.4.6 Sorting and Filtering Tables

By clicking on any column heading, you have the ability to sort a table in ascending or descending order based on that column. By default, tables are typically sorted in ascending order based on the values in the first column. To sort multiple columns, you can simply hold down the Shift key and click on multiple column headers. This action enables you to specify the desired sorting order for multiple columns simultaneously.

You can also filter data for one or more columns. By default, all column data is displayed. To filter data for one or more columns, click on the magnifying glass in the top-right corner of the column heading and select the data to filter. Repeat this action for each column that you want to filter. The filtering order is based on which column you filtered first. The results of that filtering action are then filtered based on the filtering criteria specified for the second column, and so on.

The following demo shows how to sort and filter multiple table columns:

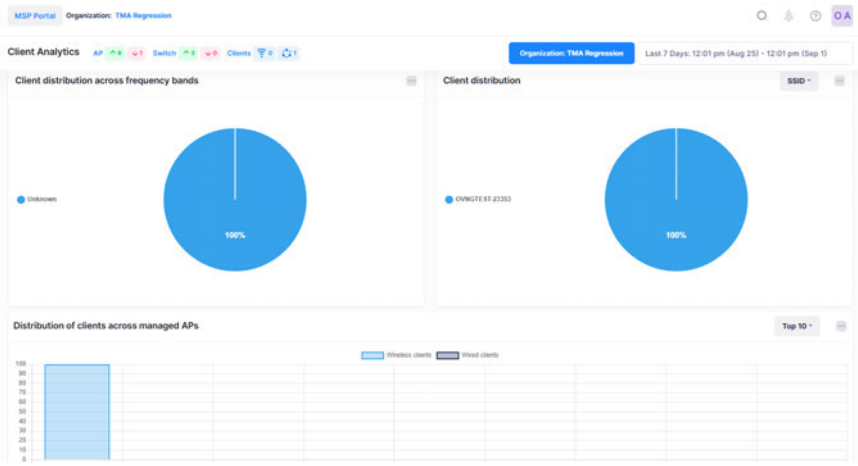


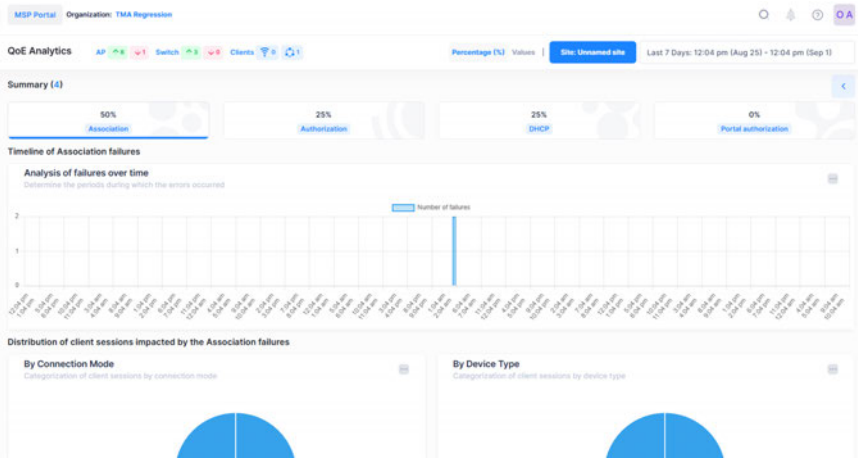
21 Oct 2025

2.4.7 Responsive Display

OmniVista Terra supports the Responsive Design approach allowing you to access the same page from different devices.

Responsive design is a graphic user interface (GUI) design approach used to create content that adjusts smoothly to various screen sizes. Designers size elements in relative units (%) and apply media queries, so their designs can automatically adapt to the browser space to ensure content consistency across devices.

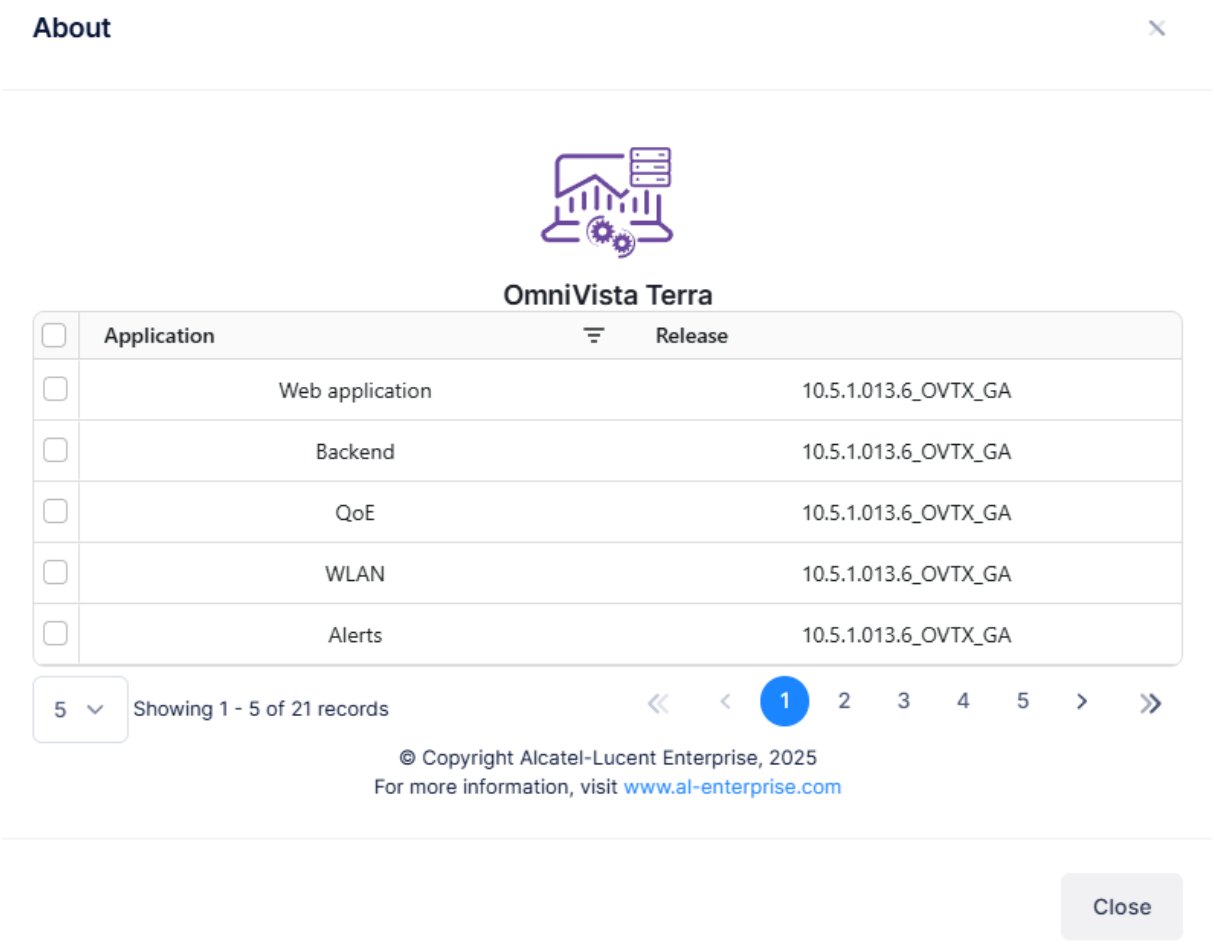




21 Oct 2025

2.4.8 About

The About page displays information about the currently running OmniVista Terra Applications. The list includes the name and version of each Application. Copyright information is also provided.



The various Applications with the Release versions for OmniVista Terra are described below:

- Web Application - 10.5.1.013.6_OVTX_GA
- Backend - 10.5.1.013.6_OVTX_GA
- QoE - 10.5.1.013.6_GA
- WLAN - 10.5.1.013.6_GA
- Alerts - 10.5.1.013.6_GA
- Event Monitoring - 10.5.1.013.6_GA
- IoT - 10.5.1.013.4.6_GA
- Network Events - 10.5.1.013.6_GA
- Reporting - 10.5.1.013.4.4_GA
- Terminal SSH - 10.5.1.013.6_GA
- Network Configuration - 10.5.1.013.6_OVTX_GA

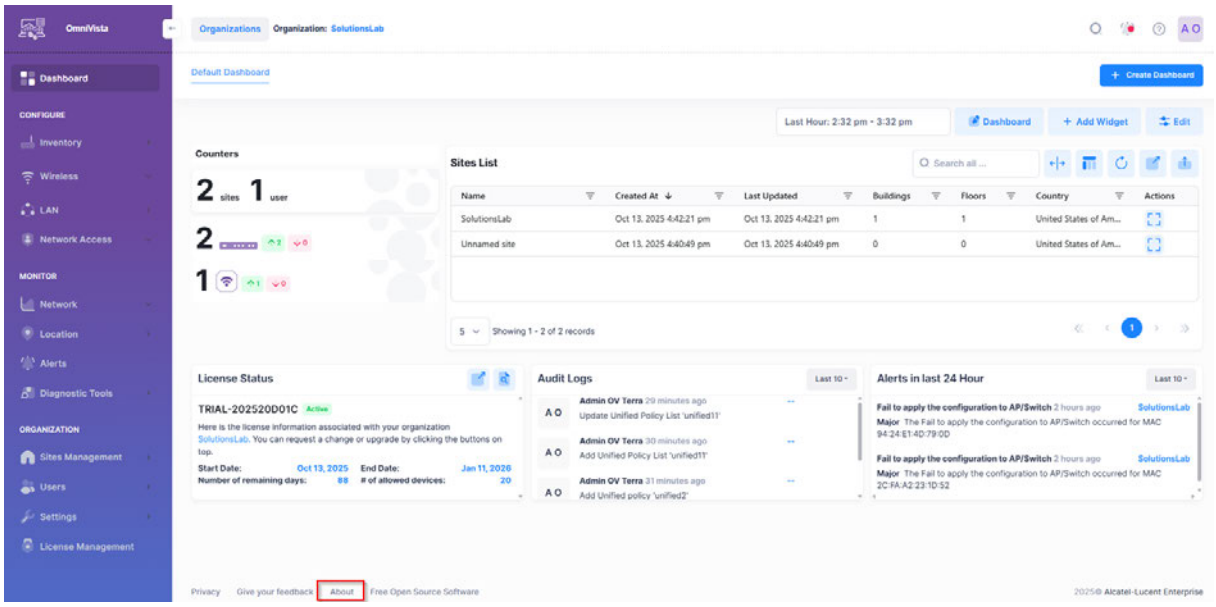
- Activation - 10.5.1.013.6_OVTX_GA
- API Analytics - 10.5.1.013.6_GA
- Wi-Fi RTLS - 10.5.1.013.6_GA
- UPAM - 10.5.1.12
- LAN Monitoring - 10.5.1.013.6_GA
- GDPR - 10.5.1.013.6_GA
- LAN - 10.5.1.013.6_OVTX_GA
- LAN State - 10.5.1.013.6_GA
- LAN Support - 10.5.1.013.6_GA
- DPI - 10.5.1.013.6_GA

There are two ways to access the About Page:

- Click on the **About** link at the bottom of each OmniVista Terra screen (see page 56).
- Click the **About** menu item on the left-hand side of the My Profile screen (see page 56).

2.4.8.1 Accessing the About Page From OmniVista Terra Screens

You can access the About page at the bottom of each OmniVista Terra screen by clicking on the **About** link at the bottom of the Organization Dashboard screen, as shown below.



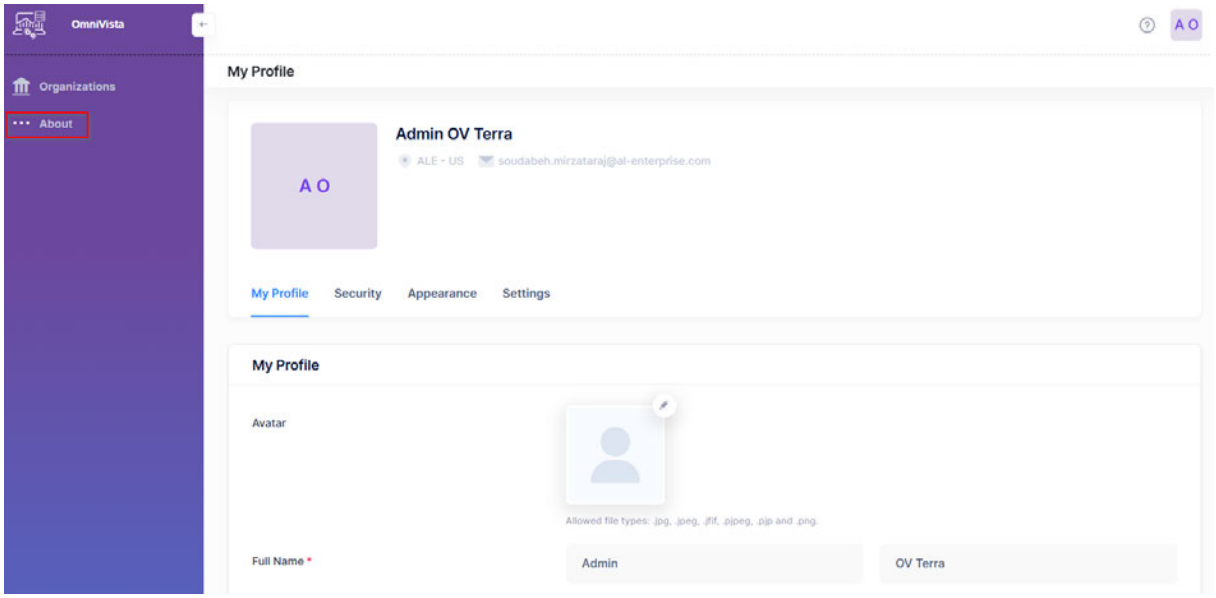
When you click on the **About** link, you will be directed to the page that displays the applications running on the system with the latest release versions.

2.4.8.2 Accessing the About Page From the My Profile Screen Menu

You can go to your basic User Profile, which was created from the information you entered when you created your OmniVista Terra Account (e.g., Name, Company Name, Password). Open the **User Profile**

Menu by clicking on your name in the upper-right corner of any screen, then select **My Profile** to bring up the Account Information Screen.

At the upper-left-hand side of the Menu list, you can view the **About** menu item, as shown below:

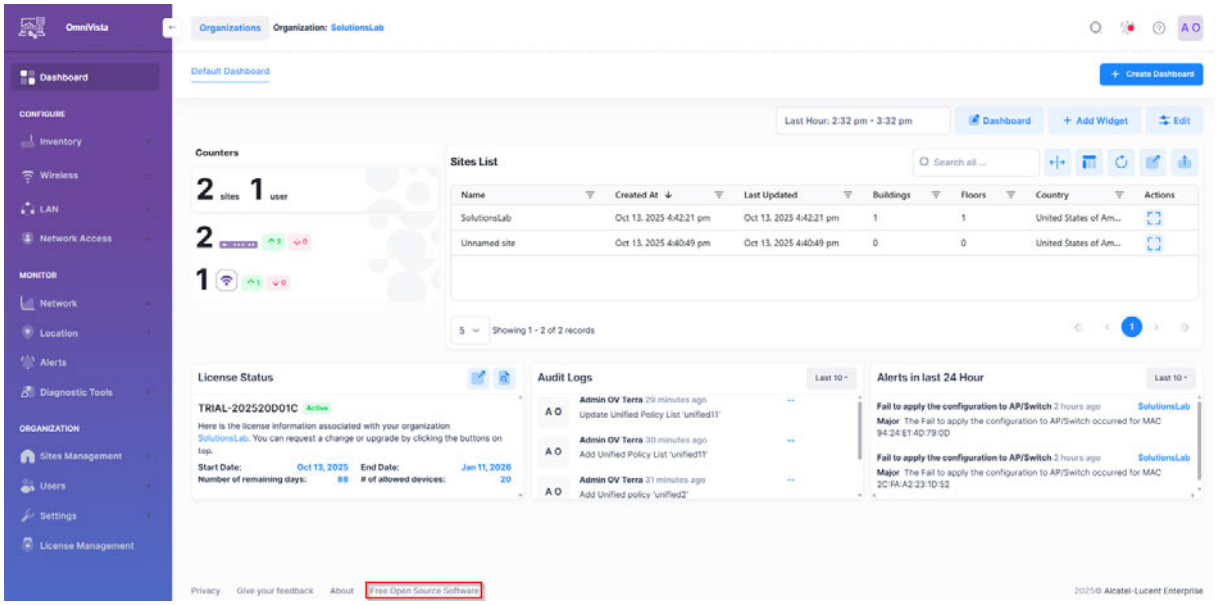


When you click on **About**, you will be directed to the About detail screen which displays the applications running on the system with the latest release versions.

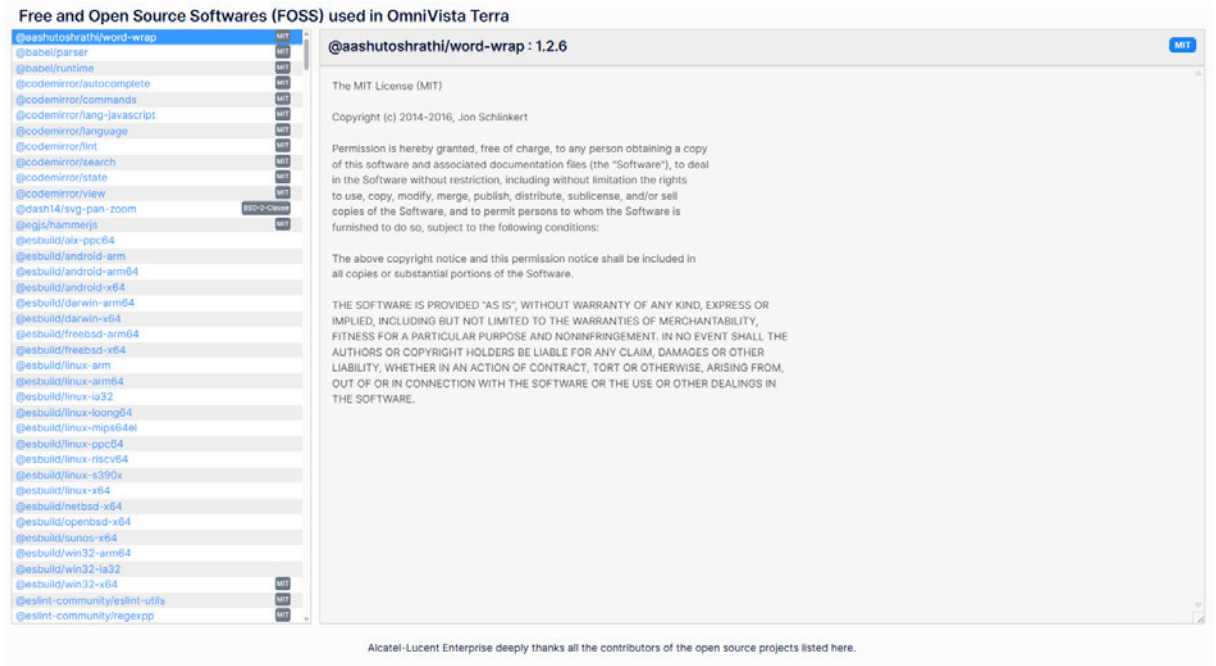
21 Oct 2025

2.4.9 Free and Open Source Software (FOSS) Used in OmniVista Terra

A list of components and libraries, along with their respective license text in full and a copy of the original Copyright and Notice file, is provided for all Open Source Application level components and libraries that OmniVista Terra depends upon. To access this list, click on the **Free Open Source Software** link located at the bottom of every OmniVista Terra screen, as shown below:



When you click on the **Free Open Source Software** link, the attributes page shown below opens. This page provides a clean and efficient display that is organized by the open source projects used in OmniVista Terra. Each project entry provides quick links to the project home page, copyright information, and project license.



21 Oct 2025

3 Configure Organizations for Network Management

Organization networks are monitored and managed using the Organization's Dashboard (see page 71). This section details what you need to know to configure and manage Organizations in OmniVista Terra, including creating Organizations, creating/modifying sites, adding devices, and adding users.

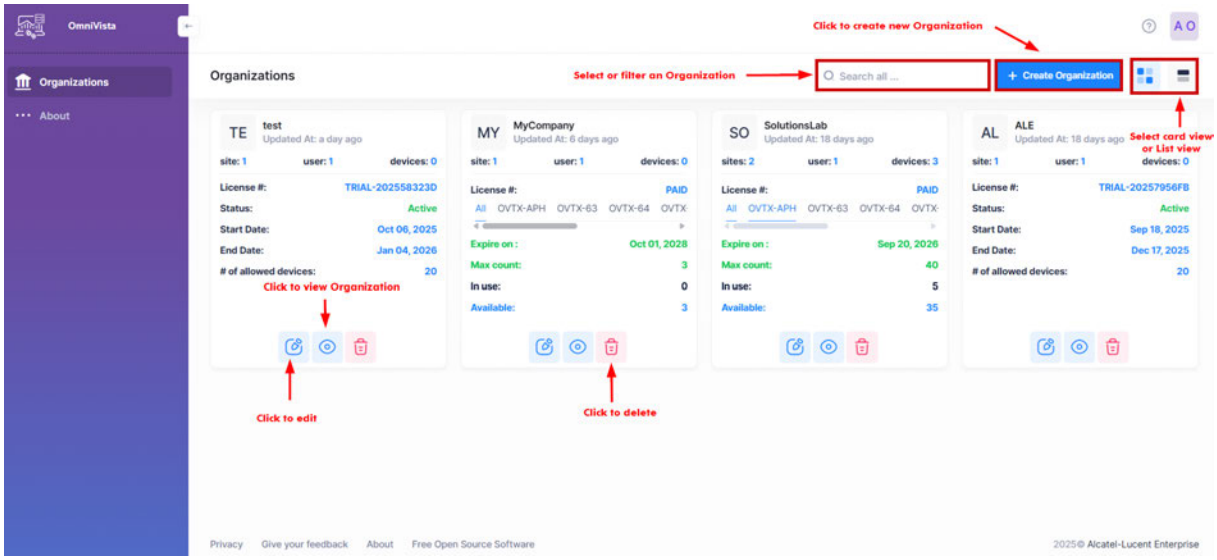
Once you have access to an Organization's Management Portal, you can configure the Organization for network management. Configuring a Management Portal for an Organization includes the tasks listed below. Any Organization User with Admin privileges can perform these tasks. The order shown below is suggested; however, you can create sites, buildings, floors, devices, and users at any time. Click on a task hyperlink for more detailed procedures.

1. Configure and Manage an Organization (see page 61)
2. Configure and Manage a Site (see page 72)
3. Configure and Manage a Building (see page 83)
4. Configure and Manage a Floor (Floorplans) (see page 92)
5. Configure and Manage a Device (see page 168)
6. Configure and Manage Walls (see page 101)
7. Configure and Manage Users (see page 109)
8. Configure and Manage Organization Settings (see page 126)
9. Configure and Manage an Organization License (see page 139)
10. View Audit Log Events at the Organization Level (see page 122)
11. Review Login Attempts at the Organization Level (see page 119)

21 Oct 2025

3.1 Configure and Manage an Organization

Organizations are created from the OmniVista Main Dashboard (see page 31). The Dashboard displays widgets for any Organizations a User is managing.



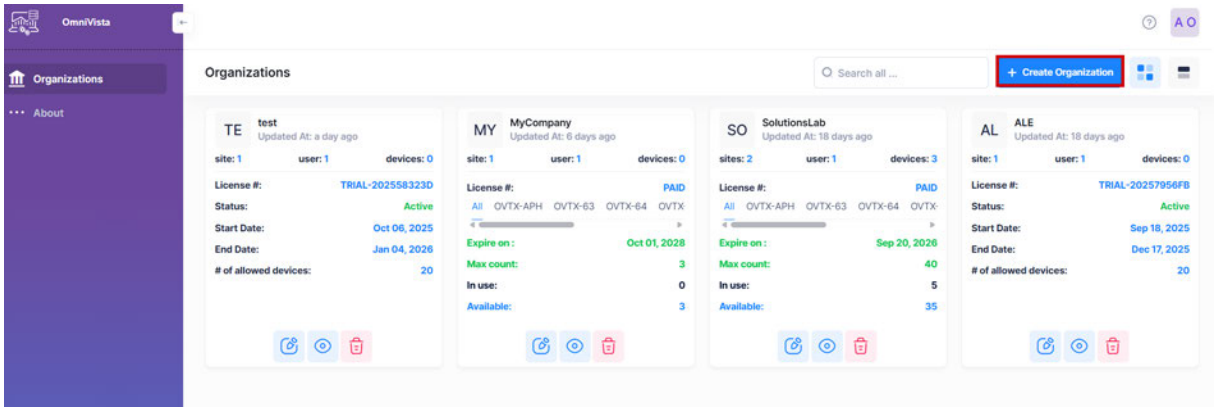
The Dashboard is used to:

- Create an Organization (see page 62)
- Edit an Organization (see page 67)
- Delete an Organization (see page 69)

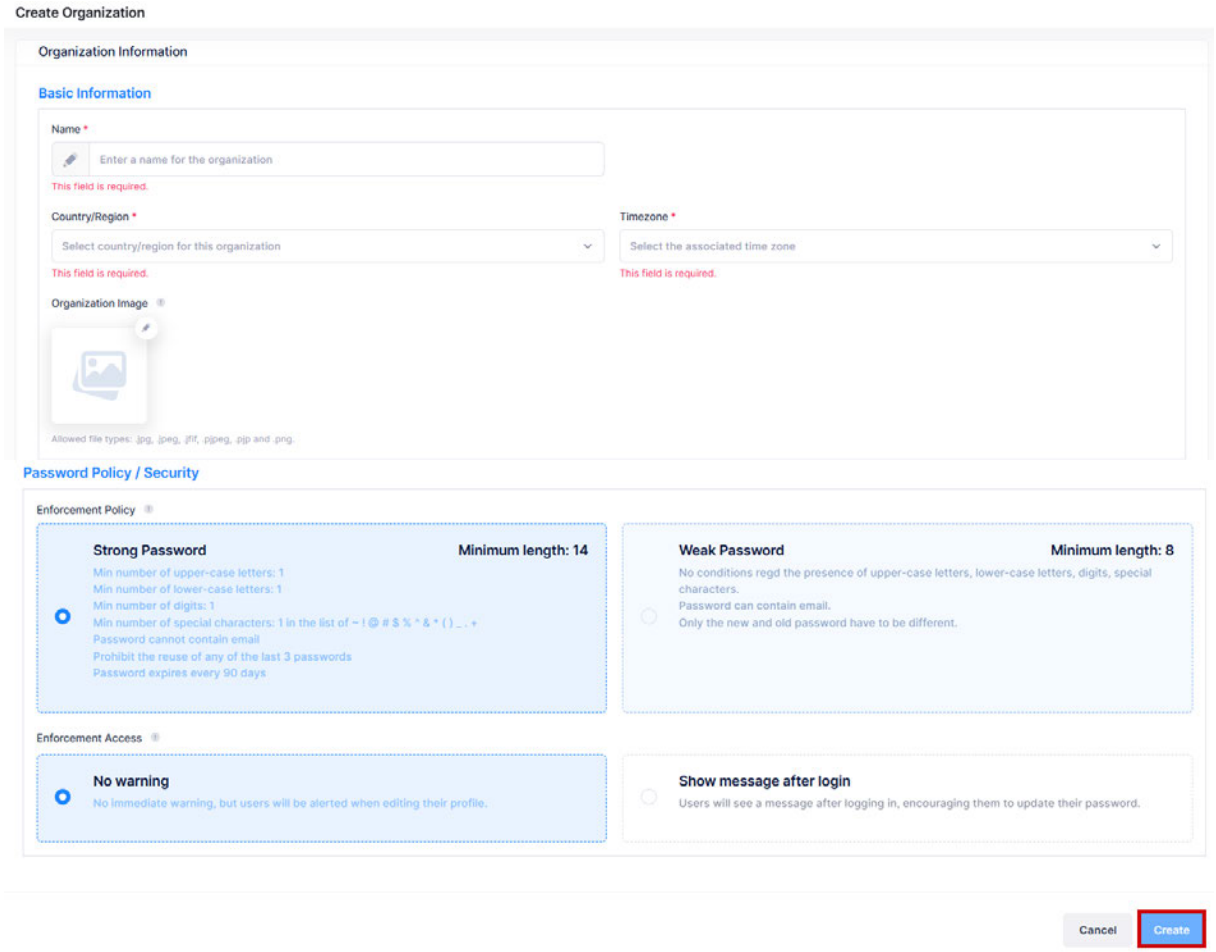
21 Oct 2025

3.1.1 Create an Organization

To create a new Organization, click on **Create Organization** at the OmniVista Main Dashboard (see page 31) to bring up the Organization Information Form.

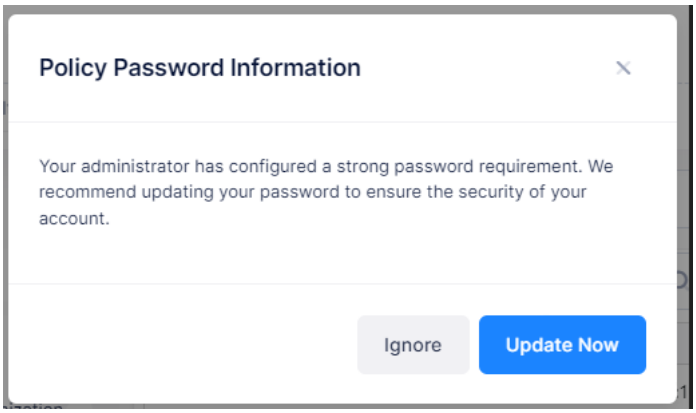


Enter the Basic Information and Password settings as described below and click on **Create**.

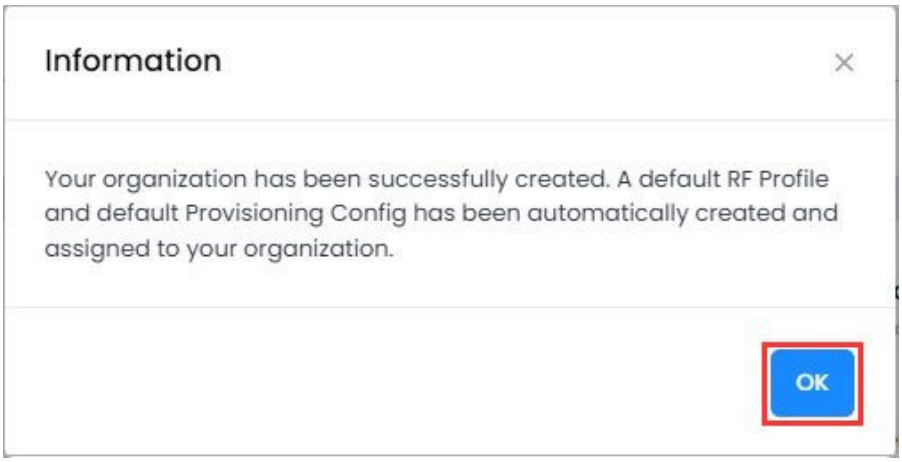


- **Name** - Enter a name for the organization.
- **Country/Region** - Select the country or region for this organization from the drop-down menu.
- **Timezone** - Select the associated time zone for the Region.

- **Organization Image** - Select a image from your computer for the organization.
- **Enforcement Policy** - This setting applies strong password rules when creating or editing OmniVista Terra users. The existing users with the weak passwords can still continue to login even if strong password is chosen.
  - **Strong Password** - Minimum password length is 14 with the following required guidelines:
    - Min number of upper-case letters: 1
    - Min number of lower-case letters: 1
    - Min number of digits: 1
    - Min number of special characters: 1 in the list of ~ ! @ # $ % ^ & * ( ) _ . +
    - Password can not contain e-mail
    - Reuse of any of the last three passwords is prohibited
    - Password requires to change every 90 days
  - **Weak Password** - Minimum password length is 8 with no required guidelines. Password can contain username. Only the old and new password have to be different.
- **Enforcement Access** - Selecting this option will apply the chosen password policy settings to the existing users within the organization or site. The existing users with only weak passwords will be prompted to update their passwords based on this policy. After the message, the user can choose to skip it. There is no mandatory condition to change the password.
  - **No warning** - There will be no immediate warning message will be sent to the users to update passwords but the users will be alerted while editing their profile.
  - **Show message after login** - The users will see a message after they log in to the network to update their passwords and if the user's current password does not meet the strong password requirements, a modal will prompt the user to change their password to a strong one after they log in as shown below.



When you click on **Create**, the following Information prompt displays to inform you that the Organization was created and that a default RF Profile and Provisioning Configuration were created and assigned to the Organization.

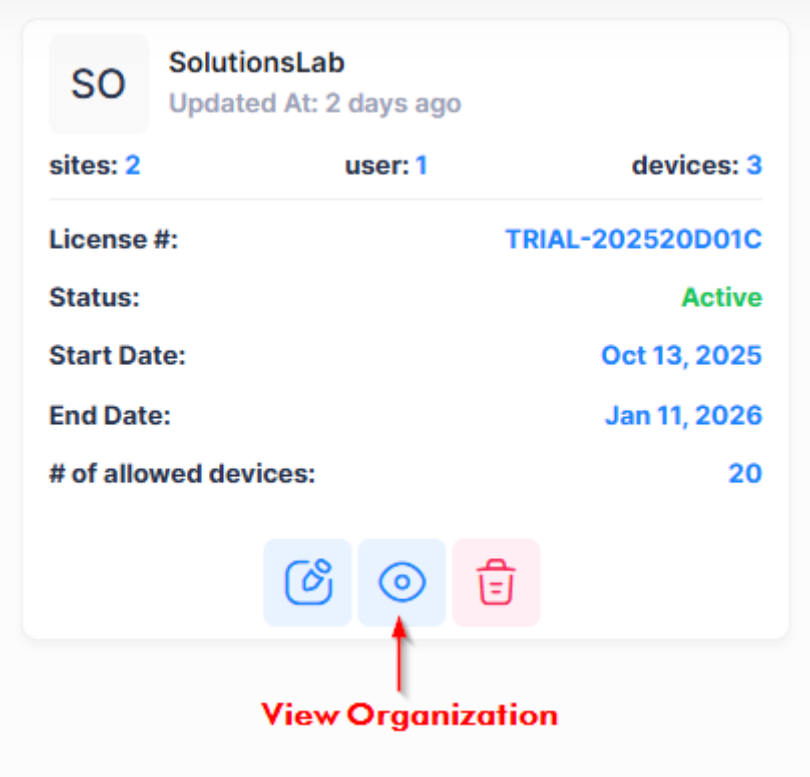


Click **OK** to close the Information prompt. You will be returned to the Main Dashboard and the new Organization widget is displayed on the left side of the Dashboard.

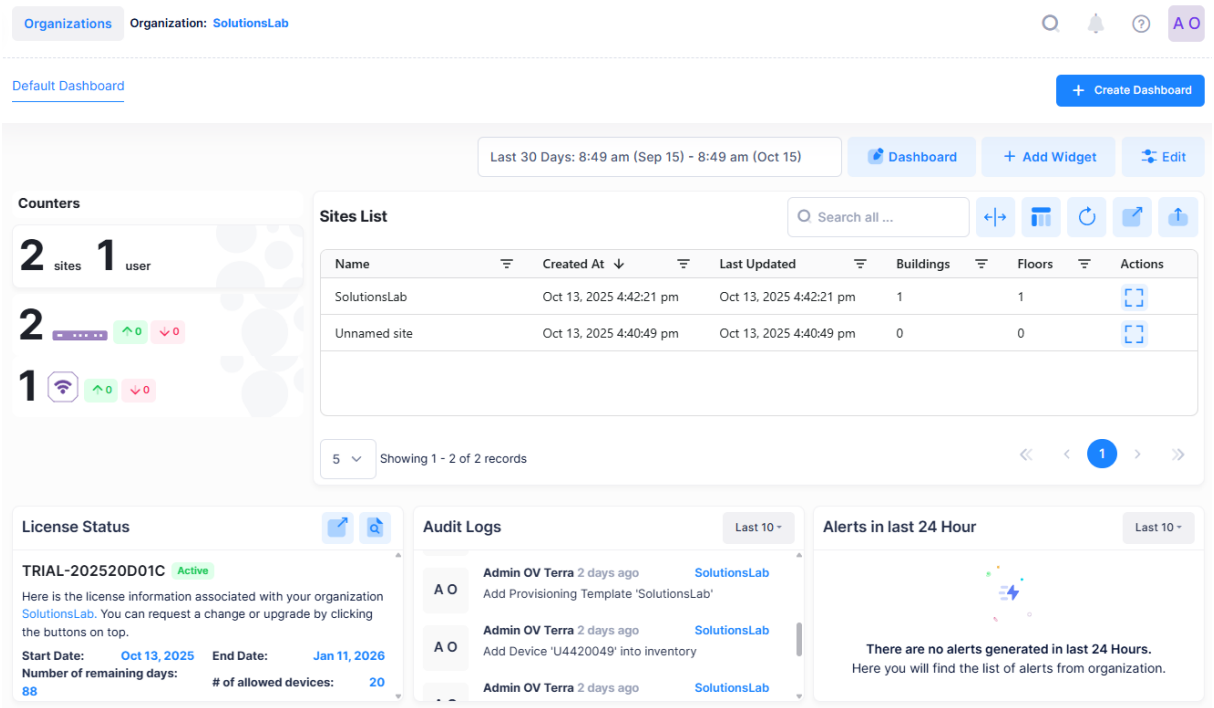
21 Oct 2025

3.1.2 View an Organization

When an Organization is created, it is automatically authorized for a free, teaser period license (see page 142). You can immediately access the Organization by clicking on the **View Organization** icon at the bottom of the Organization widget.



The dashboard for the Organization you want to view is displayed.

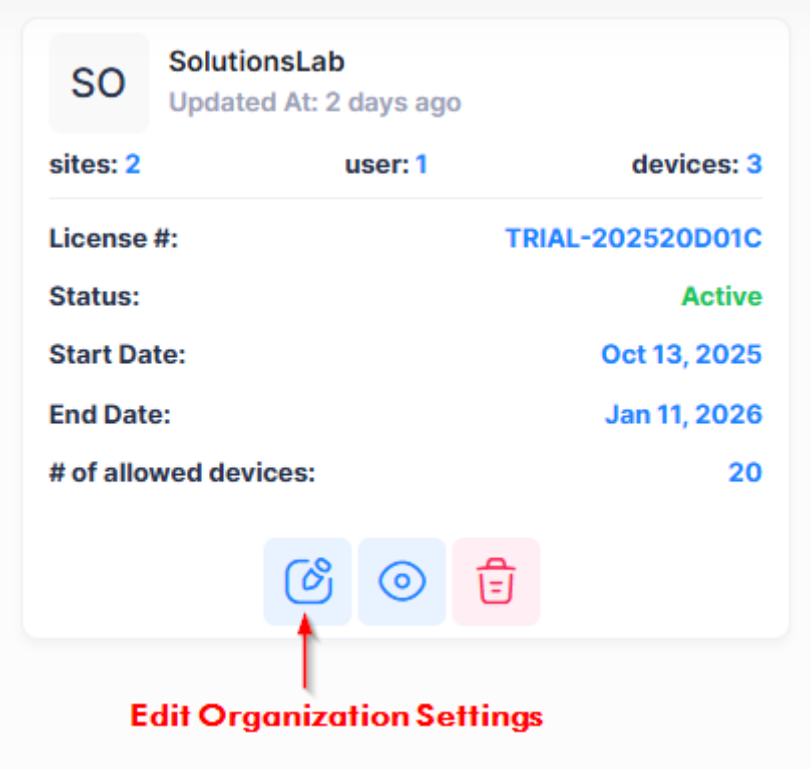


From the Organization Dashboard, you can create sites, buildings, and floors. You can also add devices, invite users to the Organization, manage Organization licenses, and monitor the Organization's network.

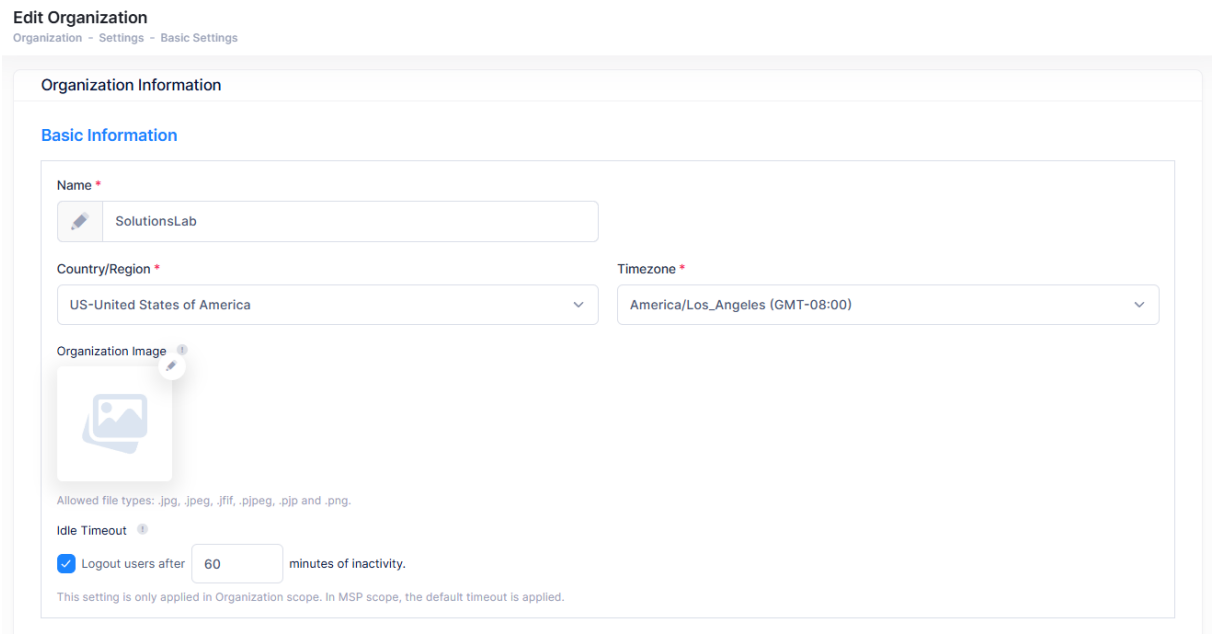
21 Oct 2025

3.1.3 Edit an Organization

To edit Organization settings, click on the **Edit** icon located at the bottom of the Organization widget.



You are redirected to the Edit Organization (see page 127) (Organization > Basics Settings > Settings) screen.



On the Edit Organization screen, you can modify basic information for the Organization, such as Name, Country/Region, Timezone, and upload an optional Organization image. In addition, you can modify the

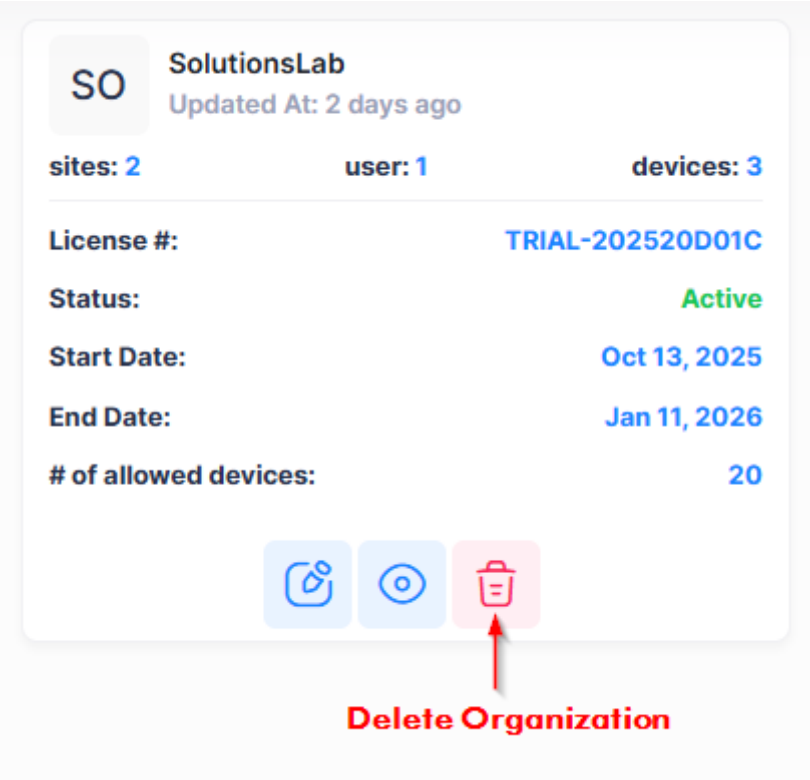
data retention period for certain applications, the Password Settings to apply password enforcement rules, and the frequency of periodic configuration audits.

Click on **Save** to save the changes. You are redirected back to the Organization Dashboard.

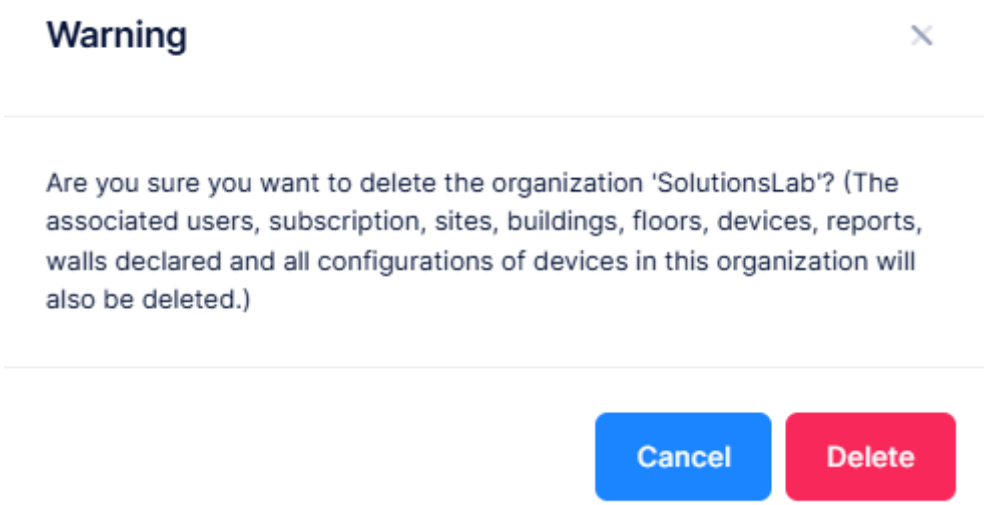
21 Oct 2025

3.1.4 Delete an Organization

To delete an Organization from the OmniVista Main Dashboard (see page 31), click on the **Delete** icon located at the bottom of the Organization widget.



Click on **Delete** at the Confirmation Prompt. The Organization Widget will be removed from the OmniVista Main Dashboard.

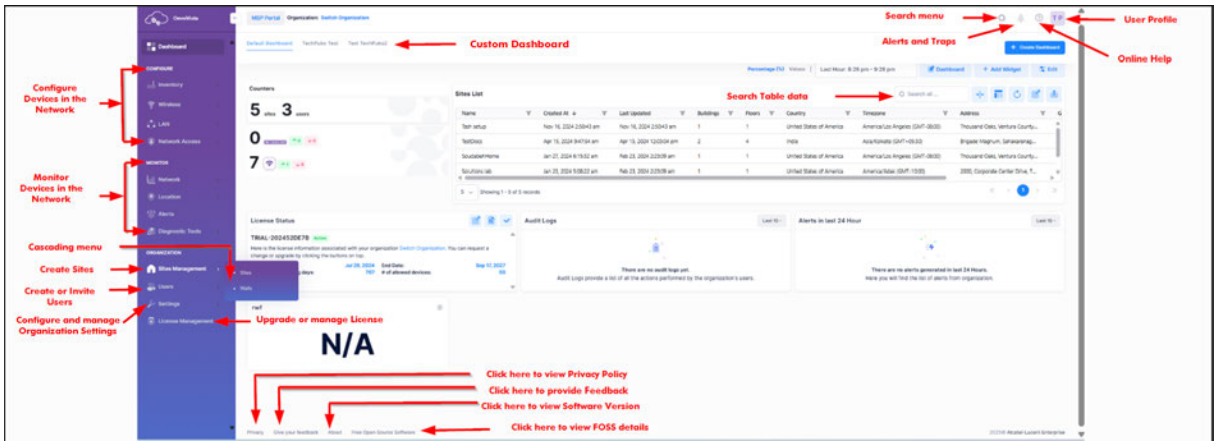


When you delete an Organization, the associated users, subscription, sites, buildings, floors, devices, reports, walls declared, and all the configurations of devices in this Organization are also deleted.

21 Oct 2025

3.1.5 The Organization Dashboard

The Organization Dashboard is used to configure and monitor the Organization network. The Dashboard provides an overview of the number of sites, users, and both sites and devices managed by the Organization. The Dashboard also provides an overview of the OmniVista license subscriptions and a list of any audit logs and alerts for the Organization. The OmniVista Terra Menu on the left-hand side provides links to all of the OmniVista applications used to configure and monitor the Organization's network, as well as manage the Organization.



The Organization Dashboard is used to:

- Configure and Manage a Site (see page 72)
- Configure and Manage a Building (see page 83)
- Configure and Manage a Floor (Floorplans) (see page 92)
- Add Devices (see page 195)
- Configure and Manage Users (see page 109)
- View Audit Logs (see page 122)
- View License Status (see page 143)
- View Alerts in last 24 Hour (see page 948)
- Create Custom Dashboards (see page 36)

21 Oct 2025

3.2 Configure and Manage a Site

Multiple sites can be created and managed under a single Organization. For example, the ALE International Organization may have sites in different countries. Each country may have multiple cities where AP devices are installed. A site can be created to identify and manage a group of devices installed at the site location. Within a site there may be more than one building in which AP devices are located.

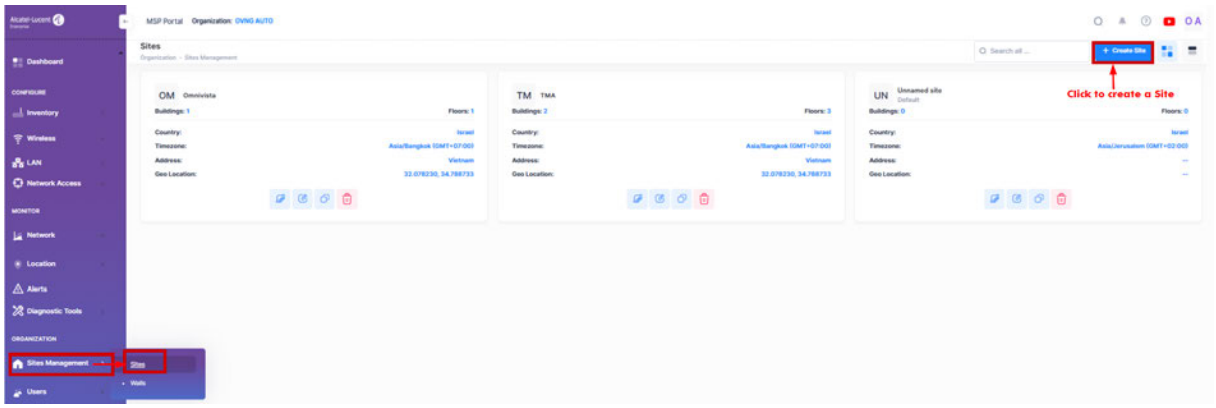
The Organization Dashboard (see page 71) is where organization sites can be created and managed. Click on **Sites Management** under the “Organization” section of the OmniVista Terra Menu (see page 45). Use the Sites option to complete the following tasks:

- Create a Site (see page 73)
- Clone a Site (see page 76)
- Geolocate a Site (see page 79)
- Edit Site Settings (see page 80)
- Delete a Site (see page 82)

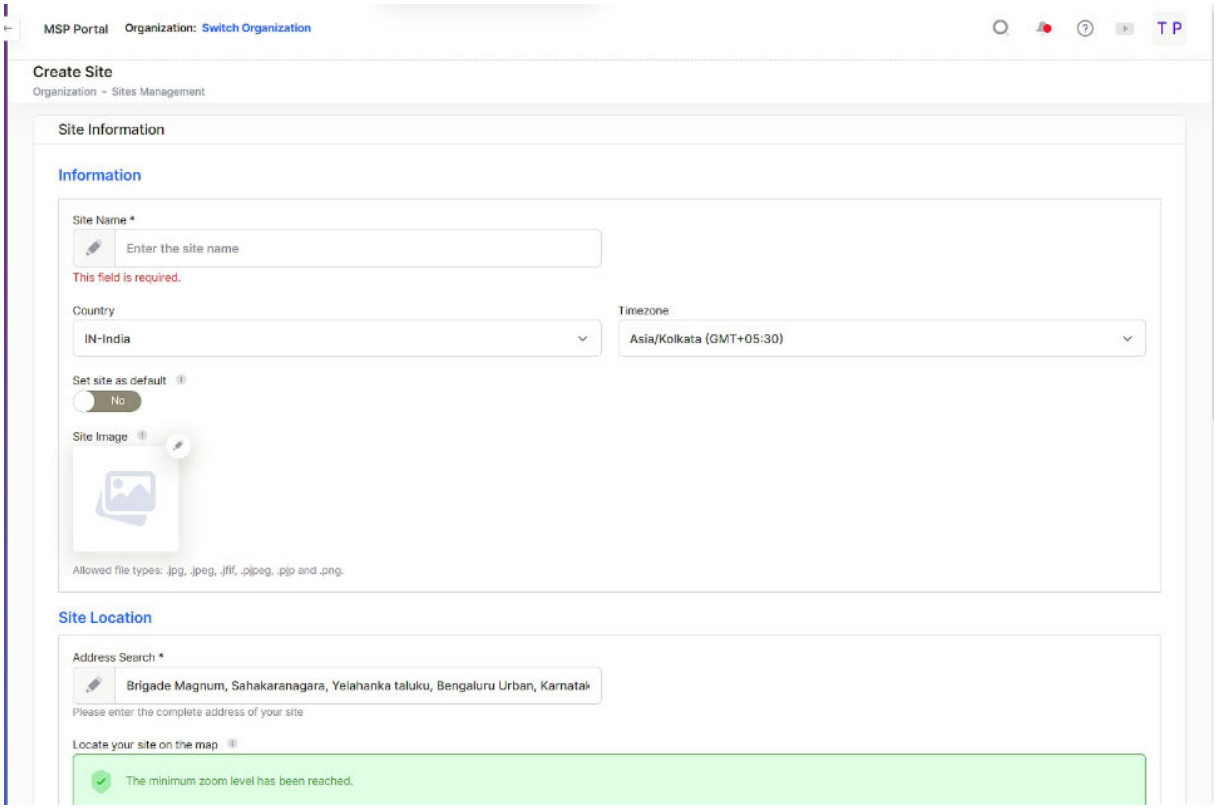
21 Oct 2025

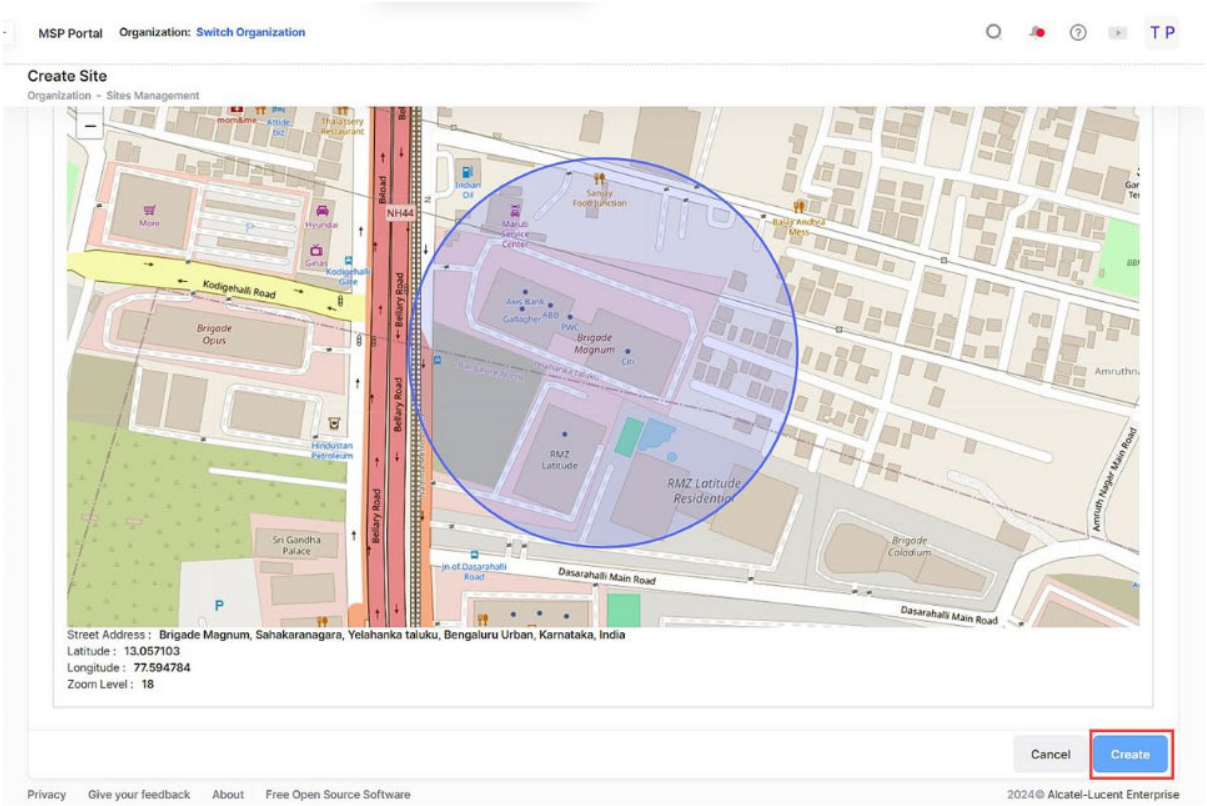
3.2.1 Create a Site

To create a site for an existing organization, click on **Sites Management** under the Organization section of the OmniVista Menu. The menu cascades to display two additional items: Sites and Walls. Click on **Sites** to display the following screen for creating and managing sites:

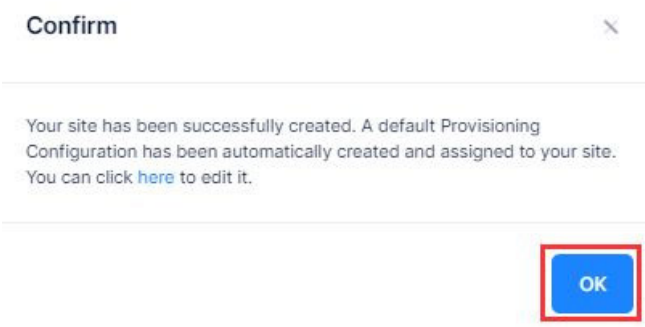


On the Sites screen, click on **Create Site** at the top-right of the screen to bring up the Create Site form.

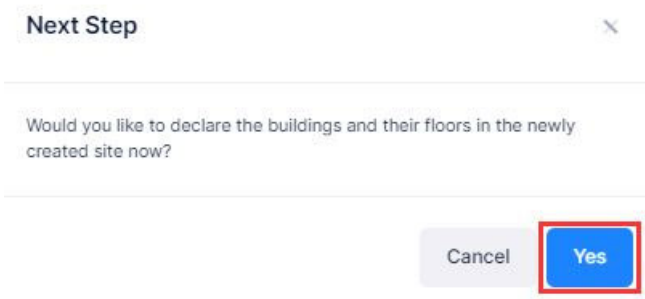




Fill out the required and optional fields for the new site and click on **Create Site**. You will get a confirmation screen about creation of a default provisioning configuration for the site. Click **OK**



You will be returned to the Sites screen, where a widget for the new site was added and you are prompted if you want to declare the buildings and floors in the new site.

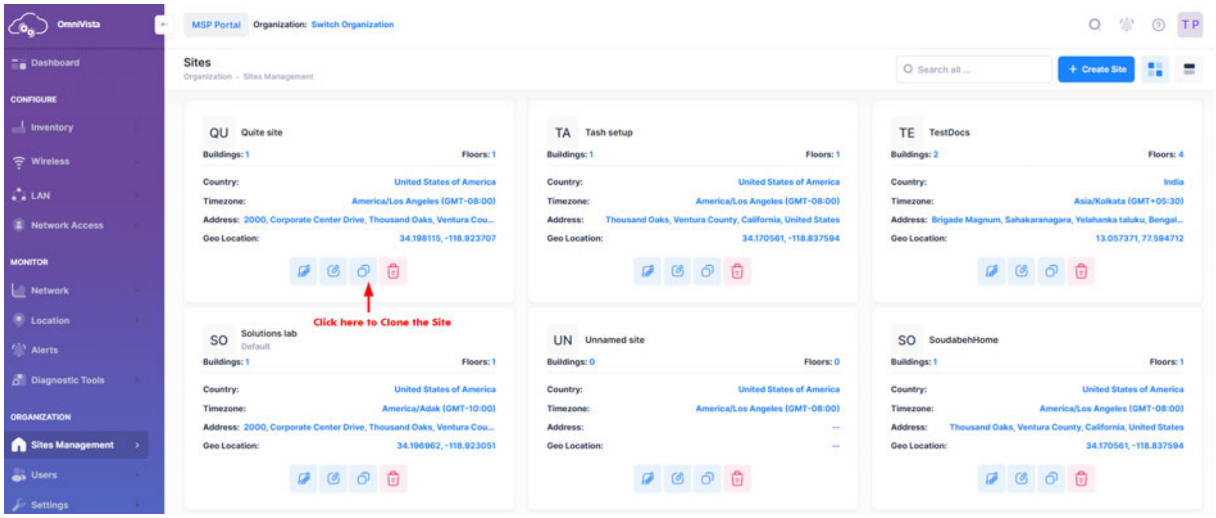


If you want to declare the buildings and floors at this point, click on **Yes**. If not, click **Cancel**.

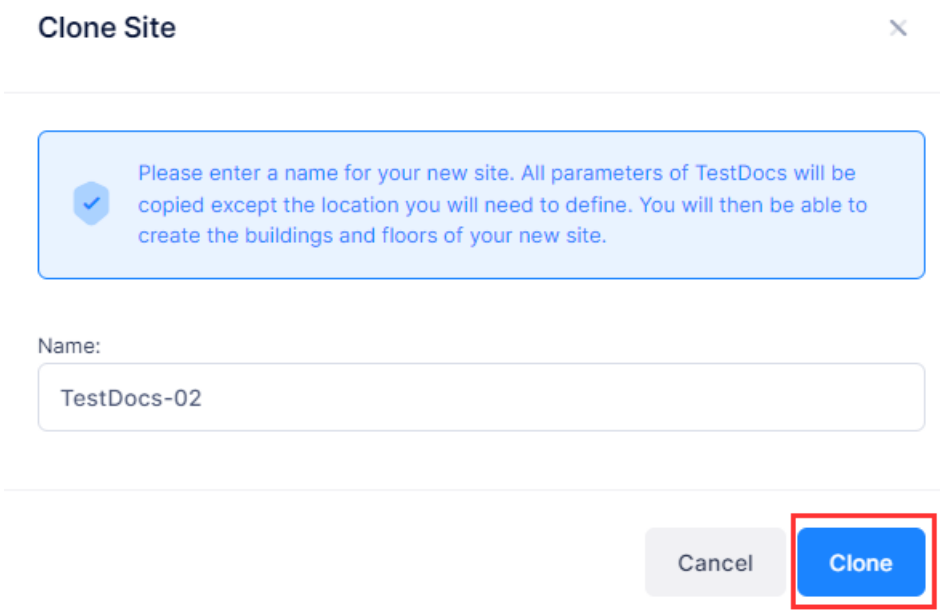
21 Oct 2025

3.2.2 Clone a Site

You can clone an existing Site and edit it to create a new Site. To clone an existing Site, click on the Actions icon and select **Clone** from the drop-down menu.

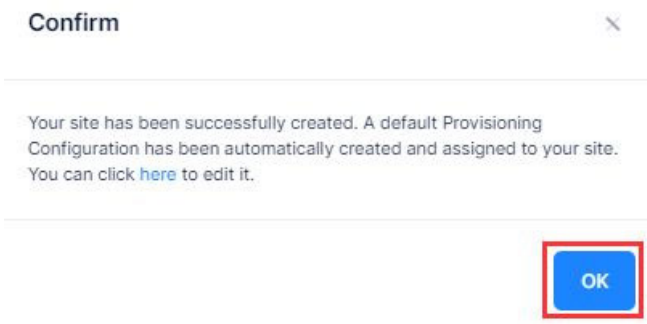


After you click on **Clone**, the following Clone Site prompt opens.

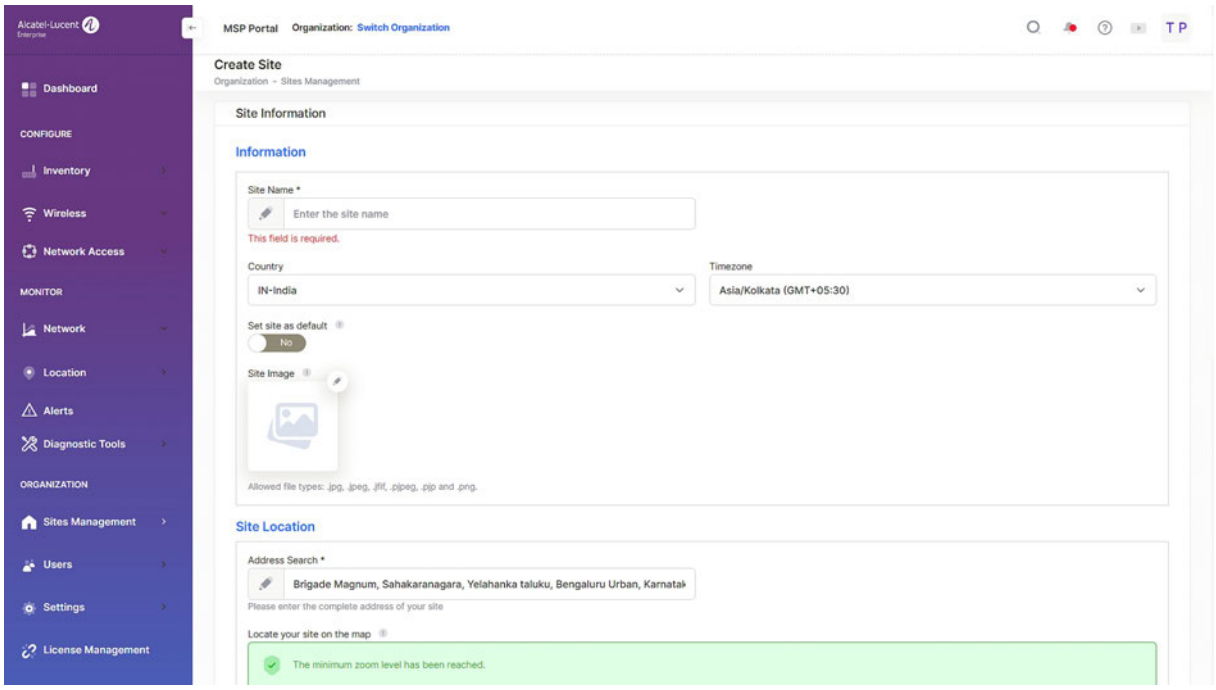


Enter the name you want to assign to the new site and click **Clone**. The Create Site screen (see page 73) will open containing all the information copied from the Site you were cloning. You can change any of the Site parameters and will need to locate your site on the map. Click on **Create Site** when you are done.

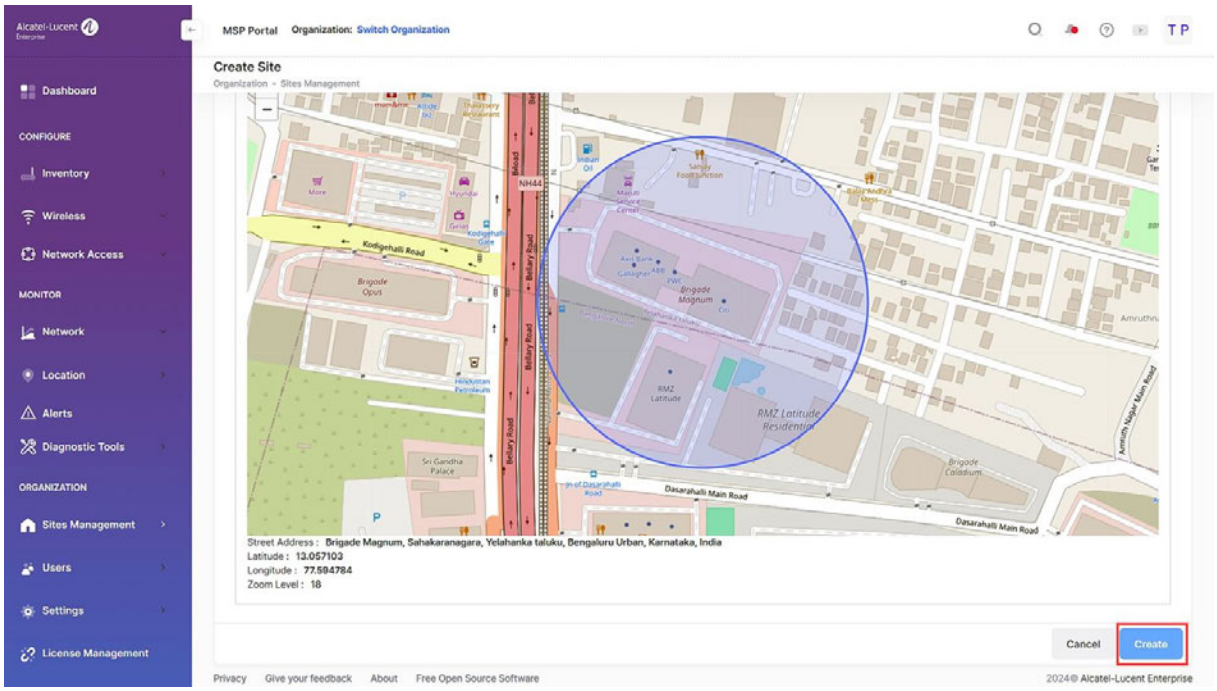
The following prompt displays informing you that your Site was created and a default Provisioning Configuration was automatically assigned to your site.



You will now be redirected to Create Site window.



Enter the site details and click on **Create**.

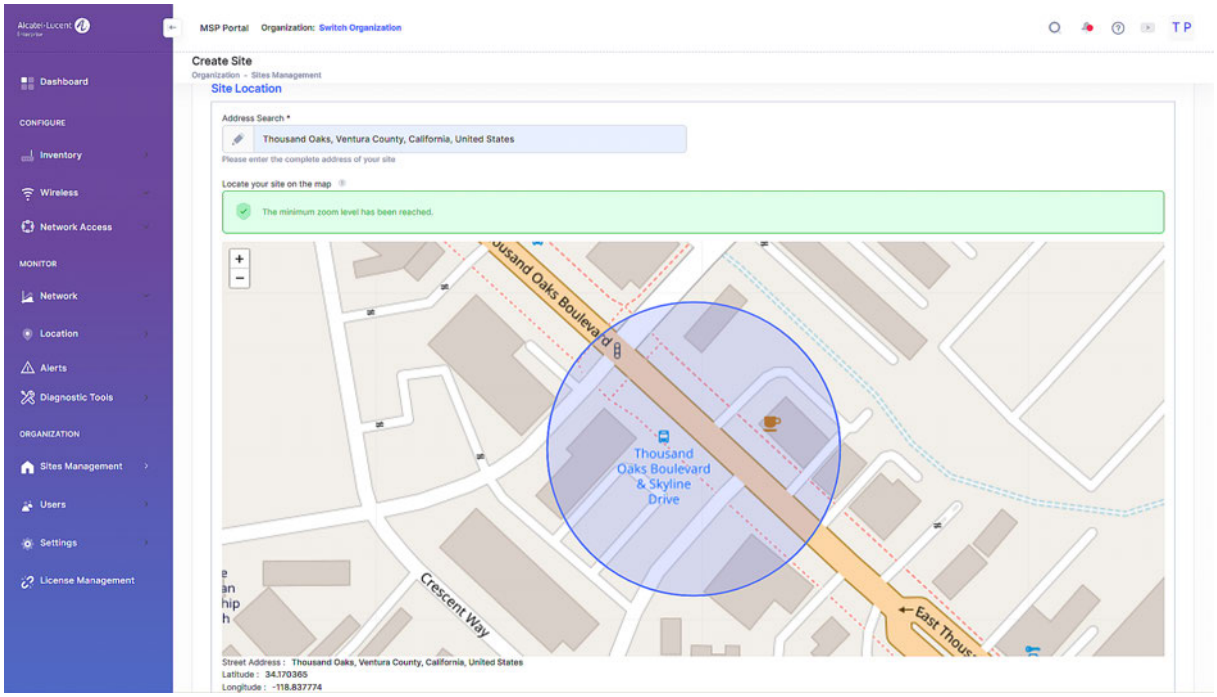


Your cloned site is now created.

21 Oct 2025

3.2.3 Geolocate a Site

The following Site Location section is on the Create Site (see page 73) form and is used to identify the location of your site:



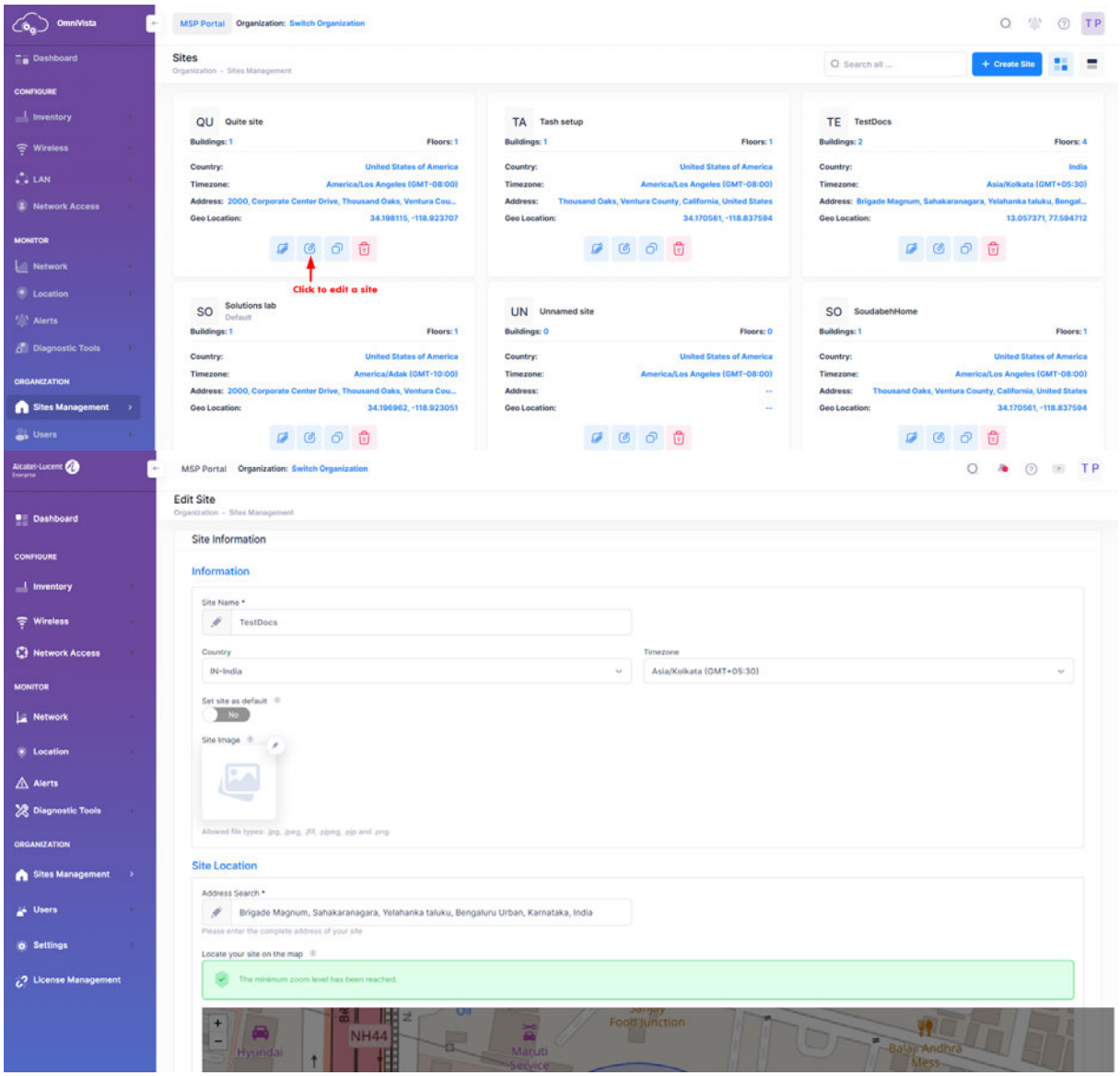
When you enter the site address, the map automatically moves to include the geographic area of the address within the map. Once this is done, move the map with your cursor until the site-building is within the circle. You may have to zoom in on the map to locate the building.

After locating the Organization site and completing any other required or optional fields on the form, click on Create Site in the lower, right-hand corner of the screen (not shown).

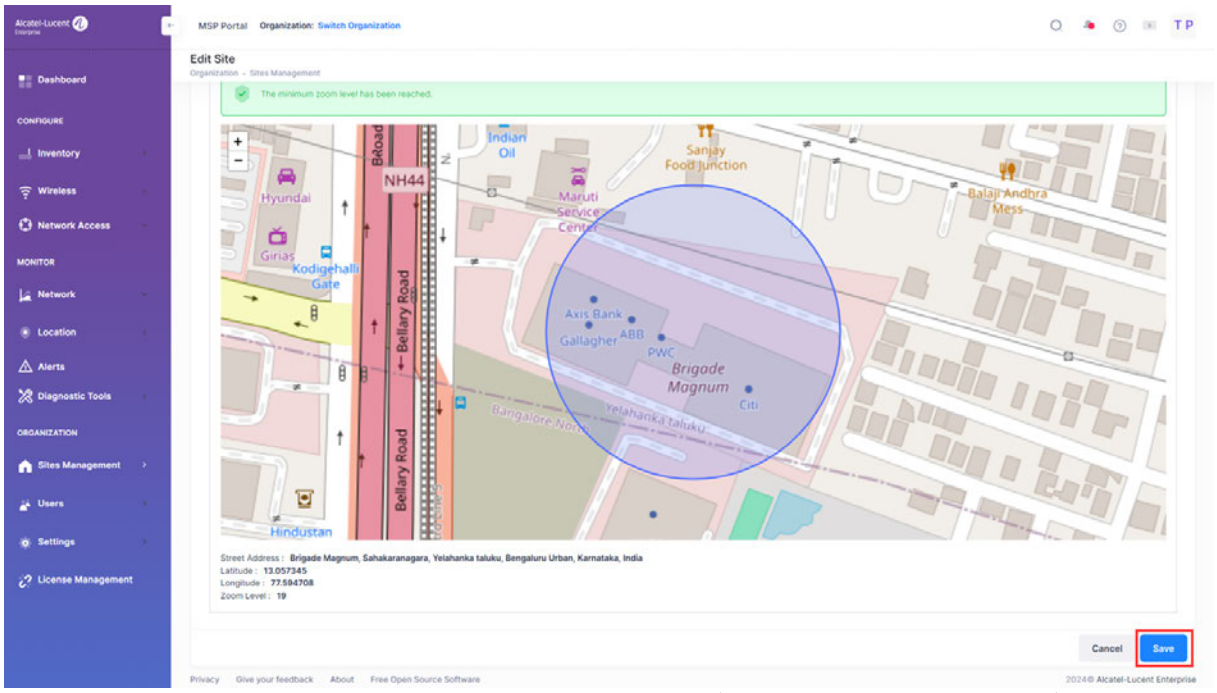
21 Oct 2025

3.2.4 Edit Site Settings

On the Sites screen, click on Pencil button bring up the Site Edit form.



1 **Site Edit Form**

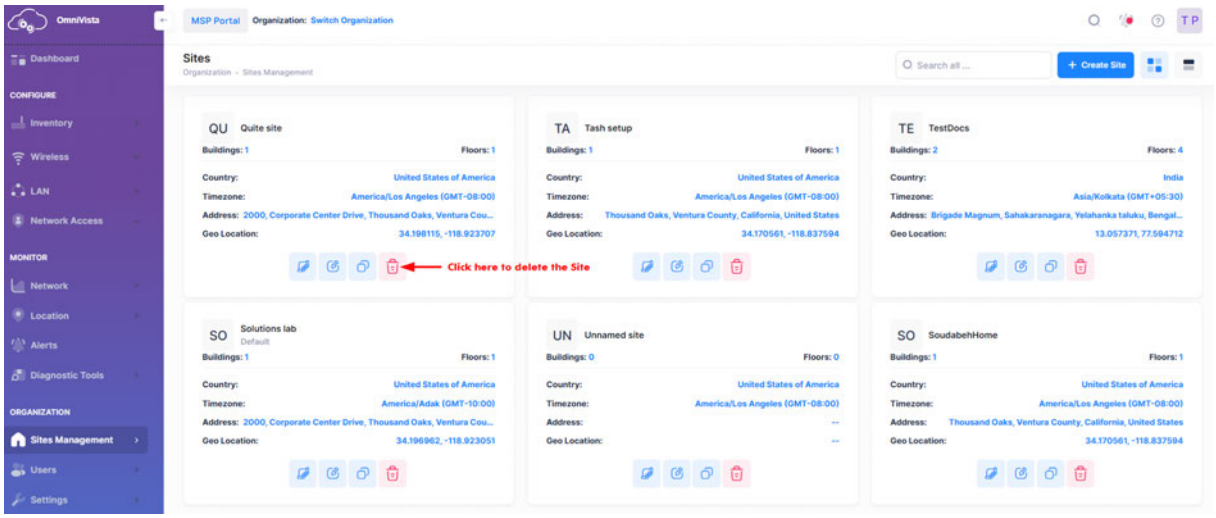


On the Site Edit Form page you can edit the site information (such as the name of the site), the location of the site, and change the optional image associated with the Site Widget. Click on **Save** to save the changes and return to the list of sites for the organization.

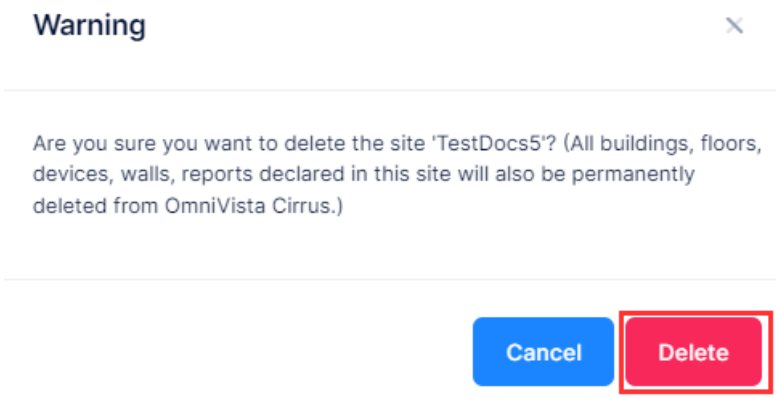
21 Oct 2025

3.2.5 Delete a Site

On the Sites screen, select a site and click on **Delete.**



On confirmation, click **Delete.** The Site Widget will be removed from the list of organization sites.



2 **Delete Confirmation Prompt**

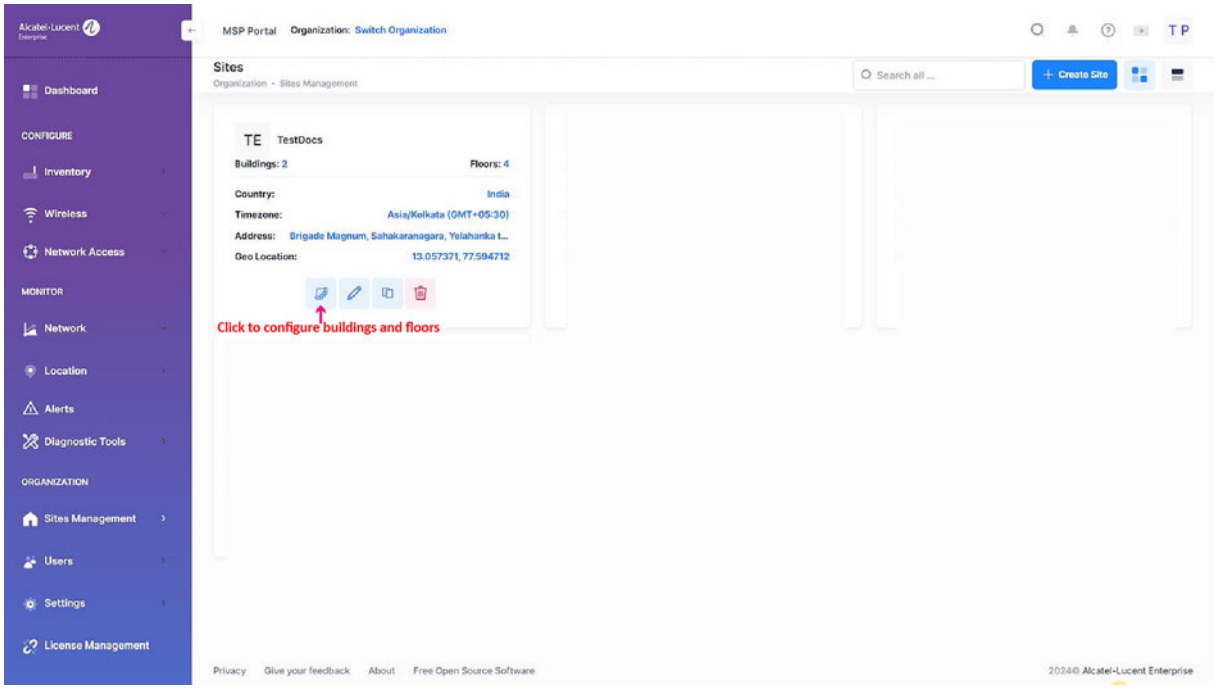
When you delete a Site, the associated buildings, floors, devices, and walls declared in the Site are also deleted.

21 Oct 2025

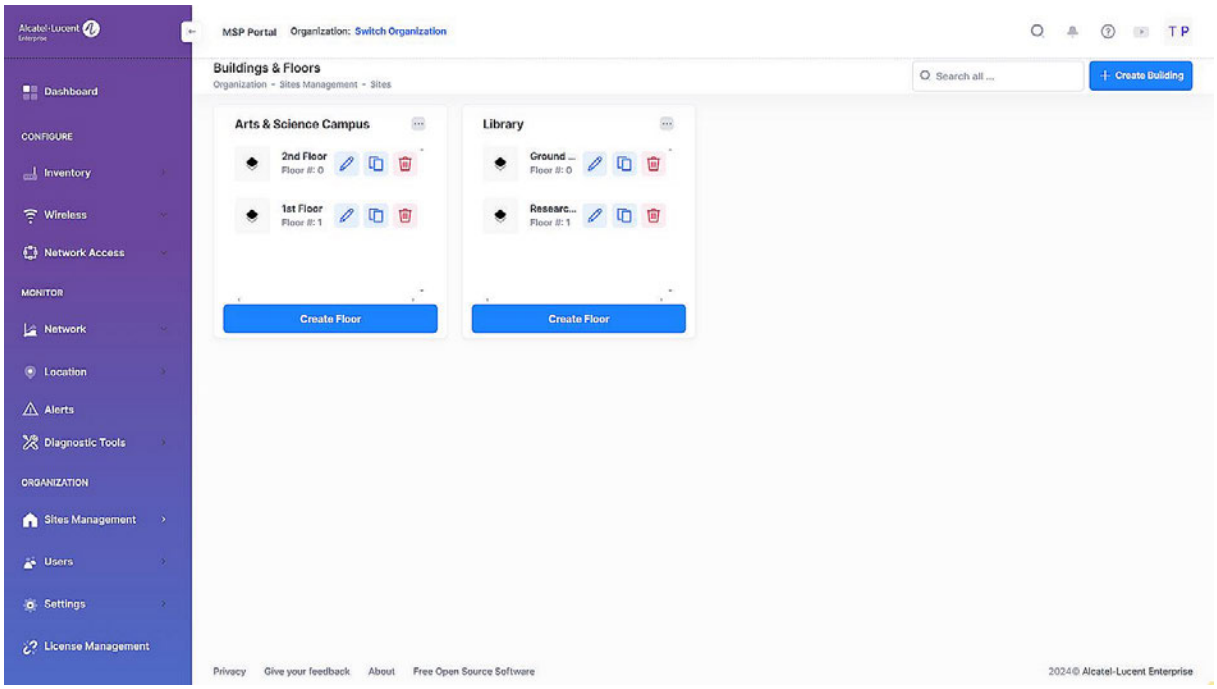
3.3 Configure and Manage a Building

After creating a Site for an Organization (see page 73), you can declare buildings and floors that exist within the Site. When an AP device is added to OmniVista Terra for monitoring, the building in which the device is located must be specified. Make sure Site buildings and floors have been defined before attempting to add a device to the Site.

On the Site Widget, click on **Configure Buildings & Floors** to open the Buildings & Floors screen.



3 **Sites Home Page**



4 **List of Buildings in the Site**

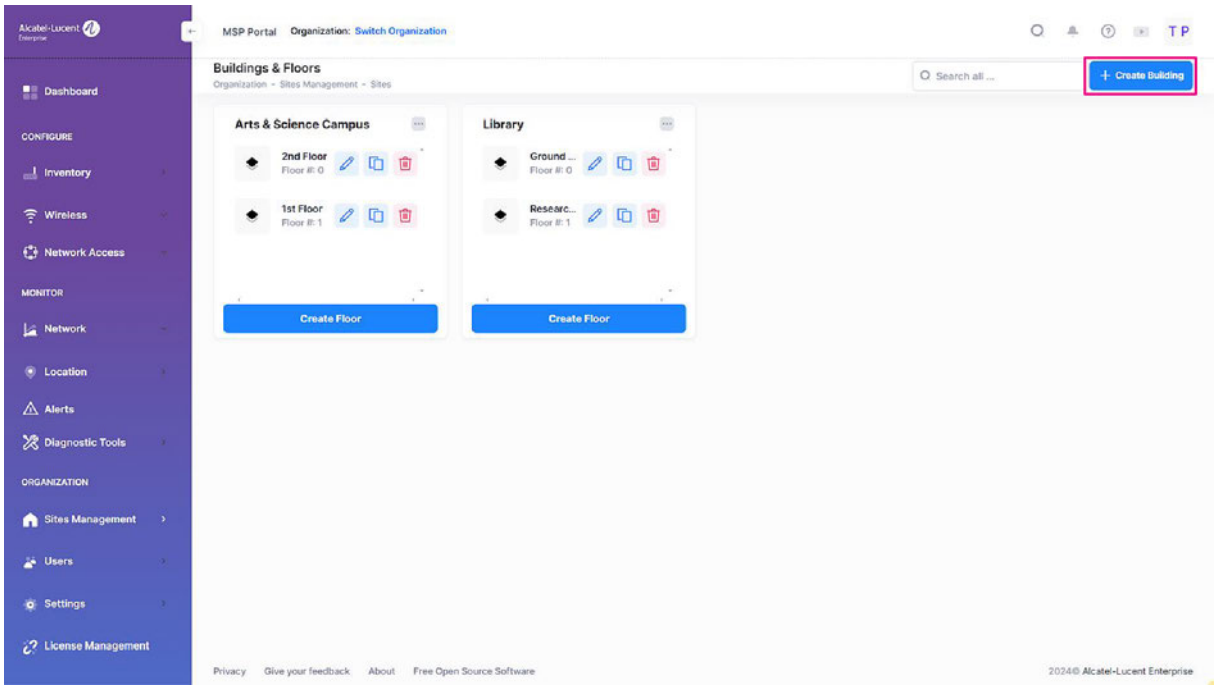
Use the options on the Buildings & Floors screen to complete the following tasks:

- Create a Building (see page 85)
- Clone a Building (see page 87)
- Edit Building Settings (see page 89)
- Delete a Building (see page 90)
- Configure and Manage a Floor (see page 92)

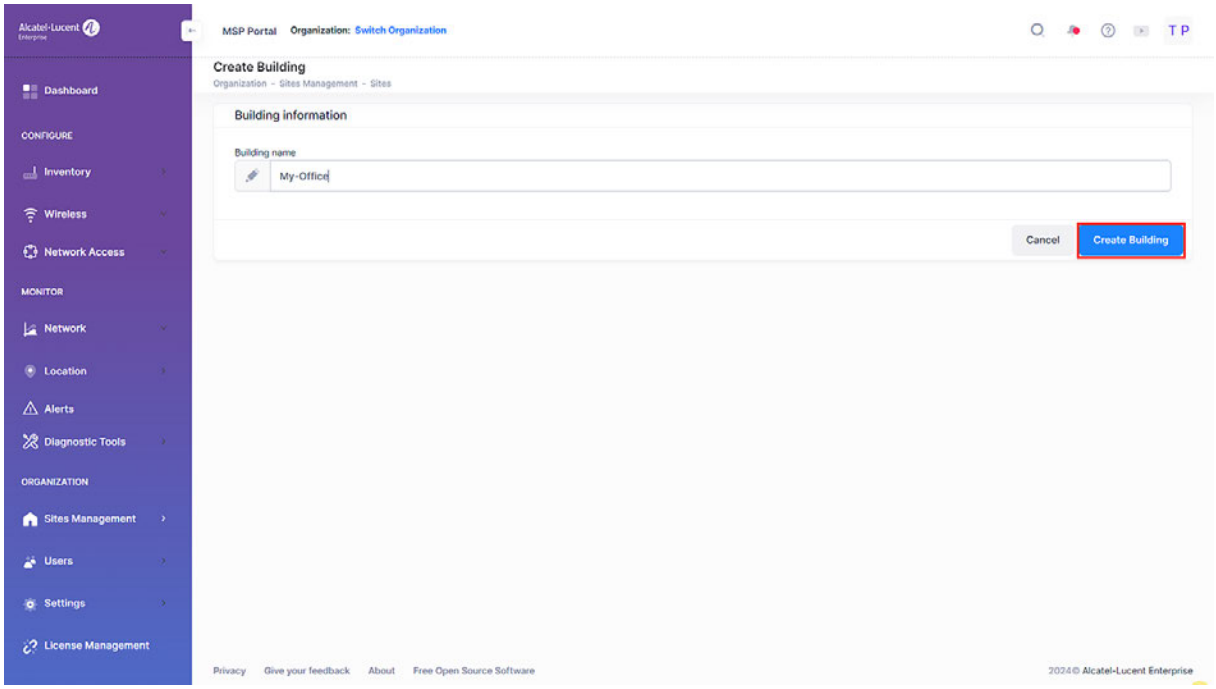
21 Oct 2025

3.3.1 Create a Building

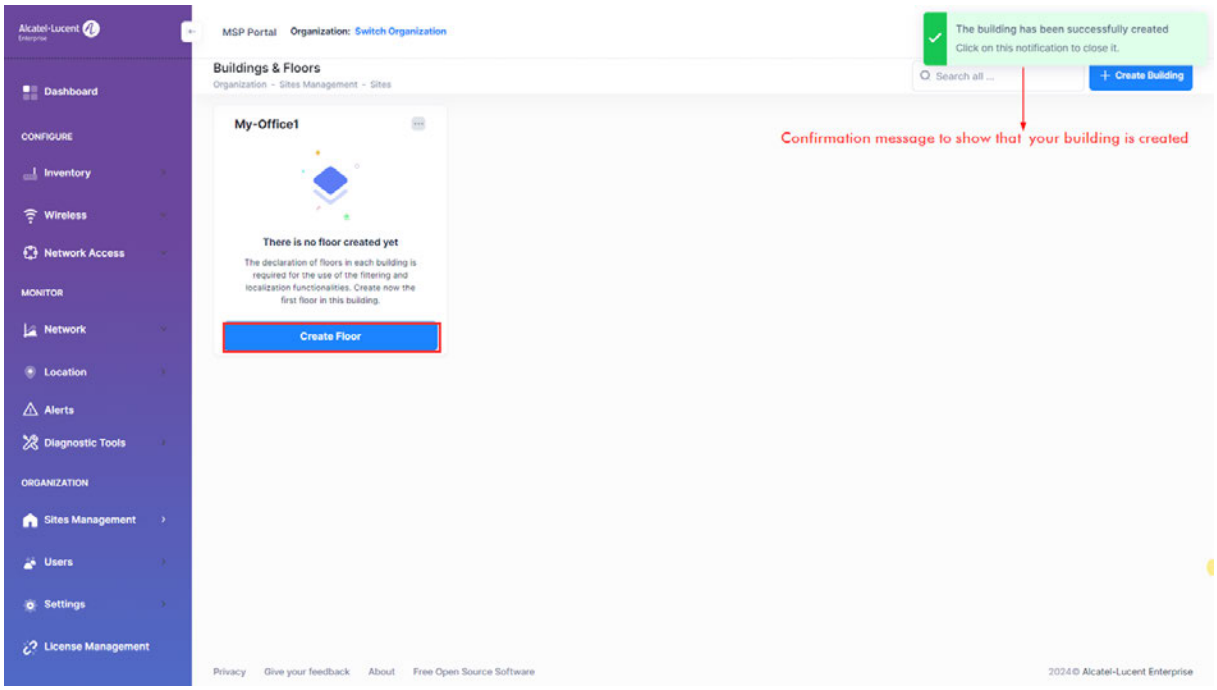
To create a building for an existing Site, click on **Create Building** to bring up the Create Building form.



Enter the name you want to assign to the building and click on **Create Building**.



A confirmation message is displayed to show that your building is created.

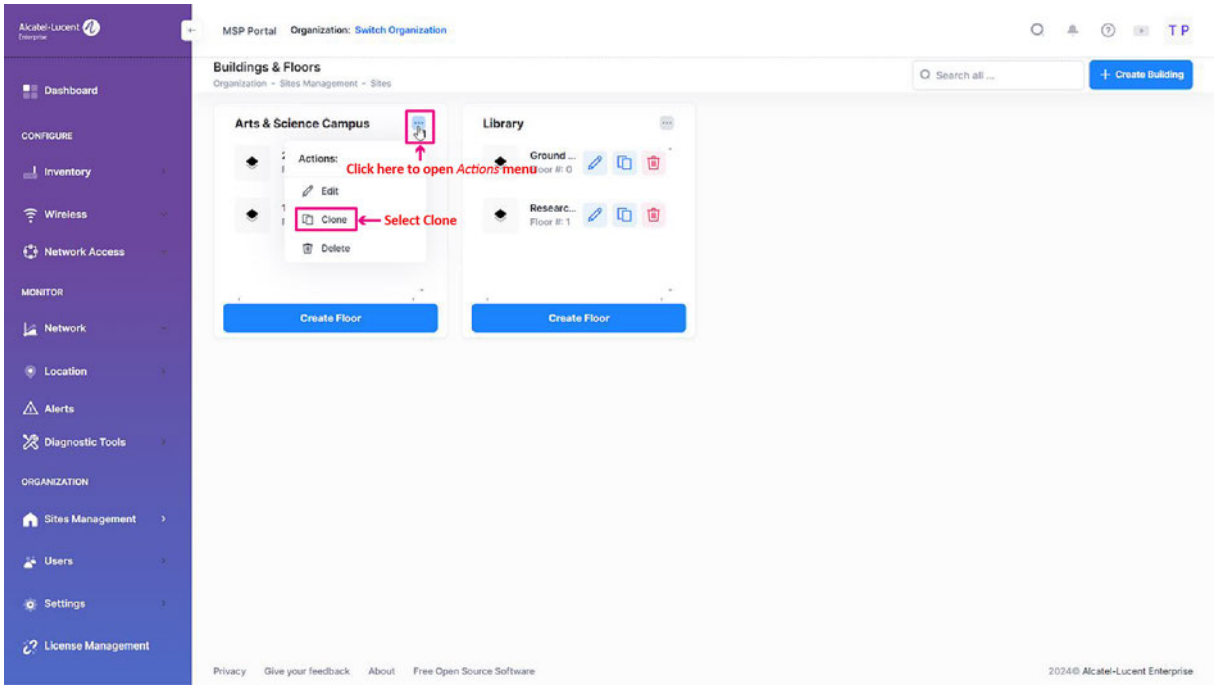


You will be returned to the Buildings & Floor screen, where a widget for the new building has been added.

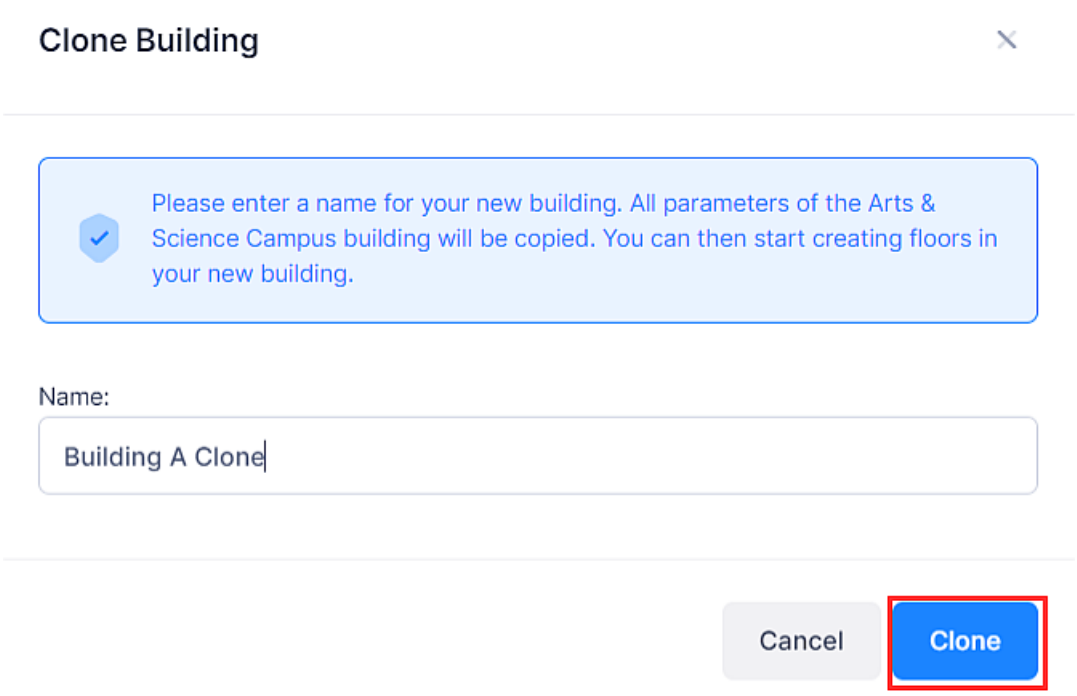
21 Oct 2025

3.3.2 Clone a Building

You can clone an existing Building to create a new Building. To clone an existing Building, click on the three dots option to open ***Actions*** menu and select **Clone** from the drop-down menu.



After you click on **Clone**, the following Clone Building prompt opens:

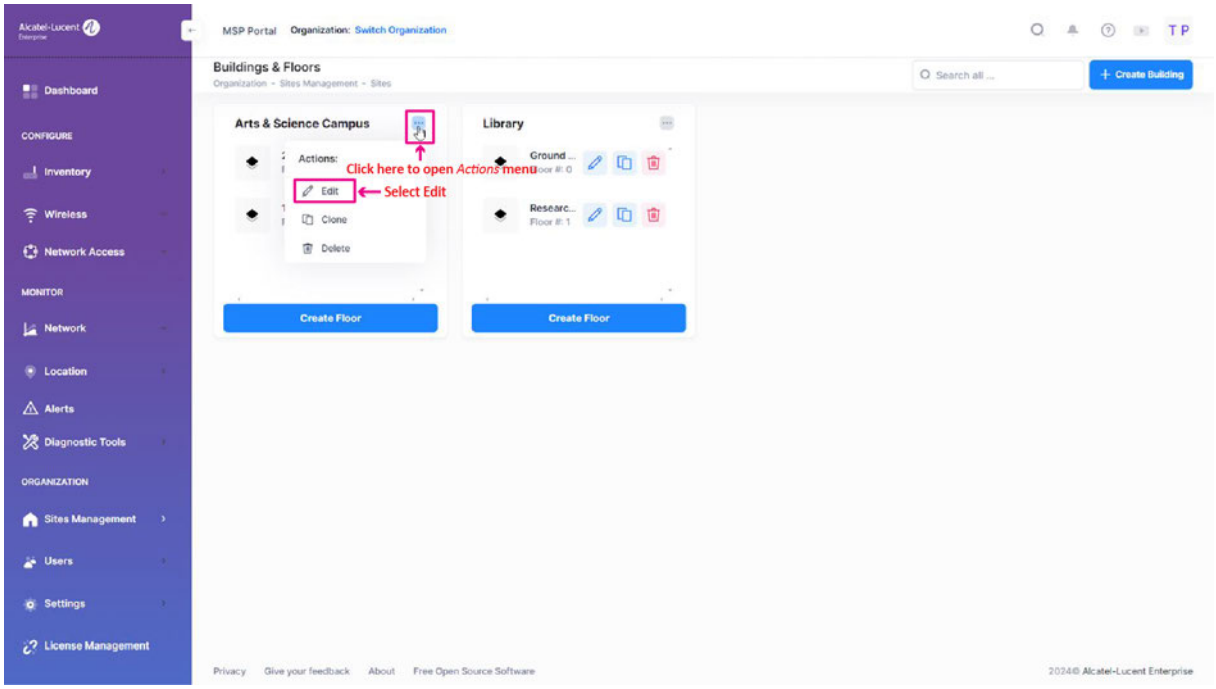


Enter the name you want to assign to the new building and click **Clone**. The new Building widget is displayed on the left side of the Buildings & Floors screen.

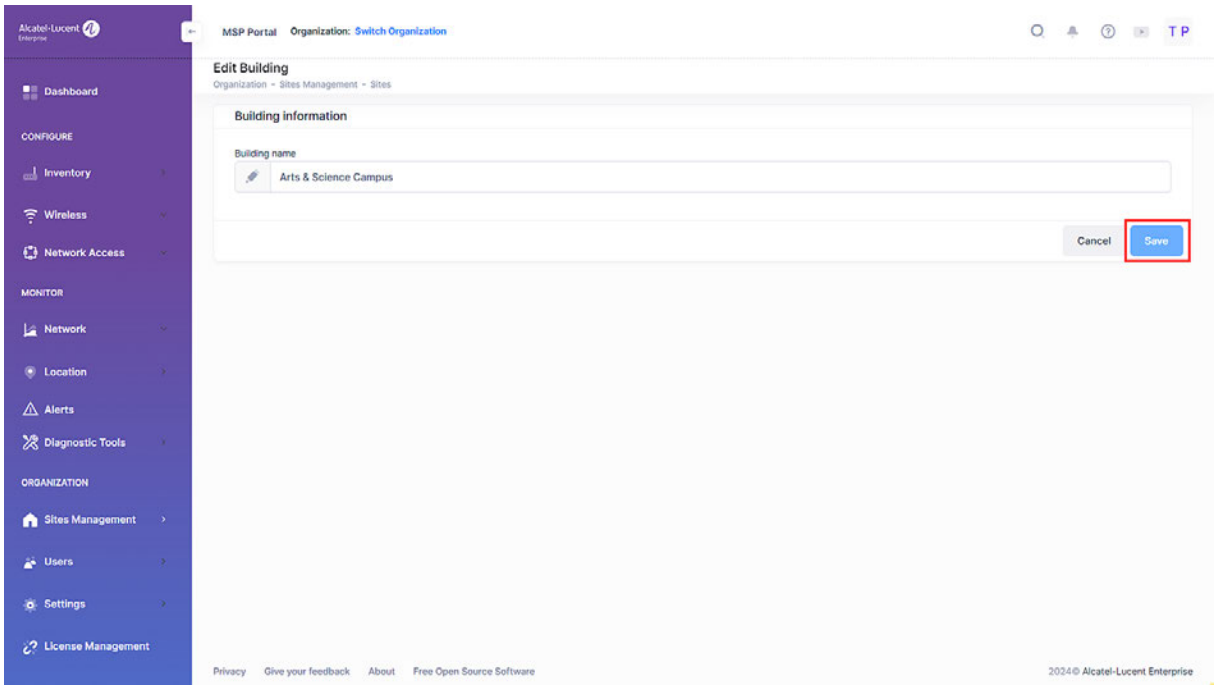
21 Oct 2025

3.3.3 Edit Building Settings

To edit an existing Building, click on the three dots option to open ***Actions*** menu and select **Edit** from the drop-down menu.



The Edit Building form opens.

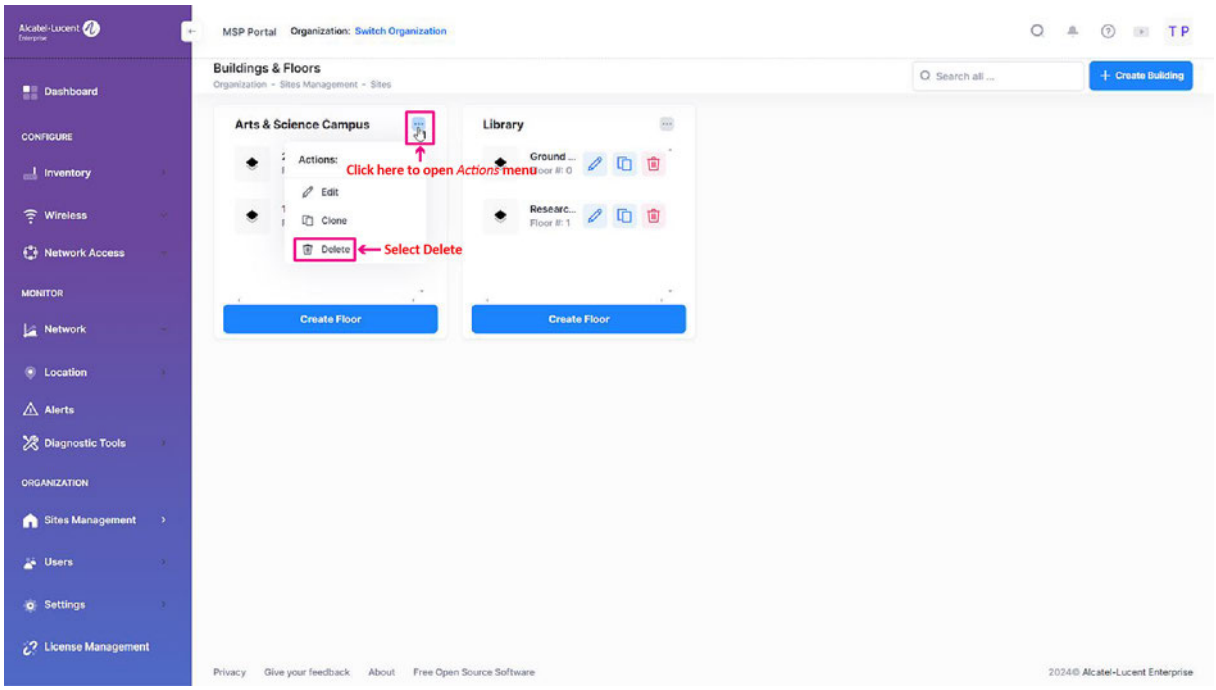


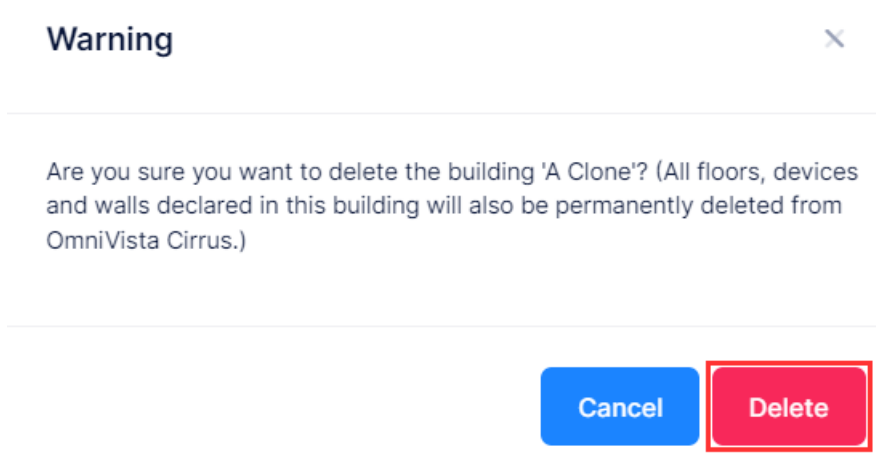
On the Edit Building form you can change the name associated with the Building Widget. Click on **Save** to save the changes and return to the Buildings & Floors screen.

21 Oct 2025

3.3.4 Delete a Building

To delete an existing Building, click on the three dots option to open ***Actions*** menu and select **Delete** from the drop-down menu. Click on **Delete** at the Confirmation Prompt. The Building Widget is removed from the list of buildings for the site.





5 **Delete Warning Prompt**

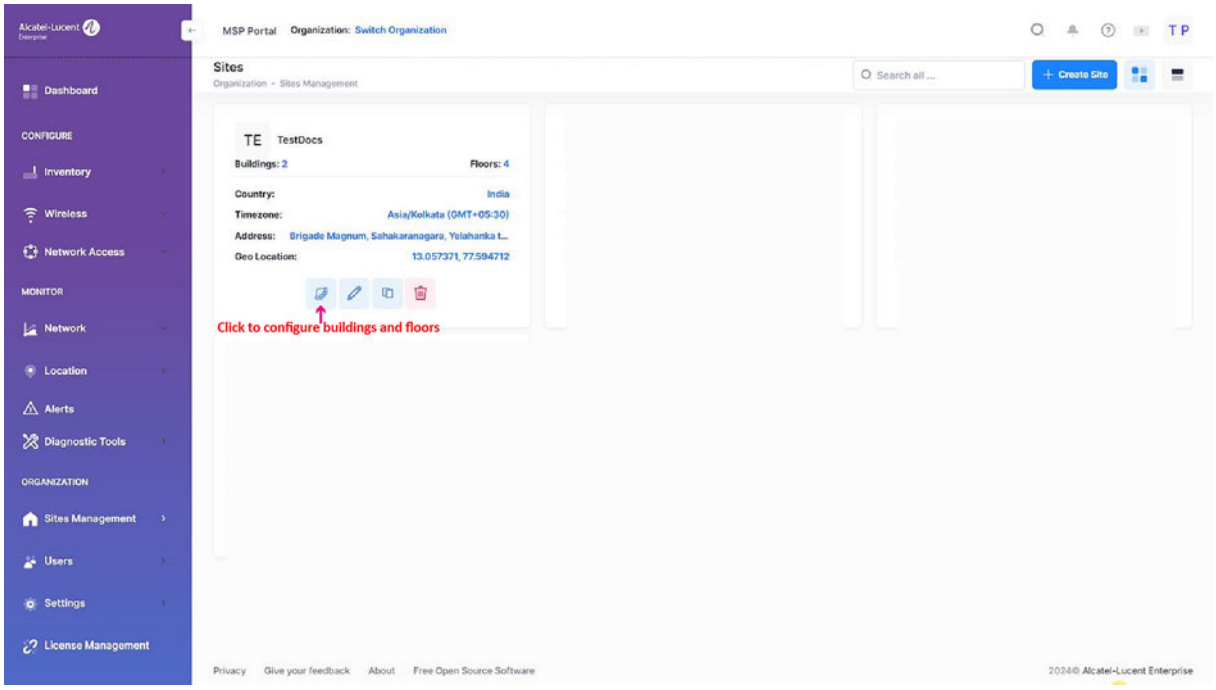
When you delete a Building, the associated floors, devices, and walls declared in the Building are also deleted.

21 Oct 2025

3.4 Configure and Manage a Floor (Floorplans)

After creating a Site for an Organization (see page 73), you can declare buildings (see page 83) and floors that exist within the Site. When an AP device is added to OmniVista for monitoring, the building and floor in which the device is located must be specified. Make sure Site buildings and floors have been defined before attempting to add a device to the Site.

On the Site Widget, click on **Configure Buildings & Floors** to open the Buildings & Floors screen.



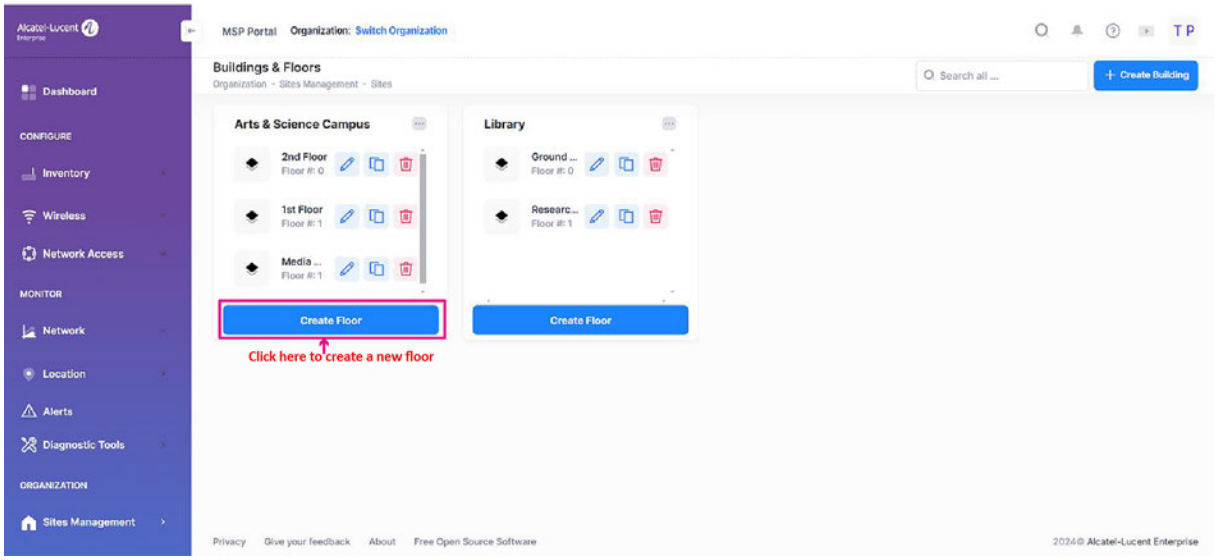
On the Buildings & Floors screen you can complete the following tasks to configure and manage floors:

- Create a Floor (see page 93)
- Clone a Floor (see page 96)
- Edit Floor Settings (see page 98)
- Delete a Floor (see page 100)

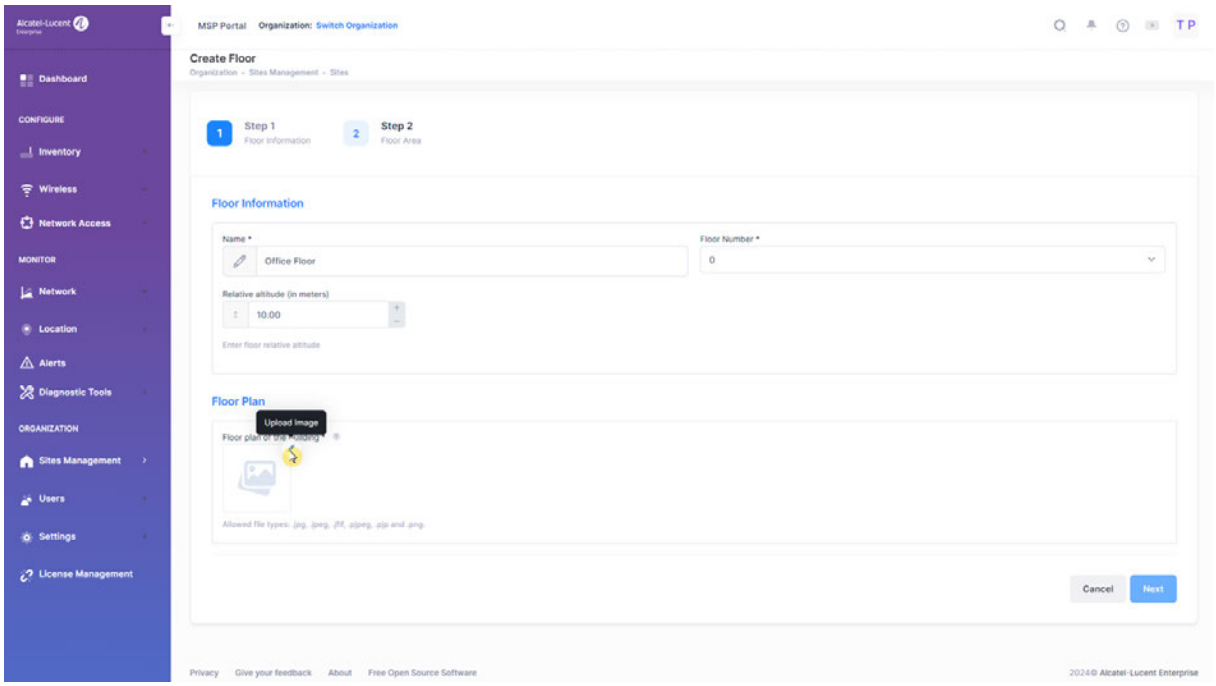
21 Oct 2025

3.4.1 Create a Floor

On the Buildings & Floor screen, click on **Create Floor** at the bottom of the Building Widget to declare a floor for that building.



This will bring up the Create Floor form.



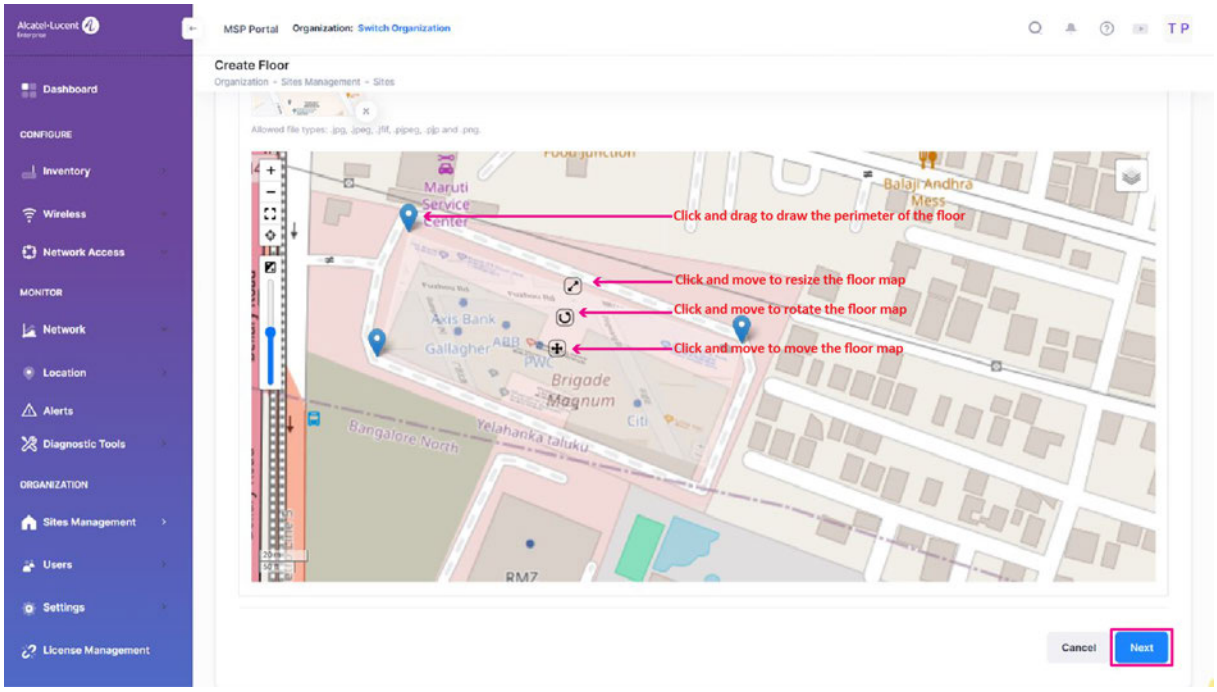
There are two parts to the Create Floor screen: Floor Information and Floor Area. Complete the required Floor Information fields as described below.

- **Name** - Enter a name to assign to the floor.
- **Floor Number** - Click on this field and select the number to assign to the floor.
- **Relative altitude** - Enter an altitude value in meters for the floor.

- **Floor Plan** - Click on this field to select an existing floor plan image file (jpg, jpeg, or png formats only).

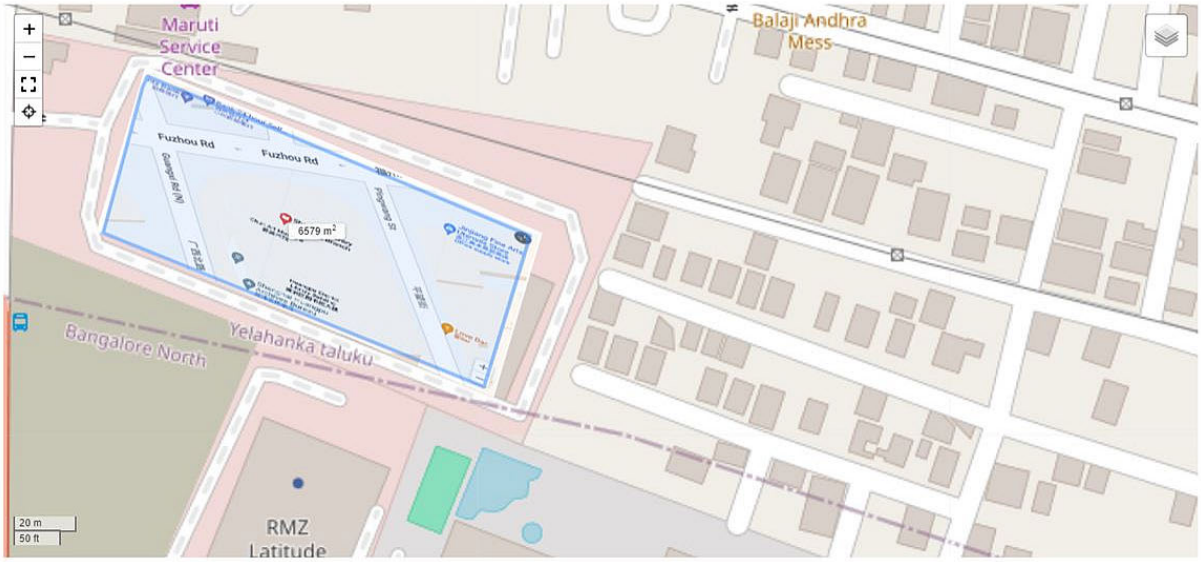
When you select a floor plan image, the image is displayed on the form and you are asked if you want to switch to full-screen mode. Click **Yes** or **No** to continue. The floor plan image is displayed over the building site map.

Upload floor pan and click on **Next**. Click on **Draw the floor perimeter** to create details for the floor.

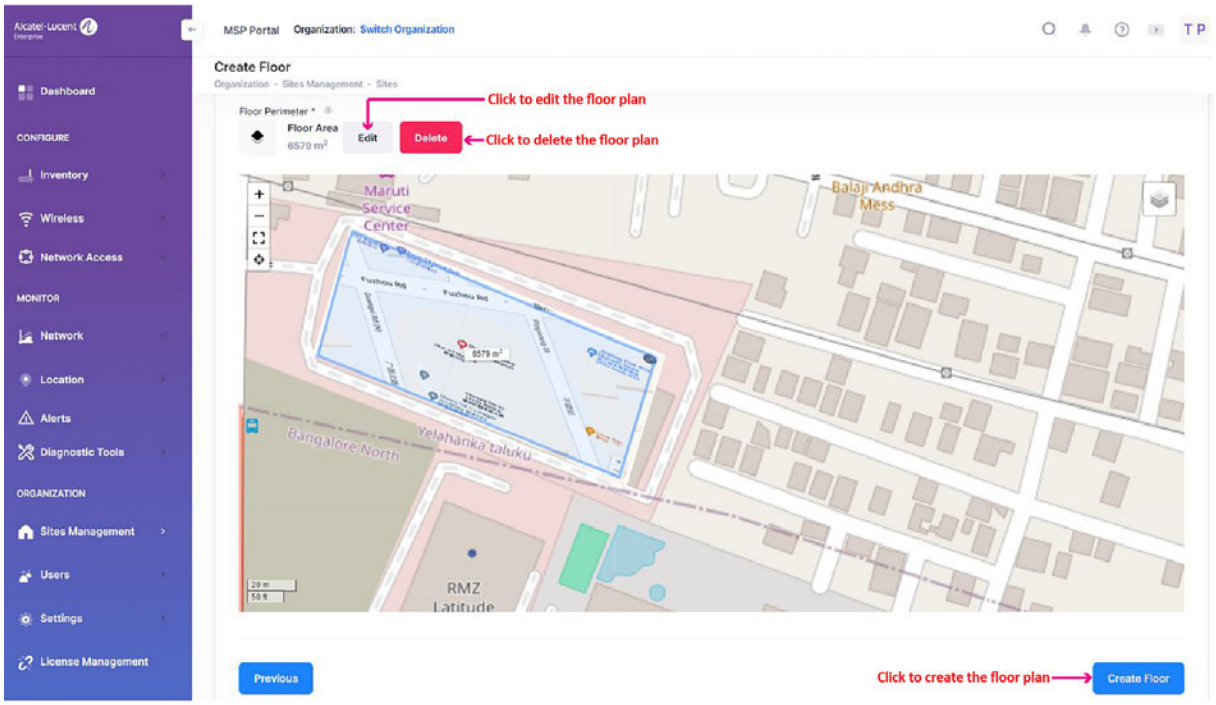


Use the three markers, as indicated on the building site map, to resize, rotate, or move the floor map to match the building footprint. Use the toolbar on the left-hand side to adjust floor map settings (such as the zoom level, enable/disable full-screen view, opacity of the floor map).

Once you have positioned the floor map to match the building site and adjusted any floor map settings, click on **Next**. The Floor Area screen is displayed (this is the second part of the Create Form screen).



Click on **Draw the floor perimeter**, then click on each corner of the floor plan to define the floor area. When you click on the last corner of the floor area, the area is defined with a solid border.



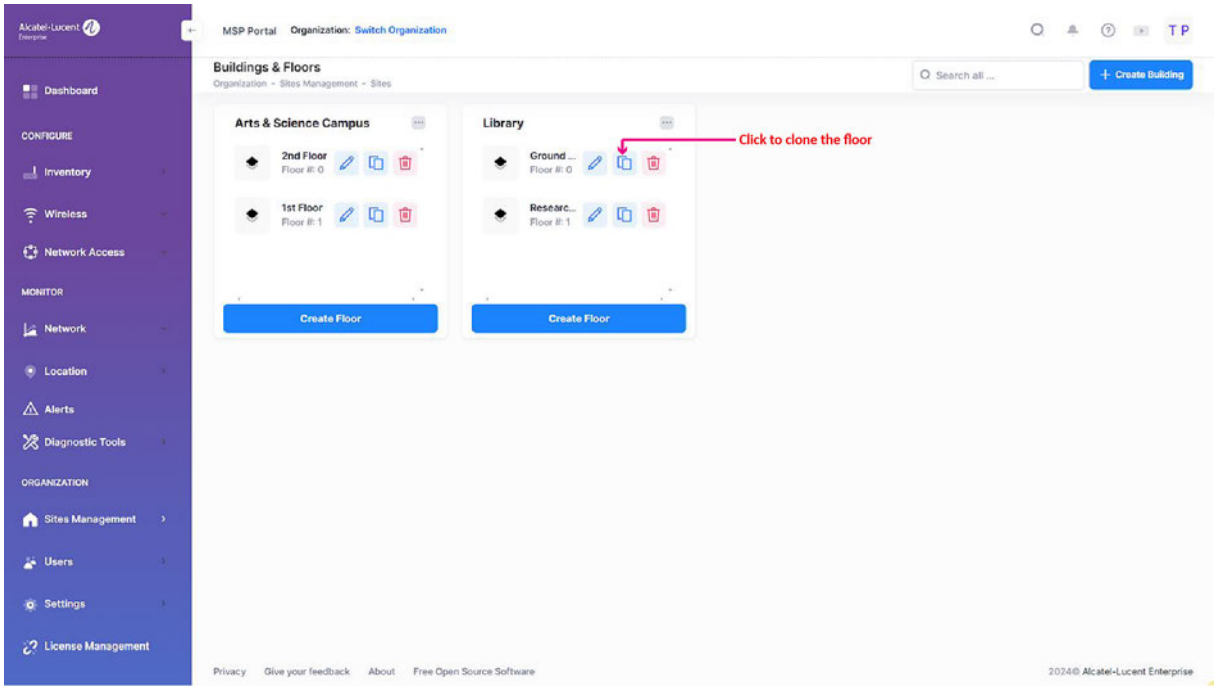
After you have defined the floor area, you can do one of the following:

- Click the **Edit** button to make changes to the floor perimeter.
- Click the **Delete** button to return to the previous Floor Area screen where you can define the floor perimeter again.
- Click the **Create Floor** button to accept the new floor information and area and add the floor to the site building. The new floor entry is displayed on the Building Widget.

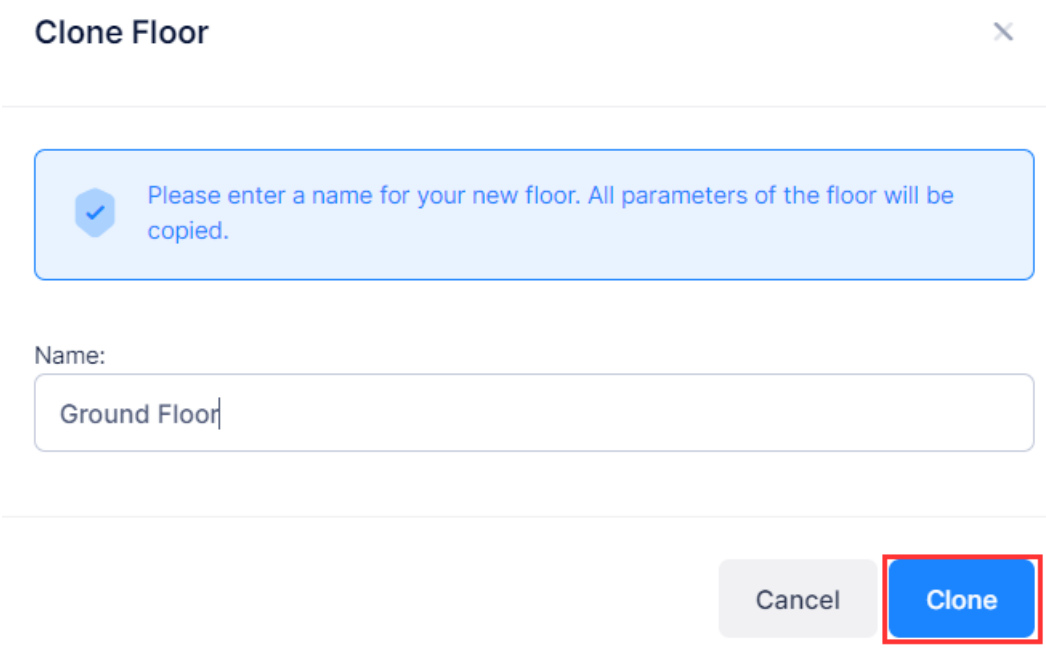
21 Oct 2025

3.4.2 Clone a Floor

You can clone an existing Floor and edit it to create a new Floor. To clone a floor, click the clone icon next to the floor name on the Building Widget.



When you click on the clone icon, the following Clone Floor prompt opens:



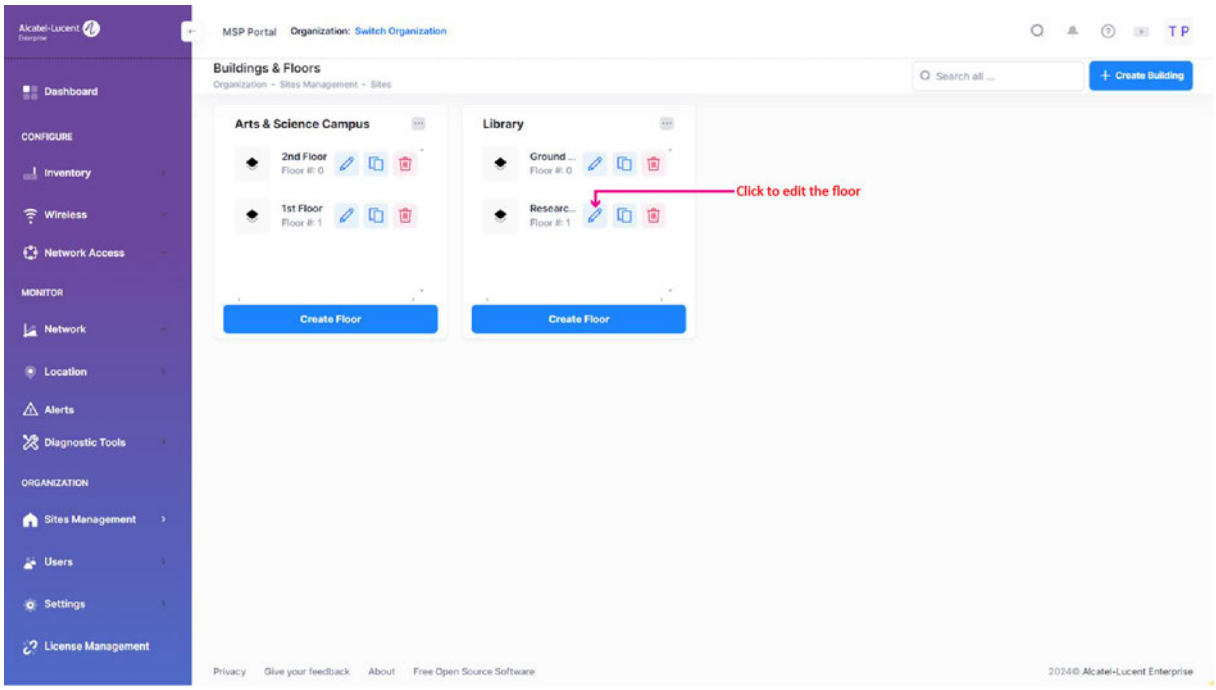
Enter the name you want to assign to the new floor and click on **Clone**. The Create Floor screen (see page 93) opens containing all the information copied from the Floor you were cloning. You can change

any of the Floor parameters and will need to specify the Floor number. Click on **Create Floor** when you are done. The cloned floor is added to the list of floors on the Building Widget.

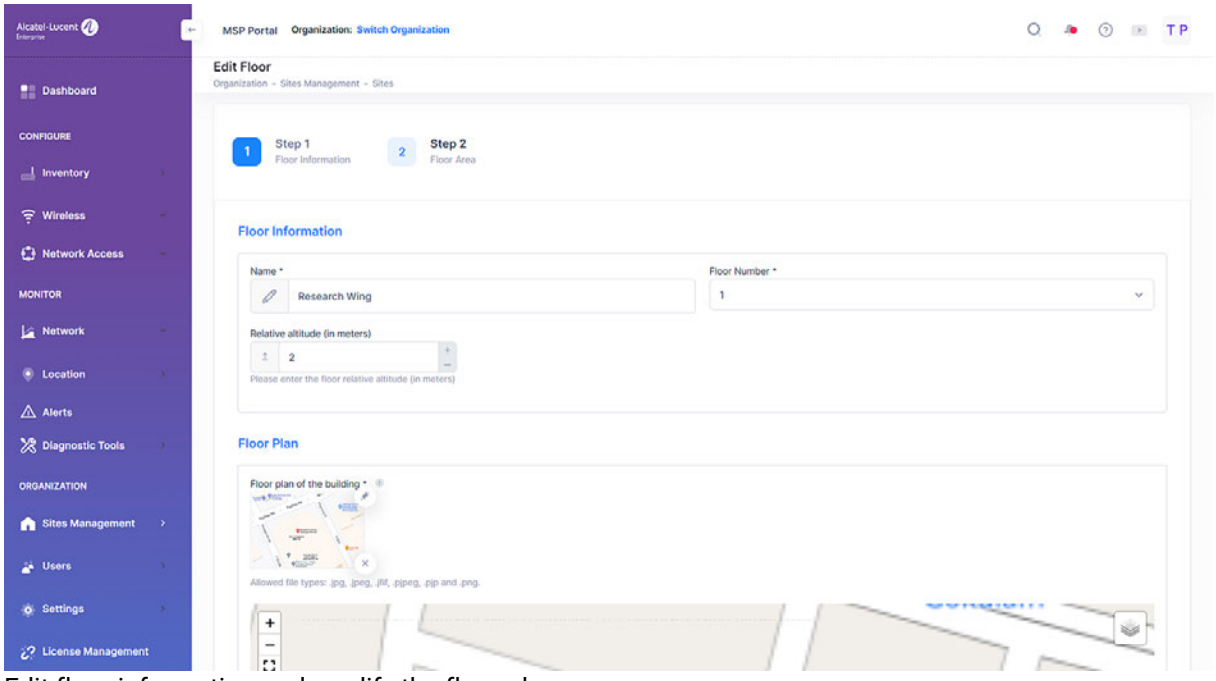
21 Oct 2025

3.4.3 Edit Floor Settings

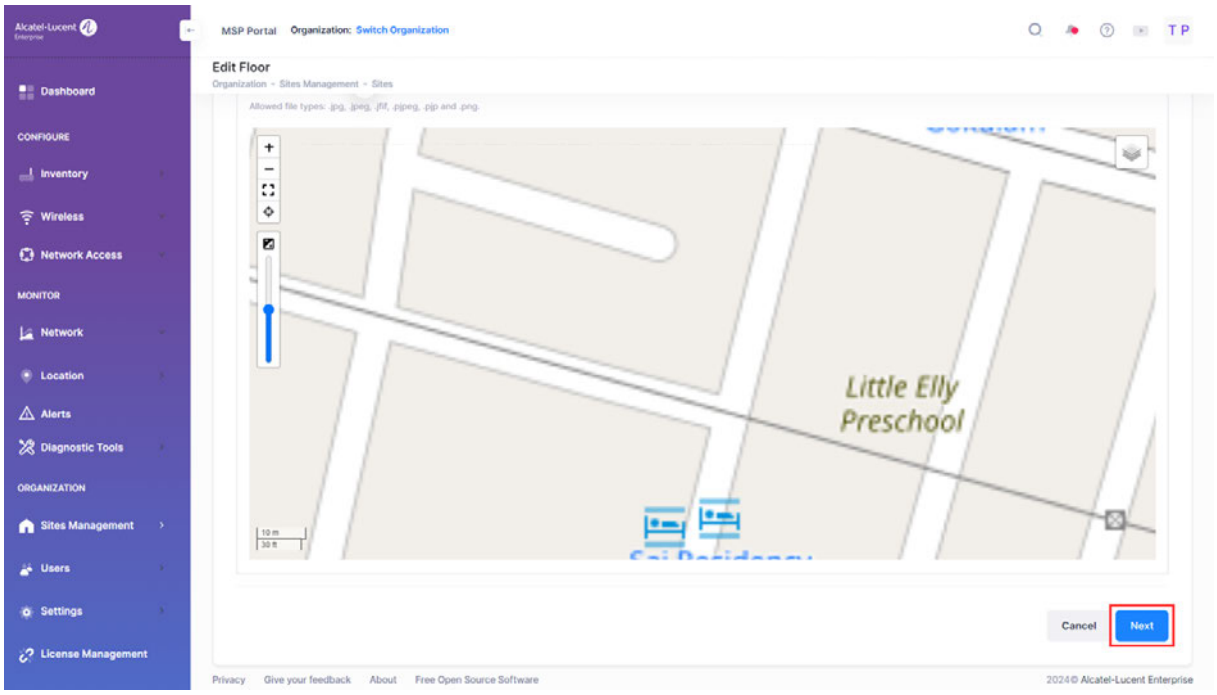
To edit a floor, click the edit icon next to the floor name on the Building Widget.



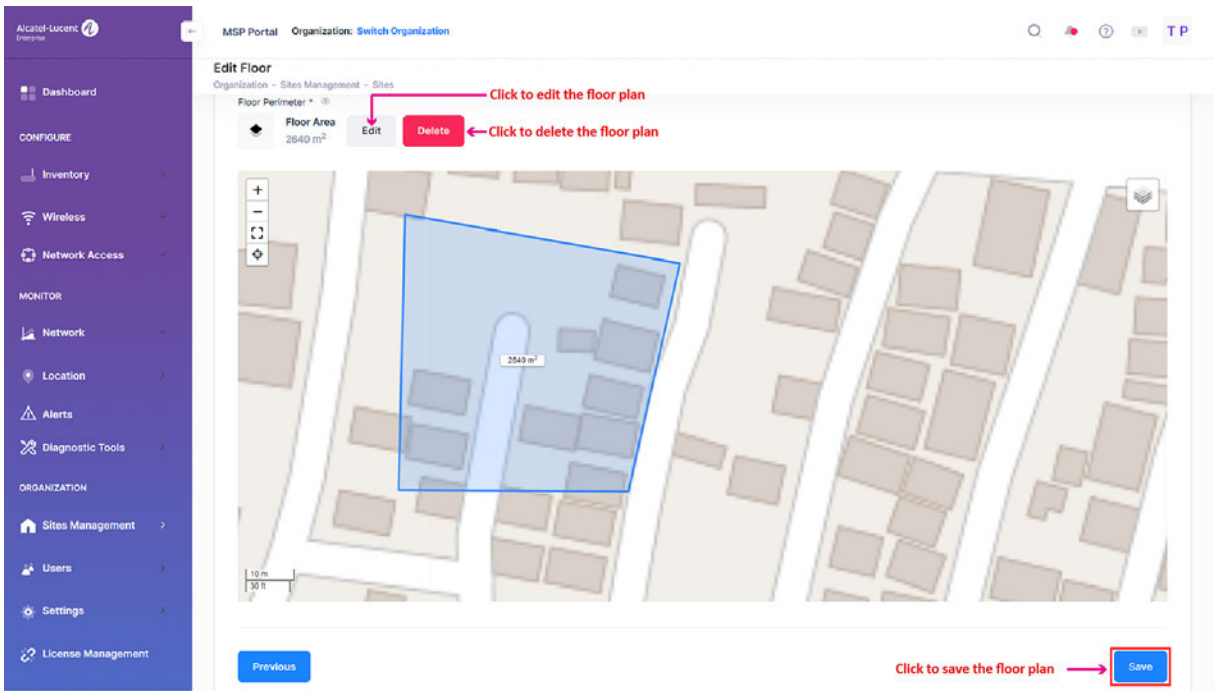
This will open the Edit Form page, where you can make changes to the Floor Information and the Floor Area.



Edit floor information and modify the floor plan.



After you have defined the floor area, you can do one of the following:

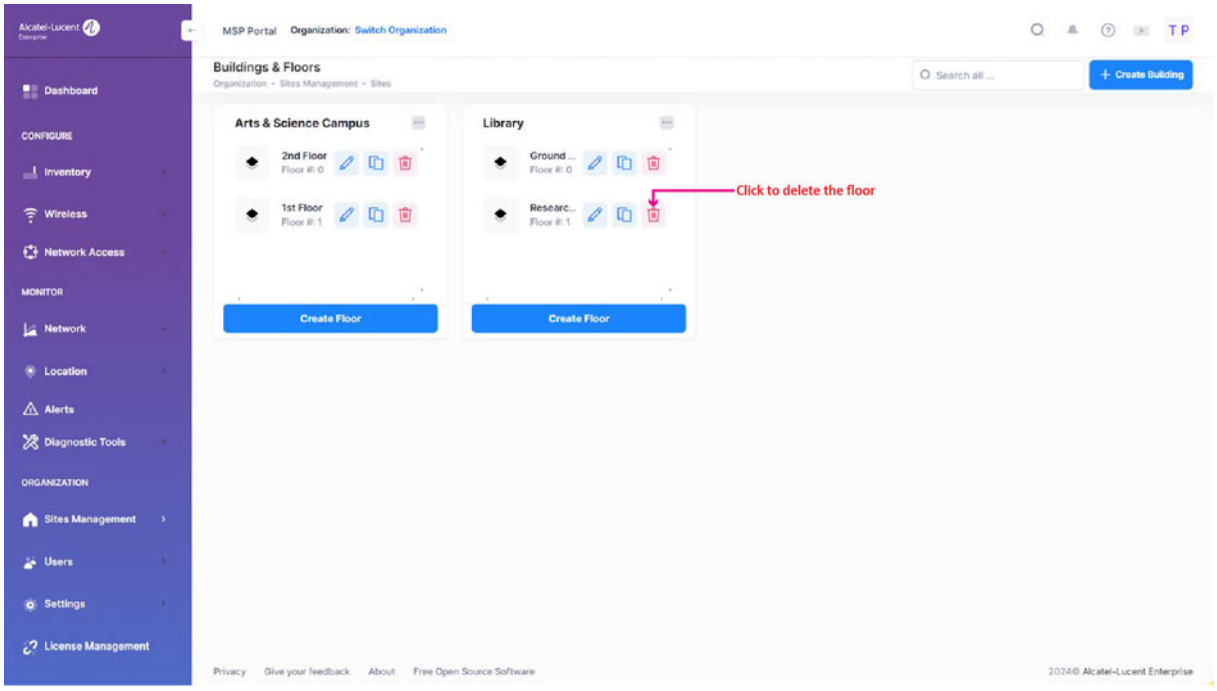


- Click the **Edit** button to make changes to the floor perimeter.
- Click the **Delete** button to return to the previous Floor Area screen where you can define the floor perimeter again.
- Click the **Save** button to accept the new floor information and area and add the floor to the site building. The new modified floor entry is displayed on the Building Widget.

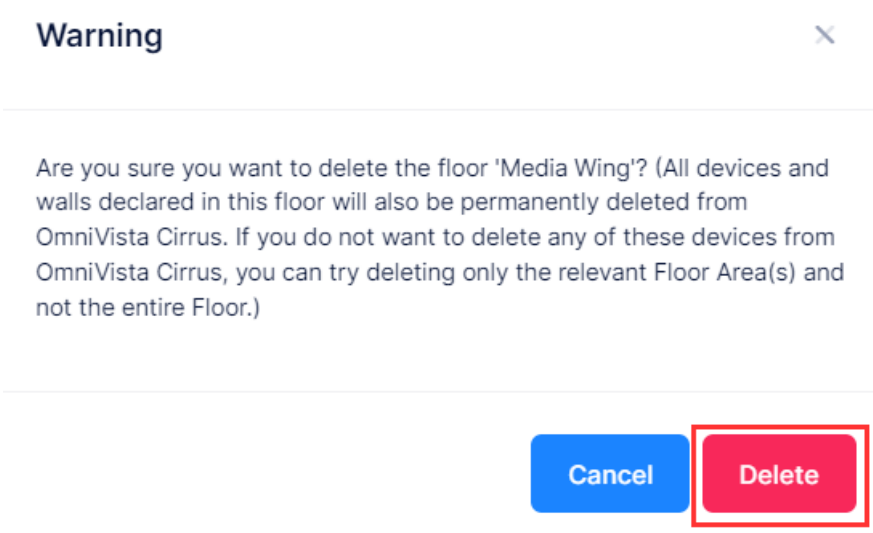
21 Oct 2025

3.4.4 Delete a Floor

To delete a floor, click the delete icon on the Building Widget. Click on **Delete** at the Confirmation Prompt. The Floor is removed from the list of floors on the Building Widget.



Buildings & Floors Screen



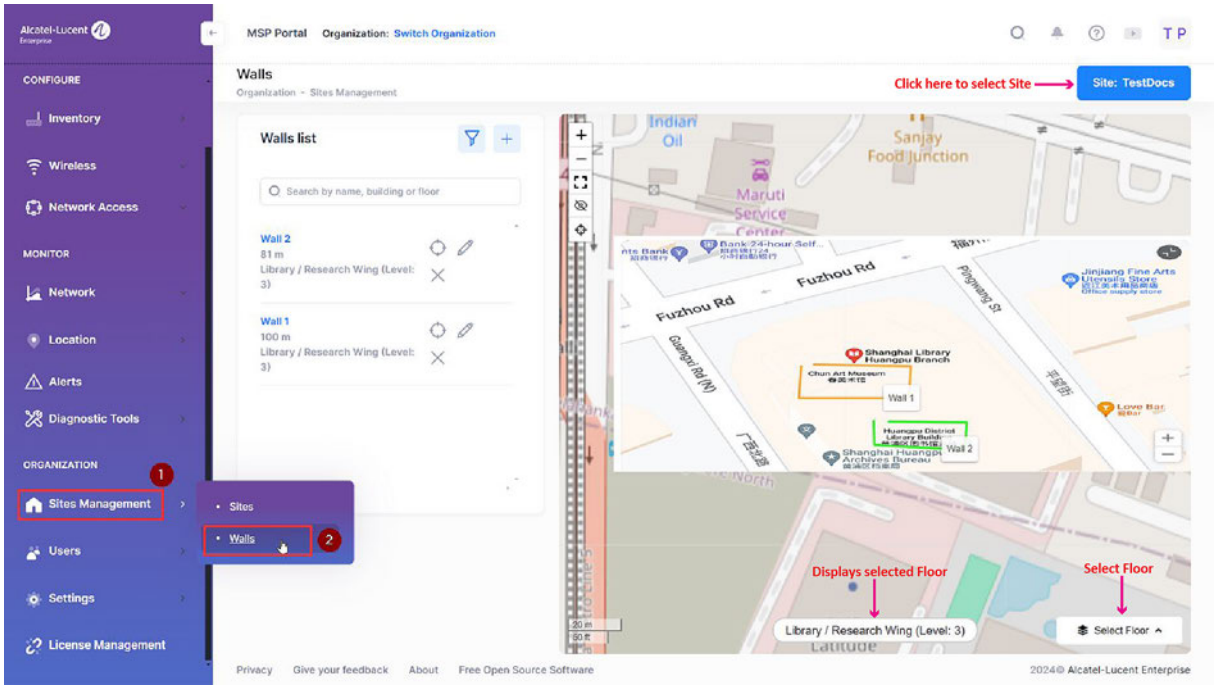
When you delete a Floor, the associated devices and walls declared on the Floor are also deleted.

21 Oct 2025

3.5 Configure and Manage Walls

After creating a Site for an Organization (see page 73), you may want to declare walls within the Site. In OmniVista Terra, walls are considered as environmental constraints that can attenuate Wi-Fi signals.

The Organization Dashboard (see page 71) is where organization sites can be created and managed. Click on **Sites Management** under the Organization section of the OmniVista Terra Menu (see page 45) and select the “Walls” from the cascading menu. The following Walls Definition screen is displayed:



The Walls Definition screen is composed of two panels:

- **The walls list panel** - Contains a list of walls defined for the selected site. Use the actions on this panel to create, edit, and delete walls.
- **The floorplan panel** - Displays the floorplan of the selected floor. This panel is also where a new wall is declared by drawing the wall on the floorplan.

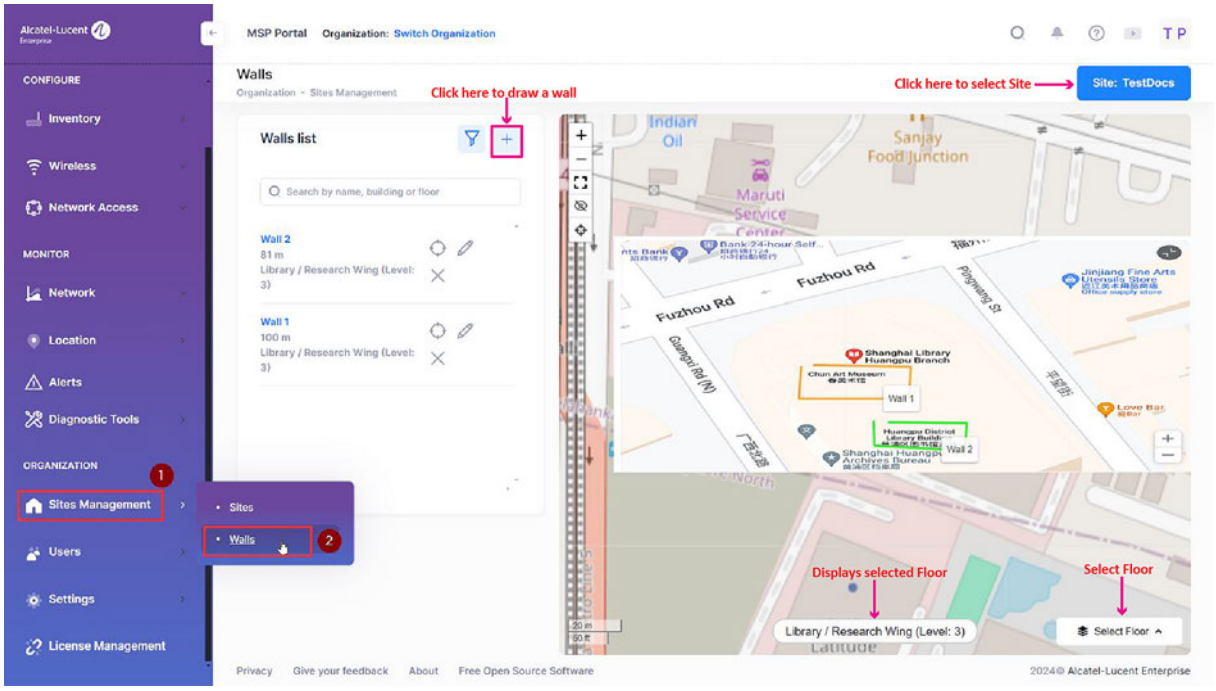
Use the Walls Definition screen to complete the following tasks:

- Draw a wall (see page 102)
- Edit a wall (see page 105)
- Delete a wall (see page 107)

21 Oct 2025

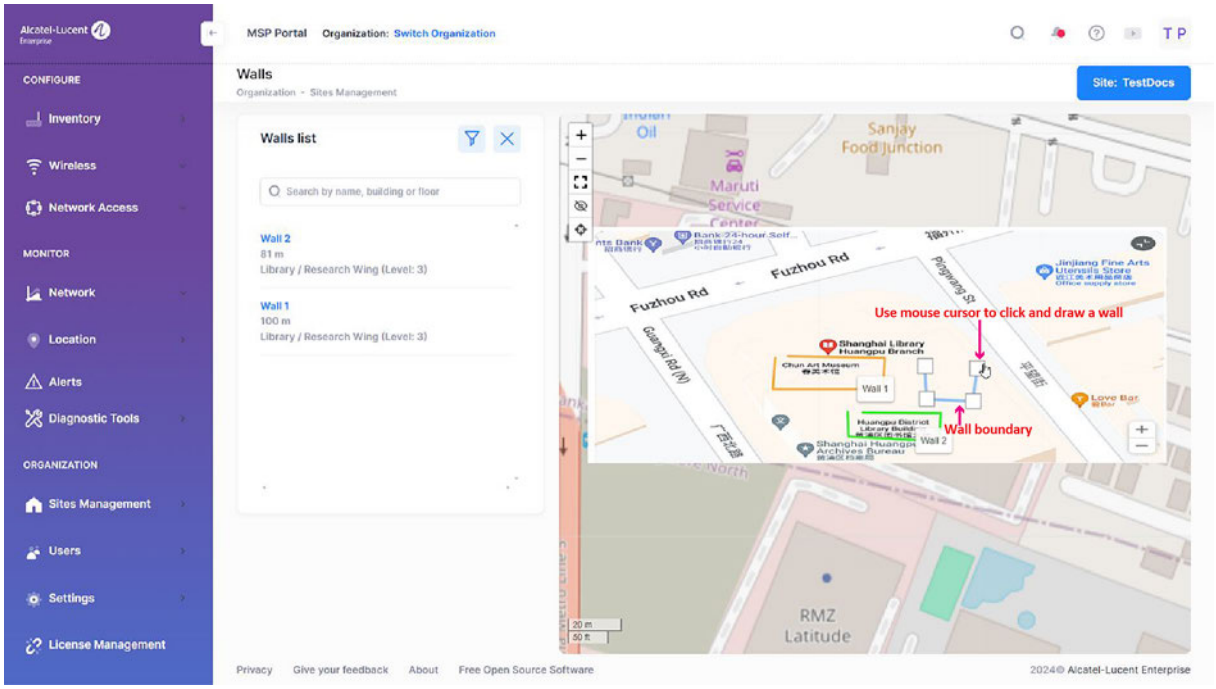
3.5.1 Draw a Wall

The Walls Definition screen (see page 101) is where new walls are declared by drawing the wall on the selected floor.



To draw a wall, click on "**+**" on the Walls list panel.

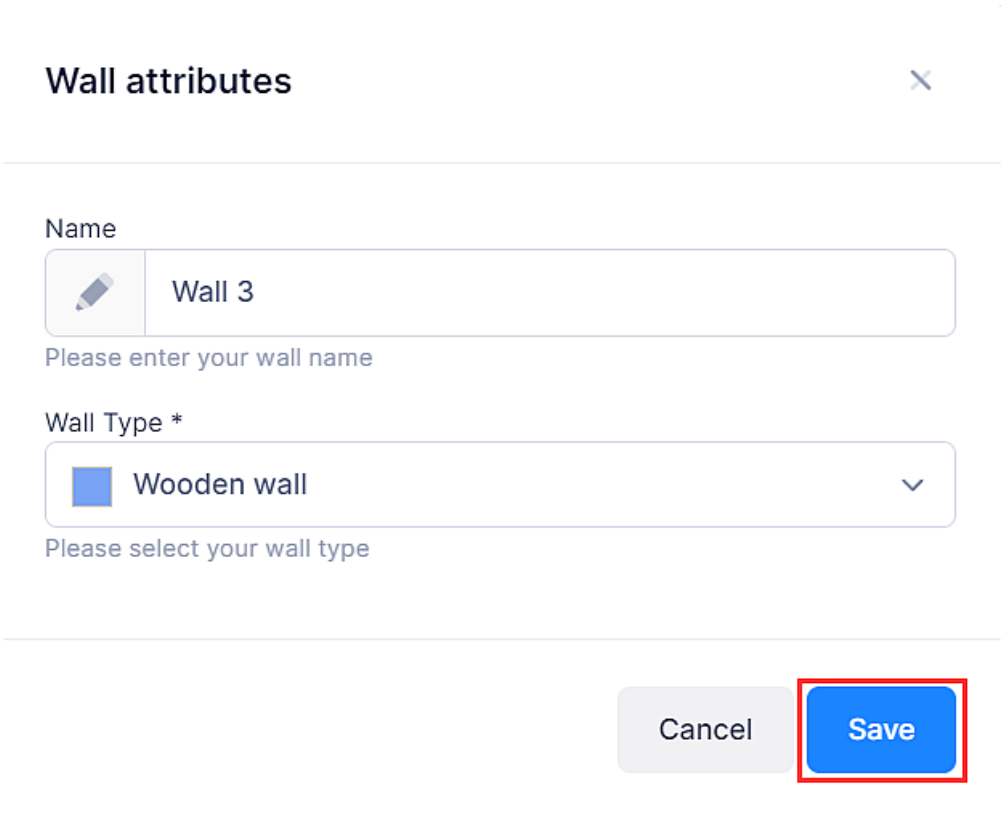
After you click on "**+**", move your mouse to the floorplan on the right. You will see that **the pointer of the cursor has changed**. Simply click somewhere on the map to start drawing the wall.



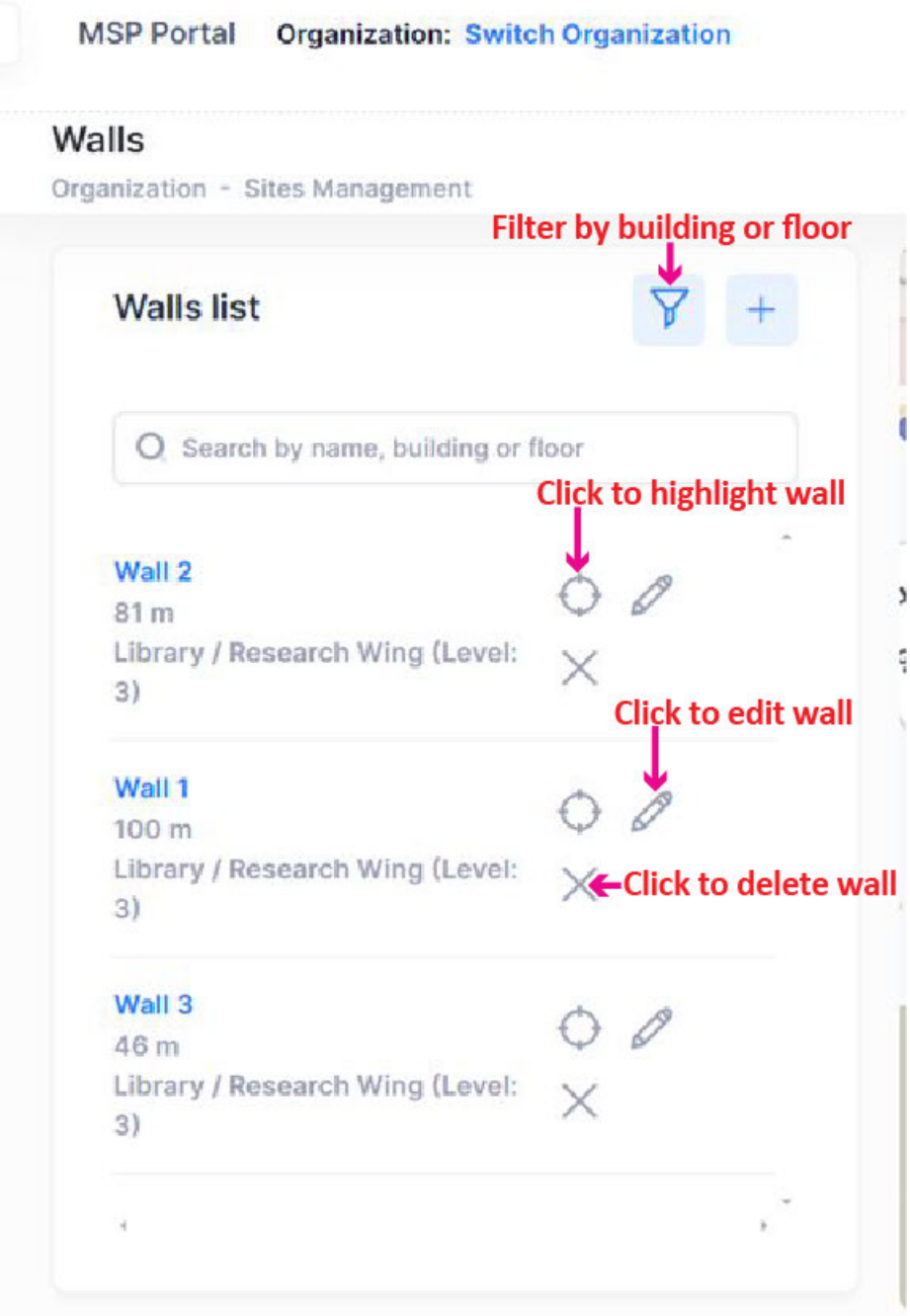
Continue to draw your wall by clicking along the wall on the floorplan. When finished, click a second time on the last point to terminate the drawing:

The Wall attributes modal is automatically displayed.

- **Name** - The wall name (a default name is shown, but is configurable).
- **Wall Type** - The type of the wall. Select the wall type from a list of types in the drop-down menu. There is a specific color could be assigned to a wall type.



After defining the wall attributes, click on **Save** to add the wall to the Walls list panel.



From the Walls list panel, **three actions** are available for each wall:

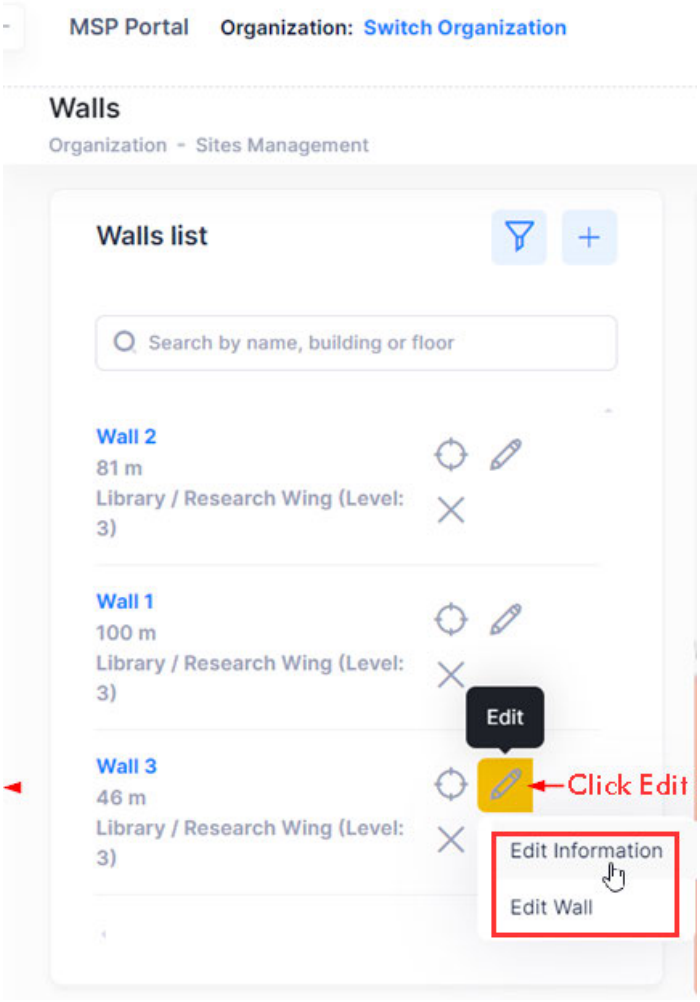
- **Highlight wall** - Click here to automatically locate this wall on the floorplan.
- **Edit wall** - Click here if you want to change the wall attributes or redraw the wall. More information on this page. (see page 105)
- **Delete wall** - Click here to delete the wall. More information on this page. (see page 107)

21 Oct 2025

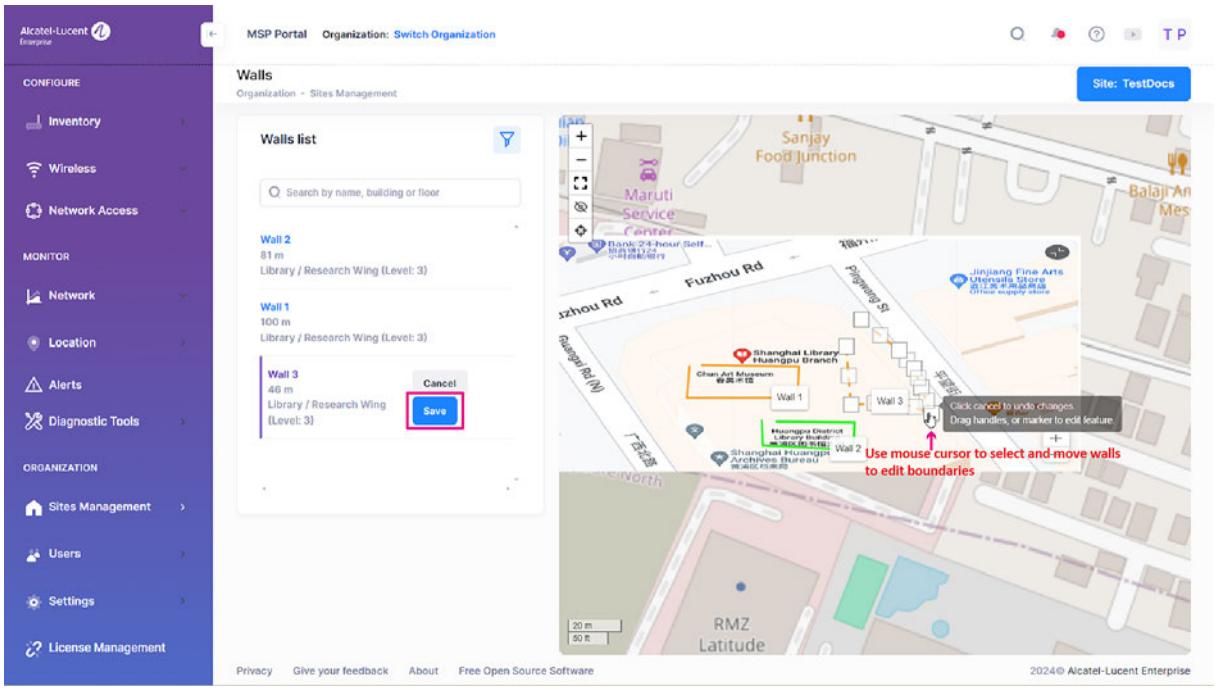
3.5.2 Edit a Wall

On the Walls Definition screen (see page 101), click on **Edit** next to the wall that you want to edit. The following two options are displayed:

- **Edit Information** - Click here to change any wall attribute, such as the wall name, the color, or the wall type.
- **Edit Wall** - Click here to redraw the geometry of the wall on the floorplan.



Select **Edit Wall** to edit the boundaries of the wall and wall attributes.

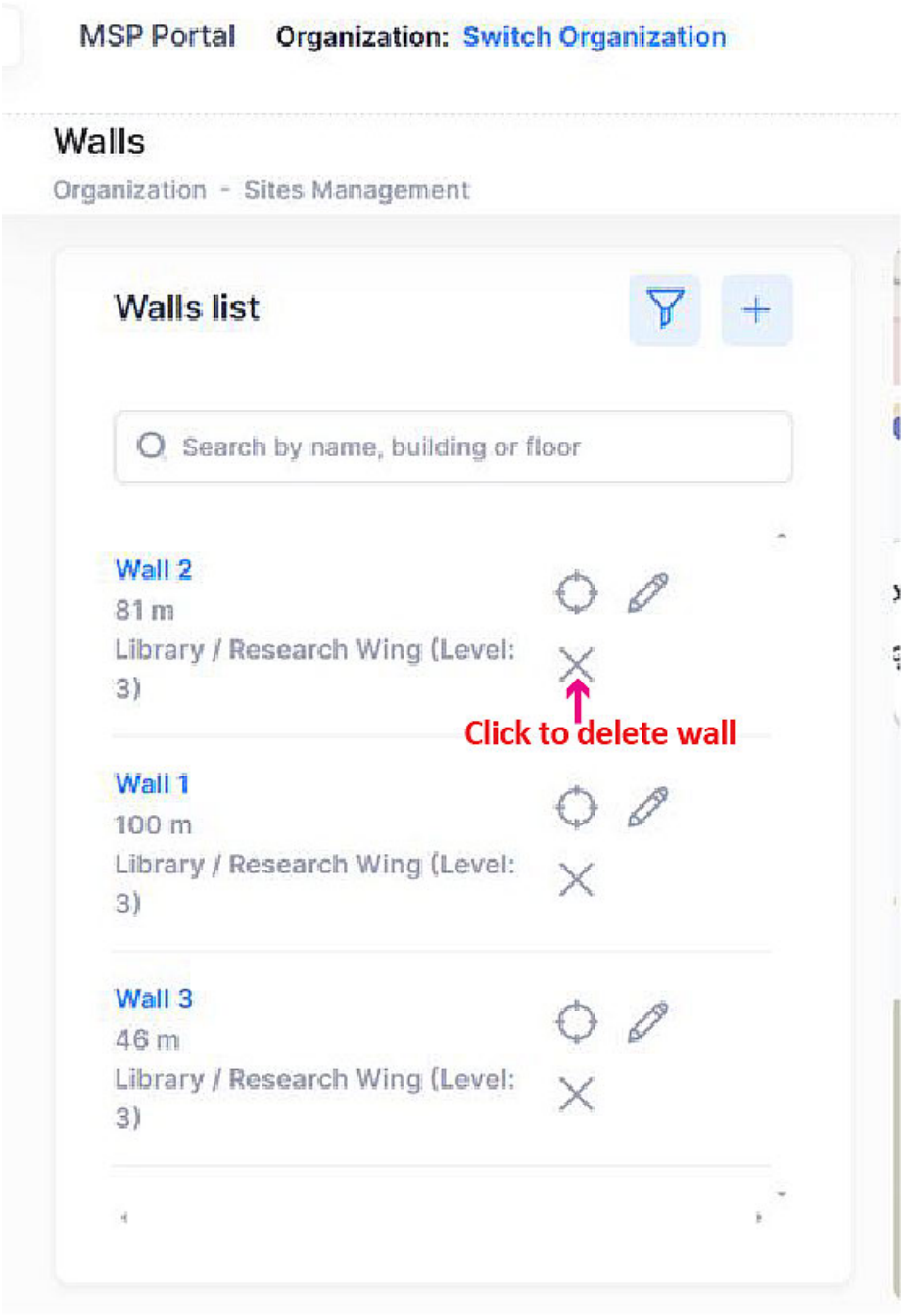


Click on **Save** to save the edited wall attributes.

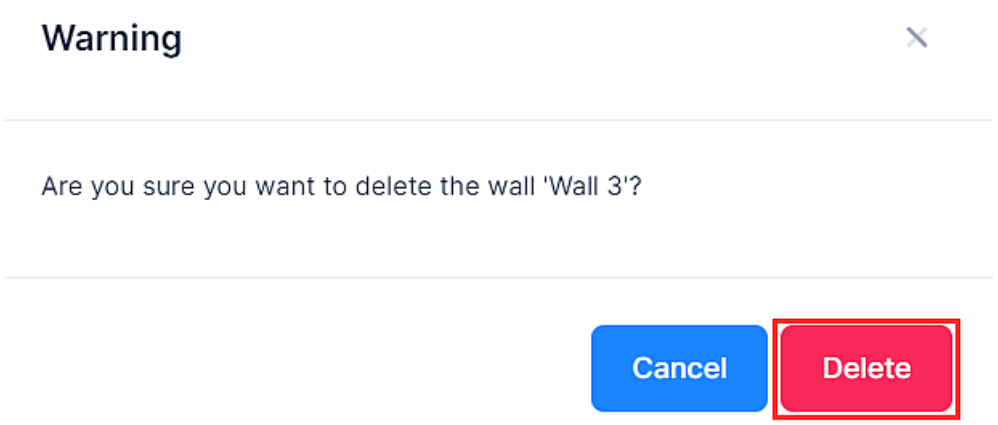
21 Oct 2025

3.5.3 Delete a Wall

To delete a wall, simply click on **delete** next to the wall that you want to remove from the floorplan. Click on **Delete** on the Confirmation Prompt. The wall is removed from the list of walls in the Walls list Widget.



6 **Walls List**



7 **Confirmation Prompt**

21 Oct 2025

3.6 Configure and Manage Users

The Users application on the Organization Dashboard (see page 71) is where user-access to the Organization is configured and managed. Access to OmniVista is controlled through the definition of user logins and passwords. To access the Users application, click on the Users option under the “Organization” section of the OmniVista Terra Menu (see page 45) (**Organization > Users**).

When you click on the Users option, the following lists of screens are provided to assist with configuring and managing user access to the Organization:

- User Accounts & Roles (see page 110) - Invite multiple users defined in an Excel (.xlxs) sheet or manually invite a single user to join the Organization.
- Login Attempts (see page 119) - Review a history of user login attempts to the Organization.
- Two-Factor Authentication (see page 120) - Enable/disable Two-Factor Authentication for user login.
- Audit Logs (see page 122) - Review a list of all actions performed by Organization users.

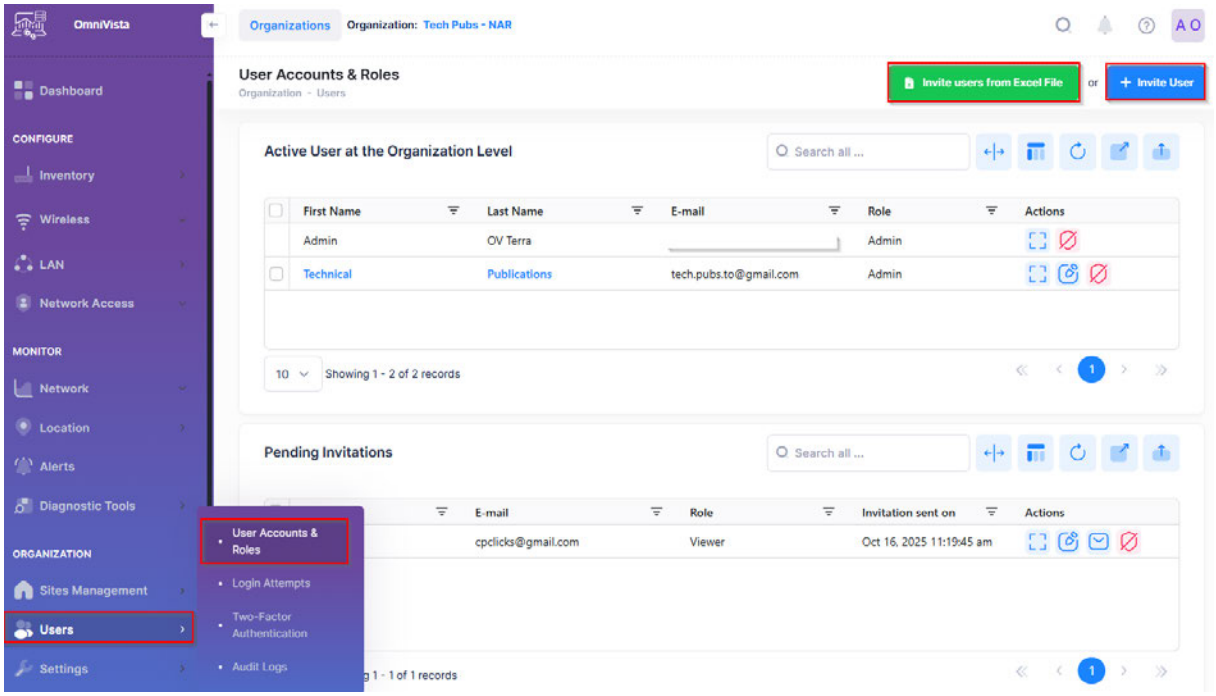
21 Oct 2025

3.6.1 User Accounts & Roles

The Accounts & Roles and Login Attempts options are used to complete the following tasks:

- Invite multiple users defined in an Excel (.xlxs) sheet. (see page 115) When the Excel sheet is imported into OmniVista Terra, each user identified in the sheet will receive an email invitation to join the Organization.
- Manually invite a single user to join the Organization (see page 117).
- Edit the User Role
- Revoke the Organization Access for Users (see page 111)
- Sign Out All Session for Users (see page 112)
- Display additional Account Information (see page 113)

When you click on the **User Accounts & Roles** option, the following list of active users is displayed:



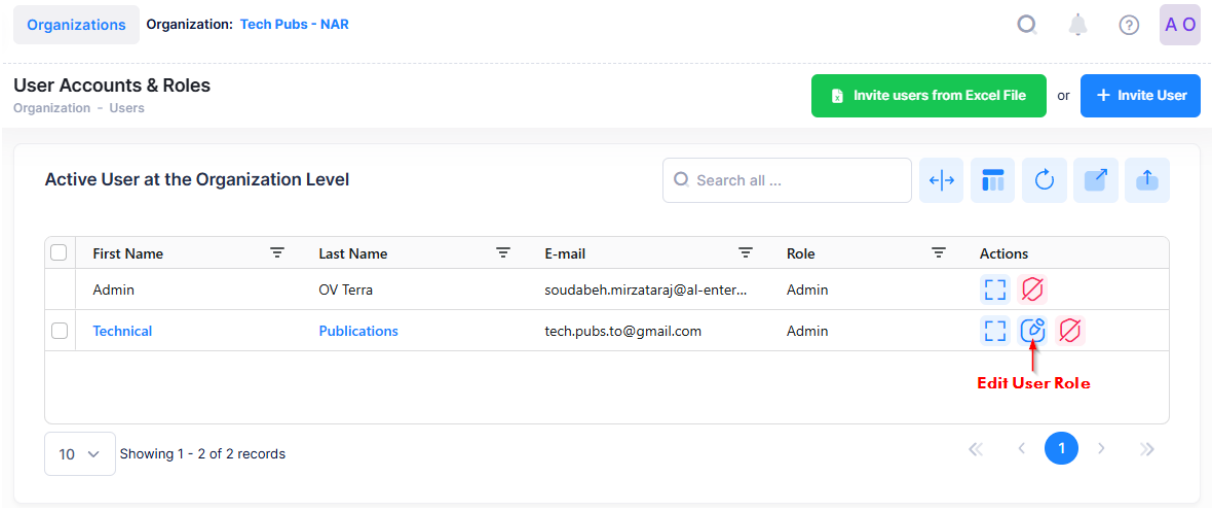
The User Accounts & Roles screen includes two sections:

- The **Active User in Organization level** section is where new users are invited to join the Organization and existing users are managed (for example, a users role is changed or user access is revoked).
- The **Pending Invitations** section displays a list of invitations that have been sent but not yet approved. You can edit or delete a pending invitation or resend another invitation email to the user.

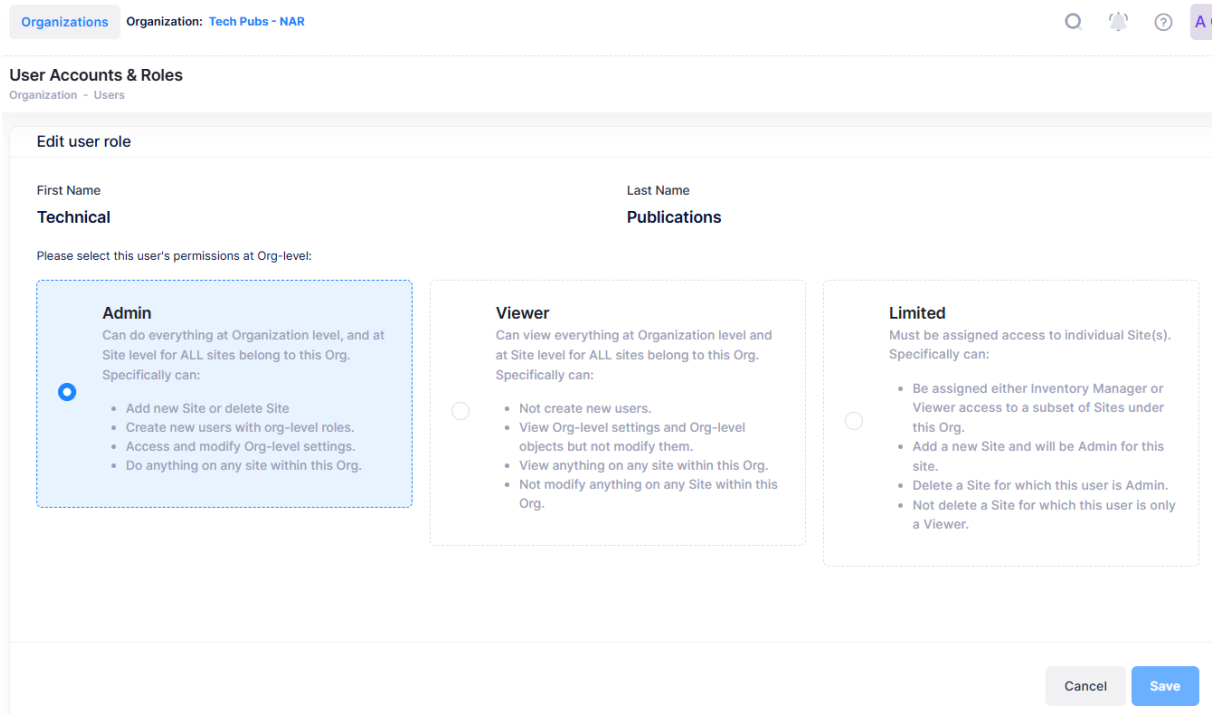
3.6.1.1 Edit the User Role

The Organization Admin User can edit the role of an existing user. For example, if the user was invited to the Organization with Admin privileges, you can change the Admin role to a Viewer or Limited role.

To edit the user role, click on the Edit icon under the “Action” column.



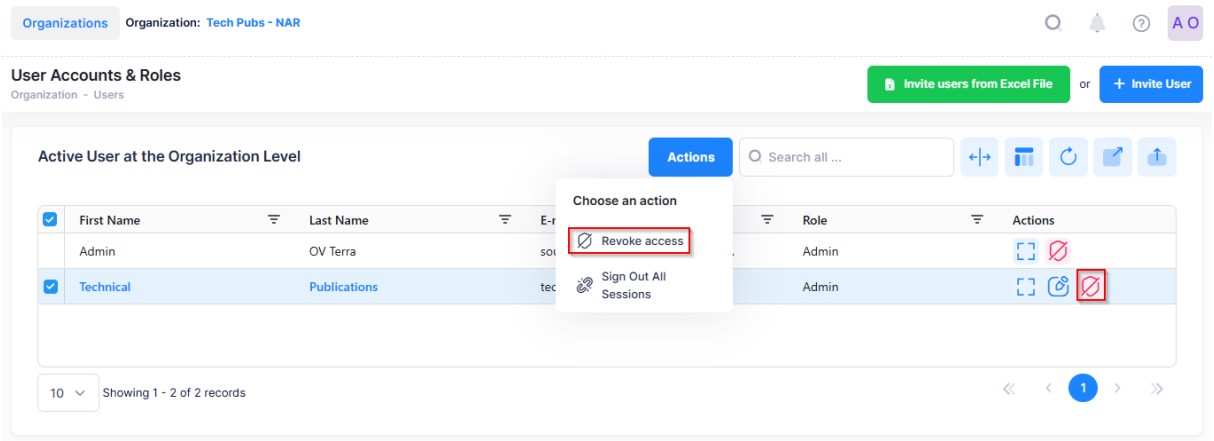
The Edit User Role screen appears.



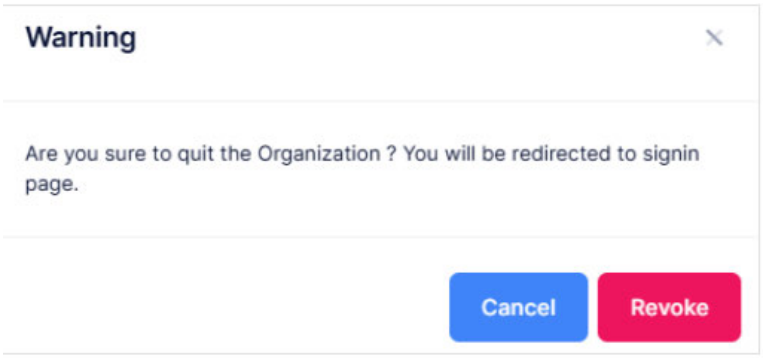
Select the user role (Admin, Viewer, or Limited) to change the level of access the user will have to the Organization. Click **Save** to apply the role change to the user.

3.6.1.2 Revoke the Organization Access for Users

The Organization Admin User can revoke access to their Organization. To perform this Action, select the User Name from the available list of active users, click on **Actions** and select **Revoke access** from the drop-down list. You can also click on the **Delete** button under “Actions” column to perform same operation as shown below:



The following confirmation prompt appears:

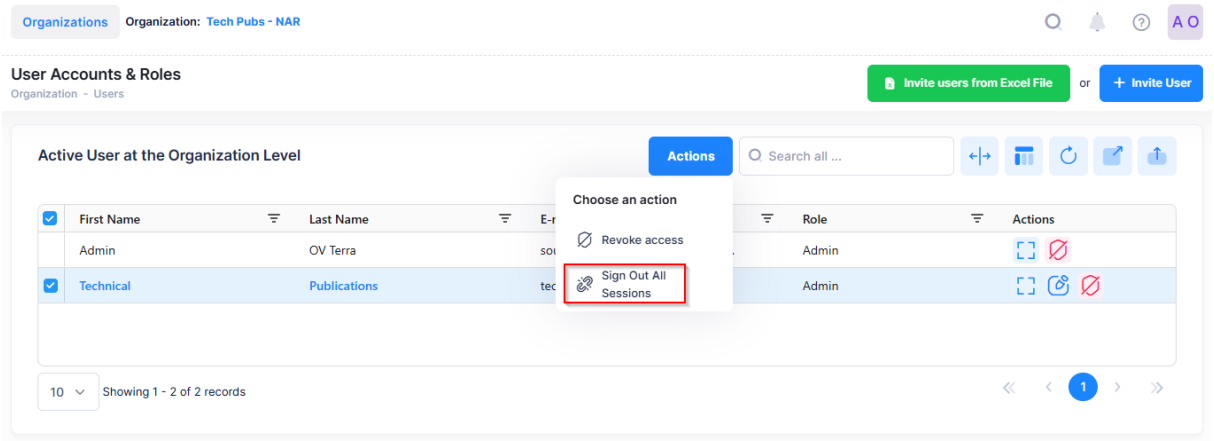


Click on **Revoke** to quit the Organization. The user's access to the Organization and sites is immediately revoked, preventing any viewing or interaction with these entities. The user will be signed out and redirected to the next login page.

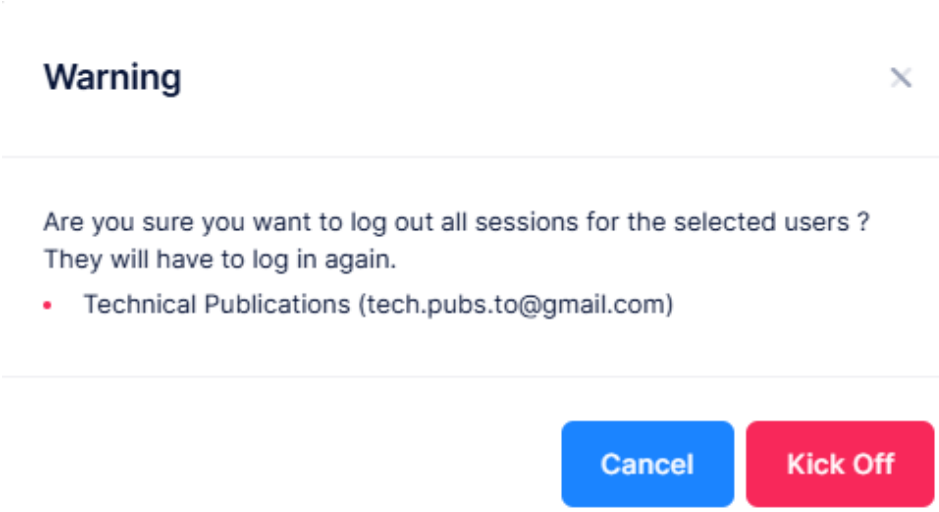
3.6.1.3 Sign Out All Sessions for Active Users

The Organization Admin User has option to sign out one or multiple users from all their active sessions, (if any). This ability enhances session management control at the Organizational level.

To perform this Action, select the User Name from the available list of active users and click on **Actions** as shown below:



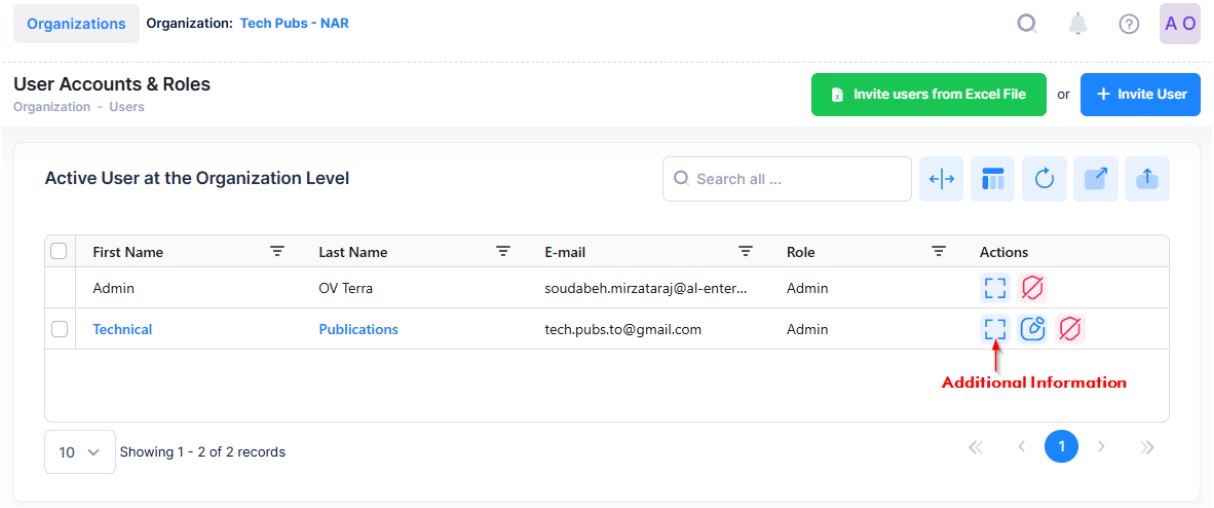
When you select the User Name for which you want to sign-out all active sessions, the following confirmation prompt appears:



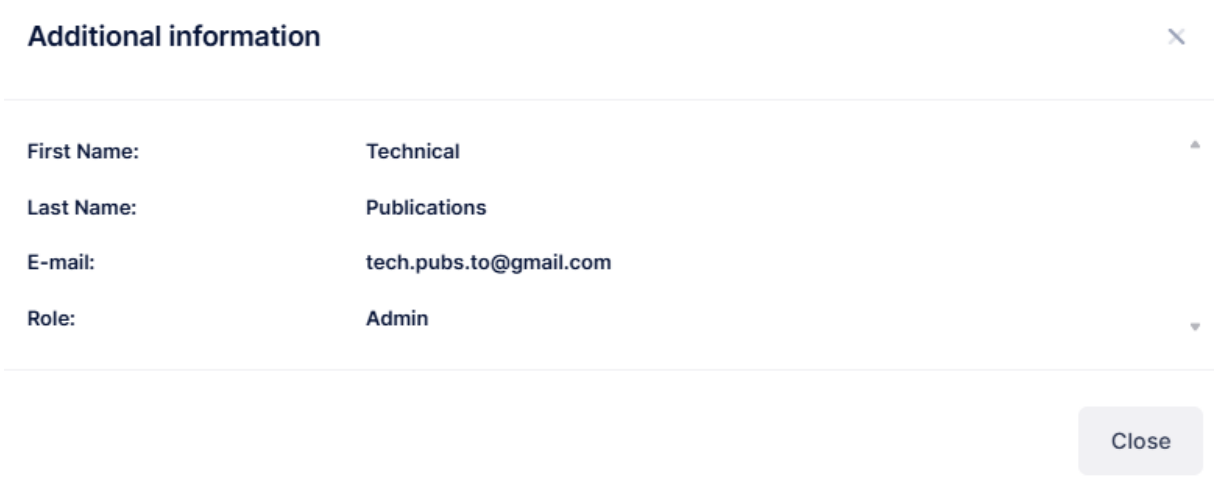
Click on **Kick Off** to confirm that you want to log out all sessions for the selected users.

3.6.1.4 Display additional Account Information for User

Select the User Name from the list and click on the Additional Information icon to view additional information for the selected User account.



The Additional Information screen appears:



The following information is displayed for the User Account:

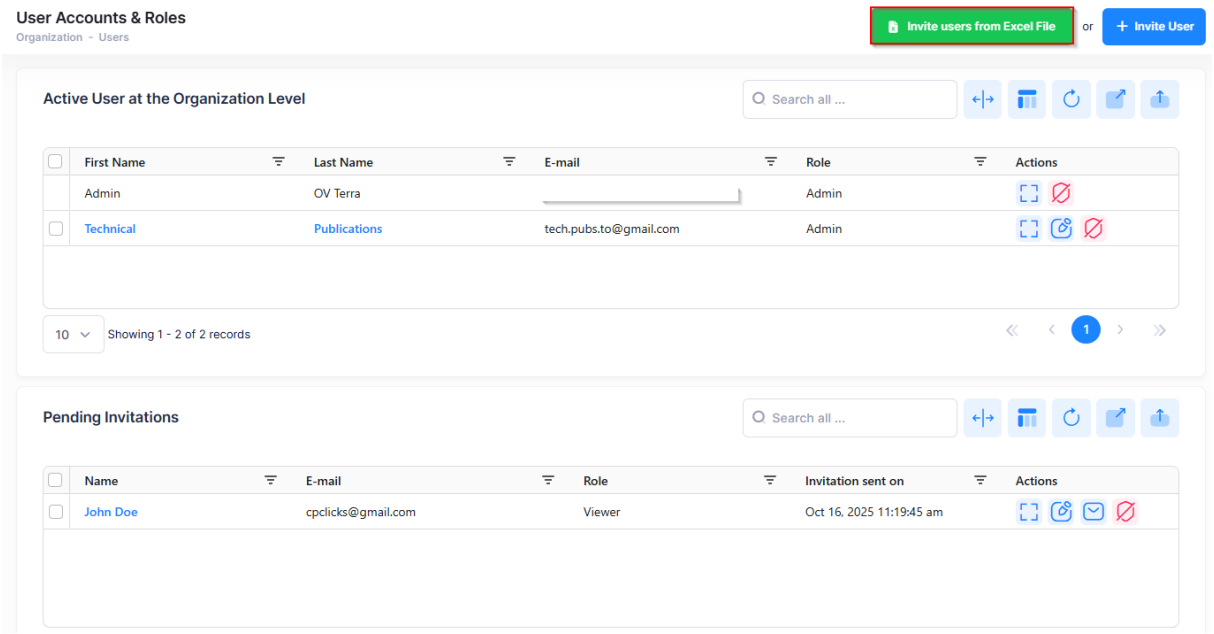
- **First Name** - First Name of the User.
- **Last Name** - Last Name of the User.
- **E-mail** - The E-mail ID associated with the User.
- **Role** - The role assigned to the user profile at the Organization level. (Admin/Viewer/Limited).

21 Oct 2025

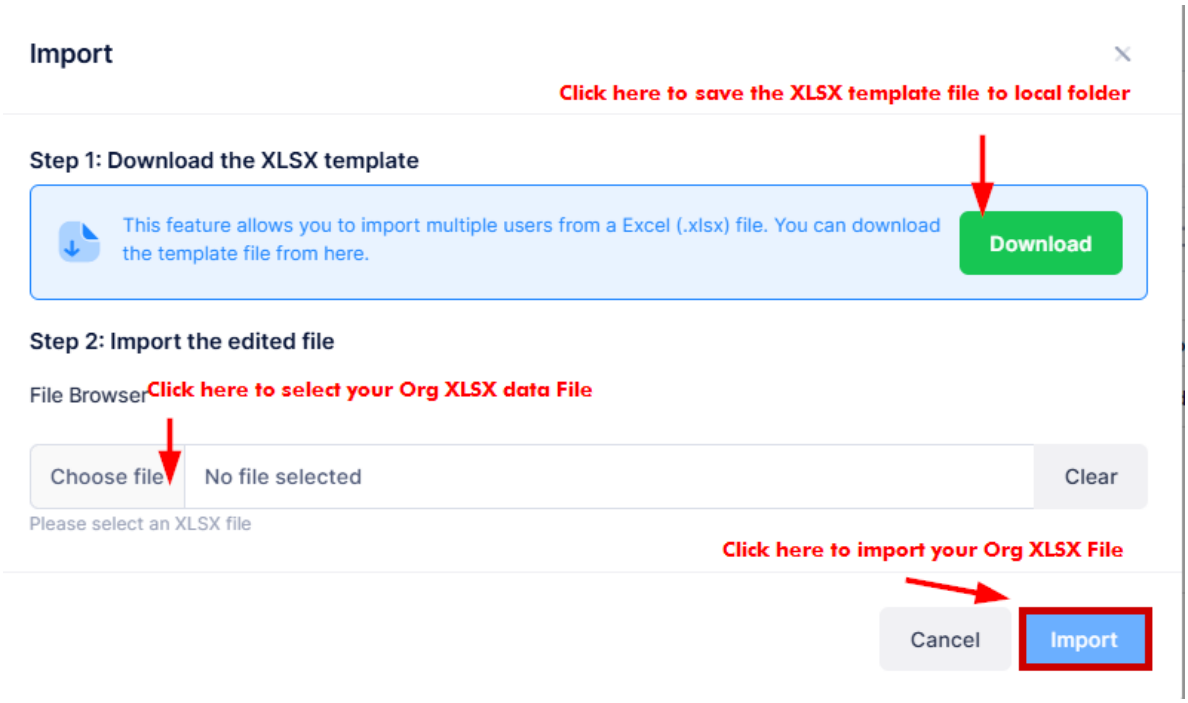
3.6.1.5 Invite Users from an Excel Sheet

The User Accounts & Roles screen displays a list of active users that are known to the organization. There are two methods for inviting a user to an organization: import multiple users from an Excel XLSX file or manually invite a single user (see page 117).

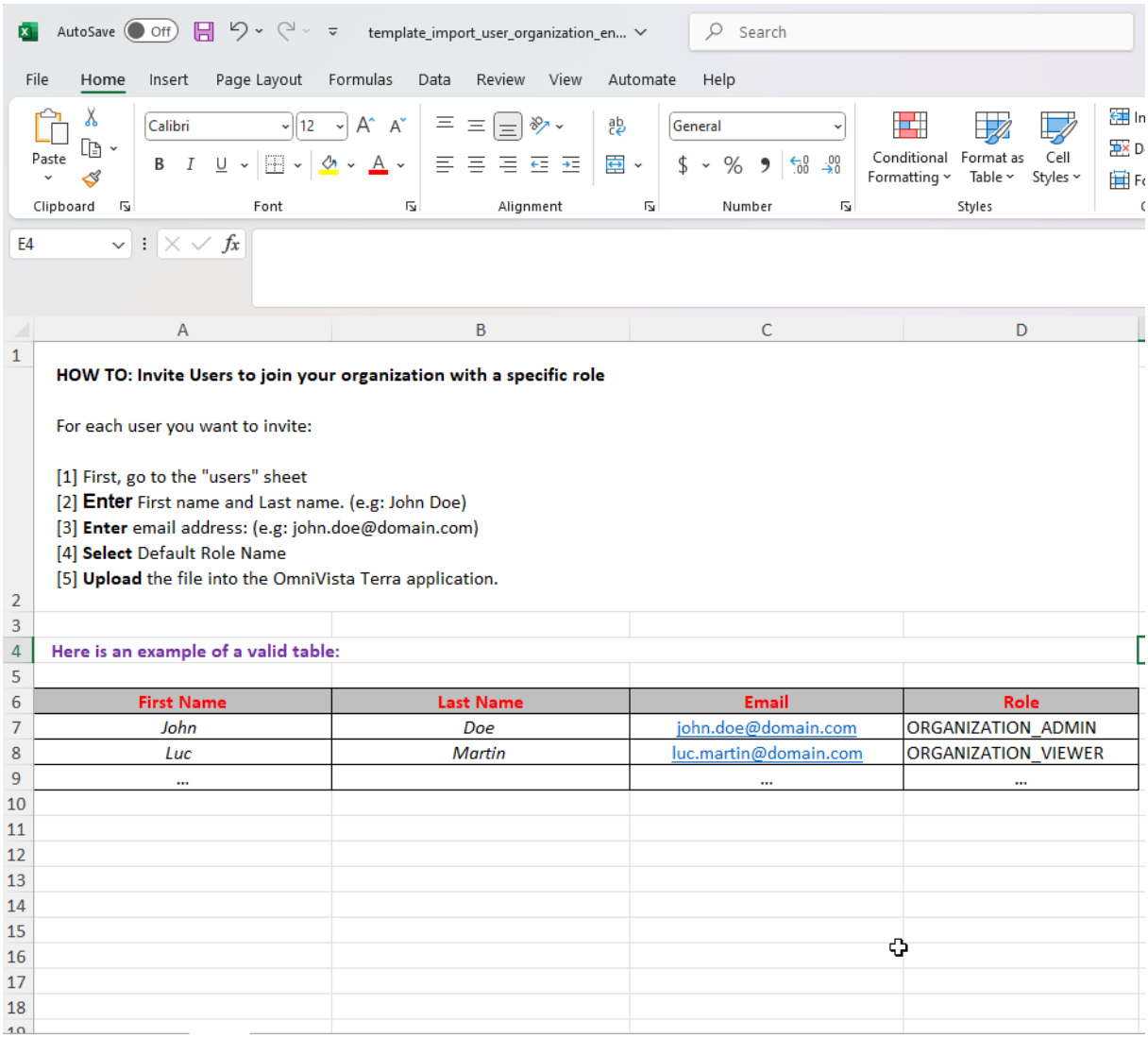
To import multiple users from an existing Excel sheet (.xlxs), click on **Invite users from Excel file** on the User Accounts & Roles screen. You will then be prompted to download an XLSX template file that contains instructions on how to configure the Excel sheet file with the necessary user information.



The following screen appears:



Click on **Download** and specify where you would like to save the template file. When you open the template file, instructions are provided about how to define the users to be invited.



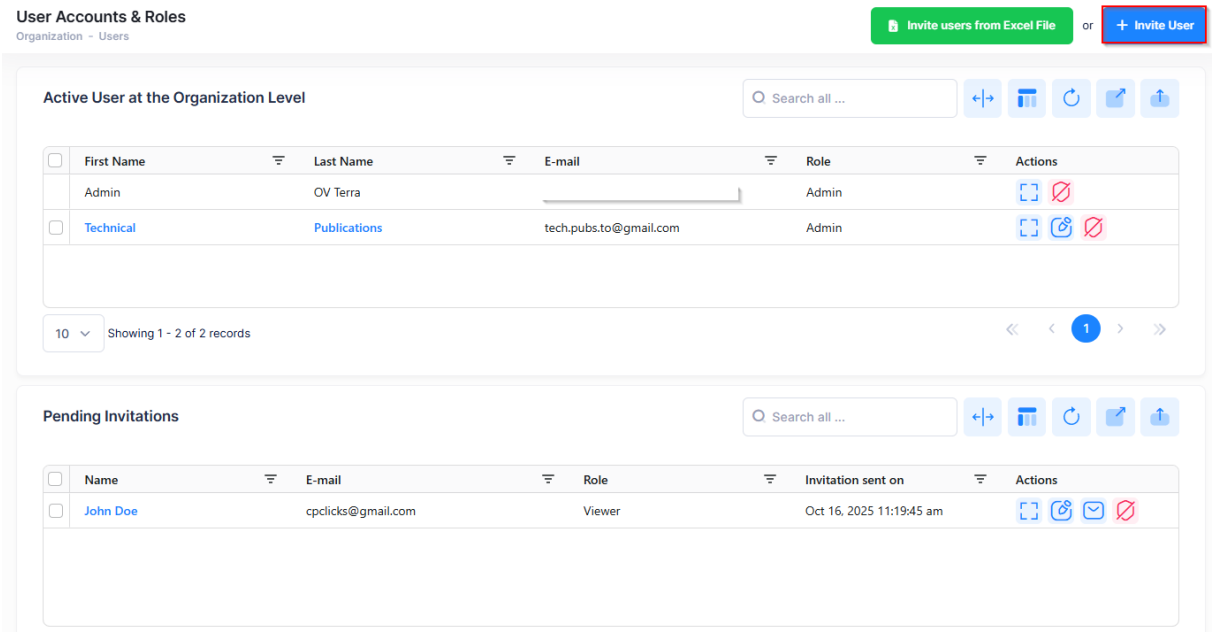
1. Fill out the template with information for each user that is to be imported. Once the Excel sheet is complete and saved, return to Step 2 of the Import screen to select the edited Excel file to import.
2. Click on **Import**. The Pending Invitation list is populated with the invitations sent to users defined in the imported Excel sheet.
3. When a user accepts the invitation and sets up their user account, their login information will be added to the active users list on the User Accounts & Roles screen.

21 Oct 2025

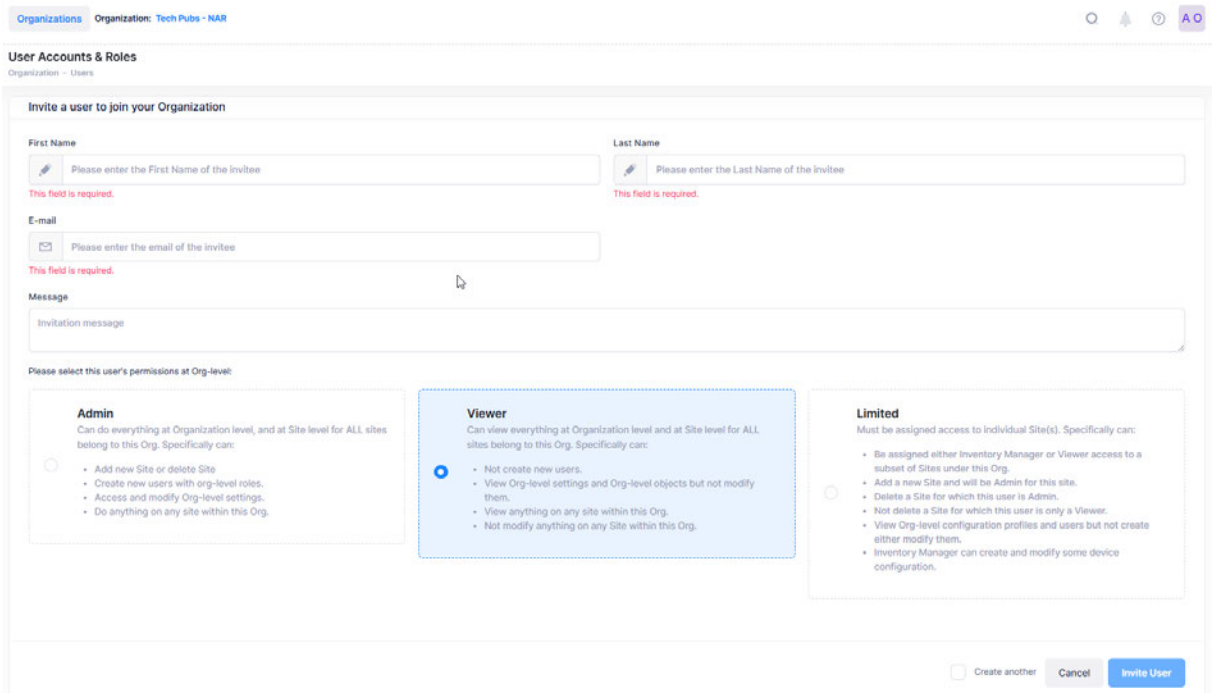
3.6.1.6 Manually Invite a User to Join the Organization

The User Accounts & Roles screen displays a list of active users that are known to the organization. There are two methods for inviting a user to an organization: invite multiple users from an Excel XLSX file (see page 115) or manually invite a single user.

To invite a single user to join the Organization, click on **Invite User** on the User Accounts & Roles screen to bring up the Invite New User form.



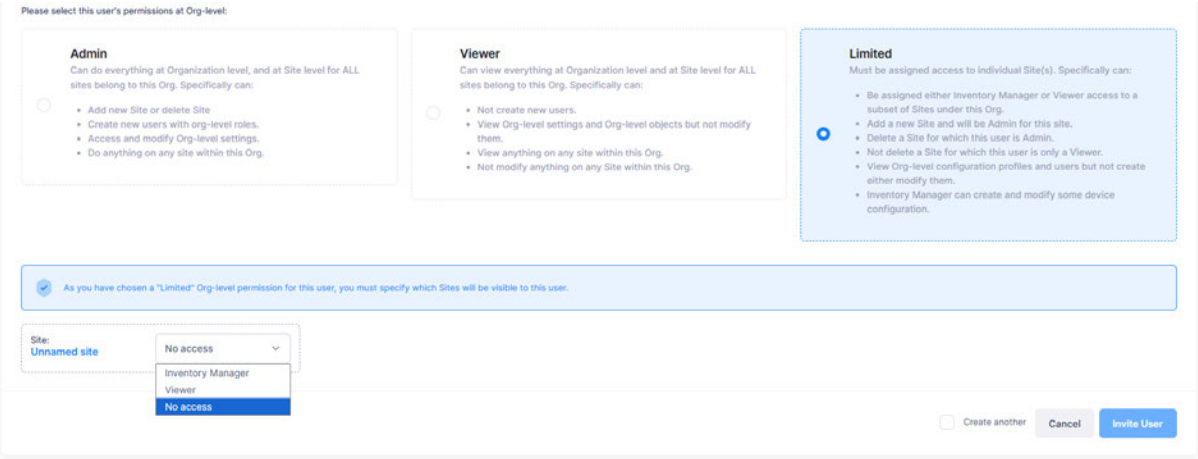
Fill out the Invite a User to Join Your Organization form as described below, then click on **Invite User** on the form to send the invite email.



Click on **Create another** to return to the Invite a User to Join Your Organization form to fill out for another user. If this box is not checked, the display returns to the User Accounts & Roles screen.

1. Enter the first and last name of the user you would like to invite.
2. Enter a valid email address for the user you would like to invite.
3. Optionally include a message to the user.
4. Select the user role (Admin, Viewer, or Limited) to specify the level of access the user will have to the Organization.

When you select Limited access for the user, you will get the following screen to provide role as Admin, Viewer or no access to selected sites.

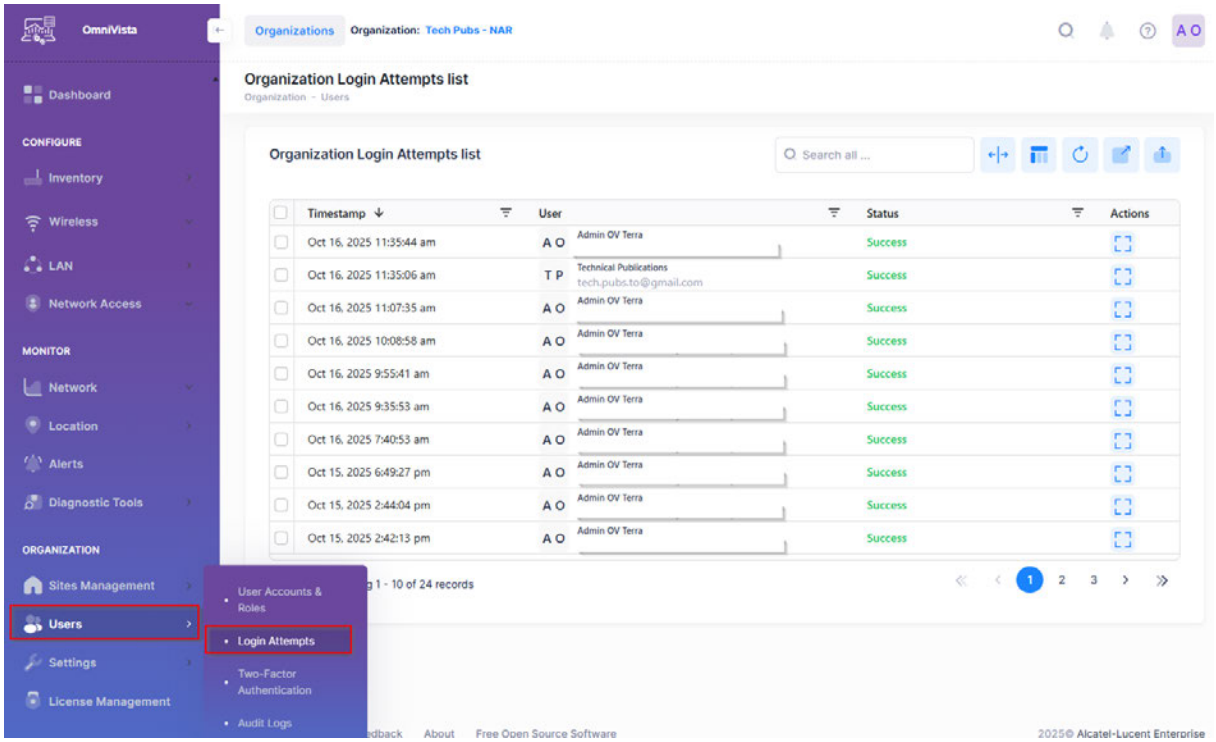


Select the Role and limited access for the user, then click on **Invite User**.

21 Oct 2025

3.6.2 Review Login Attempts at the Organization Level

When you click on **Login Attempts** under the Users menu, the following history of login attempts is displayed:



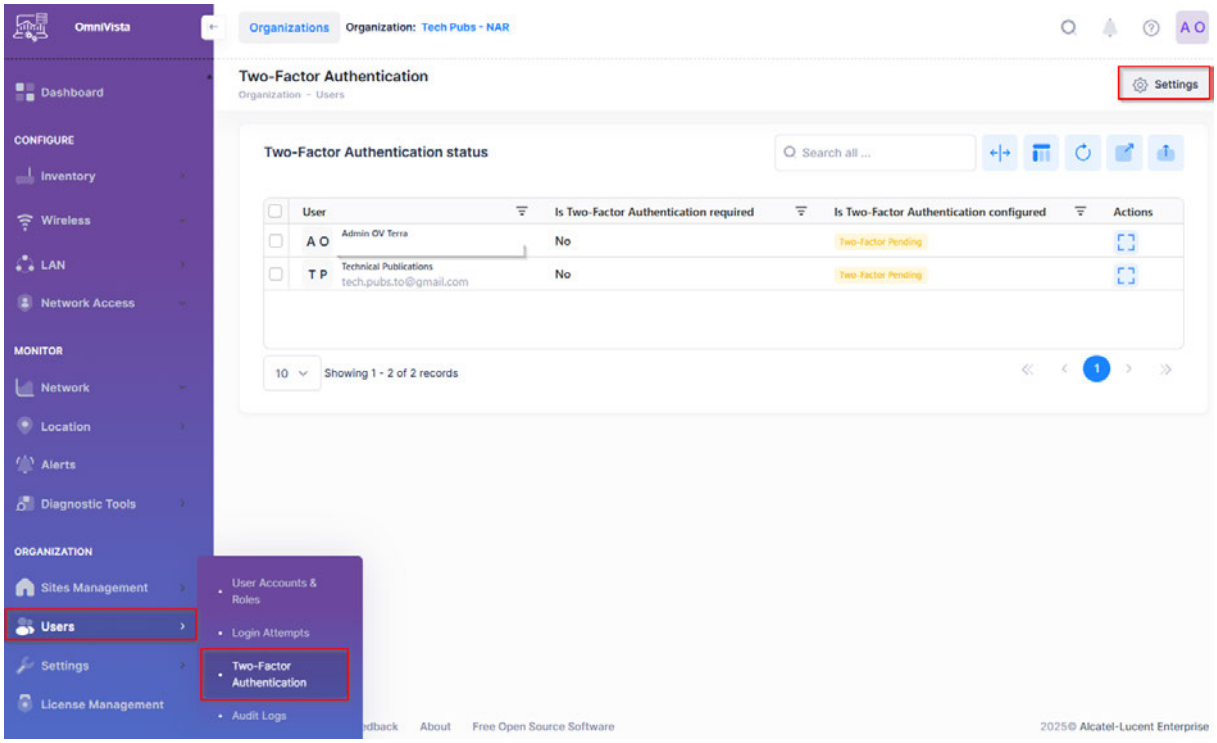
The list of login attempts provides the date and time the user attempted to log in, the user name and email, and whether the login attempt was successful.

21 Oct 2025

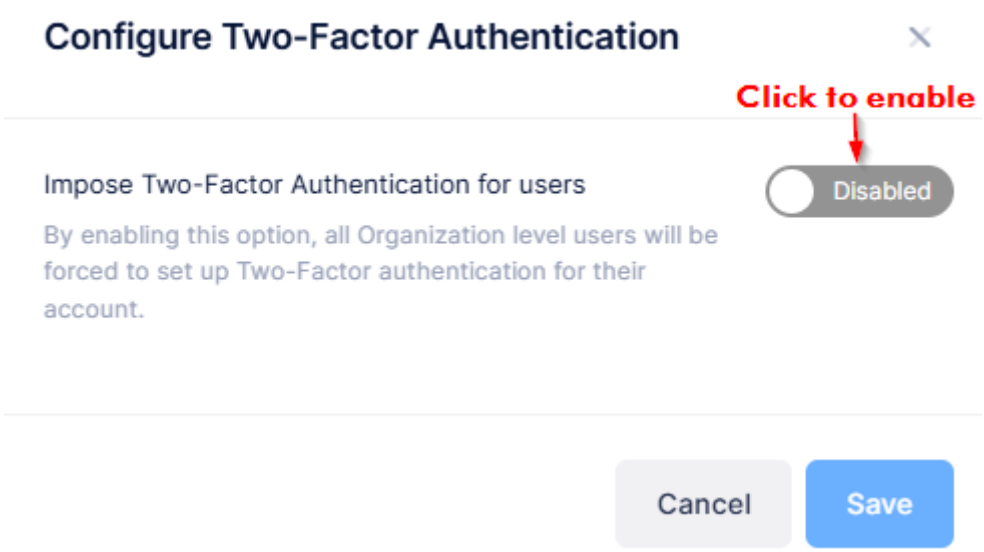
3.6.3 Two-Factor Authentication Login

Two-Factor Authentication (2FA), also called two-step verification, is a security process in which users provide two different authentication factors to verify themselves. Two-Factor authentication adds an extra layer of security to your account by requiring more than just a password to log in.

In OmniVista Terra, two factor authentication is implemented by an Organization Admin on all the users assigned to the Organization.



To enable Two-Factor Authentication for all Organization users, navigate to the Two-Factor Authentication screen (**Users > Two-Factor Authentication**) and click on **Settings** in the upper, right-hand corner of the screen. The following window opens:



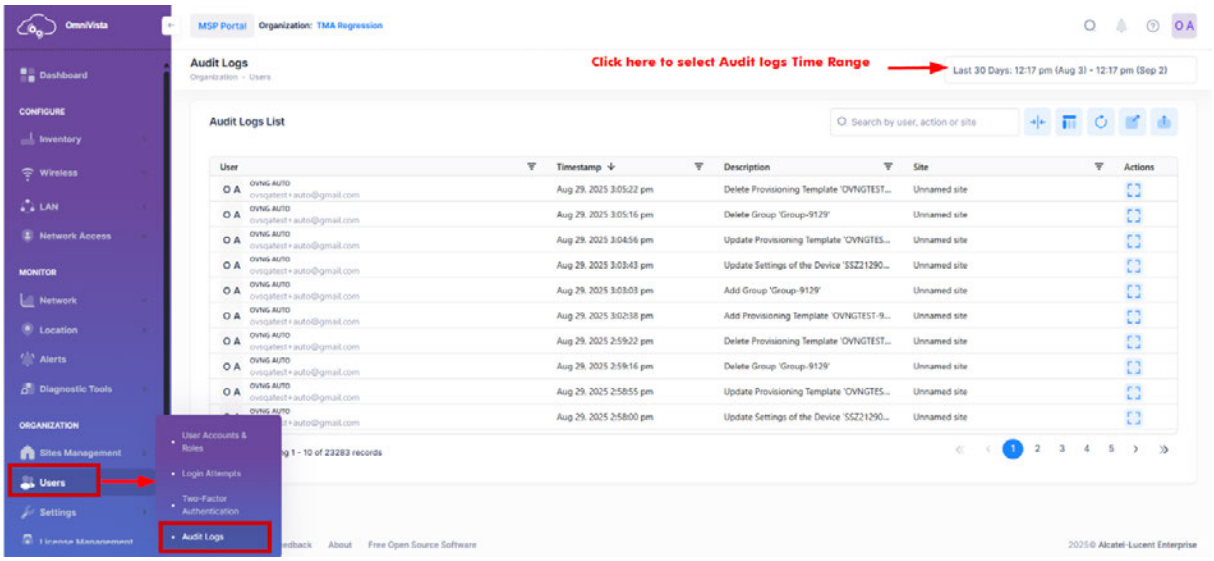
Click on the slider to enable Two-Factor Authentication for all Organization user, then click on **Save**.

See Account Information and Login Security (see page 23) for information about how to set up Two-Factor Authentication for the user account login.

21 Oct 2025

3.6.4 View Audit Log Events at the Organization Level

The Audit Log for an Organization provides a list of all the actions performed by the Organization's users. To view Audit Log details, click on Audit Logs under the Organization section of the OmniVista Terra Menu (see page 45).



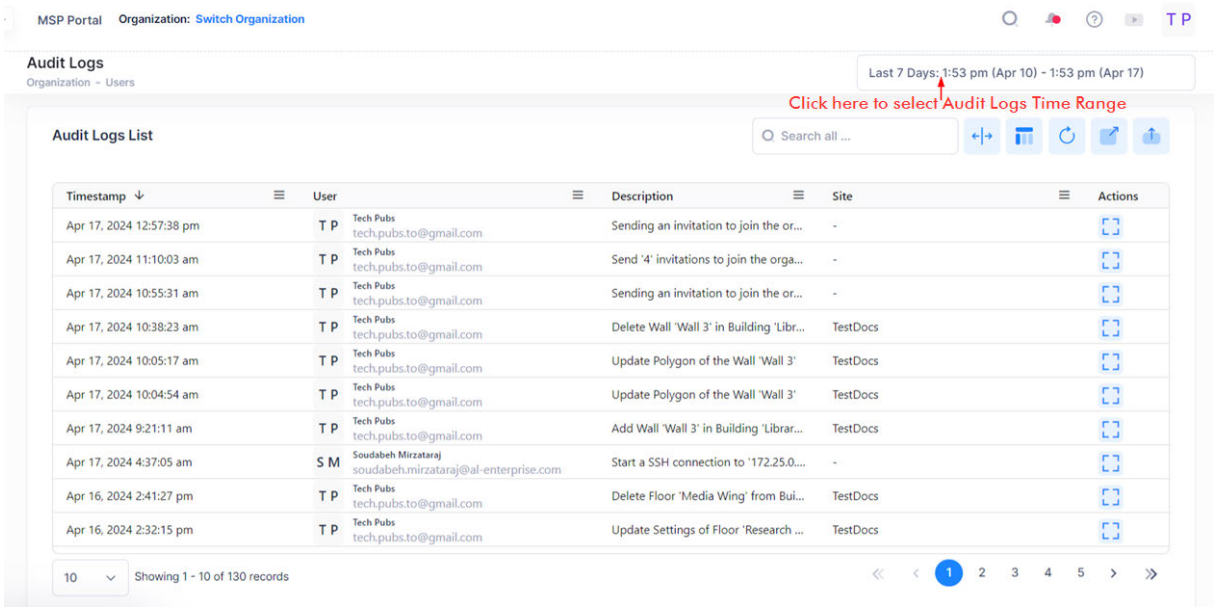
To learn more about the Audit Log list, click here (see page 123).

21 Oct 2025

3.6.4.1 Audit Logs List

Whenever an Organization user performs an action (such as inviting a user to join the Organization or updating building information for an Organization site) the action is logged as an event in the Audit Log list. The following information is logged for each user event:

- **Timestamp -** The date and time the action was taken.
- **User -** The name of the user who performed the action.
- **Description -** A description of the action taken.
- **Site -** The Organization site in which the action was taken. Note that the Site information appears blank for objects created at the Organization level (for example, SSIDs, RADIUS Server, NAS Clients).



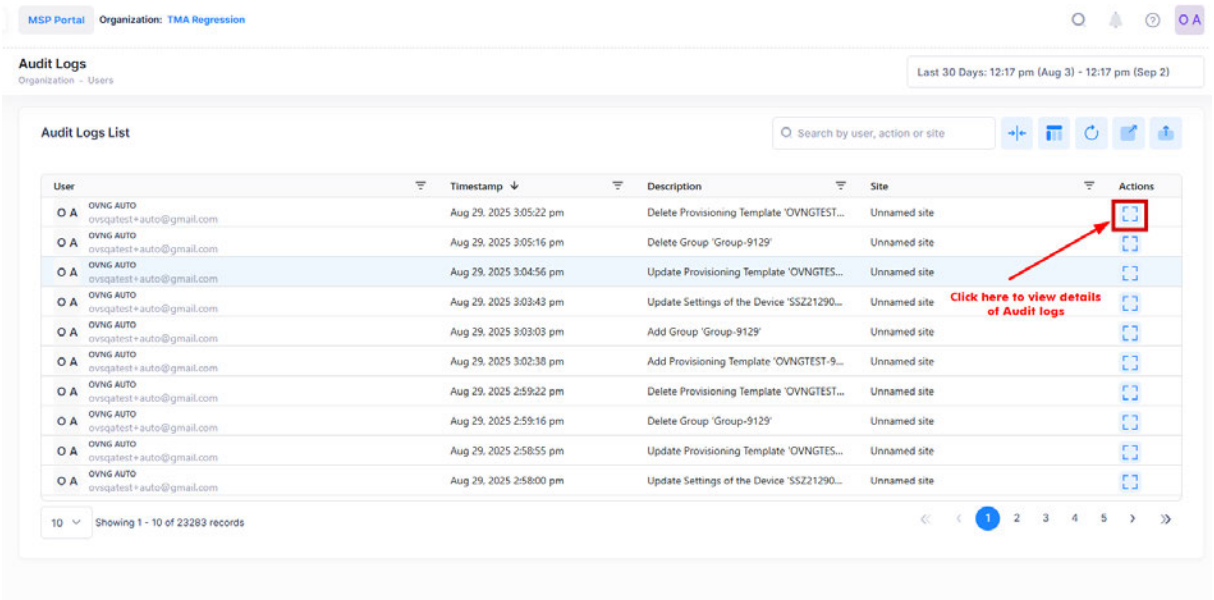
To view more detailed information for a specific user event, see View Details for an Audit Log Event (see page 124).

Audit Logs data is retained for 7 to 400 days according to the administrator user's configuration in Basic settings (see page 127) at the Organizational Level.

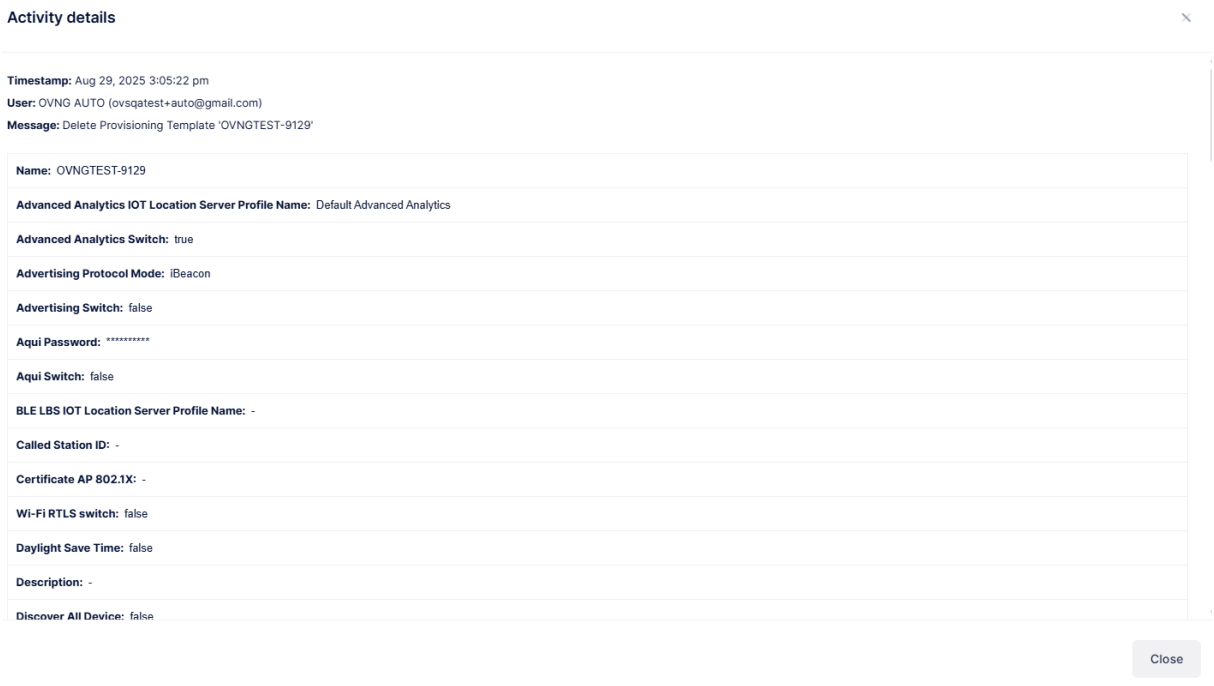
21 Oct 2025

3.6.4.2 View Details for an Audit Log Event

To view details about a specific user event, click on **View Details** under 'Actions' column of the Audit Log screen.



The following details are displayed for the specific event (including a before-the-change snapshot and an after-the-change snapshot):



Note: Updated attributes are marked in yellow for better visibility.

21 Oct 2025

3.7 Configure and Manage Organization Settings

Organizations are created from the OmniVista Main Dashboard. The Dashboard displays widgets for any Organizations an Admin User is managing. After creating an Organization, an Admin User can edit the organization parameters, as per the organizational requirement. The following parameters can be configured and managed for an organization.

- Basic Settings (see page 127)
- Email Templates (see page 131)
- Notifications (see page 133)
- Pii Requests (see page 138)

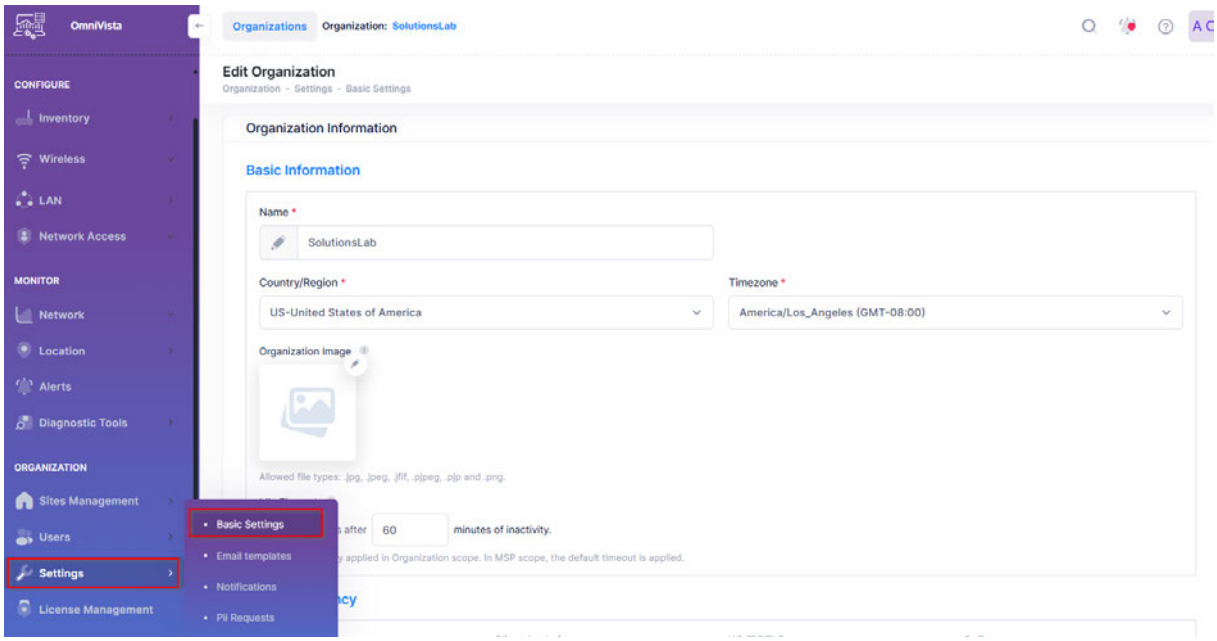
For information on creating an organization, see Create an Organization (see page 62).

21 Oct 2025

3.7.1 Basic Settings

To edit basic settings of an Organization, click on **Basic Settings > Settings** under the “Organization” section of the OmniVista Terra Menu (see page 45). The Edit Organization screen will open. You can modify the basic information for the Organization, such as Name, Country/Region, Timezone, and upload an optional Organization image. In addition, you can modify the data retention period (see page 127) for certain applications, the Password Settings (see page 129) to apply password enforcement rules, and the frequency of periodic configuration audits (see page 130).

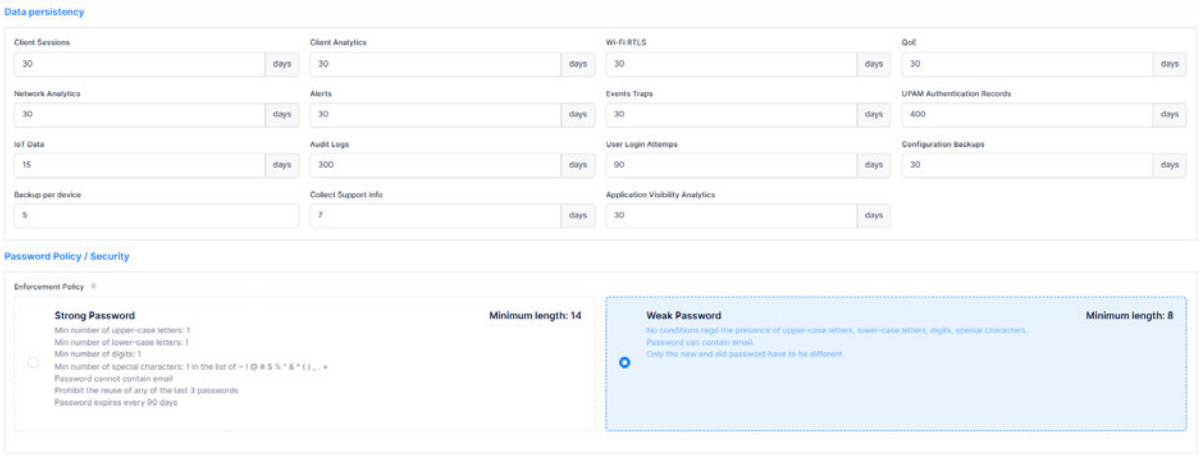
When you are done editing any of the basic settings, click on **Save**.



3.7.1.1 Data Persistency

In OmniVista Terra, data persistence refers to the capability of data to remain stored and accessible even after the application or system that created or utilized it has been closed or shut down.

The data retention period for different parameters can be customized and saved based on the organizational requirements in OmniVista Terra. However, a default period has already been set in OmniVista Terra.



- **Client Sessions** - Displays the duration in days for which data on wireless clients association with access points is stored.
- **Client Analytics** - Displays the duration in days for which data on information about client metric values is retained.
- **WiFi RTLS** - Displays the duration in days for which information is stored on the usage of OmniVista Terra WiFi RTLS and OmniAccess Stellar Asset Tracking Server for providing Location Based Services (LBS).
- **QoE** - Displays the duration in days for which information about QoE analytics is stored. QoE analytics allows you to evaluate the actual end-user experience on the network.
- **Network Analytics** - Displays the duration in days for which information about Network analytics is stored. Network analytics allows you to evaluate WiFi network performance using WLAN metrics (such as AP uptime, AP health, session metrics).
- **Alerts** - Displays the duration in days for which information about Alerts is stored. Alerts provides a list of basic alert information (for example, severity, date/time received).
- **Events Traps** - Displays the duration in days for which information about notification of events from devices is stored.
- **UPAM Authentication Records** - Displays the duration in days for which data on authentication information for all devices authenticated via UPAM (Unified Policy Access Management) is retained.
- **IoT Data** - Displays the duration in days for which data on all endpoint devices that are connected to the network (e.g., PCs, Tablets, Smartphones) is retained.
- **Audit Logs** - Displays the duration in days for which data on Audit logs is stored.
- **User Login Attempts** - Displays the duration in days for which data on User Login Attempts is stored.
- **Configuration Backups** - Displays the duration in days for which configuration backup and all its files, Collect support info and its archived logs file data is stored.
- **Backup per device** - Displays the count of backup which can be stored per device.
- **Collect Support Info** - Displays the duration in days for which Collect Support Info data and its archived logs file, configuration backup and all its files data is stored.

- **Application Visibility Analytics** - Displays the duration in days for which Application Visibility analytics data and its archived logs file, configuration backup and all its files data is stored.

3.7.1.2 Password Policy/Security

There are enforcement password guidelines for existing users which they have to follow to enhance the security compliance.

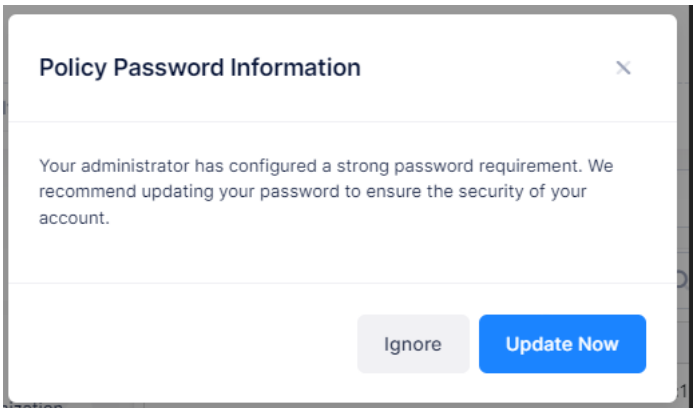
The existing user accounts can continue to work even if they have weak passwords. The enforcement policy will apply only when creating or editing OmniVista Terra users. Please follow the below guidelines for password settings:

1. When the Enforcement Password Policy (EPP) is ON and affected users access the Edit profile, Change password, or Reset password screen, they will have to change their password to meet the EPP rules if their current password does not comply with the strong password rules. Criteria to decide if a user is affected or not (except default super admin account, created by provisioning job):
    a. If you have access to only one Organization, follow the EPP of the Organization.
    b. If you have access to many Organizations, if at least one Organization has EPP ON, follow this EPP, unless EPP is OFF for the user.
2. If the affected user's password meets the strong password conditions, the user is not required to change the password.
3. When EPP is ON for an Organization, the new users who are invited to the Organization (user clicks the Create Account button in the invitation email then creates a new account on Sign up page) have to create a new account with strong password rules.
4. OmniVista Terra will block the creation of a new user if the user login credentials violate the password rules based on the Organization EPP.
5. When EPP is ON for an Organization and an existing user is invited into the Organization, the user does not have to update their password when accepting the invitation.
6. After 90 days of the first creation or of the last updated time password, while login, the affected user has to change the password before accessing the Home dashboard page.
7. Any existing users of OmniVista Terra will not be forced to change passwords just because the Organization Settings associated with them are modified.

The strong and weak password criteria are described below:

- **Strong Password** - Minimum password length is 14 with the following required guidelines:
    - Min number of upper-case letters: 1
    - Min number of lower-case letters: 1
    - Min number of digits: 1
    - Min number of special characters: 1 in the list of ~ ! @ # $ % ^ & * ( ) _ . +
    - Password can not contain e-mail
    - Reuse of any of the last three passwords is prohibited
    - Password requires to change every 90 days

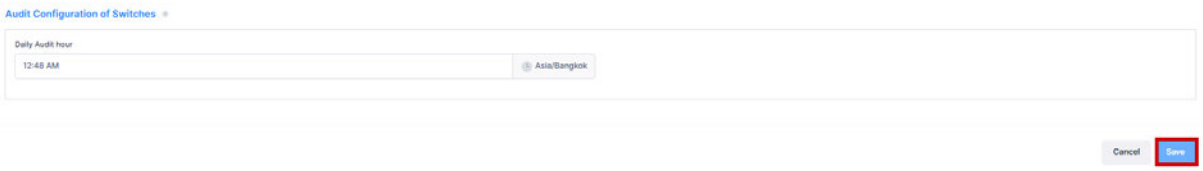
- **Weak Password** - Minimum password length is 8 with no required guidelines. Password can contain username. Only the old and new password have to be different.
- **Enforcement Access** - Selecting this option will apply the chosen password policy settings to the existing users within the organization or site. The existing users with only weak passwords will be prompted to update their passwords based on this policy. After the message, the user can choose to skip it. There is no mandatory condition to change the password.
  - **No warning** - There will be no immediate warning message sent to the users to update passwords but the users will be alerted while editing their profile.
  - **Show message after login** - The users will see a message after they log in to the network to update their passwords and if the user's current password does not meet the strong password requirements, a modal will prompt the user to change their password to a strong one after they log in as shown below.



3.7.1.3 Audit Configuration of Switches

OmniVista Terra allows you to mark the switch Running Configuration as a Golden Configuration. When this is done, a periodic audit is automatically started to compare the Running Configuration to the Golden Configuration to detect any differences between the two. See the Auditing the OmniSwitch Running Configuration (see page 248) online help for more information.

By default, the periodic audit is performed once a day. You can specify the time of day that the audit is performed by configuring the Audit Configuration setting.



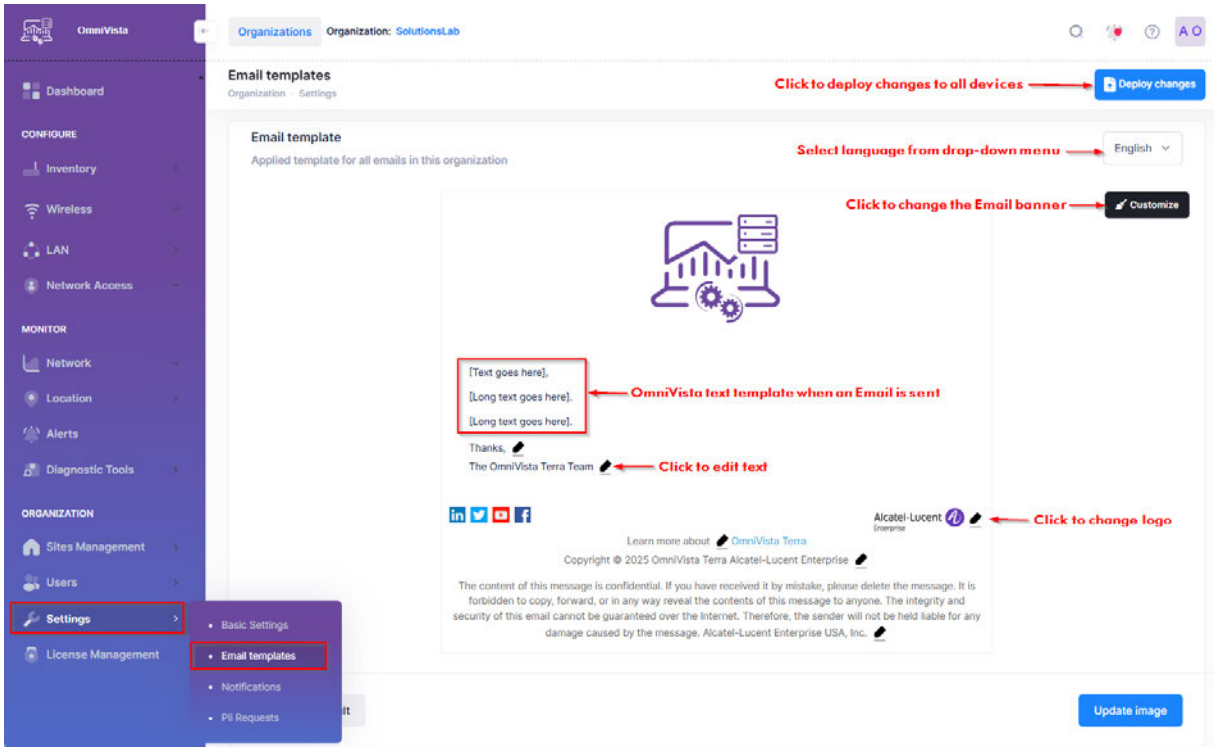
Daily Audit hour - Select the daily Audit time from the drop-down list. The time zone is automatically set to the region time zone for your Organization.

After you have finished configuring any of the field values on the Basic Settings screen, click on **Save**.

3.7.2 Email Templates

A default Email template is used for all Emails sent by OmniVista Terra. For example, an Email is sent during user interactions, such as guest self-registration or when a user is invited to join an Organization.

You can customize specific objects of the Email template, the template language, and deploy an updated template to OmniVista Terra services. To access the Email template, click on **Settings > Email Template** under the “Organization” section of the OmniVista Terra Menu (see page 45).



When you click on any one of the template objects to customize, you will then be prompted to modify text or upload image files, depending on the object you selected to customize. In addition to customizing template objects, you can perform the following tasks:

- Select the language for the Email template, click on the drop-down menu, as shown in the image above, and click on **English** (default), **Chinese**, or **French**.
- Click on **Reset to default**, to restore the original object values for the template.
- Click on **Save template** when you are done customizing template objects.
- Click on **Deploy changes** to push the updated Email template out to OmniVista Terra services. The next time an email is sent, the updated template is used. Note that if you don’t deploy the updated template, then OmniVista Terra will not use that template for subsequent Emails.

The text for the template objects in square brackets, shown above, is filled in by OmniVista Terra when the Email is sent. If the Email is sent to users as part of an Employee/Guest account strategy, you can modify the text for these objects by editing the content template that is filled in when the Email is sent. See the Email & SMS (see page 702) online help for more information.

21 Oct 2025

3.7.3 Notifications

- SMS Provider (see page 133)
- Rainbow (see page 135)

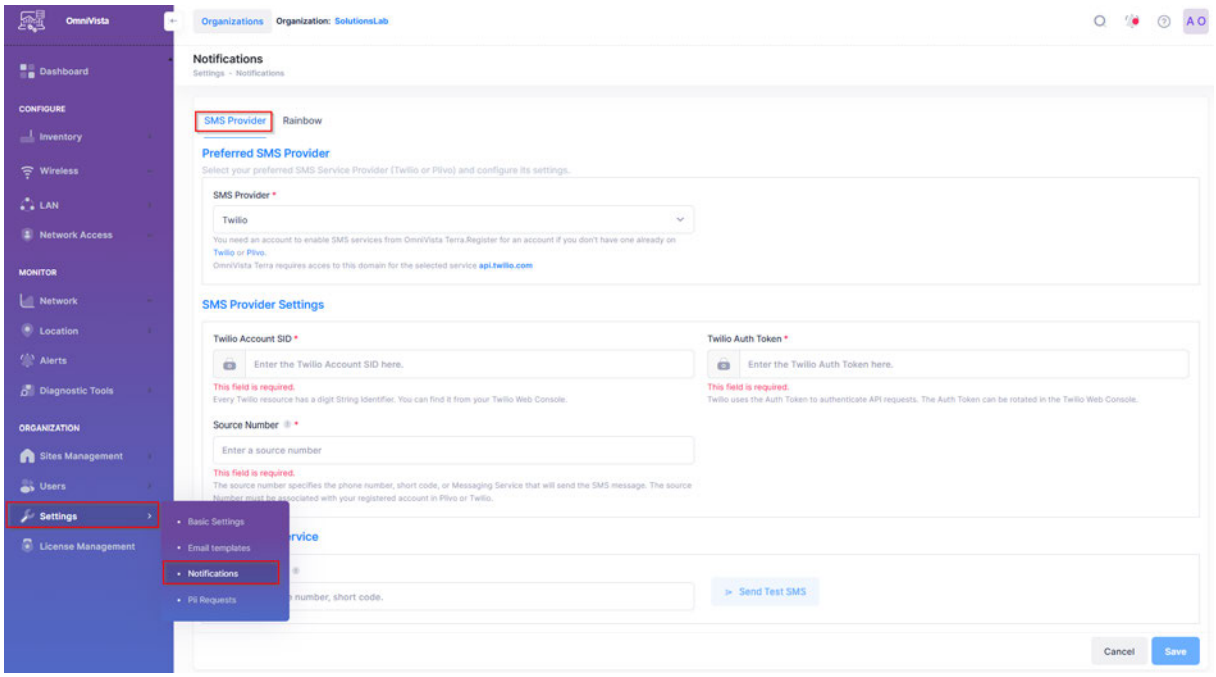
3.7.3.1 SMS Provider

SMS notifications are sent through SMS service providers to inform the users with short messages about the services which they have configured in OmniVista Terra.

For each organization, Organization Admin users can configure which SMS Service will be used to send SMS notifications. In OmniVista Terra, the SMS service configuration is available for two services.

1. Plivo
2. Twilio (see page 134)

To configure SMS provider settings, click on **Settings > Notifications** under “Organization” to view the SMS Provider page.



Select your preferred SMS Service Provider (Twilio or Plivo) and configure its settings.

3.7.3.1.1 Preferred SMS Provider

You need an account to enable SMS services from OmniVista Terra. Register for an account if you don't have one already on Twilio or Plivo.

OmniVista Terra requires access to the following provider domains:

- Plivo SMS: api.plivo.com

- Twilio SMS: api.twilio.com

3.7.3.1.2 Plivo SMS Provider Settings

- **Plivo Auth ID** - Every Plivo resource has an authentication ID. You can find it from your Plivo Web Console.
- **Plivo Auth Token** - Plivo uses the Auth Token to authenticate API requests. The Auth Token can be located in the Plivo Web Console.

3.7.3.1.3 Twilio SMS Provider Settings

- **Twilio Account SID** - Every Twilio resource has a digit String Identifier. You can find it from your Twilio Web Console.
- **Twilio Auth Token** - Twilio uses the Auth Token to authenticate API requests. The Auth Token can be rotated in the Twilio Web Console.

3.7.3.1.4 Source Number

The source number specifies the phone number, short code, or Messaging Service that will send the SMS message. The source Number must be associated with your registered account in Plivo or Twilio.

After configuring SMS Provider Settings, you can test the SMS Service by sending a test SMS.

3.7.3.1.5 Testing the SMS Service

SMS Service settings of Trillo or Pilvo can be tested by providing a recipient number and send a test message to that number.
A Recipient number should be in the form of:

- A Short Code is a 5 or 6 digits number (e.g.12345, 123456).
- A Long Code includes:
  - Country code: from 1 to 3 digit number.
  - Area Code: 1 to 5 digit number

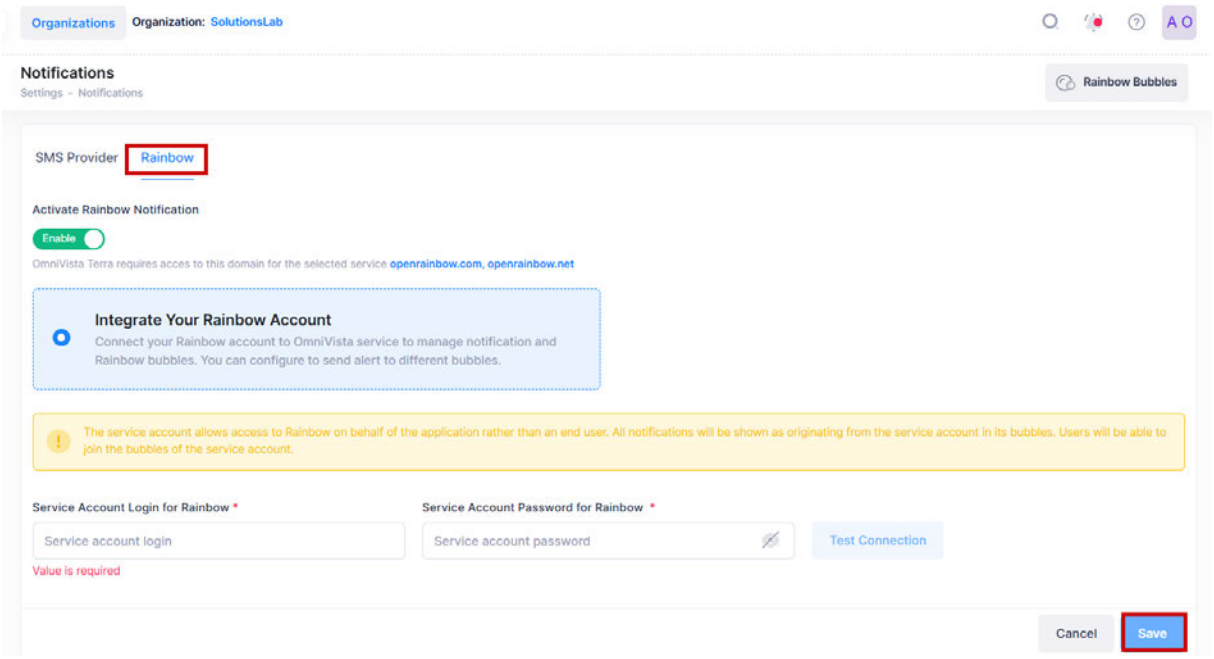
(eg. +1-425-555-0100, +1 425 555 0100, +14255550100 or mixed type +1-425 5550100).

Note that you need to have a registered SMS service account (Twilio or Plivo) for testing the SMS Service.

3.7.3.2 Rainbow

Use the Rainbow configuration to send notifications from OmniVista Terra to an existing and/or new Rainbow Bubble. For each Organization, Admin users can enable the sending of alerts to the specified Rainbow Bubble.

To configure Rainbow settings, click on **Settings > Notifications > Rainbow** under “Organization” to view the Rainbow page. Toggle **Activate Rainbow Notification** to enable.

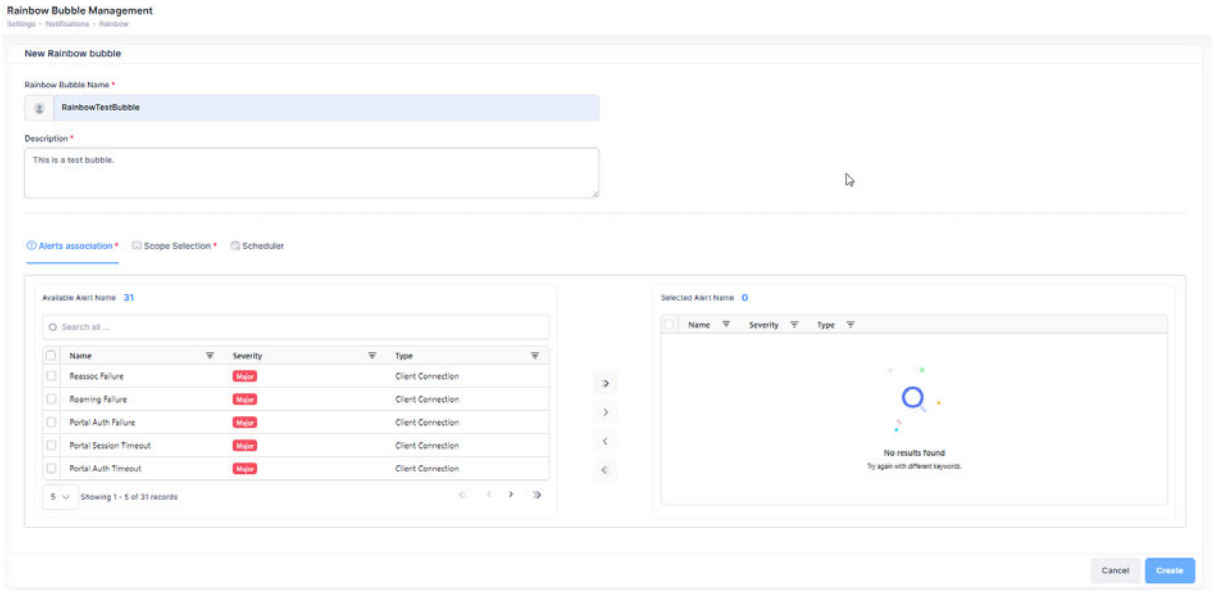


- **Integrate Your Rainbow Account**
  - Enter the Rainbow Service Account Login and Password.
  - **Test Connection** and **Save**.

Note: The service account allows access to Rainbow on behalf of the application rather than an end user. Thus, the ‘Rainbow Account’ is a service account, not a personal account.

3.7.3.2.1 Create a Rainbow Bubble

Click on **+ Create Bubble** to open the New Rainbow Bubble screen.



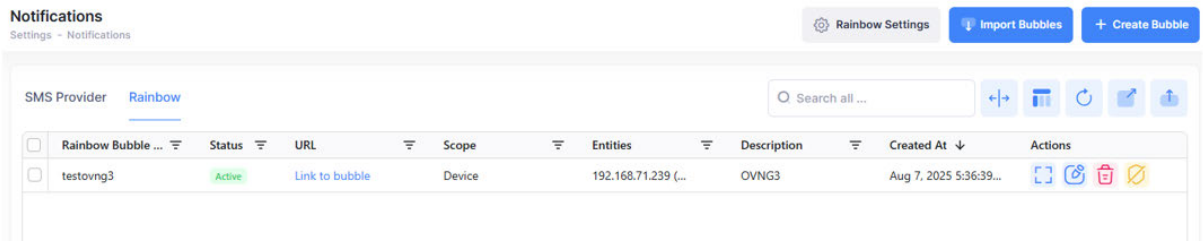
Complete the fields as described below, then click **Create**.

- **Rainbow Bubble Name** - The name of the Rainbow bubble to send notifications to.
- **Description** - The bubble description.
- **Alerts Association** - Choose the alerts to be associated with the Rainbow bubble.
- **Scope Selection** - Choose the scope of devices to associate with the alerts.
  - **Device** - This option allows you to assign a specific set of devices in the organization.
  - **Site** - This option allows you to assign all the devices in a site to the configuration.
  - **Floor** - This option allows you to assign all the devices in a floor to the configuration.
- **Scheduler** - The Scheduler can be used to setup days and times when alerts will be sent. By default alerts are always enabled.

Note: OmniVista Terra users must have an active Rainbow account. A dedicated service account is required for the setup of OmniVista Terra. If you don't have an account, go to the following URL to sign up.
https://web.openrainbow.com

3.7.3.2.2 Import Rainbow Bubbles

When **Integrate Your Rainbow Account** is enabled there is an option to import existing Rainbow Bubbles by clicking on **Import Bubbles**.



- To access the Rainbow bubble, click on **Link to bubble** under the URL column.
- To view more information about the Rainbow Bubble, click on **Additional Information Details** icon.
- To edit the existing Rainbow Bubble information, click on the **Edit** icon.
- To delete the Rainbow Bubble information, click on the **Delete** icon.
- To disable the Rainbow Bubble, click on the **Disable** icon.

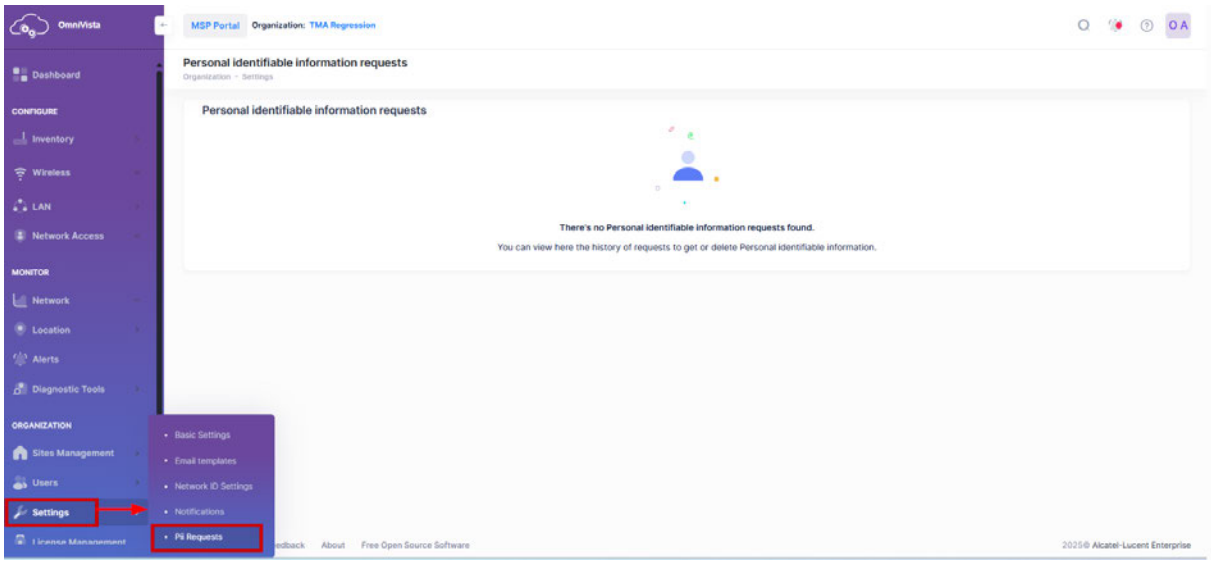
21 Oct 2025

3.7.4 Personal Identifiable Information Requests

Personally Identifiable Information (PII) is a legal term pertaining to information security environments. it is the information that can be used by organizations on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Organizations use the concept of PII to understand which data they store, process and manage that identifies people and may carry additional responsibility, security requirements, and in some cases legal or compliance requirements.

Click on **Settings > Pii Requests** under the “Organization” section of the OmniVista Terra Menu (see page 45) to go to the Personal identifiable information requests screen.



Here, you can delete an organization's personal identifiable information requests (PII data), either for yourself, or in response to requests from users in your network. You can view the history of requests to get or delete Personal identifiable information.

> The deleted PII data is not allowed to re-enter into the network database but is stored in a blocked list that can only be undone by user.

21 Oct 2025

3.8 License Management in OmniVista Terra

A license to an Organization is required to access and configure the Organization for network management. This release of OmniVista offers a Trial license that provides a period of 90 days and 20 devices to evaluate and utilize OmniVista features (additional time and number of devices can be requested). You can then upgrade from the free trial version to a paid licensed version of OmniVista Terra.

> OmniVista Terra licenses and OmniVista Cirrus 10 licenses are not interchangeable. For example, you cannot use OmniVista Terra licenses for OmniVista Cirrus 10 device management.

3.8.1 License Management Overview

The following components and individuals are involved in the process of obtaining a license for your OmniVista Terra Organization:

- **License Types**:
  - Trial License (see page 142) - Provides a free teaser period that is automatically activated when you create an Organization.
  - CAPEX Subscription (see page 158) - Paid license subscription.
- **Alcatel-Lucent Business Partner (BP)** - Your BP contact creates and activates the purchased CAPEX Subscription licenses. The BP forwards the paid licensing information to you, which you can then import into OmniVista and bind to Organization devices.

3.8.1.1 How It Works

1. Create an Organization to manage devices in OmniVista. A free Trial License is automatically approved for the Organization, offering a 90-day teaser period to evaluate managing up to 20 devices.
2. Decide if you want to extend or renew the Trial License duration and number of devices. See the Trial License (see page 142) online help for more information.
3. Decide if you want to upgrade to a paid license subscription. If so, contact your Business Partner to discuss CAPEX Subscription licensing options.
4. Upgrading to a paid CAPEX Subscription involves the following process between you and your Business Partner:
   a. BP purchases and activates the required licenses using eBuy and Subscription Manager. Note that during the license activation process, the BP will require the OmniVista ID for your OmniVista Terra installation. This ID is located at the top of the OmniVista Admin Center (see page 1064) screen.
   b. BP sends an email to you containing a Subscription ID, an Activation Code, and an attached Subscription File.

c. When you receive the license confirmation email from the BP, use the information provided to import the licenses into OmniVista. See Upgrade from a Trial to a Paid License Subscription (see page 149) online help for more information.

d. After you have imported the CAPEX licenses into OmniVista and assigned the licenses to your devices, export an Entitlement File from the License Management screen. See the License Management Using a CAPEX Subscription (see page 158) online help for more information.

e. Send the Entitlement File to your BP to upload into Subscription Manager. The entitlement file exports the list of devices assigned to the CAPEX Subscription. Subscription Manager uses the information to identify devices under service and support. (For example, Premium and Business subscription types include service and support for the device, such as Support Plus for Partner - > Business and Support Plus end customer -> Premium.)

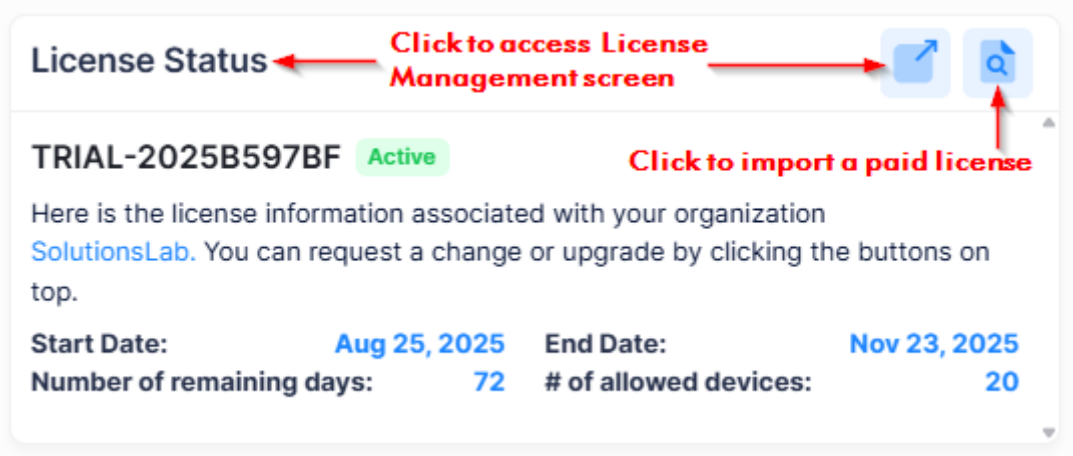
3.8.2 Configure and Manage an Organization License

The License Management screen displays information about the Organization's OmniVista Terra License, such as the license type (free trial or paid subscription). A user is allowed to manage up to the maximum number of devices allowed for that license for the length of the trial or paid subscription contract.

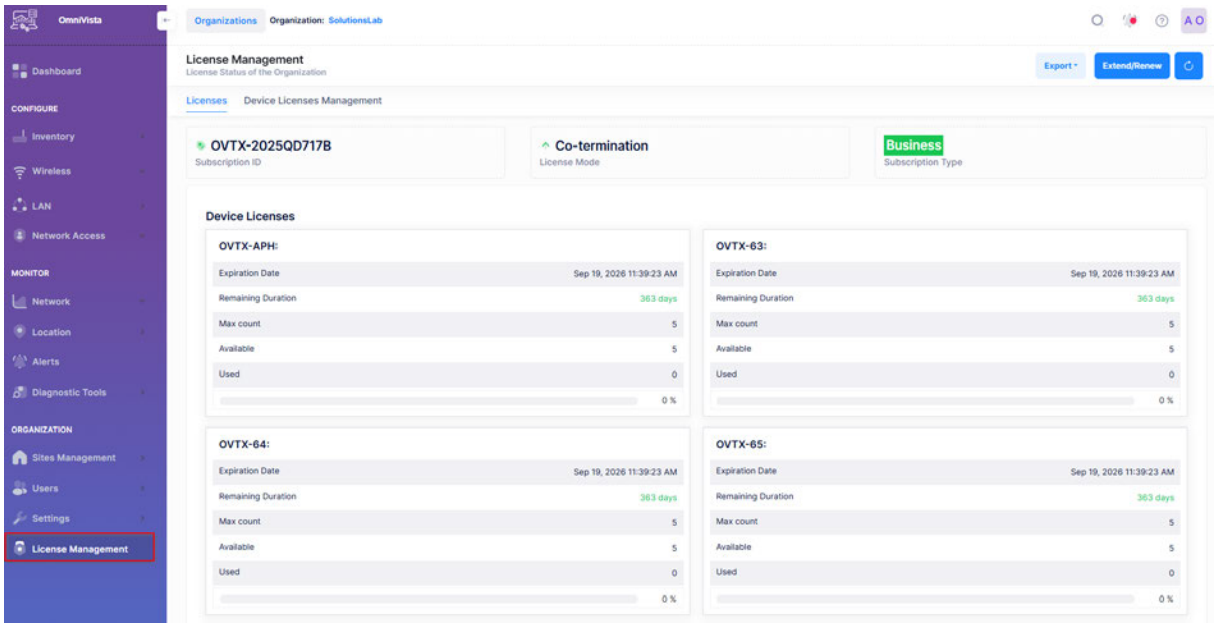
> You have to obtain a license subscription from your Business Partner before you can import licenses for your Organization.

There are two ways to access the License Management screen for the current Organization:

- Click on the **License Status** shortcut located on the Organization Dashboard (see page 71).



- Click on **License Management** under the "Organization" section of the OmniVista Terra Menu (see page 45).



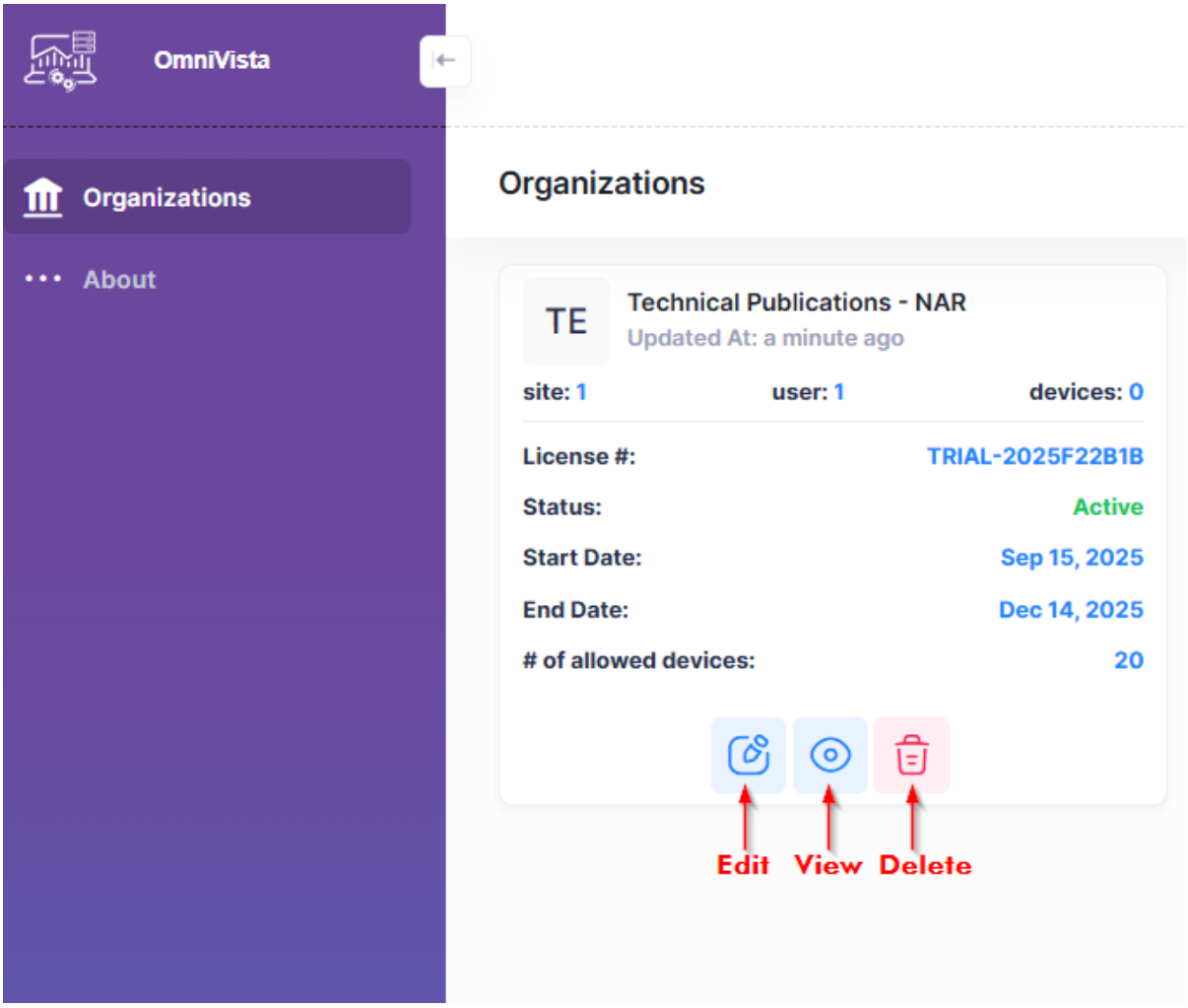
The License Management screen provides an overview of the licenses purchased and activated by the user, including the start and end dates for the license as well as the number of devices that can be managed with the current license.

21 Oct 2025

3.8.3 Trial License: The Basics

When a new Organization is created, a Trial License is automatically approved and assigned to the Organization. The Trial License provides a Teaser Period of 90 days for managing up to 20 devices.

An Organization Widget representing the new Organization appears on the OmniVista Main Dashboard (see page 31). You can immediately start to configure the Organization for network management without having to request access to the Organization.



When you click on the **View organization** icon, the Organization Dashboard (see page 71) will appear. From the Organization Dashboard, you can create sites, buildings, and floors. You can also add devices, create Organization Users, and monitor the Organization's network.

During the Trial License period, you can evaluate and use OmniVista features. At any time, you can request an extension (see page 143) for additional time or more devices. You can also decide to upgrade to a paid licensed (see page 149) version of OmniVista.

21 Oct 2025

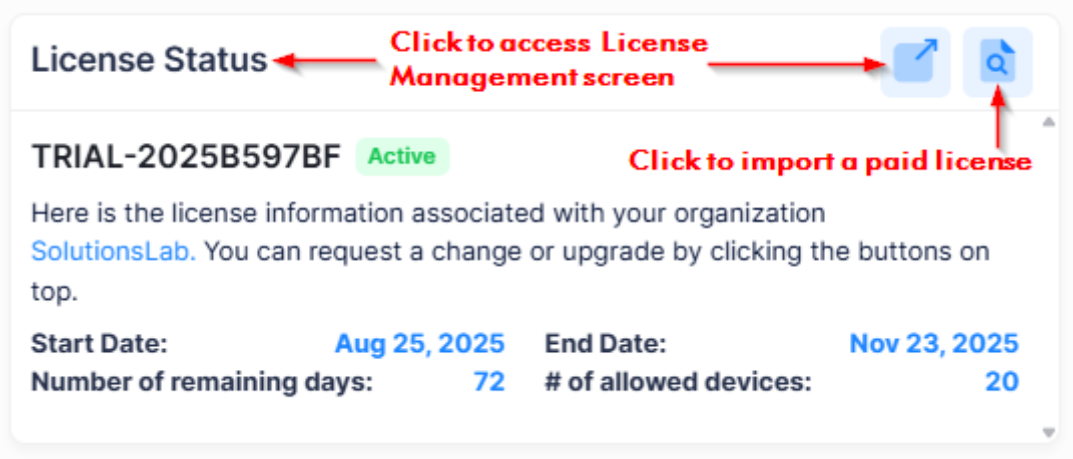
3.8.3.1 Update an Existing Trial License

Use the License Management screen to request an update to the Trial License time frame and/or the number of devices to manage.

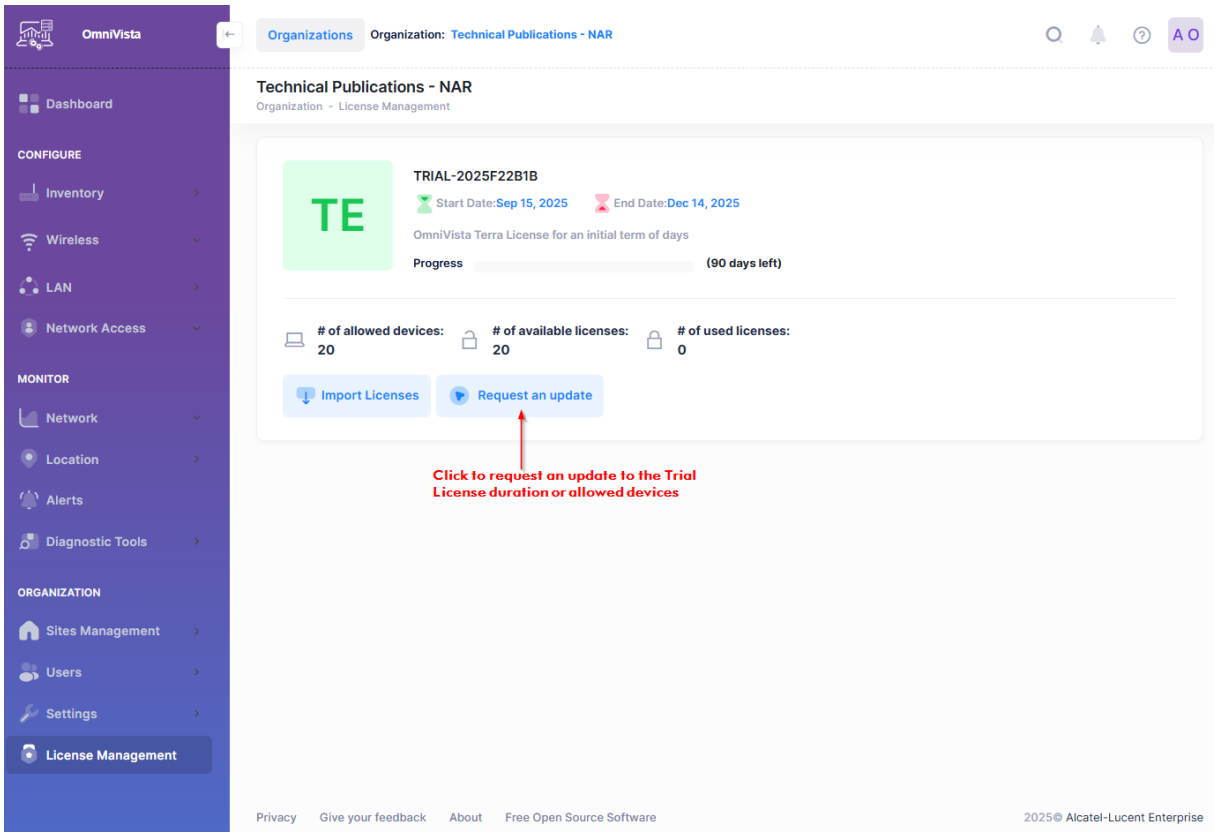
> Requesting an update to the Trial License requires a Trial Activation Code from your Business Partner.

You can access the License Management screen in one of the following ways:

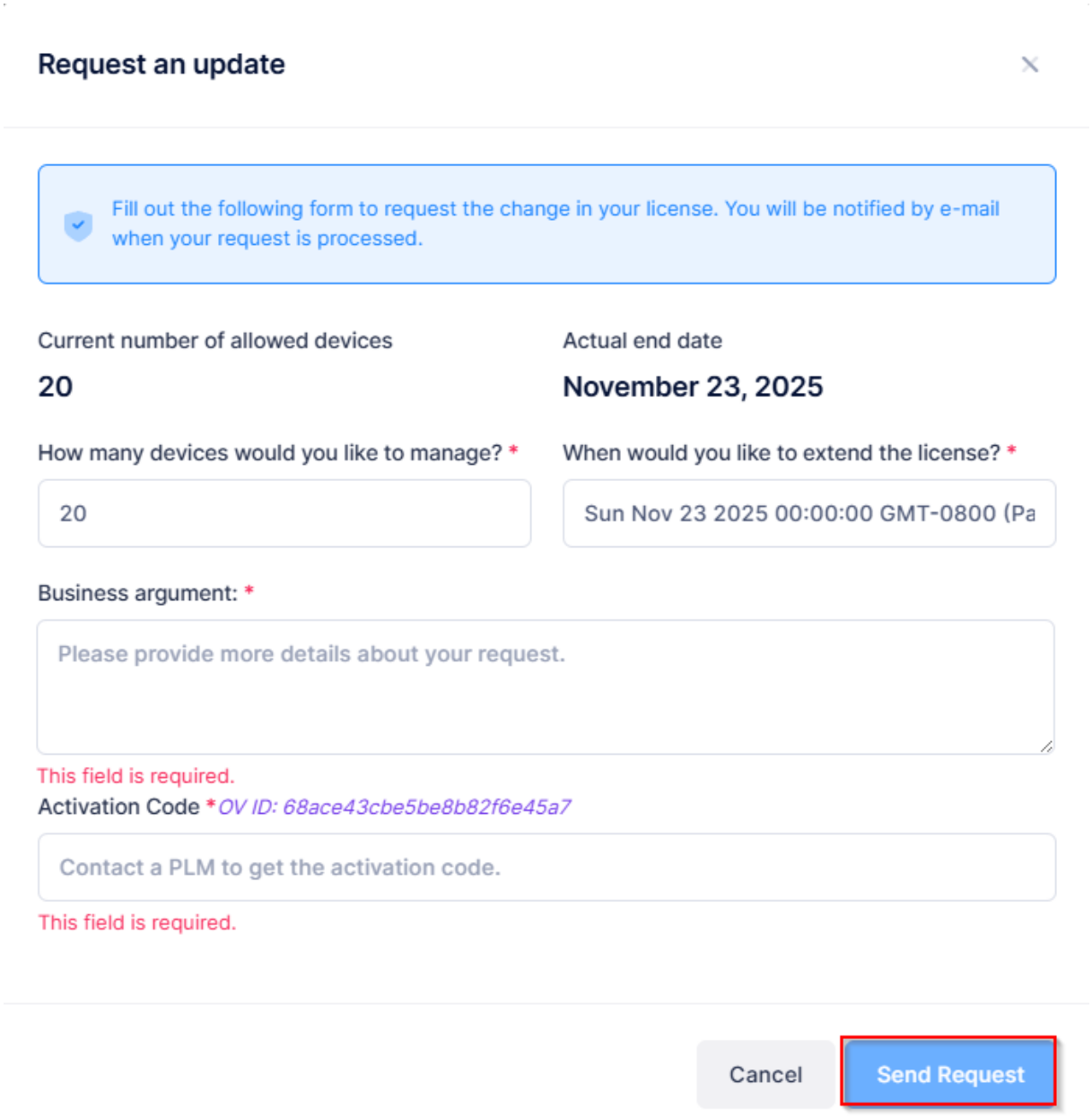
- Click on the License Status panel located in the lower-left corner of the Organization Dashboard.



- Click on **License Management** under the “Organization” section of the OmniVista Terra menu (see page 45).



The Request an Update form displays. Complete the fields you want to update, as described below, and click on **Send Request**.

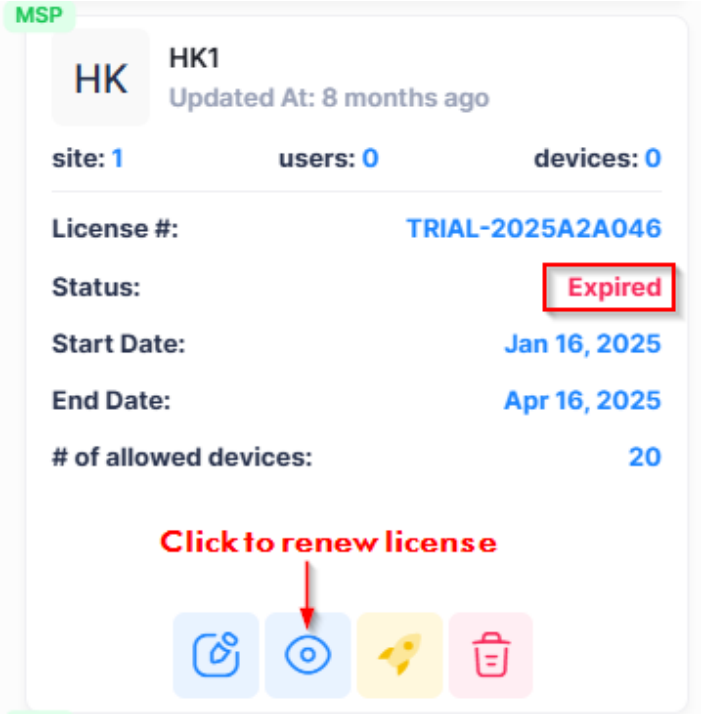


- **Current number of allowed devices** - The number of devices that you are allowed to manage with the current license.
- **How many devices would you like to manage?** - Click on the arrows in this field to adjust the number of devices you want to manage with this license.
- **Actual end date** - The original end date of the license period.
- **When would you like to extend the license?** - Enter a new end date to extend the license period.
- **Business argument** - Explain why you would like to make the requested changes to your license.
- **Activation Code** - Enter the Activation Code provided by your Business Partner.

21 Oct 2025

3.8.3.2 Renew an Expired Trial License

When the **Status** field on the Organization Widget indicates that the Trial License has expired, click on the **View organization** icon to open the Renew License form.

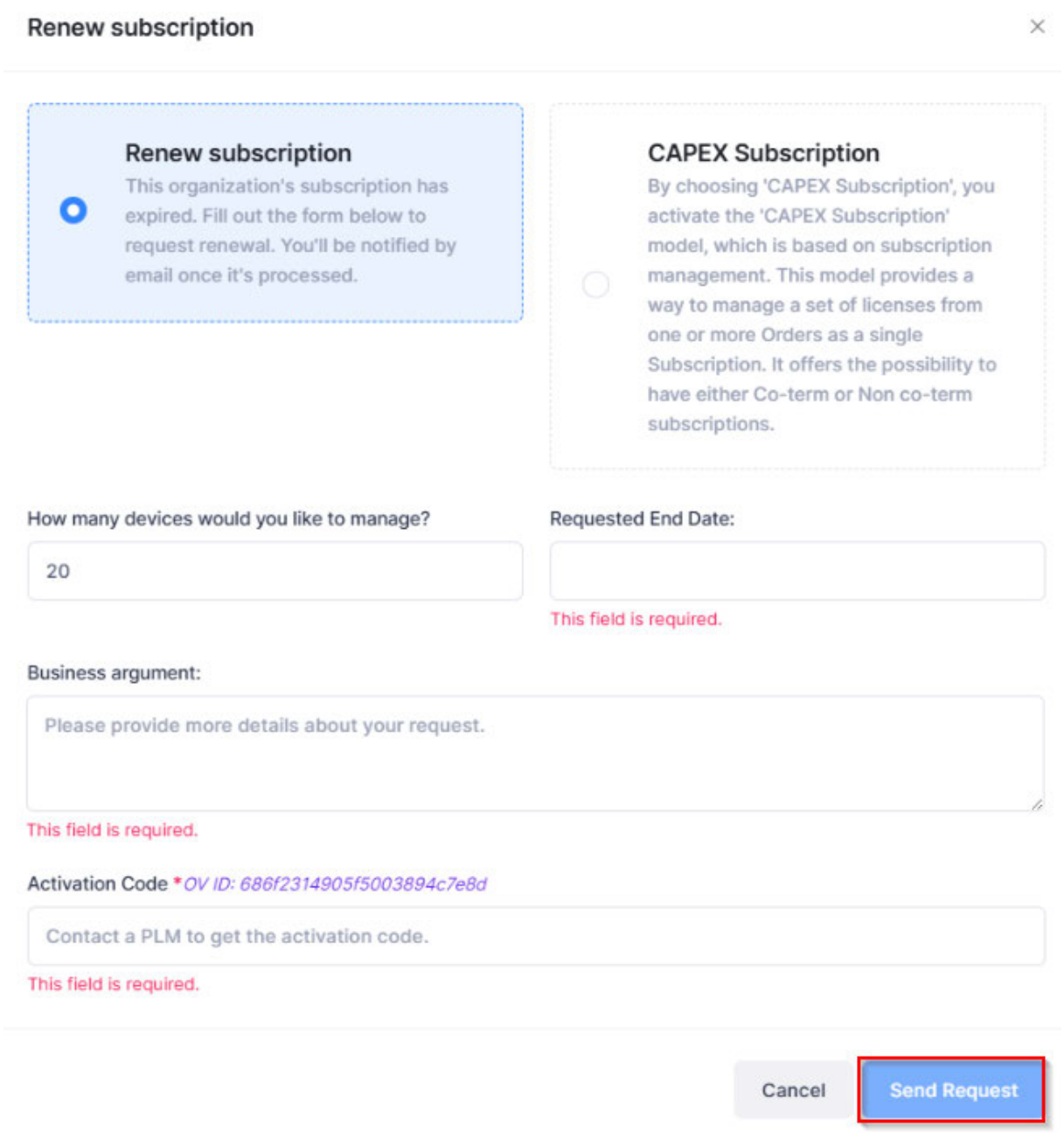


A Renew Subscription form is displayed. On this form, you have the option to renew the Trial License (see page 146) or directly apply a paid CAPEX Subscription to the Organization.

3.8.3.2.1 Renew Subscription

> Renewing an expired Trial License requires a Trial Activation Code from your Business Partner.

When you select the “Renew Subscription” option, the form displays the fields that you need to complete to renew the Trial License.

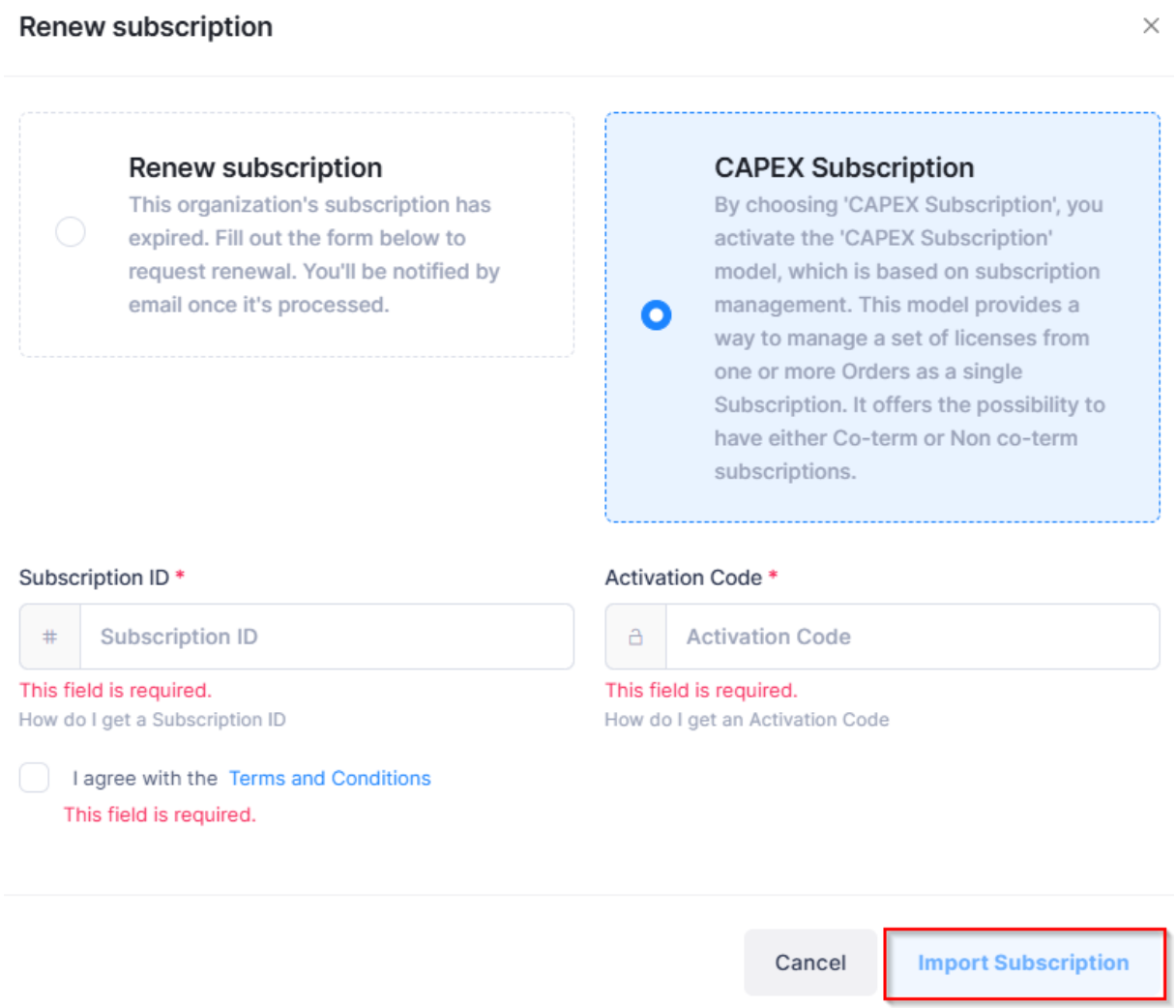


Complete the following fields on the Renew Subscription form as necessary and click on **Send Request**.

- **How many devices would you like to manage?** - Enter the number of devices that you would like to manage with this license.
- **Requested End Date** - Enter the new end date for the license.
- **Business argument** - Enter a required explanation as to why you want to renew the license.
- **Activation Code** - Enter the Trial Activation Code provided by your Business Partner.

3.8.3.2.2 CAPEX Subscription

When you select the “CAPEX Subscription” option, the form displays the fields required to apply for a paid CAPEX license subscription for the Organization.



Complete the fields as described below, then click on **Import Subscription** in the lower-right corner of the form. You must complete the mandatory fields and agree to the Terms and Conditions.

- **Subscription ID** - The CAPEX Subscription ID number you received in the licensing email.
- **Activation Code** - The CAPEX Activation Code number you received in the licensing email.
- **Terms and Conditions** - Click on the checkbox to accept the licensing terms and conditions.

For more information about applying a CAPEX Subscription license, see the online help for Using the CAPEX Subscription model (see page 158).

21 Oct 2025

3.8.4 Upgrade from a Trial to a Paid License Subscription

To manage devices in OmniVista, you need to import licenses and bind them to your devices. Licenses are imported when you are upgrading from a Trial License to a Paid License. If you are already using a paid license subscription, see License Management Using the CAPEX Subscription Model (see page 158) for more information.

Importing paid licenses requires Subscription ID, an Activation Code, and a Subscription File (containing the activated licenses). Once the licenses are imported, they are added to the license pool and will be available for use.

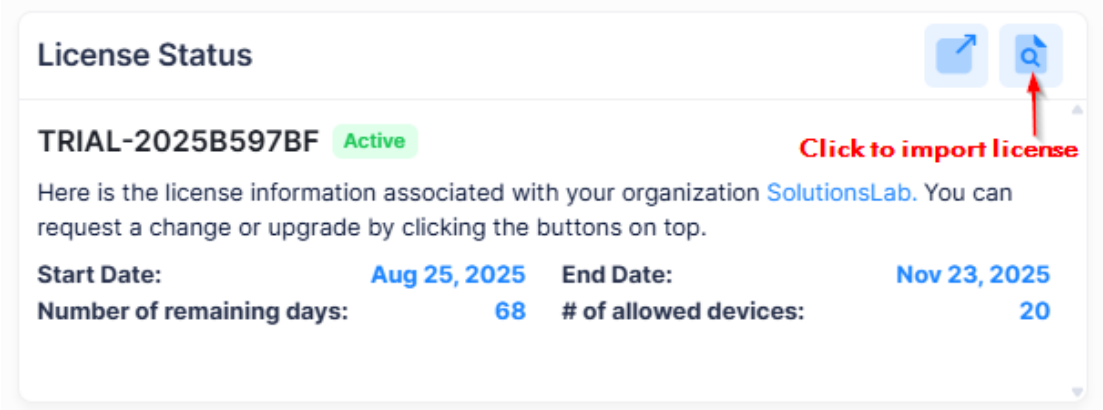
3.8.4.1 License Order ID, Activation Code, and Subscription File

To obtain an Order ID, Activation Code, and Subscription File you must contact your Alcatel-Lucent Enterprise Business Partner to request the required licenses. When your request is processed, you will receive an official email containing the Order ID, Activation Code, and a Subscription File.

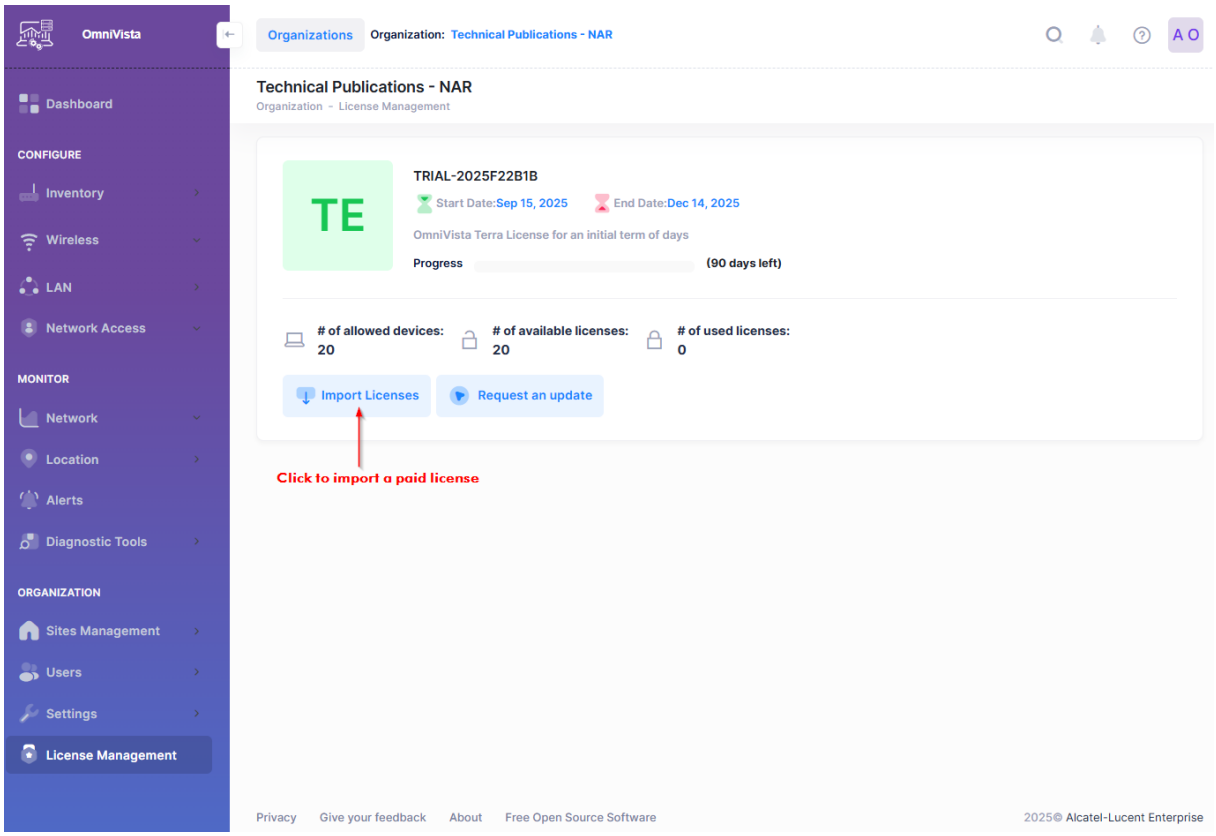
3.8.4.2 Import Device License

The Import Licenses screen is used to import licenses into your OmniVista Organization. There are two ways to access the Import Licenses screen:

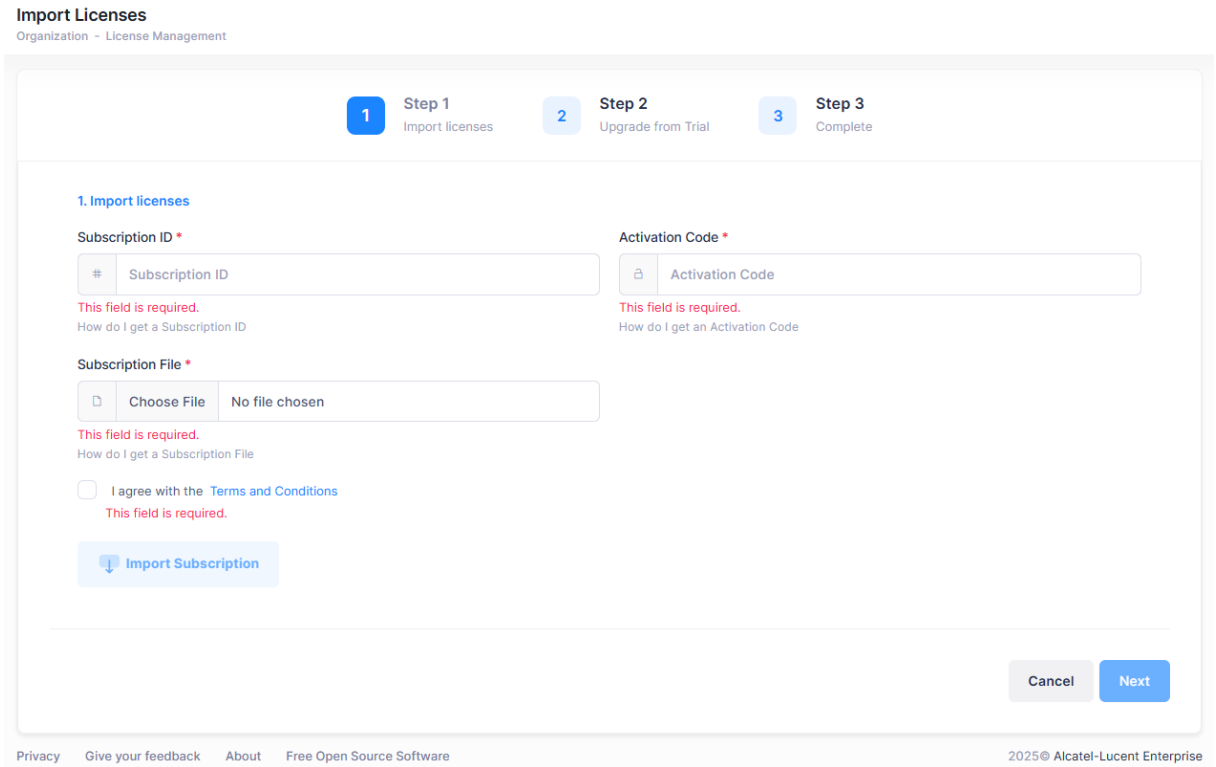
- Click on **Import Licenses** located at the top of the License Status panel on the Organization Dashboard (see page 71).



- Click on **License Management** under the “Organization” section of the OmniVista Terra Menu (see page 45) to open the License Management screen, then click on **Import Licenses**.



The following Import Licenses screen opens:



The CAPEX Subscription (see page 152) model provides a way to manage a set of licenses from one or more orders as a single pre-paid subscription. This model also offers the possibility to have either Co-

Termination or No Co-Termination subscriptions. The following license categories are available with the CAPEX Subscription model:

- OVTX-APL - Stellar AP Low End
- OVTX-APH - Stellar AP High End
- OVTX-63 - OS63 Series Switches
- OVTX-64 - OS64 Series Switches
- OVTX-65 - OS65 Series Switches
- OVTX-68 - OS68 Series Switches
- OVTX-69 - OS69 Series Switches
- OVTX-99 – OS99 Series Switches

21 Oct 2025

3.8.4.3 Importing CAPEX Subscription Licenses

Once you receive the CAPEX Subscription licensing information from your Business Partner (BP), you can import the subscription licenses into OmniVista Terra. The import process consists of the following steps:

Step 1. **Import Licenses** (see page 152) - Enter the Subscription ID, Activation Code, and upload the Subscription File for the CAPEX Subscription that you purchased. The Subscription File contains the activated licenses that you will upload into OmniVista Terra.

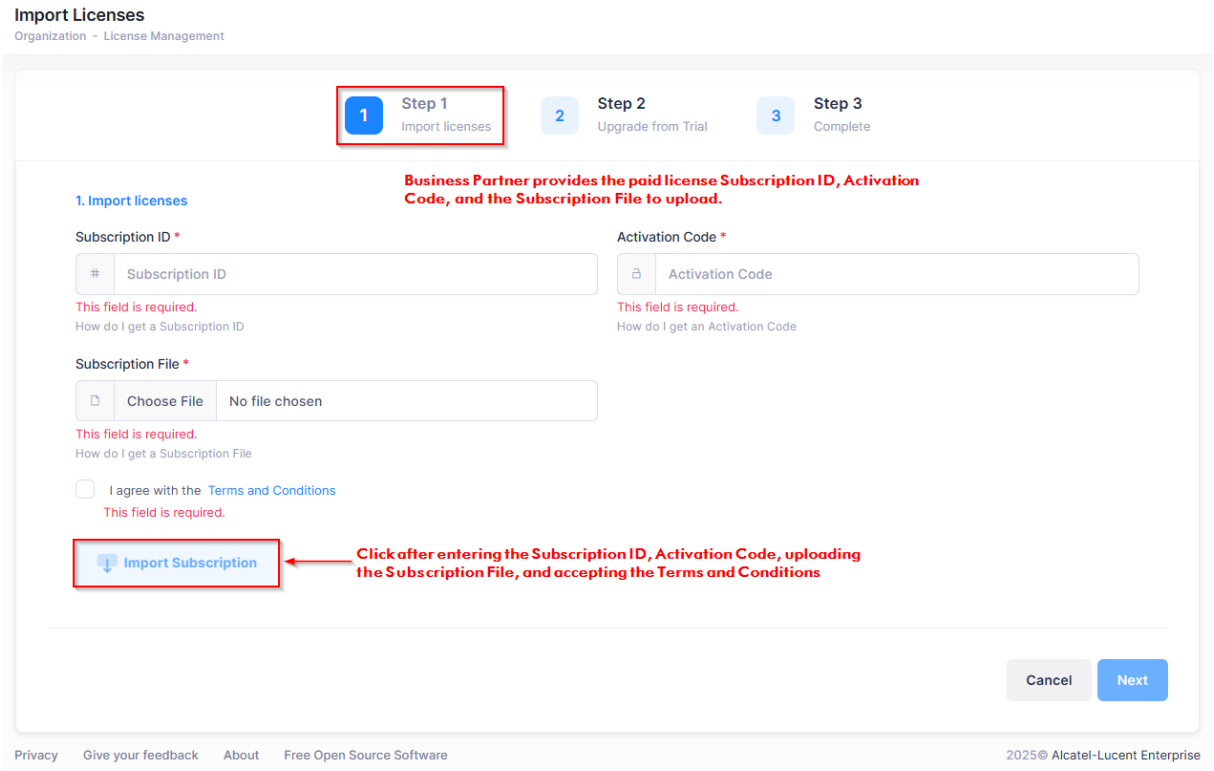
Step 2. **Upgrade from Trial** (see page 153) - Assign licenses to your devices.

Step 3. **Complete** (see page 155)- Review and complete importing device licenses to upgrade from a Trial license to a CAPEX Subscription.

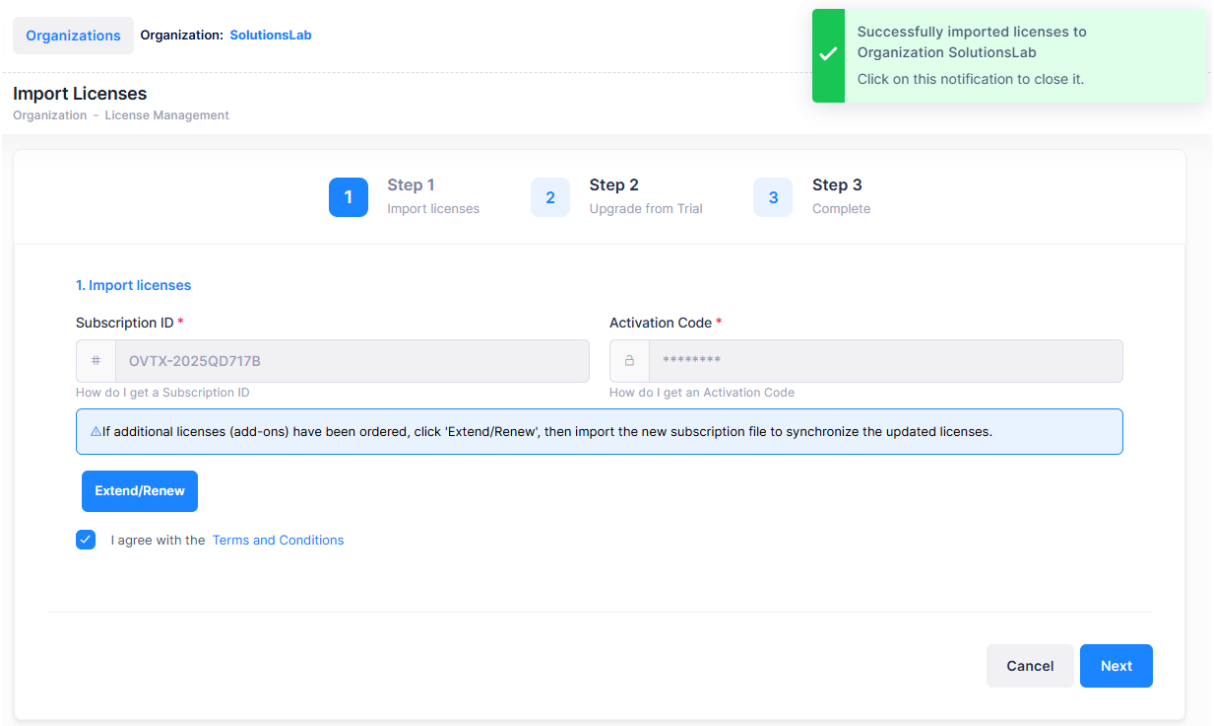
Step 4. **Export the Entitlement File** (see page 156) - Download an Entitlement File from the License Management screen and send the file to your BP. This file contains the mapping between devices and CAPEX Subscription licenses that the BP will upload into Service Manager. Note that this step is done after Step 3 of the import process and is not included on the Import Licenses screen.

3.8.4.3.1 Step 1. Import Licenses

The Import Licenses screen allows you to import the subscription license order, as described below.



1. Enter the Subscription ID, Activation Code, and upload the Subscription File for your paid licenses.
2. Accept the Terms and Conditions, then click on **Import Subscription**. The licenses are imported into the Organization.



3. If additional licenses (add-ons) were also purchased, click on **Extend/Renew** to upload the Subscription File for the add-ons.

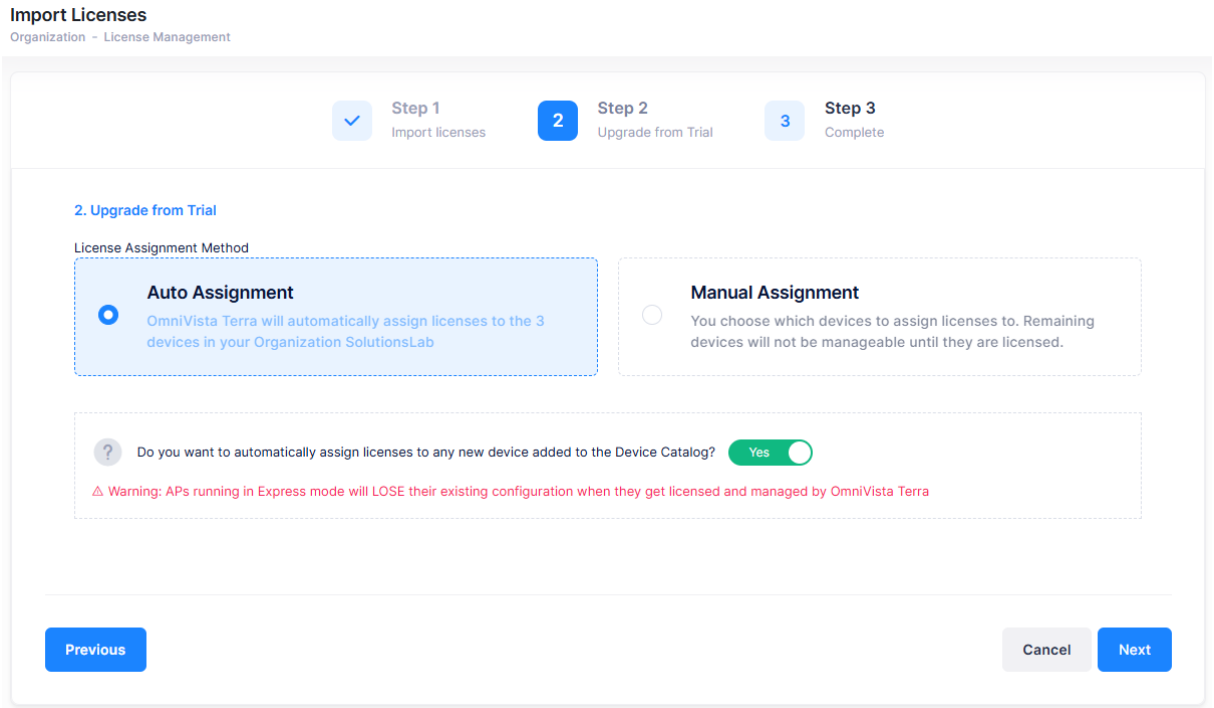
4. Upload the Subscription File (provided by your Business Partner) for the activated add-on licenses, then click on **Apply**.
5. Click on **Next** to move to the “Step 2 Upgrade from Teaser” tab.

3.8.4.3.2 Step 2. Upgrade from Trial

The next step in upgrading from a Trial license to a paid licensing model is to assign subscription licenses to your devices. The Upgrade from Trial screen allows you to manually assign licenses or select automatic assignment of licenses to devices in your Organization.

- **License Assignment Method** - Select one of the following methods for assigning subscription licenses:
  - **Auto Assignment** (see page 154) - Licenses are automatically assigned to the devices within your Organization.
  - **Manual Assignment** (see page 155) - You select which devices to license. Any devices not licensed remain unmanageable until the devices are licensed.

3.8.4.3.2.1 Automatically Assign Device Licenses

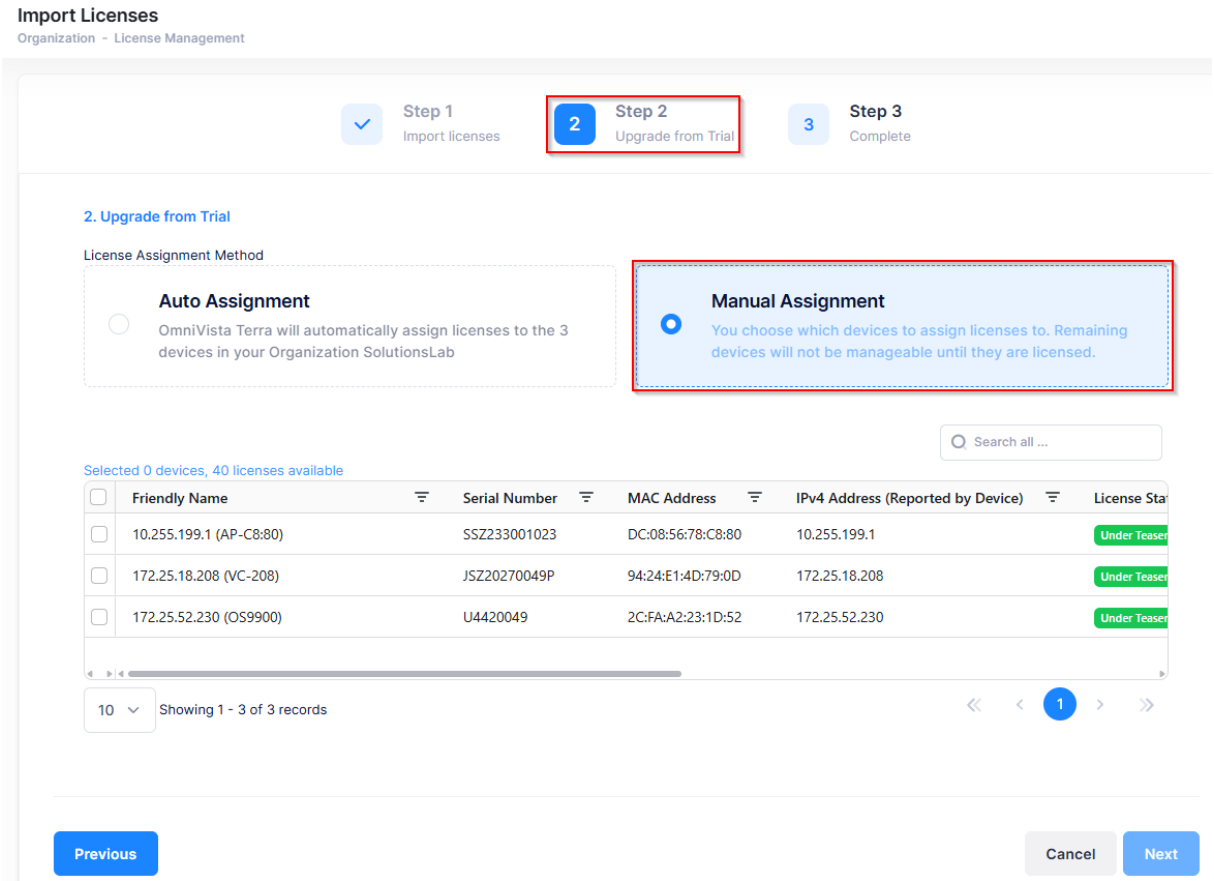


- If you set the automatic assignment status to “Yes” (enabled), a license is automatically assigned to a device when the device is added to the Device Catalog.

> ⚠ APs running in Express mode will lose their existing configuration when they get licensed and managed by OmniVista Terra.

- If you set the automatic assignment status to “No” (disabled by default), the device is added to the Device Catalog without a license until you manually assign a license to the device. See Using the Device Catalog (see page 164) online help for information about manually assigning or releasing device licenses.

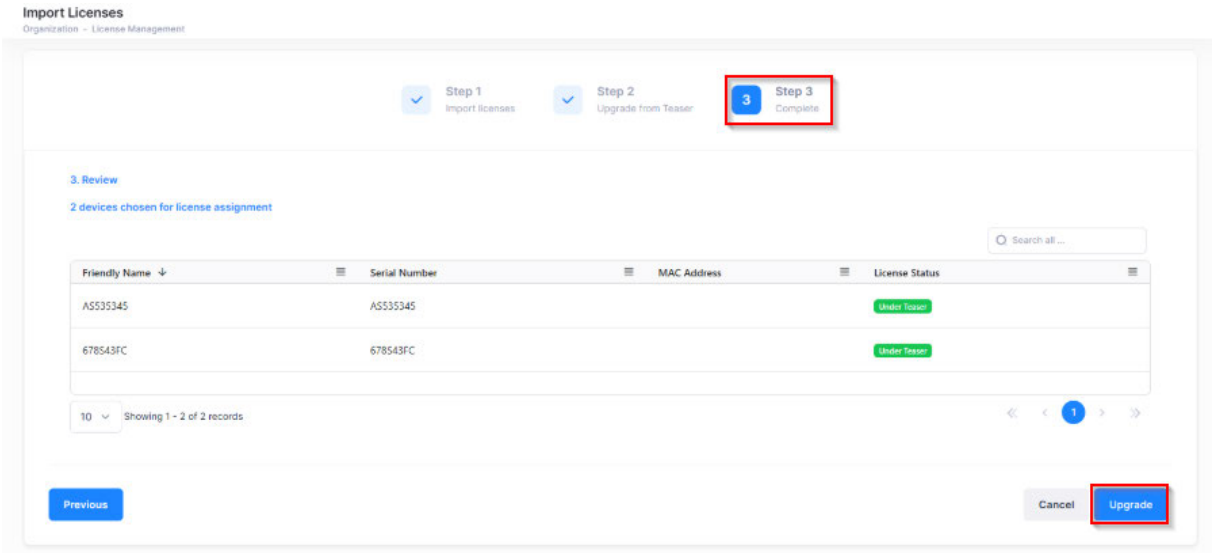
3.8.4.3.2.2 Manually Assign Device Licenses



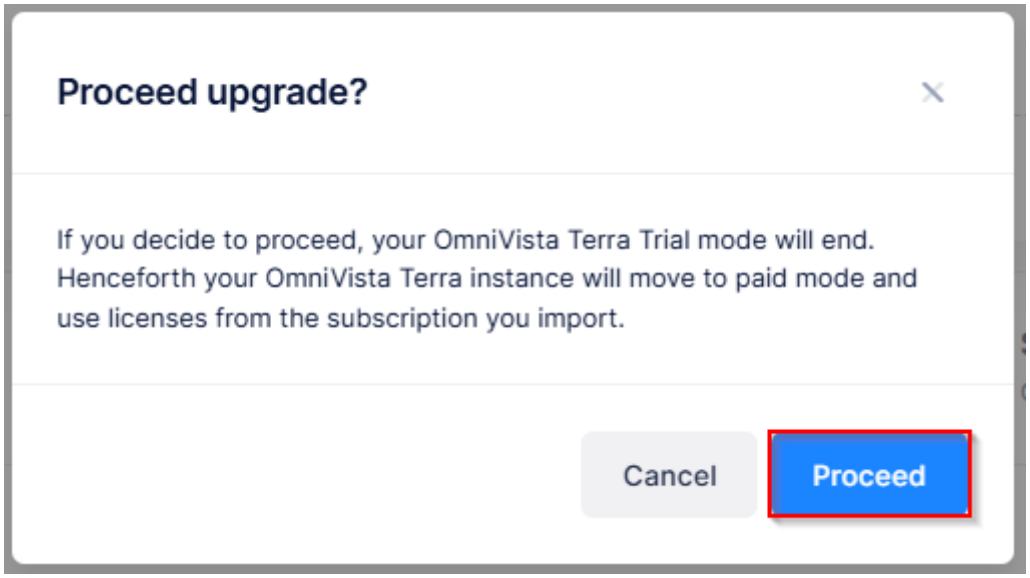
Once you have selected the License Assignment Method, click **Next** to proceed to the “Step 3 Complete” tab.

3.8.4.3.3 Step 3. Complete

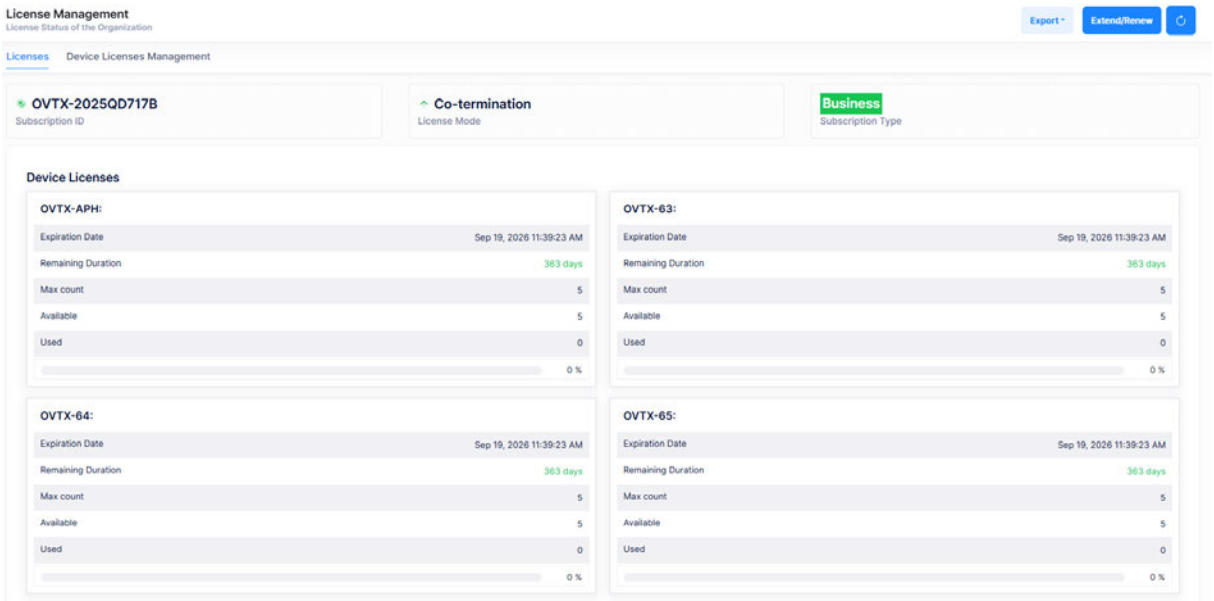
The Complete screen allows you to review the devices selected for license assignment.



Review the information on the screen, then click on **Upgrade** to proceed with upgrading from a Trial license to a paid licenses model (CAPEX Subscription) for your Organization. The following proceed to upgrade confirmation prompt appears:



Click on **Proceed** to upgrade to the paid subscription licenses. The paid CAPEX Subscription licenses are loaded into your Organization and are visible on the License Management screen.



3.8.4.3.4 Step 4. Export the Entitlement File

After the licenses for your Organization are loaded into OmniVista and assigned to your devices, you must then export an Entitlement File from the License Management screen. For example:

Click **Export**, select **Entitlement**, and choose a location on your computer to download the Entitlement File. Next, send the Entitlement File to your BP to upload into Service Manager.

You can now assign devices (see page 158) to the subscribed license to manage and configure devices.

21 Oct 2025

3.8.5 License Management Using a CAPEX Subscription

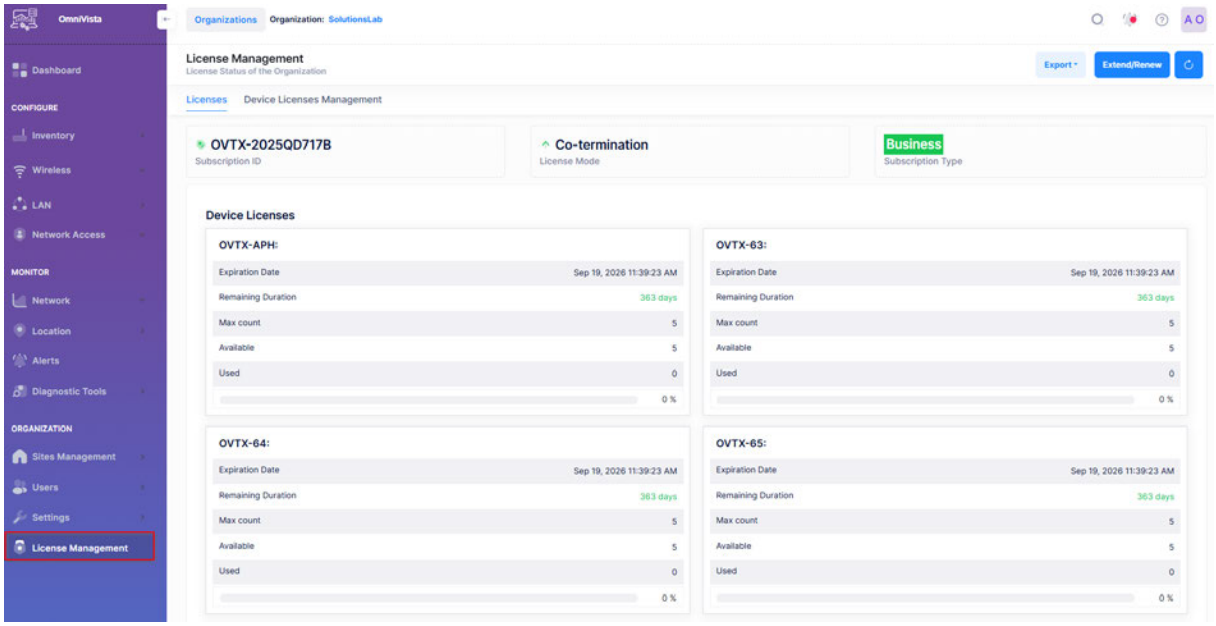
The License Management screen provides details about the Organization's OmniVista Terra License. Licensing depends on your purchased subscription, which allows you to manage up to the maximum number of devices permitted for the duration of the subscription contract.

> You have to obtain a paid license subscription from your Business Partner before you can import licenses for your Organization.

There are two ways to access the License Management screen for the current Organization:

- Click on the **License Status** shortcut located on the Organization Dashboard (see page 71).
- On the Organization Dashboard, click on the **License Management** option under the “Organization” section of the OmniVista Terra Menu (see page 45).

If you purchased a CAPEX Subscription for your Organization, the License Management screen displays the following device license information:



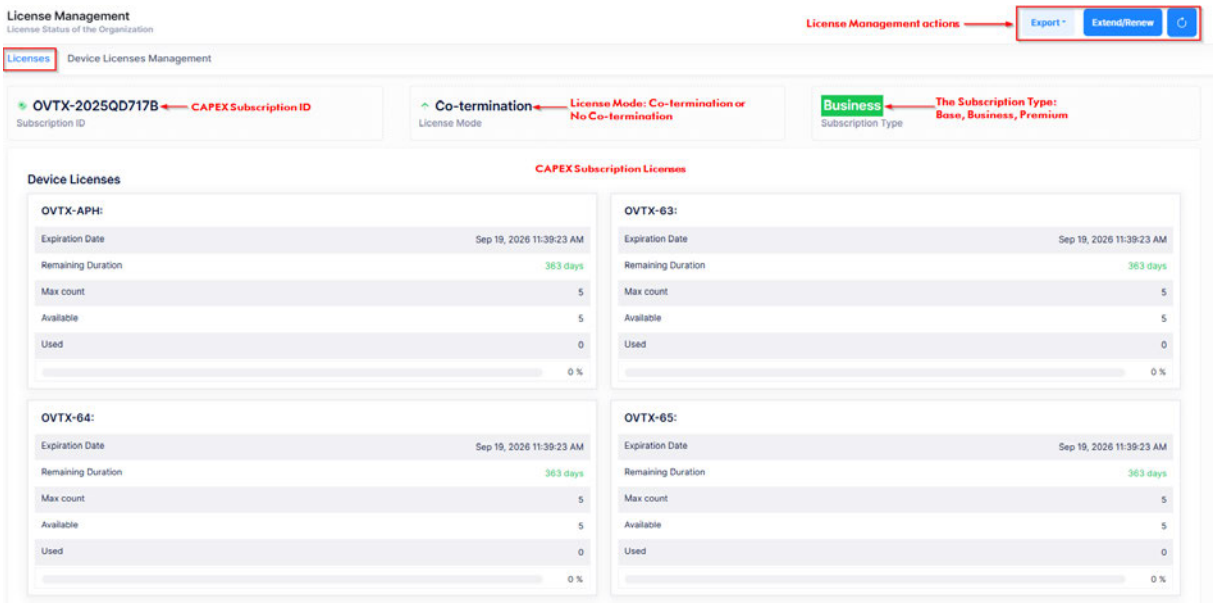
The License Management screen for the CAPEX Subscription model provides an overview of the licenses purchased and activated by the user, including the start and end dates for the license as well as the number of devices that can be managed with the current license.

There are two License Management screen tabs:

- Licenses (see page 159)- Provides an overview of the licenses purchased and activated by the user, including the end dates for the license as well as the number of devices that can be managed with the current license.
- Device License Management (see page 161) - Allows you to manage device licenses by assigning or releasing licenses. You also have the option to set up auto-assignment for licenses when creating a new device.

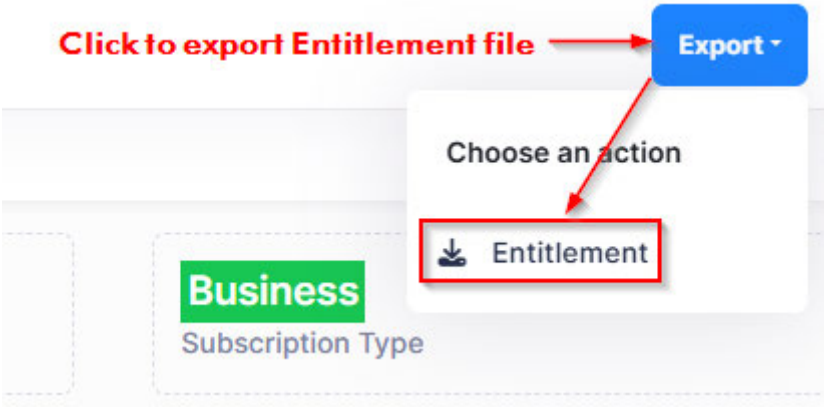
3.8.5.1 Licenses

The Licenses tab displays the licenses purchased for the CAPEX Subscription.

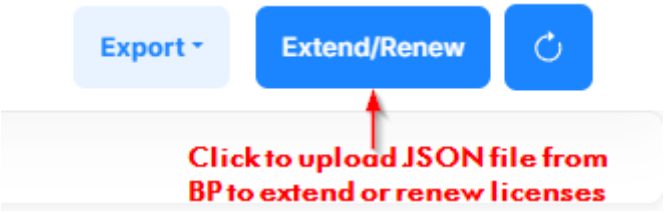


- The top section of the Licenses screen provides information about the purchased licenses:
  - **Subscription ID** - This is the CAPEX Subscription ID number you received in the licensing email.
  - **License Mode** - Whether the subscription is a Co-termination or No Co-termination license.
  - **Subscription Type** - The Service and Support bundle for the type of subscription.
    - **Base** - No service and Support bundle (Support Plus/AVR associated with the part)
    - **Business** - Business Service and Support bundle included (Business/Partner Plus level with AVR)
    - **Premium** - Premium/End customer level bundle included (Premium/End customer support with AVR)
- The bottom section of the Licenses screen displays the license categories included in the CAPEX Subscription. There are eight licensing categories based on the device model. Licenses not included in the subscription are grayed out to indicate they are unavailable.
  - OVTX-APL - Stellar AP Low End
  - OVTX-APH - Stellar AP High End
  - OVTX-63 - OS63 Series Switches
  - OVTX-64 - OS64 Series Switches
  - OVTX-65 - OS65 Series Switches
  - OVTX-68 - OS68 Series Switches
  - OVTX-69 - OS69 Series Switches
  - OVTX-99 – OS99 Series Switches
- The upper-right corner of the Licenses screen provides the following License Management actions:

- **Export** - After the CAPEX Subscription licenses are imported or additional licenses (add-ons) were purchased, click on **Export** to download an Entitlement File. This file identifies the devices assigned to the licenses for the CAPEX Subscription. Send the Entitlement File to your Business Partner, who will then upload the file into Subscription Manager to track and manage licenses for your Organization.



- **Extend/Renew** - If add-ons were purchased to extend or renew licenses, click on **Extend/Renew** to upload the Subscription File for the add-ons.



The following Extend/Renew window opens.

Upload the Subscription File (provided by your Business Partner) for the activated add-on licenses, then click on **Apply**. The Device Licenses display is updated with the information uploaded from the Subscription File.

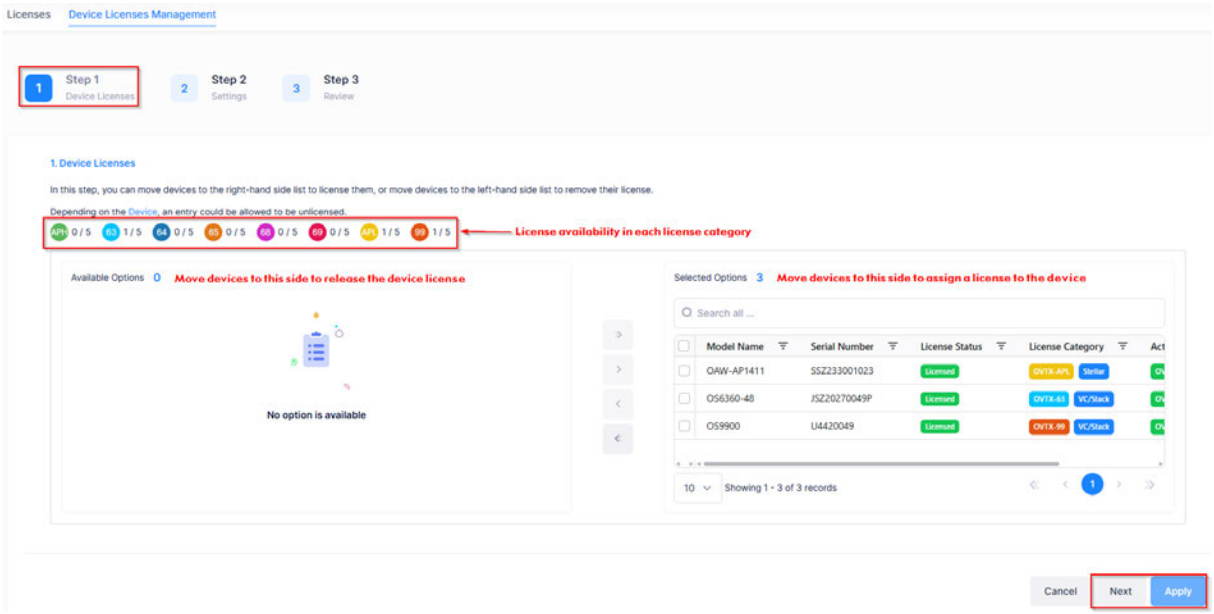
- **Refresh** - Update to the latest subscription information.

3.8.5.2 Device Licenses Management

The Device Licenses Management screen is used to manage device licenses. This includes assigning and releasing licenses for selected devices. When you click on the Device Licenses Management tab, the following steps are available for configuring and managing device license assignments.

3.8.5.2.1 Step 1. Device Licenses

The Device Licenses screen allows you to assign or release licenses for the selected device(s). This screen also provides information about how many licenses are available in each CAPEX license category.



- To assign a license to a device, move the selected device(s) from the left (Available Options) to the right side (Selected Options).
- To release a license from a device, move the selected device(s) from right side to the left side (Selected Options) to the left side (Available Options).

If any license assignment exceeds the assignment limit for the license category, a warning color appears to indicate which device licenses are violating the limit. This prevents you from assigning licenses for those devices until you resolve the licensing limit.

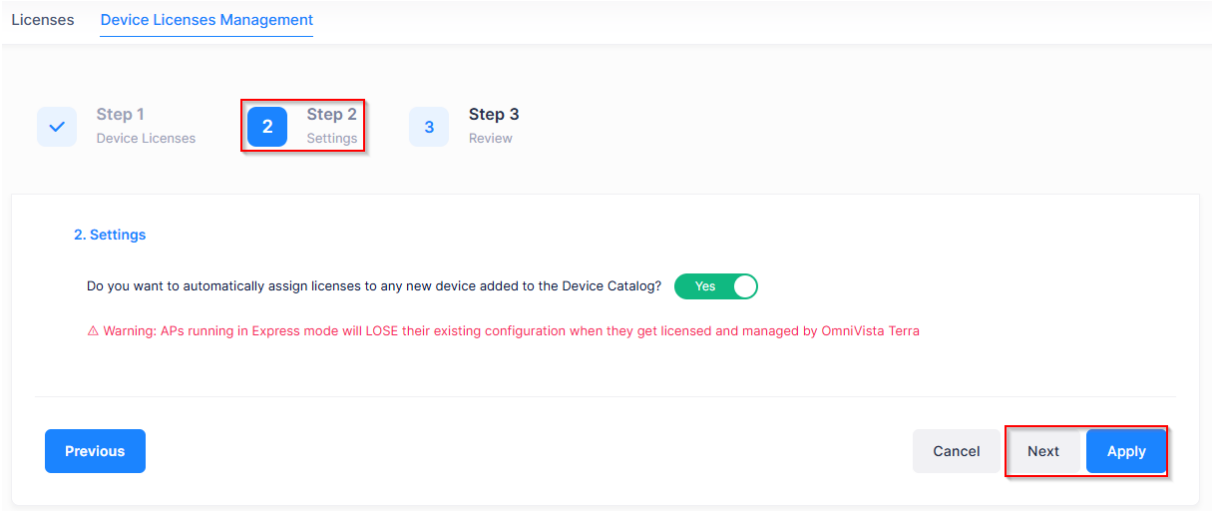
Once you have completed selecting devices for license assignment and/or for releasing a license, click **Apply** to apply licenses to the selected device(s) or click **Next** to go to “Step 2 Settings”.

Consider the following when releasing device licenses:

- When a device becomes unlicensed (license is released) or the license grace period ends, the unlicensed device is no longer manageable by OmniVista and the device activation status moves to “Register”. However, all the device data known to applications (such as Device Catalog, Topology, Network Analytics, etc.) is still retained by OmniVista and displayed in the UI.
- All known device data is only removed from the OmniVista UI when the device is deleted from the Device Catalog.
- When you release a license assignment from an AP device, the device does not immediately reboot to reset the AP Management Mode. Instead, The AP remains managed by OmniVista until the next call home (15 minutes by default), when the AP Management Mode is changed to Cluster. Once in Cluster mode, license assignment is required again for OmniVista to manage the AP.

3.8.5.2.2 Step 2. Settings

The Settings screen allows you to specify whether you want licenses automatically assigned to device(s) when the device is added to the Device Catalog.



- If you set the automatic assignment status to “Yes” (enabled), a license is automatically assigned to a device when the device is added to the Device Catalog.

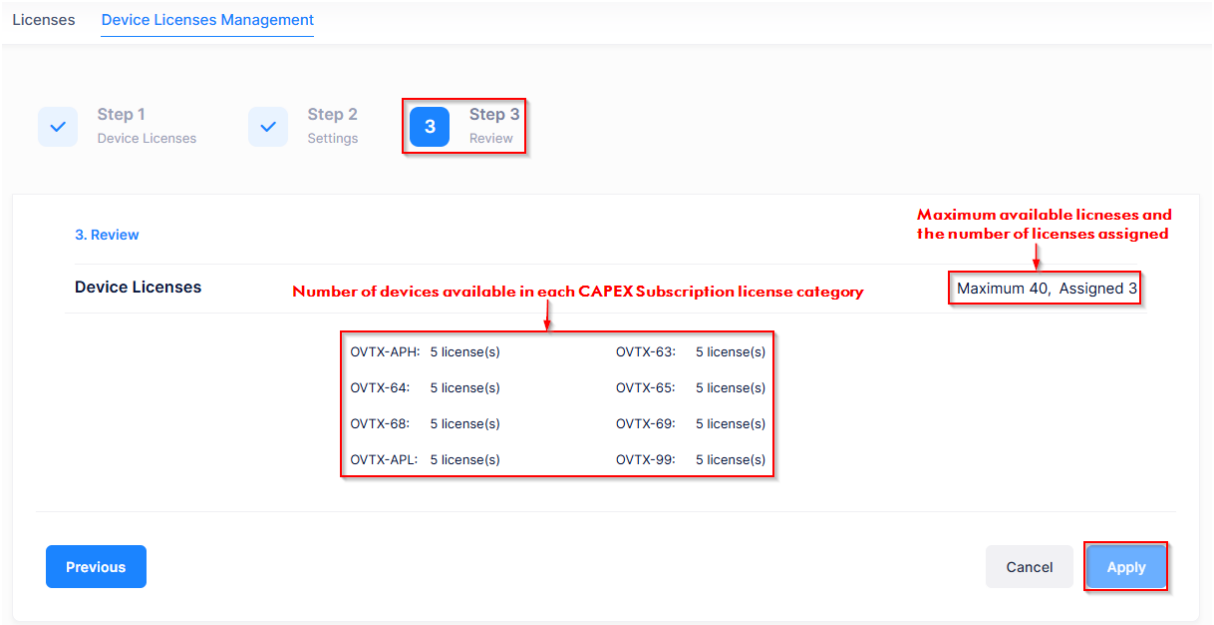
> ⚠ APs running in Express mode will lose their existing configuration when they get licensed and managed by OmniVista Terra.

- If you set the automatic assignment status to “No” (disabled by default), the device is added to the Device Catalog without a license until you manually assign a license to the device. See Using the Device Catalog (see page 164) online help for information about manually assigning or releasing device licenses.

Once you have set the status for automatic license assignment, click **Apply** to apply the status change or click **Next** to go to “Step 3 Review”.

3.8.5.2.3 Step 3. Review

The Review screen displays the maximum number for each license category and the number of licenses that will be assigned.



Click on **Apply** to complete the license configuration and management process.

21 Oct 2025

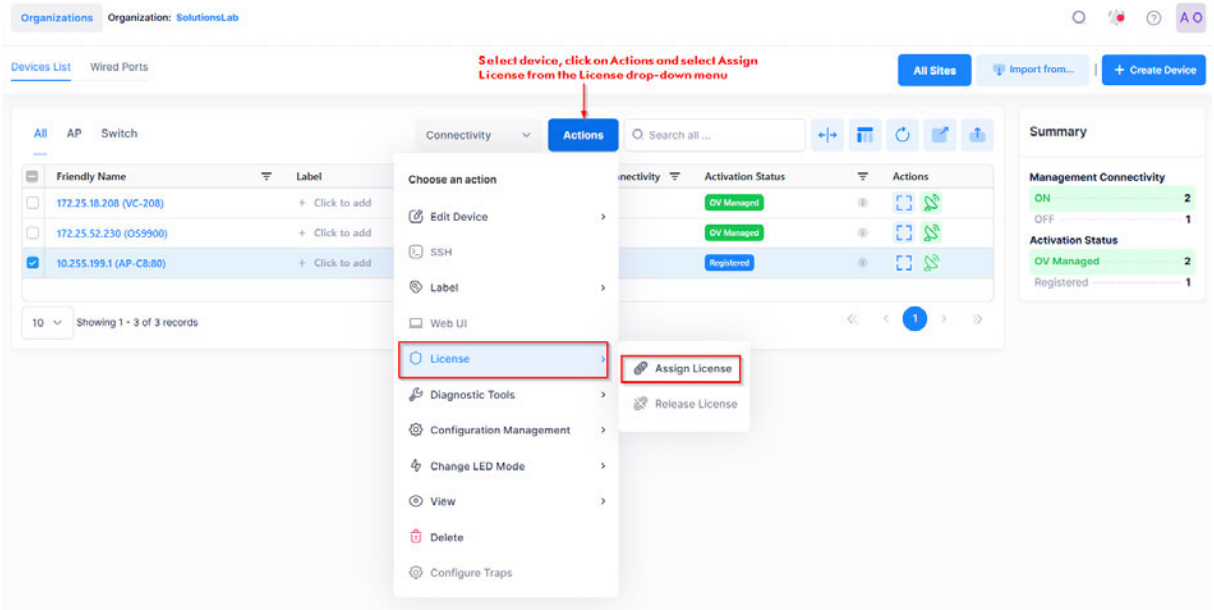
3.8.6 Using the Device Catalog to Manage Licenses

The Device Licenses Management (see page 158) tab allows you to specify whether or not licenses are automatically assigned to a device when the device is added to the Device Catalog. If automatic license assignment is disabled, you can manually bind the license to the device from the Device Catalog.

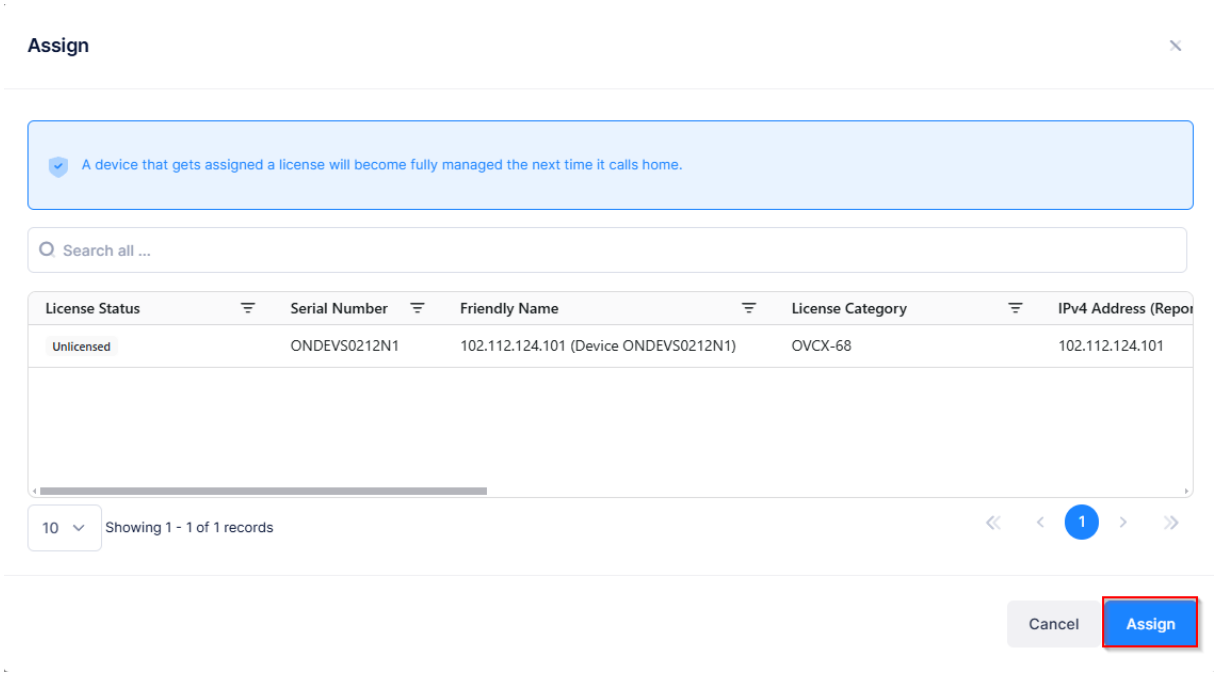
To access the Device Catalog, hover the mouse over **Inventory** under the “Configure” section of the OmniVista Terra Menu (see page 45), then click on **Device Catalog**. The Device List tab (see page 170) on the Device Catalog screen displays a list of devices known to OmniVista Terra. Use this screen to manually bind (assign) or unbind (release) device licenses. Note that you can only unbind device licenses that were manually assigned to the device.

3.8.6.1 Assign a License to a Device

To bind a license to a device, select the device(s) in the Device Catalog list, click on **Actions**, then select **License > Assign License** from the drop-down menu.

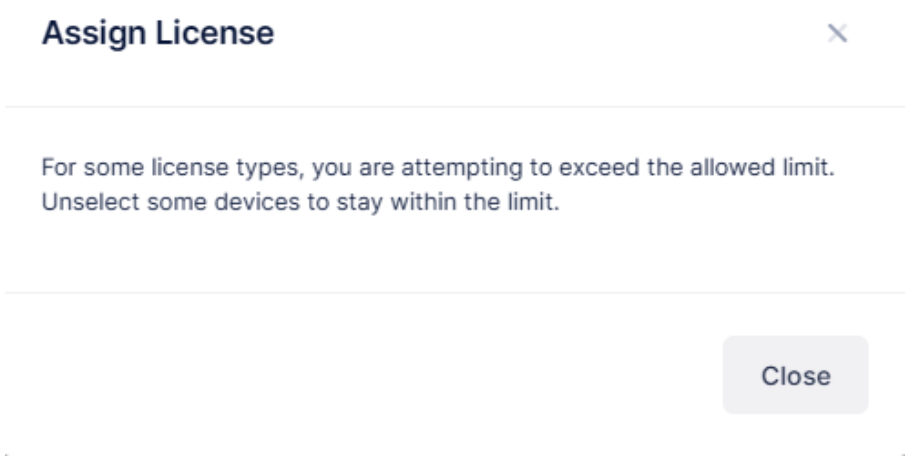


The Assign screen opens. Click on **Assign** to bind the license to the device(s).



For multiple license assignments, the device is bound to the license after the call home. Once the device is successfully bound to the license, it becomes fully managed during the next call home.

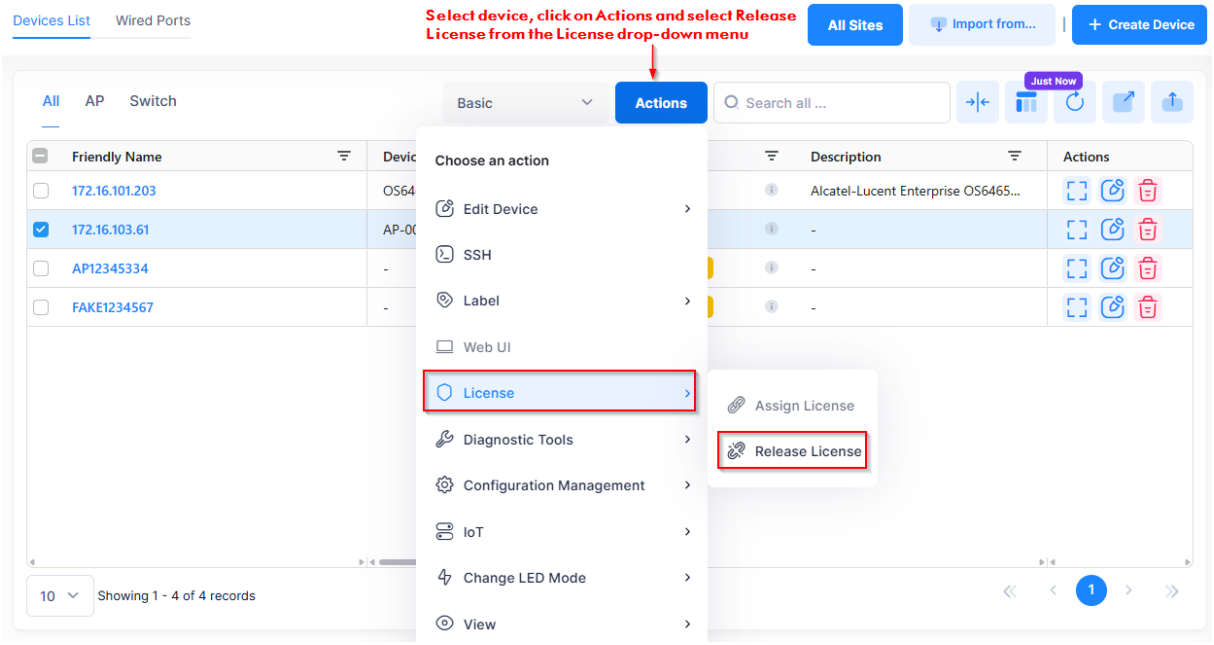
If the number of licenses has reached the limit for the license type, the following message appears:



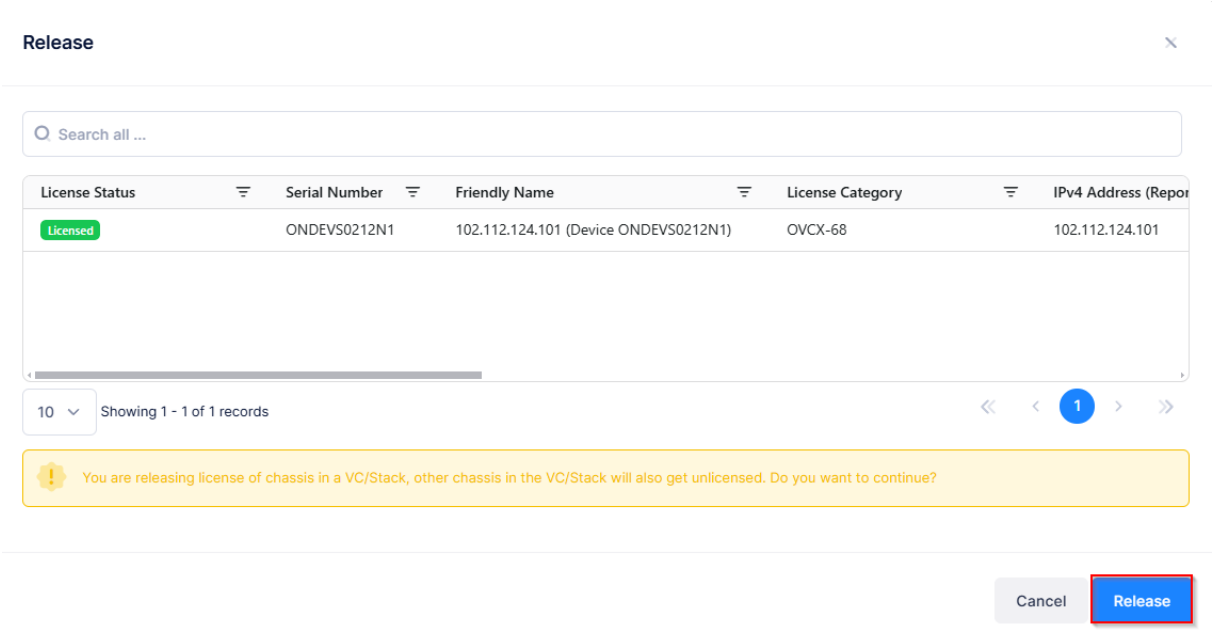
When the limit is reached, you can no longer assign licenses until you free up some licenses to stay within the limit.

3.8.6.2 Release License

To unbind a license from a device, select the device(s) from the Device List, click on **Actions**, then select **License > Release License** from the drop-down menu.



The Release screen opens. Click on **Release** to unbind the licenses from the device(s).



The license for the device is released.

Consider the following when releasing device licenses:

- When a device becomes unlicensed (license is released) or the license grace period ends, the unlicensed device is no longer manageable by OmniVista and the device activation status moves to “Register”. However, all the device data known to applications (such as Device Catalog, Topology, Network Analytics, etc.) is still retained by OmniVista and displayed in the UI.
- All known device data is only removed from the OmniVista UI when the device is deleted from the Device Catalog.

21 Oct 2025

4 Configure and Manage Device Inventory

The Inventory application is used to manage OmniVista Terra device inventory. This includes adding, editing, or deleting network devices from the inventory. To access the Inventory application, click on the **Inventory** option under the “Configure” section of the OmniVista Terra Menu (see page 45).

When you click on the **Inventory** option, the following list of applications are provided to assist with managing the inventory:

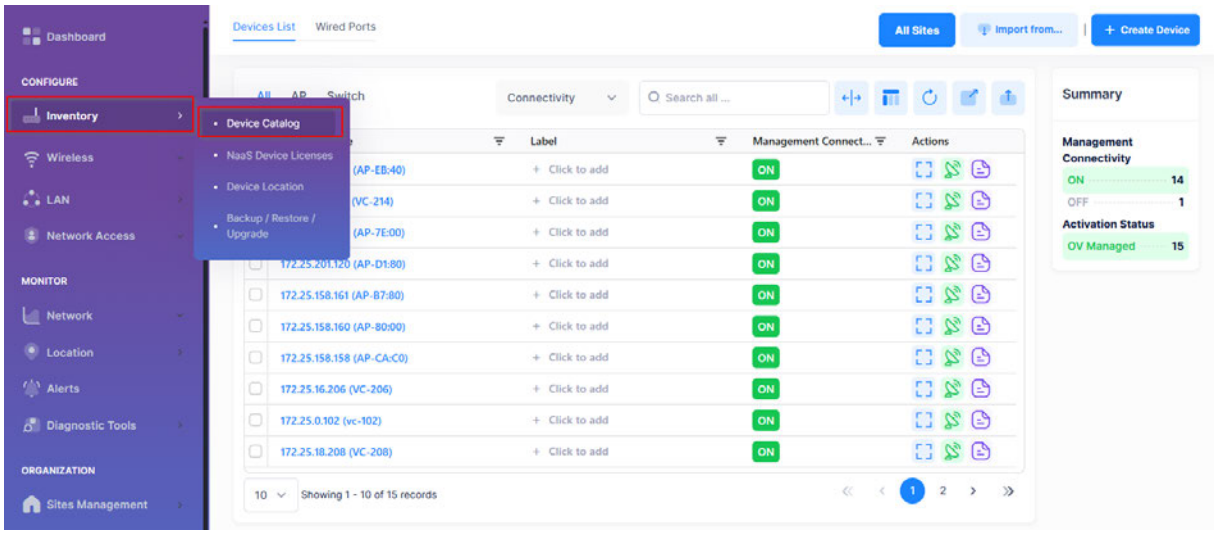
- Device Catalog (see page 169) - Used to add, edit, delete network devices to/from OmniVista Terra.
- NaaS Device Licenses (see page 262) - Displays the Network as a Service (NaaS) licensing information for managed network devices.
- Device Location (see page 271) - Manage where a network device is located on a floorplan for a specific building within an Organization Site.
- Scheduled Upgrades (see page 276) - Used to schedule automatic upgrades to specific network devices during specific time windows (e.g., non-business hours) to ensure minimal network disruption.
- Configuration Backups (see page 290) - Used to initiate and manage backups of switch configuration files.

21 Oct 2025

4.1 Device Catalog

The Inventory Device Catalog screen displays detailed information about all devices known to OmniVista Terra. This screen is also where devices are added, edited, or removed from the catalog list and are licensed for management. There are two ways to access the Device Catalog list:

- Click on the Devices shortcut located on the Organization Dashboard (see page 33).
- On the Organization Dashboard (see page 33), hover the mouse over **Inventory** under the "Configure" section of the OmniVista Terra Menu (see page 45), then click on **Device Catalog**.



> There are certain prerequisites (see page 9)that you must first verify and/or configure for devices to communicate with OmniVista Terra.

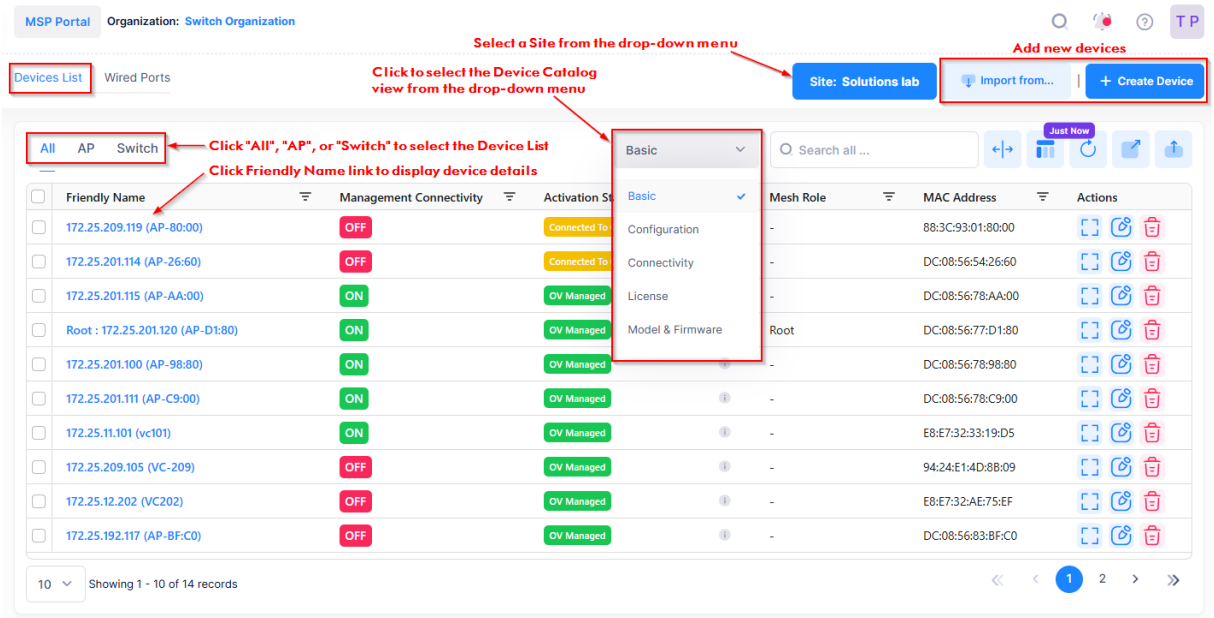
The Device Catalog provides the following screens that are used for device onboarding and management:

- **Device List** (see page 170) - Displays detailed device information, add/remove devices from the Device Catalog, edit device settings, and performs actions on specific devices.
- **Wired Ports** (see page 255) - Displays information about wired ports on network devices (APs/ Switches). You can also administratively enable or disable the port status from this screen.

21 Oct 2025

4.1.1 Using the Device List

The Device List tab on the Device Catalog (see page 169) screen displays a list of devices known to OmniVista.



There are three device lists available to view from this screen:

- **All** - Displays a list of all devices (Access Points and Switches).
- **AP** - Displays a list of Access Points.
- **Switch** - Displays a list of Switches.

By default, all devices are listed. Click on **All**, **AP**, or **Switch** to view the related device list.

From this screen, you can perform any of the following actions:

- Select the Device List view (see page 170).
- Display information about a specific device (see page 186).
- Add devices to the Device List. (see page 195)
- Edit device settings. (see page 217)
- Remove devices from the Device List. (see page 225)
- Perform additional device operations (see page 227).
- Display and configure the AP Mesh Configuration. (see page 238)
- Audit the OmniSwitch Running Configuration (see page 248)

4.1.1.1 Select the Device List View

The Device List provides the following dedicated views for Device List information:

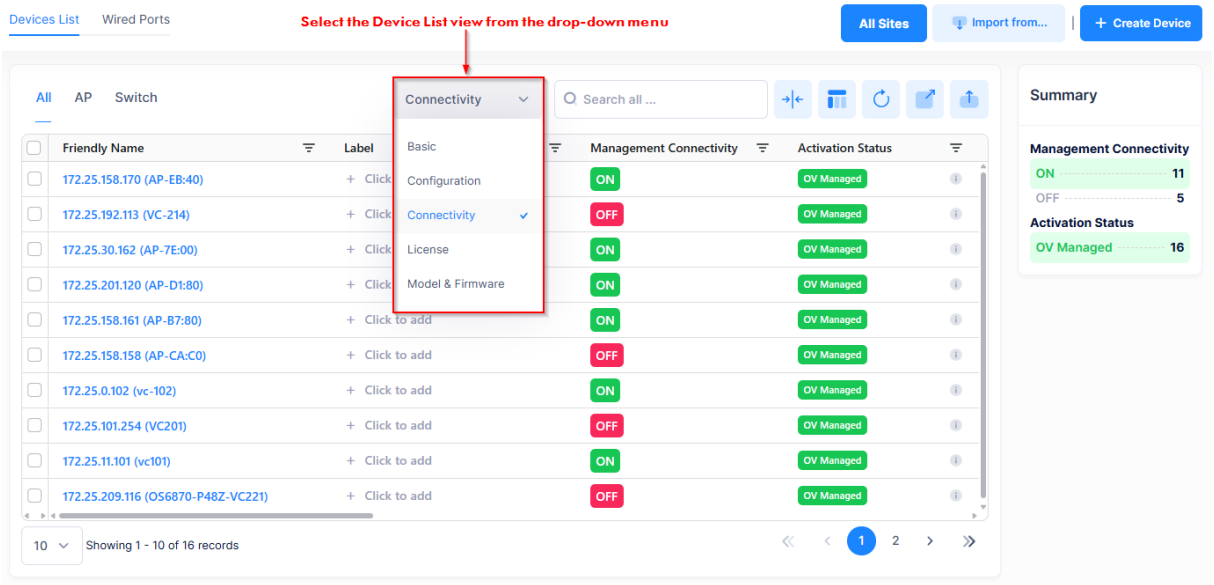
- **Basic** (see page 171)- Displays the overall configuration for each device.

- **Configuration** (see page 175)- Displays configuration information for your OmniSwitch devices and allows you to manage Golden Configuration settings and perform auditing functions.
- **Connectivity** (see page 179)- Displays specific management connectivity information for each device.
- **License** (see page 181)- Displays license information, such as license type and status, for each device.
- **Model & Firmware** (see page 183) - Displays the model number and firmware version for each device.

Each Device List view also displays a summary of statistics counters for analytics purposes. In addition, the icons provided under the “Actions” column vary based on the theme of the view.

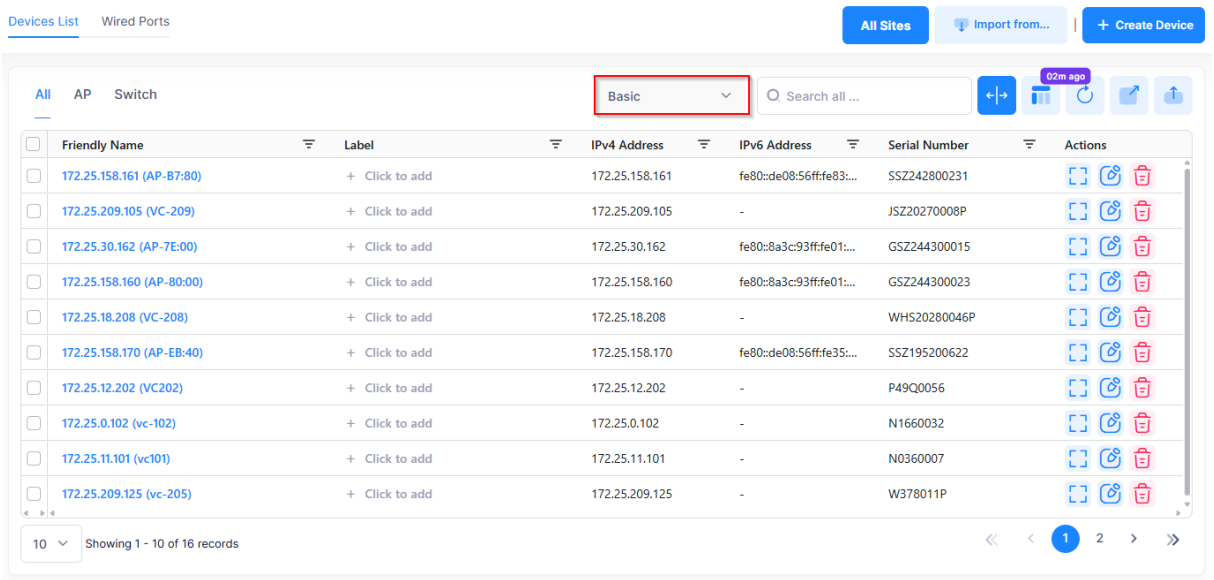
> The OmniVista polling interval is once an hour to collect switch information. If some information appears out of date, wait until the next polling interval.

By default, the Connectivity Device List view is displayed. To display a different view, select the Device List view you want to use from the drop-down menu.



4.1.1.1.1 Basic Device List View

The Basic Device List view offers field definitions (see page 172) and action icons (see page 175) that provide configuration details for devices in the Device Catalog.



The following Device List fields are displayed when you select the Basic view:

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Label** - The label(s) assigned to the device. See the online help for Assigning Device Labels.
- **IPv4 Address (Reported By the Device)** - The IP v4 address of the device.
- **IPv6 Address (Reported By the Device) -** The IP v6 address of the device.
- **Serial Number** - The Serial Number for the device.
- **MAC Address** - The device MAC address.
- **AP Work Mode** - The Access Point work mode:
  - **AP Basic -** Access Point is serving wireless clients
  - **Mesh Mode -** Access Point is working as a wireless mesh node.
  - **Bridge Mode -** Access Point is working as a wireless bridge node.
- **Mesh Role (AP only)** - The role of an Access Point that is operating in mesh mode (Root, Repeater).
- **Root AP Friendly Name** - Identifies the root AP for the mesh.
- **Last Seen -** Date and time Access Point activity was last seen by the OmniVista Terra Infrastructure.
- **Last Call Home Time** - The date and time the device last called home.
- **Management Connectivity** - The following management connectivity values indicate the various stages of device connectivity with OmniVista Terra.
  - **Blank** - The device is in an initial state (not yet onboarded).
  - **On** - When a device is successfully provisioned or OmniVista Terra receives heartbeat from the device, management connectivity transitions to “On”.
  - **Unknown** - If OmniVista Terra does not receive any heartbeat, the management connectivity status transitions from “On” to “Unknown”.

    - **Off** - After a certain amount of time with no heartbeat, the management connectivity status transitions from “Unknown” to “Off”.
- **Activation Status** - The real-time device activation/provisioning status for the device, if applicable (for example, Waiting for Validation, First Contact Pending, OV Managed).
- **Time to Next Call-Home** - The amount of time until the next call home.
- **Up Time** - The amount of time the device has been "Up" since the last time it was "Down" or rebooted.
- **Role During Activation** - The role of the device during activation (Master, Slave).
- **Approximate Time to Next Call-Home** - The approximate amount of time until the next call home.
- **Managed VPN IP** - The public WAN IP address through which the OpenVPN tunnel is established.
- **License Status** - Indicates the license type applied to the device: Licensed (CAPEX or Flexible Pay), Under Teaser (trial period license), Automatic Assigning (licensed is assigned when device calls home), or Unlicensed.
- **License Category** - The license that is assigned to the device based on the subscription model:
    - CAPEX Subscription Model - There are eight license categories that are assigned based on the device model. See Using the CAPEX Model (see page 158) online help for more information.
- **Device Licensed Mode** - The Device License mode of operation for the switch (NaaS, CAPEX, CAPEX Undecided). See the NaaS Device Licenses (see page 262) online help for more information.
- **AP Mgmt Mode**
    - **OVNG** - AP is managed by OmniVista Terra.
    - **Cluster** - AP was added to the Device Catalog, but is still in Cluster mode and is not being managed by OmniVista. You can move the device to OmniVista Terra by licensing (if necessary) and restarting the activation process on the device.
- **LED Mode (AP only)** - The LED Mode configured for the Access Point.
    - **Normal Mode** (Default) - The LED displays in normal mode (Red/Green/Blue).
    - **Night Mode** - The LED indicator is shut off.
    - **Blink Mode** - LED alternately blinks Red/Green/Blue so that you can visually locate the AP(s).
- **LACP Status (AP only)** - Indicates whether or not the Access Points supports link aggregation (Supported/Unsupported).
- **Link Status (AP only)** - The LACP link state (Up/Down).
- **Site Name** - The name of the site on which the device is declared.
- **IoT Status** - Indicates if IoT is enabled or disabled (the default) for the device. When enabled, OmniVista collects IoT information for endpoints connected to the device.
- **Building** - The name of the building in which the device is located.
- **Floor** - The name of the floor on which the device is located.
- **Device Name** - The name associated with the device. This field is not available when you are adding a device to the Device Catalog; however, you can edit the name once the device is fully

managed. Note that for switches, the device name displayed is the same name displayed with the **show system** CLI command.

- **Type** - The model number for the device.
- **Part Number** - The part number of the Access Point device or switch module/sub-module. Note that the “Part Number” field is displayed only in the Basic and Model & Firmware (see page 183) Device List Views.
- **Current Software Version** - The current software version for the device.
- **Upgrade Schedule (AP only)** - The name of the Scheduled Upgrade (see page 285) to which the device is assigned.
  - If a schedule is specified, the device is updated only during the time window of the schedule.
  - If this field is blank, the device is updated on the next call home.
- **Desired Software** - The "Desired Software Version" version configured for the device. The field will display the software version configured or "Do Not Upgrade".
- **Last Updated** - The date and time the device was last updated.
- **Location** - Where the device is physically located.
- **Geo-Location** - GPS Coordinates of the localized device.
- **System Contact** - Contact information for the device.
- **Description** - The description for the device. This field is configurable when adding an AP to the Device Catalog, but is not configurable when adding a switch to the Device Catalog. The description displayed for the switch is the same description displayed with the **show system** CLI command. In addition, you cannot edit the switch description through the OmniVista Terra UI.
- **Access Point Group (AP only)**- The name of the Access Point group to which the device belongs.
- **RF Profile (AP only)** - The Radio Frequency (RF) Profile that defines a wireless RF configuration for the Access Point.
- **BLE MAC (AP only)** - The MAC address for the AP beacon, if applicable.
- **Address (Switch only)** - The IP address of the Switch.
- **Activated Licenses (Switch only)** - The type of license available.
- **Running From (Switch only)** - Indicates whether the switch is running from the Certified directory or from the Working directory. The directory structure that stores the Switch image and configuration files in flash memory is divided into two parts:
  - The Certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory.
  - The Working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

- **VC Name (Switch only)** - If the Switch is participating in a Virtual Chassis (VC) configuration, this field displays the name of the VC configuration.
- **Changes** - Indicates the state of changes made to the device configuration. This field can display the following values:
  - **Certified -** Changes were saved to the working directory, and the working directory was copied to the certified directory. The working directory and the certified directory are thus identical.
  - **Uncertified -** Changes were saved to the working directory, but the working directory was not copied to the certified directory. The working directory and the certified directory are thus different.
  - **Unsaved -** Changes were made to the running configuration of the device, but the changes were not saved to the working directory. For Stellar APs, an unsaved configuration may not be an issue because when APs reboot, they always receive and build their configuration from OmniVista. Saving the configuration on Stellar APs is helpful if an AP reboots and OmniVista is not reachable. In this case, APs use the previously saved configuration.
  - **Blank -** When this field is blank, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Flash Synchronized Status (Switch only)** - Whether the Primary CMM's working directory is identical to the working directory on the other CMM module (if present).
  - **Synchronized -** The primary CMM's working directory is identical to the working directory on the secondary CMM. Note that if a switch is in Virtual Chassis (VC) mode, and it is VC of 1, the Synchronized Status is always "Synchronized".
  - **Not Synchronized -** The primary CMM's working directory is not identical to the working directory on the secondary CMM.
  - **Not Applicable -** Only one CMM module is installed.
  - **Unknown -** The synchronization state is unknown.

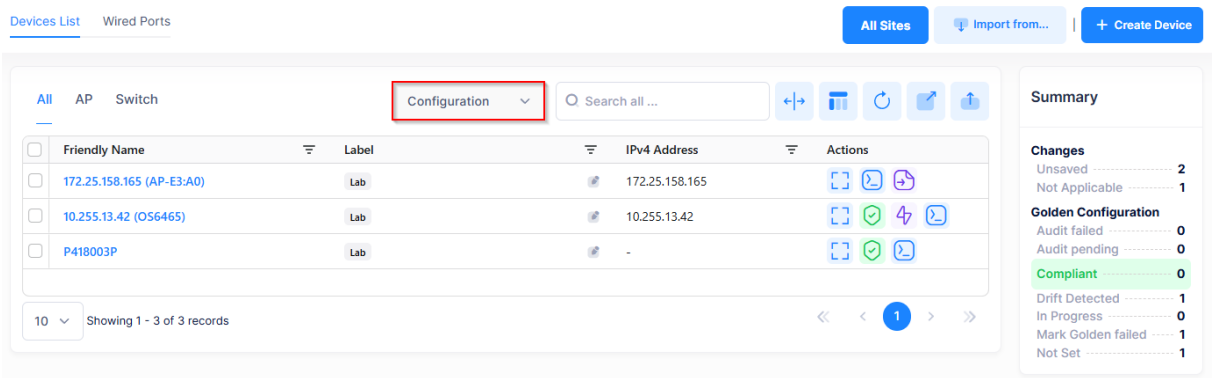
4.1.1.1.1.1 Actions Icons

The following icons are available under the “Actions” column in the Basic Device List view.

- **Additional Information** - Displays the Device Information screen (see page 186) for the specific device.
- **Edit** - Opens the Edit Device Information screen (see page 217) for the device that you want to edit.
- **Delete** - Delete the device (see page 225) from the Device List. When you delete the device, it is removed from the Device Catalog and no longer managed by OmniVista.

4.1.1.1.2 Configuration Device List View

The Configuration Device List view includes field definitions (see page 176), action icons (see page 177), and a Summary panel (see page 178) that you can use to manage Golden Configuration settings and perform auditing functions for devices in the Device Catalog. For information about how to use this view to audit the running configuration of a switch, see the Auditing the OmniSwitch Running Configuration (see page 248) online help.



The following Device List fields are displayed when you select the Configuration view:

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Label** - The label(s) assigned to the device. See the online help for Assigning Device Labels.
- **IPv4 Address (Reported By the Device)** - The IP v4 address of the device.
- **IPv6 Address (Reported By the Device) -** The IP v6 address of the device.
- **Changes** - Indicates the state of changes made to the device configuration. This field can display the following values:
  - **Certified -** Changes were saved to the working directory, and the working directory was copied to the certified directory. The working directory and the certified directory are thus identical.
  - **Uncertified -** Changes were saved to the working directory, but the working directory was not copied to the certified directory. The working directory and the certified directory are thus different.
  - **Unsaved -** Changes were made to the running configuration of the device, but the changes were not saved to the working directory. For Stellar APs, an unsaved configuration may not be an issue because when APs reboot, they always receive and build their configuration from OmniVista. Saving the configuration on Stellar APs is helpful if an AP reboots and OmniVista is not reachable. In this case, APs use the previously saved configuration.
  - **Blank -** When this field is blank, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Flash Synchronized Status (Switch only)** - Whether the Primary CMM's working directory is identical to the working directory on the other CMM module (if present).
  - **Synchronized -** The primary CMM's working directory is identical to the working directory on the secondary CMM. Note that if a switch is in Virtual Chassis (VC) mode, and it is VC of 1, the Synchronized Status is always "Synchronized".
  - **Not Synchronized -** The primary CMM's working directory is not identical to the working directory on the secondary CMM.
  - **Not Applicable -** Only one CMM module is installed.
  - **Unknown -** The synchronization state is unknown.

- **Running From (Switch only)** - Indicates whether the switch is running from the Certified directory or from the Working directory. The directory structure that stores the Switch image and configuration files in flash memory is divided into two parts:
  - The Certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory.
  - The Working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.
- **VC Name (Switch only)** - If the Switch is participating in a Virtual Chassis (VC) configuration, this field displays the name of the VC configuration.
- **Access Point Group** - The name of the Access Point group to which the device belongs.
- **RF Profile** - The Radio Frequency (RF) Profile that defines a wireless RF configuration for the Access Point.
- **Serial Number** - The Serial Number for the device.
- **MAC Address** - The device MAC address.
- **Golden Config** - The status of the Golden Configuration (for example, “Compliant”)
- **Last Audit At** - The date and time of the last device audit.
- **Audit Enabled** - Whether periodic auditing is enabled for the device.
- **Golden Marked At** - The date and time the running configuration was marked as golden.
- **Last Backup Created At** - The date and time of the last configuration backup.
- **Backup Version** - The software version that was backed up.
- **Schedule Backup Name** - The name of the scheduled backup (see page 290) associated with the device.
- **Next Execution** - The date and time of the next backup.

4.1.1.1.2.1 Action Icons

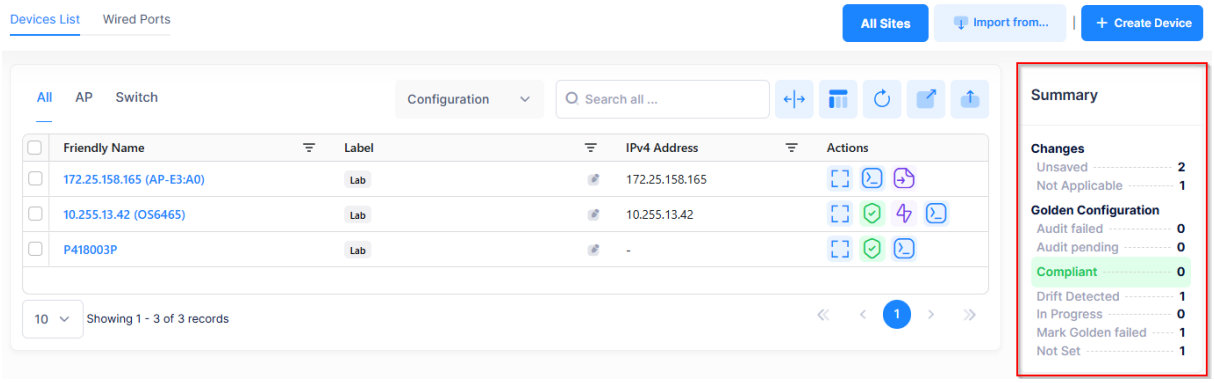
The following icons are available under the “Actions” column in the Configuration Device List view.

- **Additional Information** - Displays the Device Information screen (see page 187) for the specific device.
- **Mark as Golden Config** - Sets the current Running Configuration as the Golden Configuration (see page 248) for the switch.
- **Perform Audit** - Triggers an immediate audit.
- **Pause/Resume Periodic Audit -** Click to pause or resume the periodic audit. By default, a periodic audit is performed once a day.
- **SSH** - Opens up an SSH or Telnet session with the selected device on the Terminal screen.

- **Collect Support Info** - Collects log information from the device that you can then send to the Alcatel-Lucent Enterprise (ALE) team to troubleshoot problems. Note that his action icon is available only for Access Points.

4.1.1.1.2.2 Configuration View Summary

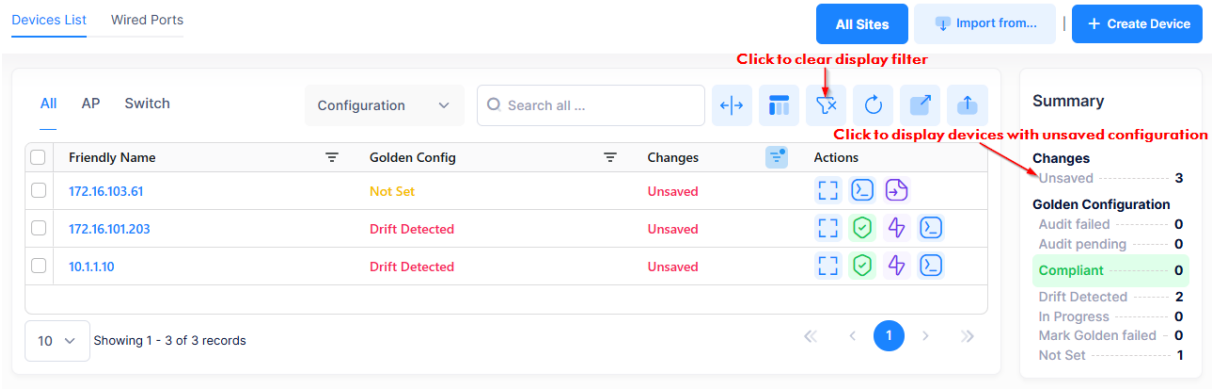
The Summary panel located on the right side of the Configuration view screen, provides statistics for the number of changes to the Running Configurations and the Golden Configuration statistics that are updated on the next automatic poll of the OmniSwitch.



Use this summary to analyze the following:

- **Changes** - Provides statistics for the number of changes to switch configurations.
  - **Certified** - The number of Running configurations that are saved to the Certified Directory on the switch.
  - **Unsaved** - The number of Running Configurations that are not saved.
  - **Uncertified** - The number of Running Configurations that are not saved to the Certified Directory on the switch.
  - **Not Applicable** - The number of devices that changes to the Running Configuration does not apply.
- **Golden Configuration (Master only)** - The Golden Configuration statistics for all of the switch configurations.
  - **Audit failed** - The number of configuration audits that failed.
  - **Audit pending** - The number of periodic configuration audits that are pending.
  - **Compliant** - The number of managed switches with a set Golden Configuration that does not differ from the Running Configuration per the last periodic audit.
  - **Drift detected** - The number of configurations where a difference was detected between the Golden Configuration and the Running Configuration. When a drift is detected, OmniVista raises an Alert.
  - **In Progress** - The number of Running Configurations where the marking as Golden is not yet completed.
  - **Mark Golden failed** - The number of configurations where the attempt to mark the Running Configuration as Golden failed.
  - **Not Set** - The number of configurations that do not have a Golden Configuration designated.

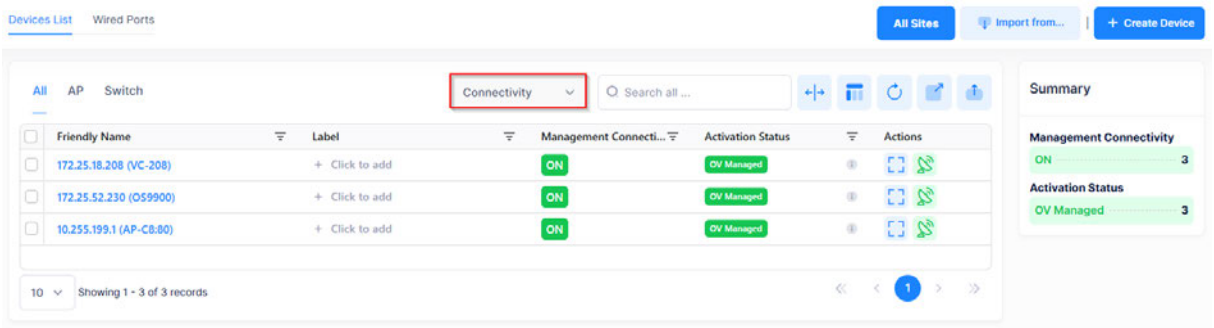
You can also use the Summary panel links to display only the devices included in the count. For example, if you click on **Unsaved** under “Changes”, the Device List displays only the devices with a Running Configuration that is not saved. To return to the full Device List display, click on the Clear Filters icon.



Refer to the Auditing the OmniSwitch Running Configuration (see page 248) online help for more information about setting a Golden Configuration and auditing the switch Running Configuration.

4.1.1.1.3 Connectivity Device List View

The Connectivity Device List view includes field definitions (see page 179), action icons (see page 180), and a Summary panel (see page 180) that provide information related to the status and health of devices in the Device Catalog.



The following Device List fields are displayed when you select the Connectivity view:

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Label** - The label(s) assigned to the device. See the online help for Assigning Device Labels.
- **Management Connectivity** - The following management connectivity values indicate the various stages of device connectivity with OmniVista Terra.
  - **Blank** - The device is in an initial state (not yet onboarded).

  - **On** - When a device is successfully provisioned or OmniVista Terra receives heartbeat from the device, management connectivity transitions to “On”.
  - **Unknown** - If OmniVista Terra does not receive any heartbeat, the management connectivity status transitions from “On” to “Unknown”.
  - **Off** - After a certain amount of time with no heartbeat, the management connectivity status transitions from “Unknown” to “Off”.
- **Activation Status** - The real-time device activation/provisioning status for the device, if applicable (for example, Waiting for Validation, First Contact Pending, OV Managed).
- **IPv4 Address (Reported By the Device)** - The IP v4 address of the device.
- **IPv6 Address (Reported By the Device) -** The IP v6 address of the device.
- **Last Seen -** Date and time Access Point activity was last seen by the OmniVista Infrastructure.
- **Last Call Home Time** - The date and time the device last called home.
- **Up Time** - The amount of time the device has been "Up" since the last time it was "Down" or rebooted.
- **Role During Activation** - The role of the device during activation (Master, Slave).
- **Approximate Time to Next Call-Home** - The approximate amount of time until the next call home.
- **Managed VPN IP** - The public WAN IP address through which the OpenVPN tunnel is established.

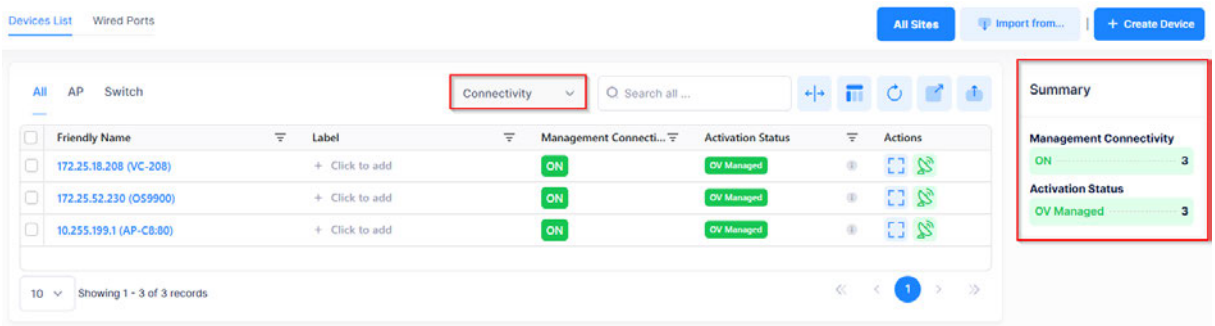
4.1.1.1.3.1 Actions Icons

The following icons are available under the “Actions” column in the Connectivity Device List view.

- **Additional Information** - Displays the Device Information screen (see page 186) for the specific device.
- **Ping** - Immediately pings the device (see page 227) to determine reachability and manageability. The “Management Connectivity” field for the device will reflect the results of the ping.

4.1.1.1.3.2 Connectivity View Summary

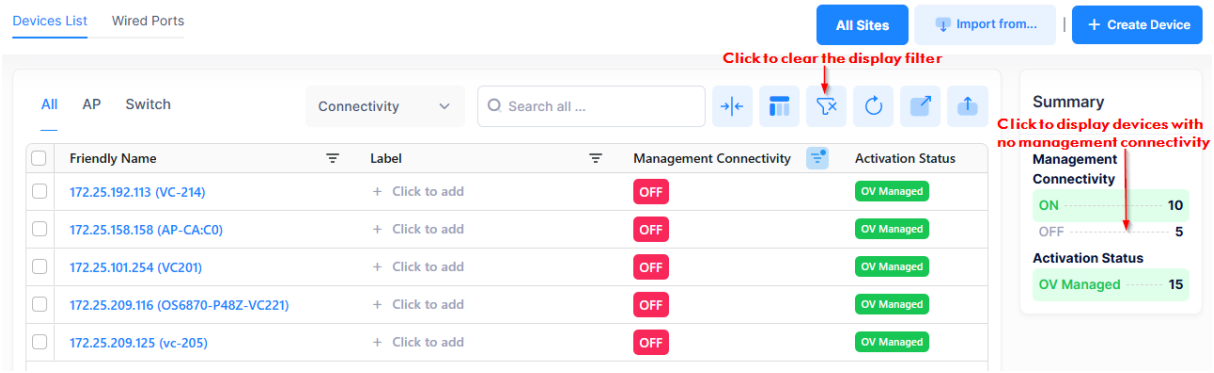
The Summary panel located on the right side of the Connectivity view screen, provides Management Connectivity and Activation Status statistics that are updated on the next automatic poll of the OmniSwitch.



Use this summary to analyze the following:

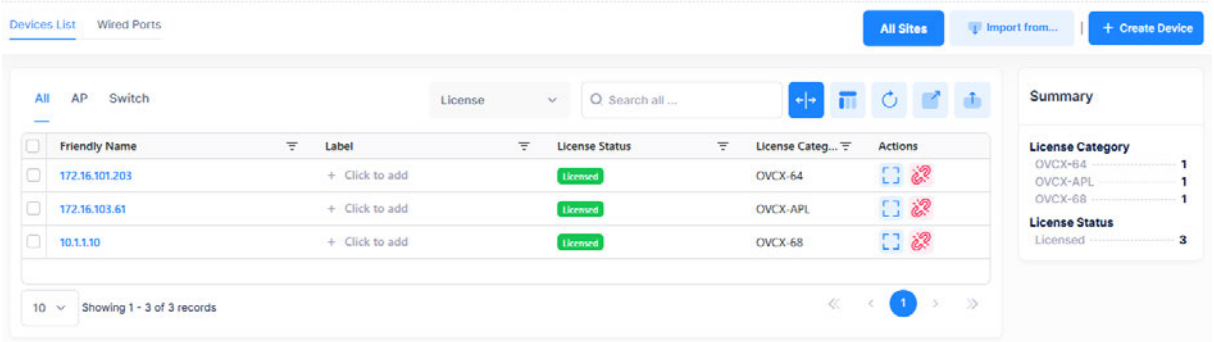
- **Management Connectivity**
  - **On** - The number of devices with device connectivity to OmniVista.
  - **Off** - The number of devices that do not have device connectivity with OmniVista.
- **Activation Status** - The number of devices that are “OV Managed”.

You can also use the Summary panel links to display only the devices included in the count. For example, if you click on **Off** under Management Connectivity, the Device List displays only those devices with no management connectivity to OmniVista. To return to the full Device List display, click on the Clear Filters icon.

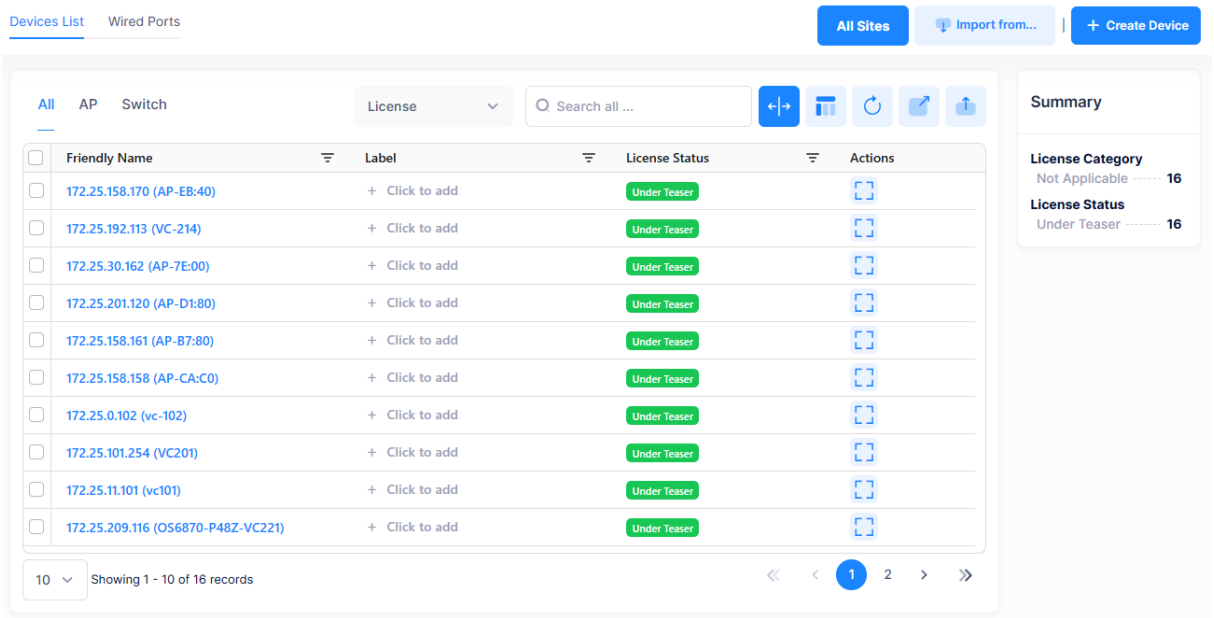


4.1.1.1.4 License Device List View

The License Device List view includes field definitions (see page 182), action icons (see page 182), and a Summary panel (see page 183) that provide the status of assigned device licenses in the Device Catalog.



If the Organization is using a Trial License, then the License Device List view displays all devices with “Teaser” as the License Type. For example:



The following Device List fields are displayed when you select the License view:

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Label** - The label(s) assigned to the device. See the online help for Assigning Device Labels.
- **License Status** - Indicates the type of licensed applied to the device: Licensed (CAPEX or Flexible Pay), Under Teaser (trial period license), Automatic Assigning (license is assigned when device calls home), or Unlicensed.
- **License Category** - The license that is assigned to the device based on the subscription model:
  - CAPEX Subscription Model - There are eight license categories that are assigned based on the device model. See Using the CAPEX Model (see page 158) online help for more information.
- **IPv4 Address (Reported By the Device)** - The IP v4 address of the device.
- **IPv6 Address (Reported By the Device) -** The IP v6 address of the device.
- **Serial Number** - The Serial Number for the device.
- **MAC Address** - The device MAC address.
- **Device Licensed Mode** - The Device License mode of operation for the switch (NaaS, CAPEX, CAPEX Undecided). See the NaaS Device Licenses (see page 262) online help for more information.
- **Number of Licenses Used** - The number of licenses used by the device.
- **Activated Licenses (Switch only)** - The type of license available.

4.1.1.1.4.1 Actions Icons

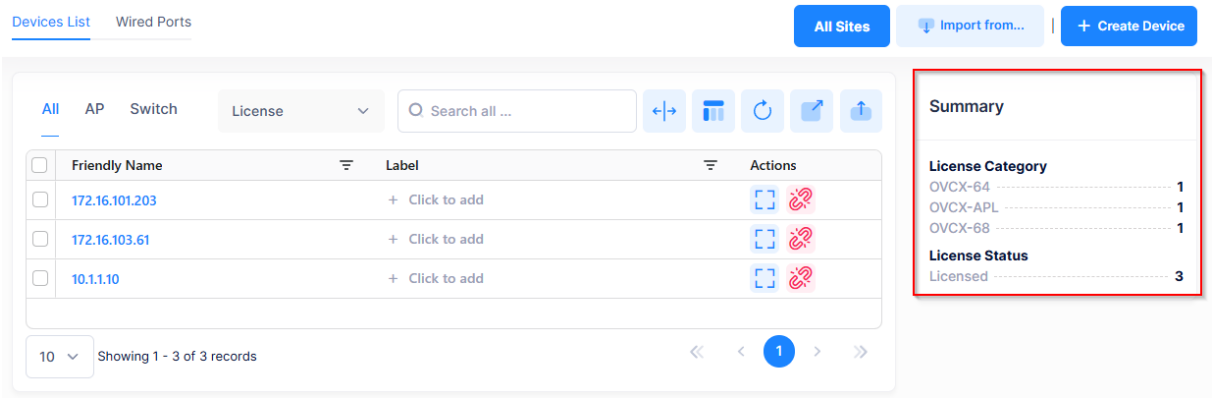
The following icons are available under the “Actions” column in the License Device List view.

- **Additional Information** - Displays the Device Information screen (see page 186) for the specific device.

- **Release/Assign License** - Assigns or unbinds a license (see page 164) from a device.

4.1.1.1.4.2 License View Summary

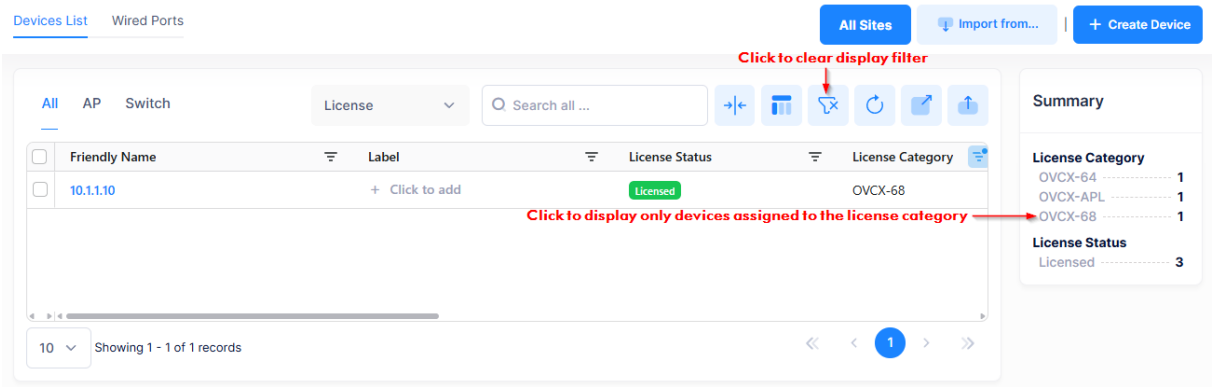
The Summary panel located on the right side of the License view screen displays the License Categories in use and the License Status. This information is updated on the next automatic poll of the OmniSwitch.



Use this summary to analyze the following:

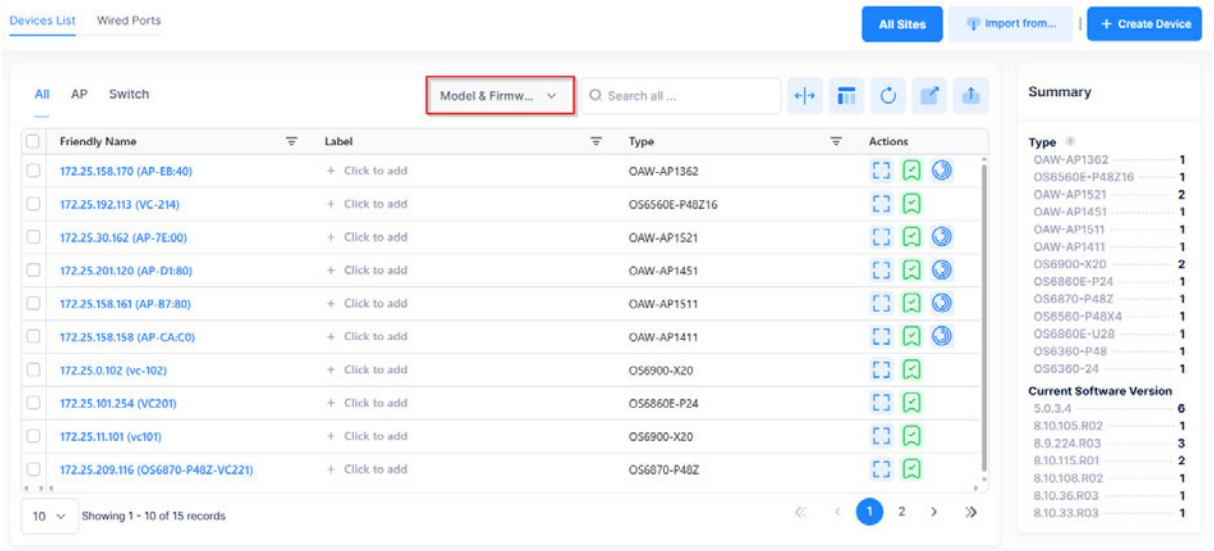
- **License Category** - The number of licenses assigned per each license category.
- **License Status** - The number of devices assigned to each type of license.

You can also use the Summary panel links to display only the devices included in the count. For example, if you click on a License Category link, the Device List displays only those devices assigned to that category. To return to the full Device List display, click on the Clear Filters icon.



4.1.1.1.5 Model & Firmware Device List View

The Model & Firmware Device List view includes field definitions (see page 184), action icons (see page 184), and a Summary panel (see page 185) that provide information about the model numbers and software versions for each device in the Device Catalog.



The following Device List fields are displayed when you select the Model & Firmware view:

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Label** - The label(s) assigned to the device. See the online help for Assigning Device Labels.
- **Type** - The model number for the device.
- **Current Software Version** - The current software version for the device.
- **IPv4 Address (Reported By the Device)** - The IP v4 address of the device.
- **IPv6 Address (Reported By the Device) -** The IP v6 address of the device.
- **Part Number** - The part number of the Access Point device or switch module/sub-module. Note that the “Part Number” field is displayed only in the Basic (see page 171)and Model & Firmware Device List views.
- **Upgrade Schedule (AP only)** - The name of the Scheduled Upgrade (see page 285) to which the device is assigned.
  - If a schedule is specified, the device is updated only during the time window of the schedule.
  - If this field is blank, the device is updated on the next call home.
- **Desired Software** - The "Desired Software Version" version configured for the device. The field will display the software version configured or "Do Not Upgrade".

4.1.1.1.5.1 Action Icons

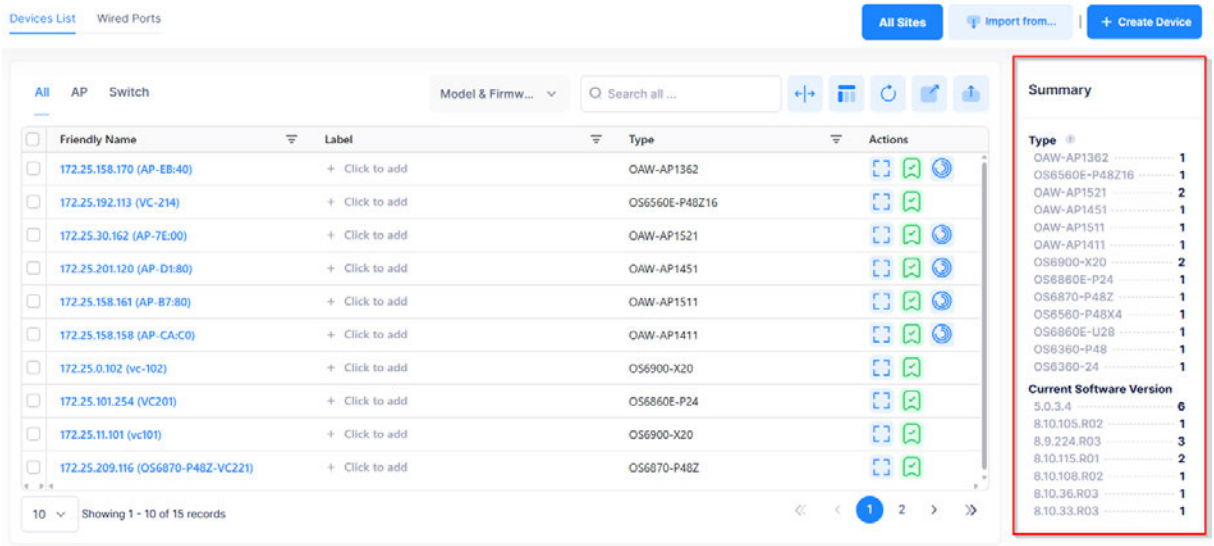
- **Additional Information** - Displays the Device Information screen (see page 186) for the specific device.
- **Set Desired Software Version** - Opens the Set Desired Software Version screen (see page 217) from which you can specify the software version that a device(s) will be update to on the next call home. This allows you to trigger an upgrade without waiting for a scheduled upgrade that is associated with the device.

- **Schedule Software Upgrade (AP only)** - Opens the Schedule Software Upgrade screen (see page 217) from which you can determine if the Access Point device is scheduled for a software update. You can also define or modify an upgrade schedule for the device.

4.1.1.1.5.2 Model & Firmware View Summary

The Summary panel located on the right side of the Model & Firmware view screen displays the number of device models and the current software versions. This information is updated on the next automatic poll of the OmniSwitch.

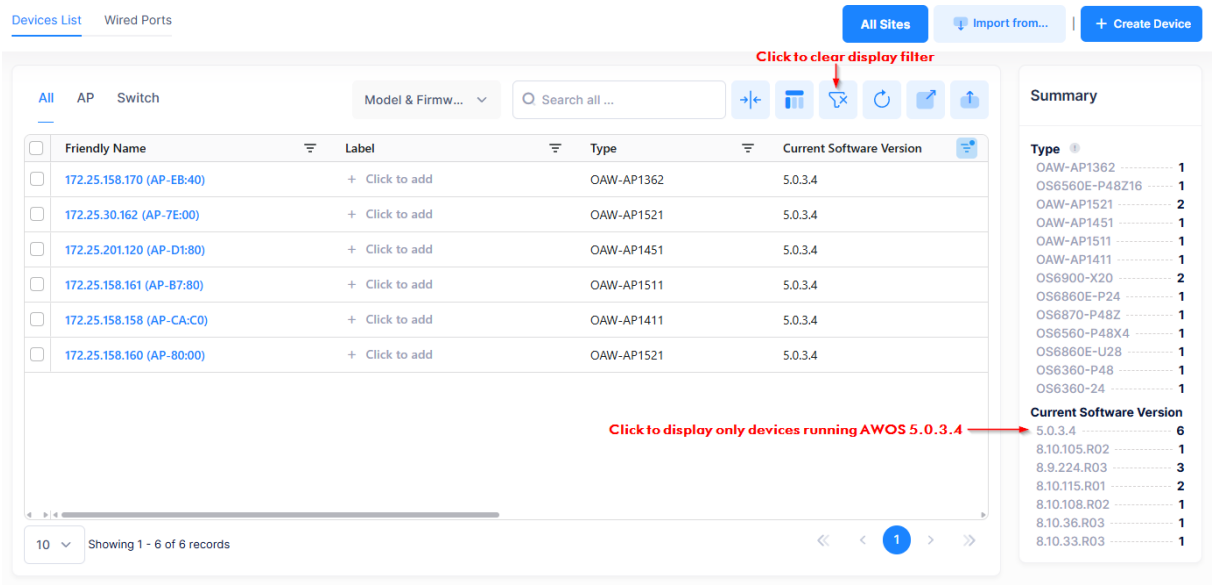
> Note that if a device model is highlighted in the “Type” list, it signifies that OmniVista may not provide complete support for that model. This could result in unpredictable behavior.



Use this summary to analyze the following:

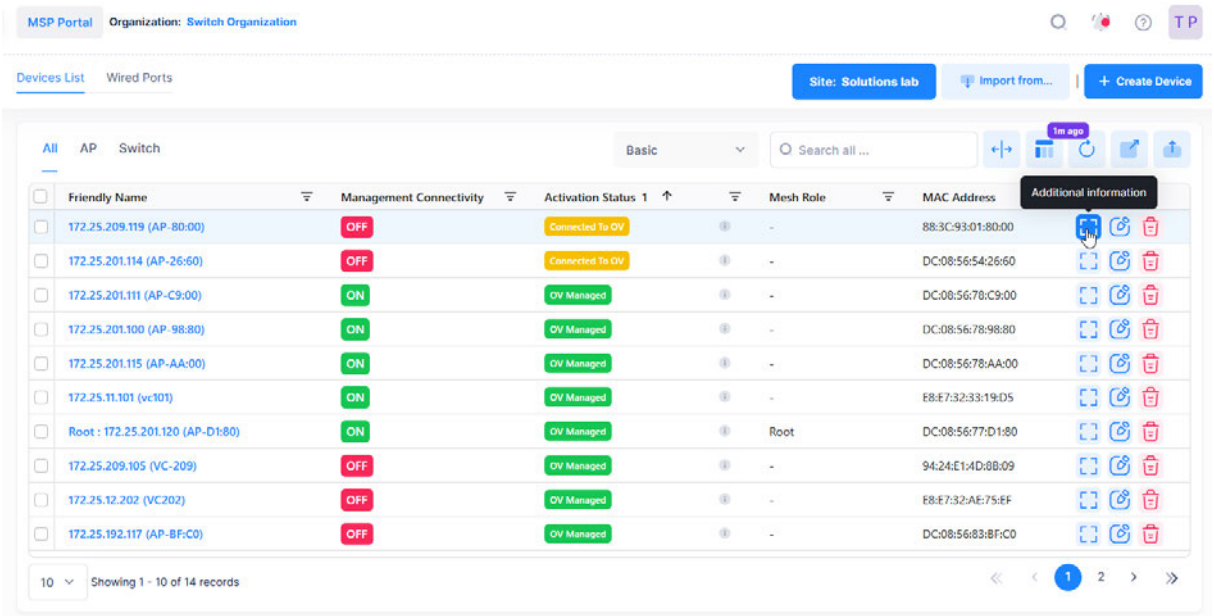
- **Type** - The number of each type of device model.
- **Current Software Version** - The number of devices running the listed software version.

You can also use the Summary panel links to display only the devices included in the count. For example, if you want to see all Access Points running AWOS 5.0.3.4, click on “5.0.3.4” under “Current Software Version”. To return to the full Device List display, click on the Clear Filters icon.



4.1.1.2 Display Information for a Specific Device

Click the Additional Information icon in the “Actions” column next to the Device List entry to display the Device Information screen. The information displayed on this screen is defined below.

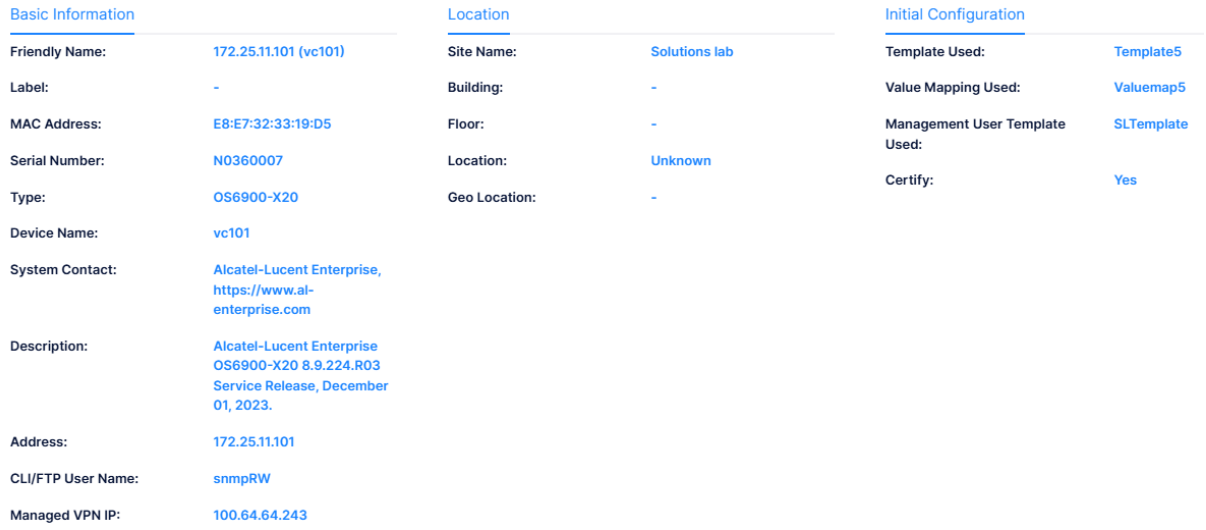


The following is displayed for each device:

- Basic Information (see page 187)
- Device Location (see page 188)
- Initial Configuration (Switch only) (see page 188)
- Software Version (see page 189)
- Device Status (see page 190)

- Device License (see page 191)
- Data VPN (see page 192)
- Other Information (see page 192)
- Switch Modules (see page 193)

4.1.1.2.1 Basic Information, Location, and Initial Configuration Information



Basic Information

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. By default, the Friendly Name is set to IP Address (System Name).
- **Label** - The label(s) assigned to the device. See the online help for Assigning Device Labels.
- **MAC Address** - The device MAC address.
- **IPv4 Address (Reported By the Device) (AP only)** - The IP v4 address of the AP device.
- **IPv6 Address (Reported By the Device) (AP only)) -** The IP v6 address of the AP device.
- **Serial Number** - The Serial Number for the device.
- **Type** - The model number for the device.
- **Device Name** - The name associated with the device. This field is not available when you are adding a device to the Device Catalog; however, you can edit the name once the device is fully managed. Note that for switches, the device name displayed is the same name displayed with the **show system** CLI command.
- **System Contact** - Contact information for the device.
- **Description** - The description for the device. This field is configurable when adding an AP to the Device Catalog, but is not configurable when adding a switch to the Device Catalog. The description displayed for the switch is the same description displayed with the **show system** CLI command. In addition, you cannot edit the switch description through the OmniVista Terra UI.
- **Address (Switch only)** - The IP address of the Switch.

- **CLI/FTP User Name (Switch only)** - The user name that OmniVista will use to establish CLI/FTP sessions with the managed devices. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored.
- **Access Point Group (AP only)**- The name of the Access Point group to which the device belongs.
- **RF Profile (AP only)** - The Radio Frequency (RF) Profile that defines a wireless RF configuration for the Access Point.
- **BLE MAC (AP only)** - The MAC address for the AP beacon, if applicable.
- **Managed VPN IP** - The public WAN IP address through which the OpenVPN tunnel is established.

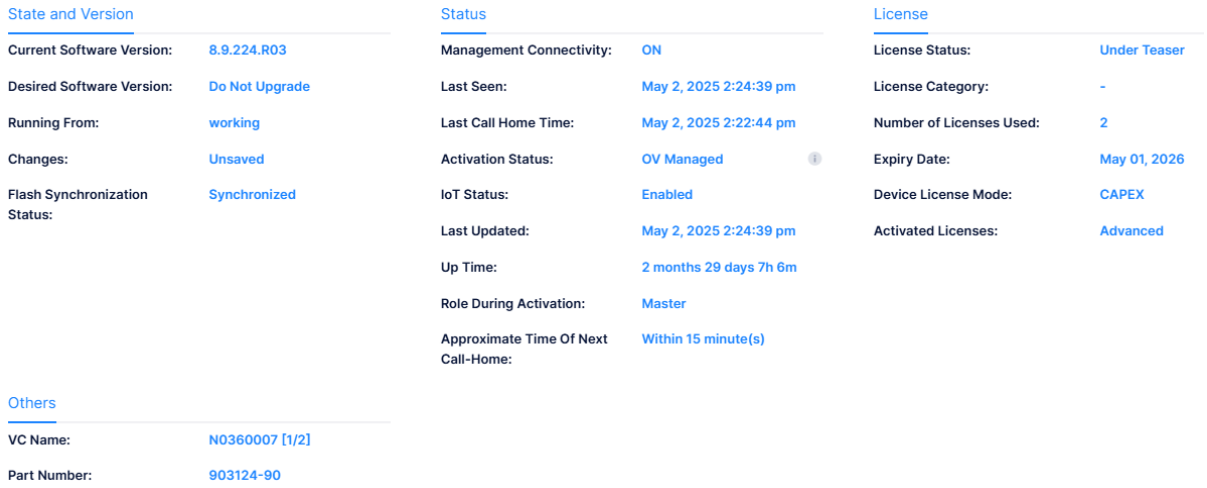
Location

- **Site Name** - The name of the site on which the device is declared.
- **Building** - The name of the building in which the device is located.
- **Floor** - The name of the floor on which the device is located.
- **Location** - Where the device is physically located.
- **Geo-Location** - GPS Coordinates of the localized device.

Initial Configuration (Switch only)

- **Template Used** - The name of the CLI-Based Provisioning Template that was used to push a configuration to the Switch during the onboarding process.
- **Value Mapping Used** - If the Provisioning Template contained variables, this field displays the name of the Value Mapping that is used to define the variables.
- **Management User Template Used** - The name of the Management User Template that contains the login credentials that OmniVista will use to connect with the Switch. The Default Management User Template credentials are used unless another template was specified.
- **Certify** - Indicates if the configuration was saved to the Certify directory on the Switch (Yes or No).

4.1.1.2.2 State and Version, Status, License, Data VPN, and Other Information



State and Version

- **Current Software Version** - The current software version for the device.
- **Desired Software** - The "Desired Software Version" version configured for the device. The field will display the software version configured or "Do Not Upgrade".
- **Running From (Switch only)** - Indicates whether the switch is running from the Certified directory or from the Working directory. The directory structure that stores the Switch image and configuration files in flash memory is divided into two parts:
  - The Certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory.
  - The Working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.
- **Changes** - Indicates the state of changes made to the device configuration. This field can display the following values:
  - **Certified -** Changes were saved to the working directory, and the working directory was copied to the certified directory. The working directory and the certified directory are thus identical.
  - **Uncertified -** Changes were saved to the working directory, but the working directory was not copied to the certified directory. The working directory and the certified directory are thus different.
  - **Unsaved -** Changes were made to the running configuration of the device, but the changes were not saved to the working directory. For Stellar APs, an unsaved configuration may not be an issue because when APs reboot, they always receive and build their configuration from OmniVista. Saving the configuration on Stellar APs is helpful if an AP reboots and OmniVista is not reachable. In this case, APs use the previously saved configuration.

  - **Blank -** When this field is blank, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.
- **Flash Synchronized Status (Switch only)** - Whether the Primary CMM's working directory is identical to the working directory on the other CMM module (if present).
  - **Synchronized -** The primary CMM's working directory is identical to the working directory on the secondary CMM. Note that if a switch is in Virtual Chassis (VC) mode, and it is VC of 1, the Synchronized Status is always "Synchronized".
  - **Not Synchronized -** The primary CMM's working directory is not identical to the working directory on the secondary CMM.
  - **Not Applicable -** Only one CMM module is installed.
  - **Unknown -** The synchronization state is unknown.

Status

- **Management Connectivity** - The following management connectivity values indicate the various stages of device connectivity with OmniVista.
  - **Blank** - The device is in an initial state (not yet onboarded).
  - **On** - When a device is successfully provisioned or OmniVista receives heartbeat from the device, management connectivity transitions to “On”.
  - **Unknown** - If OmniVista does not receive any heartbeat, the management connectivity status transitions from “On” to “Unknown”.
  - **Off** - After a certain amount of time with no heartbeat, the management connectivity status transitions from “Unknown” to “Off”.
- **Last Seen -** Date and time Access Point activity was last seen by the OmniVista Terra Infrastructure.
- **Last Call Home Time** - The date and time the device last called home.
- **LACP Status (AP only)** - Indicates whether or not the Access Points supports link aggregation (Supported/Unsupported).
- **Link Status (AP only)** - The LACP link state (Up/Down).
- **Activation Status**- The real-time device activation/provisioning status for the device, if applicable (for example, Waiting for Validation, First Contact Pending, OV Managed). Device Status error messages/failure states are detailed in the Troubleshooting (see page 210) section with explanations and possible solutions.
  - **First Contact Pending -** Device has been validated. OmniVista is waiting for the device to connect to it. Once the user connects the device to the network, the device will be ready for limited (unlicensed device) or full management (licensed device).
  - **Obtaining Certificate -** Device has contacted the OmniVista Server and the server is creating a digital certificate that is used in creating the secure VPN channel between your device and the OmniVista Server.
  - **Certificate Previously Issued -** A certificate was previously provided to this network device but it has contacted OmniVista without it.

- **Failed To Get Certificate -** Device has contacted the OmniVista Server and the server attempted to create a certificate to achieve a more secure communication but the attempt has failed.
- **Registered -** Device has successfully registered with OmniVista and is ready for limited management.
- **Upgrade -** Device software version will be or is being upgraded.
- **Upgrading -** Device is in the process of upgrading its software.
- **Upgrade Failed -** Device software version upgrade failed.
- **Assigned -** Device has contacted OmniVista and was found to be assigned to your account. The device is in the process of becoming fully managed.
- **VPN Configuring -** Device is in the process of configuring a secure transport channel for connecting to OmniVista.
- **Factory Reset Required -** The VPN profile was changed/updated. A Factory Reset is required on the device.
- **Connected to OV -** Device has connected to OmniVista over a secure transport channel and will proceed with provisioning, if required.
- **Provisioning -** Device is in the process of receiving configuration information from the Provisioning application, before it is ready for full management.
- **Provisioning Failed -** Device was unable to process the provisioning configuration sent by the Provisioning application, or OmniVista was unable to discover the device. See the Troubleshooting (see page 210) section for possible solutions to the problem.
- **OV Managed -** Device is ready for full management.
- **Unsupported Device Model -** OmniVista does not support the device.
- **PKI Update -** Indicates there are new Public Key Infrastructure (PKI) parameters available for the device on the next call-home. This can include one or more of the following:
  - New Device Private Key
  - New Device Public Key
  - New Device CSR
  - New Device Certificate
  - Updated CA Signing Chain.

- **IoT Status** - Indicates if IoT is enabled or disabled (the default) for the device. When enabled, OmniVista collects IoT information for endpoints connected to the device.
- **Last Updated** - The date and time the device was last updated.
- **Up Time** - The amount of time the device has been "Up" since the last time it was "Down" or rebooted.
- **Role During Activation** - The role of the device during activation (Master, Slave).
- **Approximate Time of Next Call-Home** - The approximate amount of time until the next call home.

License

- **License Status** - Indicates the license type applied to the device: Under Teaser (trial period license), Automatic Assigning (licensed is assigned when device calls home), or Unlicensed.
- **License Category** - The license that is assigned to the device based on the subscription model.
  - CAPEX Subscription Model - There are eight license categories that are assigned based on the device model. See Using the CAPEX Model (see page 164) Model
- **Number of Licenses Used** - The number of licenses used by the device.
- **Device Licensed Mode** - The Device License mode of operation for the switch (NaaS, CAPEX, CAPEX Undecided). See the NaaS Device Licenses (see page 262) online help for more information.
- **Activated Licenses (Switch only)** - The type of license available.

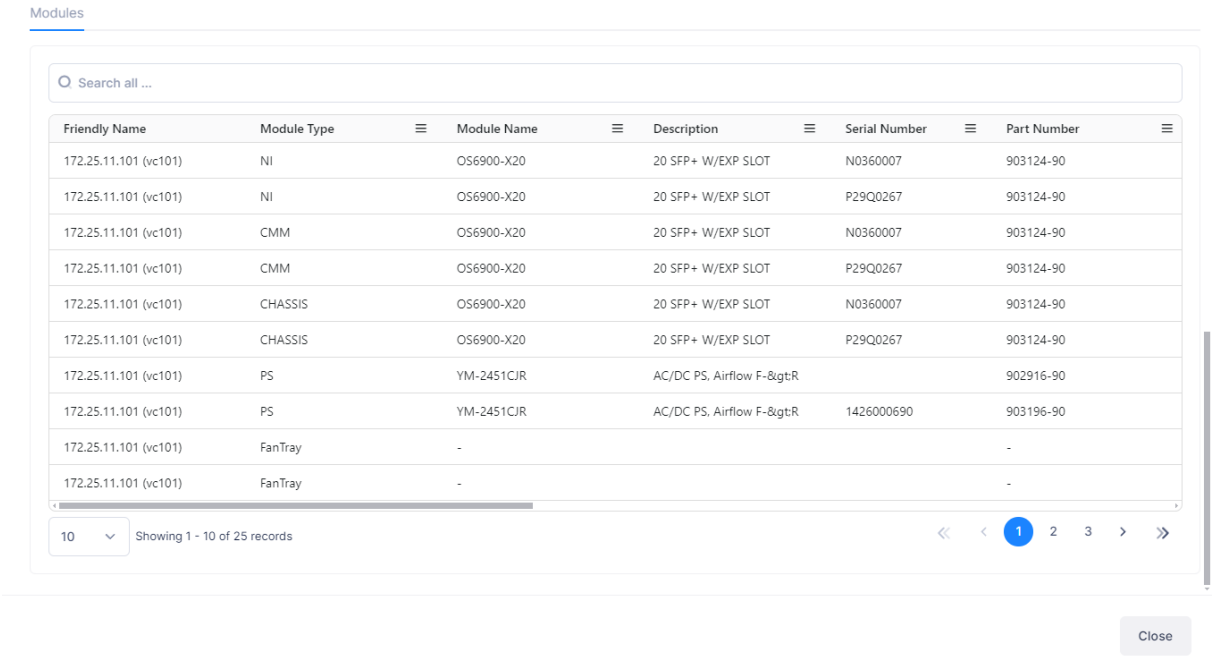
Data VPN Settings (AP only) - The name of the Data VPN Server Profile assigned to the AP. The Data VPN Server Profile defines VPN Server settings used by the AP to access remote functionality. The Data VPN Server Profile is assigned to a provisioning configuration (see page 451), which provides configuration information for the AP Group to which the AP belongs.

Others

- **AP Mgmt Mode**
  - **OVNG** - AP is managed by OmniVista Terra.
  - **Cluster** - AP was added to the Device Catalog, but is still in Cluster mode and is not managed by OmniVista. You can move the device to OmniVista Terra by licensing (if necessary) and restarting the activation process on the device.
- **LED Mode (AP only)** - The LED Mode configured for the Access Point.
  - **Normal Mode** (Default) - The LED displays in normal mode (Red/Green/Blue).
  - **Night Mode** - The LED indicator is shut off.
  - **Blink Mode** - LED alternately blinks Red/Green/Blue so that you can visually locate the AP(s).
- **AP Work Mode** - The Access Point work mode:
  - **AP Basic -** Access Point is serving wireless clients
  - **Mesh Mode -** Access Point is working as a wireless mesh node.
  - **Bridge Mode -** Access Point is working as a wireless bridge node.
- **Mesh Role (AP only)** - The role of an Access Point that is operating in mesh mode (Root, Repeater).
- **Upgrade Schedule (AP only)** - The name of the Scheduled Upgrade (see page 285) to which the device is assigned.
  - If a schedule is specified, the device is updated only during the time window of the schedule.
  - If this field is blank, the device is updated on the next call home.
- **VC Name (Switch only)** - If the Switch is participating in a Virtual Chassis (VC) configuration, this field displays the name of the VC configuration.
- **Part Number** - The part number of the Access Point device or switch module/sub-module.

4.1.1.2.3 Switch Modules

> The OmniVista polling interval is once an hour to collect switch module information. If some information appears out of date, wait until the next polling interval.



Modules (Switch only) - Provides the following detailed information about the switch modules:

- **Friendly Name -** A user-definable name for the device. If no name was configured, the IP address of the device is displayed.
- **Module Type -** The physical type of module or submodule in this physical location (e.g., Chassis, NI). Note that the value for this field displays as "Unknown" for a brief period while a newly-installed module or submodule is identified.
- **Module Name -** The manufacturer's name for the module (e.g. OS6850--C48, OS6850-BPS-PS).
- **Description -** The user-definable description of this particular module or submodule. The module description can be defined through SNMP.
- **Serial Number -** The serial number of the module or sub-module.
- **Part Number -** The part number of the module or sub-module.
- **MAC Address -** The base MAC address for the module or submodule. If not applicable, the field will be blank.
- **OS Version -** The OS version number running on the module. If not applicable, the field will be blank.
- **Uboot/Miniboot Version -** The U-Boot version running on the module. If not applicable, the field will be blank.
- **HW Revision -** The hardware revision number for the module. If not applicable, the field will be blank.

- **Firmware Version (FPGA) -** The version/revision level of the module or submodule firmware. If not applicable (e.g., Power Supply), the field will be blank or displays “0.0”.
- **Manufacturer Name -** The manufacturer of the module.
- **License -** Additional licenses (other than the Core License) active on the module (e.g., Advanced), if applicable.
- **Slot -** The slot in the chassis where the module resides. If not applicable, the field will be blank.

21 Oct 2025

4.1.1.3 Add Devices

To manage a device with OmniVista Terra, you must first add the device to the Device Catalog. After a device is added, the device is then validated by OmniVista. Once the device is validated and connected to your network, it is available for full management. An overview of the device catalog workflow is shown below (see page 195).

To add one or more devices to the Device Catalog list, use one of the following methods:

- Import Multiple Devices from an Excel Sheet (see page 197)
- Import Multiple Devices from an OmniVista CSV File (see page 200)
- Manually Add a Device in Full Management Mode (see page 203)

4.1.1.3.1 Device Catalog Workflow for Full Management

The following provides an overview of the basic process flow for adding/licensing devices:

1. Add a device to the Device Catalog.

2. OmniVista validates the device.

3. The device status changes to “First Contact Pending”. At this stage, the device has been validated and the OmniVista Server is waiting for the device to connect to it. Once the device is connected to the network, the device will be ready for licensing.

4. OmniVista licenses the device.

5. The device status changes to “OV Managed” and is now ready for full management.

> The device status is displayed in real time in the Activation Status (see page 170) column on the Device Catalog screen (see page 170). Note that a device may go through several intermediate steps (for example, Upgrading) before reaching a final step (for example, OV Managed).

4.1.1.3.2 Automatic Call Home Feature

Stellar Access Points and OmniSwitch devices support the Automatic Call Home Feature. These devices automatically contact OmniVista at regular intervals. For these devices, there is no need to manually start or restart the activation process. The devices will automatically contact OmniVista at the configured Call Home interval.

4.1.1.3.3 Starting the Activation Process on Devices

A device must connect to OmniVista to complete the activation process. If it is an **unconfigured** device (a new device, or an old device that has been reset to the factory default configuration), or a device that supports the Automatic Call Home Feature (see page 195), just connect the device to your network (see page 196). Otherwise, connect the device to your network (if necessary) and restart the activation process (see page 196) on the device.

4.1.1.3.3.1 Connecting Devices to Your Network

Connect the device to your network and power it on. The device will automatically contact the OmniVista Terra and complete the activation process, if the Network and Device Prerequisites (see page 8) are met. Refer to Onboarding Devices for OmniVista Terra Management (see page 13) for more details and requirements.

4.1.1.3.3.2 Restarting the Activation Process

If the device supports the Automatic Call Home Feature (see page 195), the device will automatically retry the activation process. Otherwise, use one of the following options to restart the activation process on the OmniSwitch or AP:

- **OmniSwitch** - Use one of the following options:
  - **Manually Reboot the Device -** Power on and power off the device.
  - **Restart the Cloud Agent on the Device -** Telnet to the device and disable the Cloud Agent using the following command: **cloud-agent admin-state disable force** (enter **y** at the confirmation prompt). Then enable the Cloud Agent using the following command: **cloud-agent admin-state enable**.
- **AP -** Use one of the following options:
  - **Manually Reset the AP -** Press the "Reset" button on the device until the LED starts flashing Red. When the light stops flashing or goes out, release the reset button.
  - **SSH to the AP and Reboot the AP -** SSH to the AP and execute "firstboot" and "reboot" commands.
  - **Use the Express UI -** If the AP Work Mode column on the Device Catalog Screen displays "Cluster", go to the Express UI, select the device(s) you want to add to OmniVista and click on the **Connect to OmniVista** button.

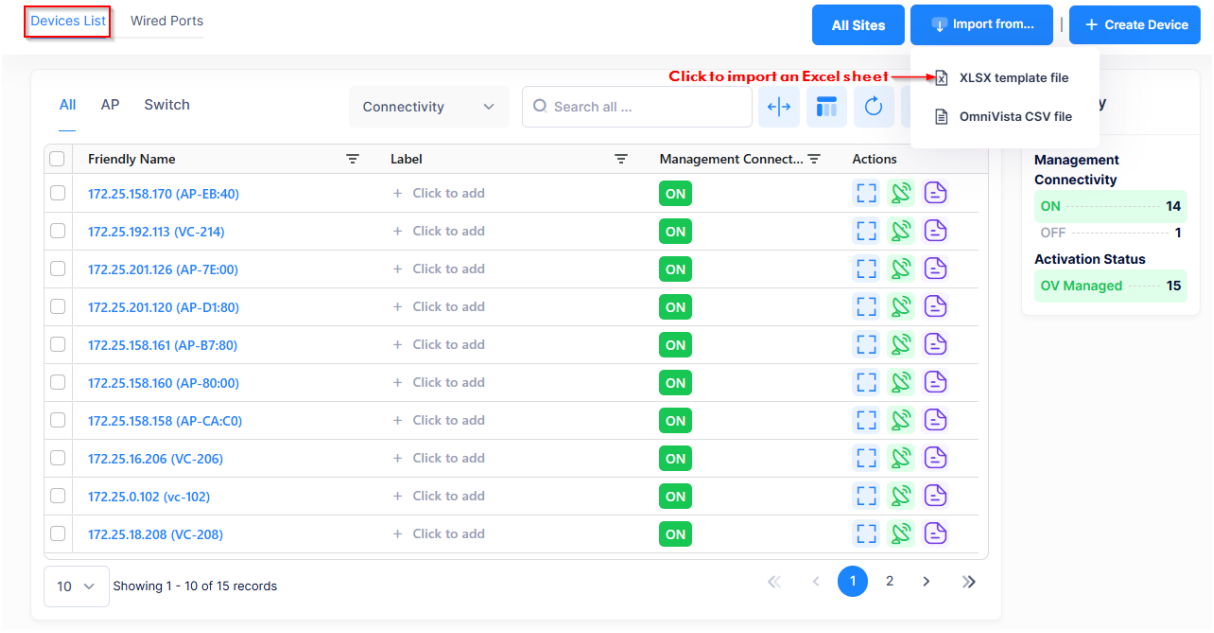
When the activation process completes, the Activation Status (see page 170) column will display "OV Managed". If you have trouble activating devices, click here (see page 210) for common problems and troubleshooting tips.

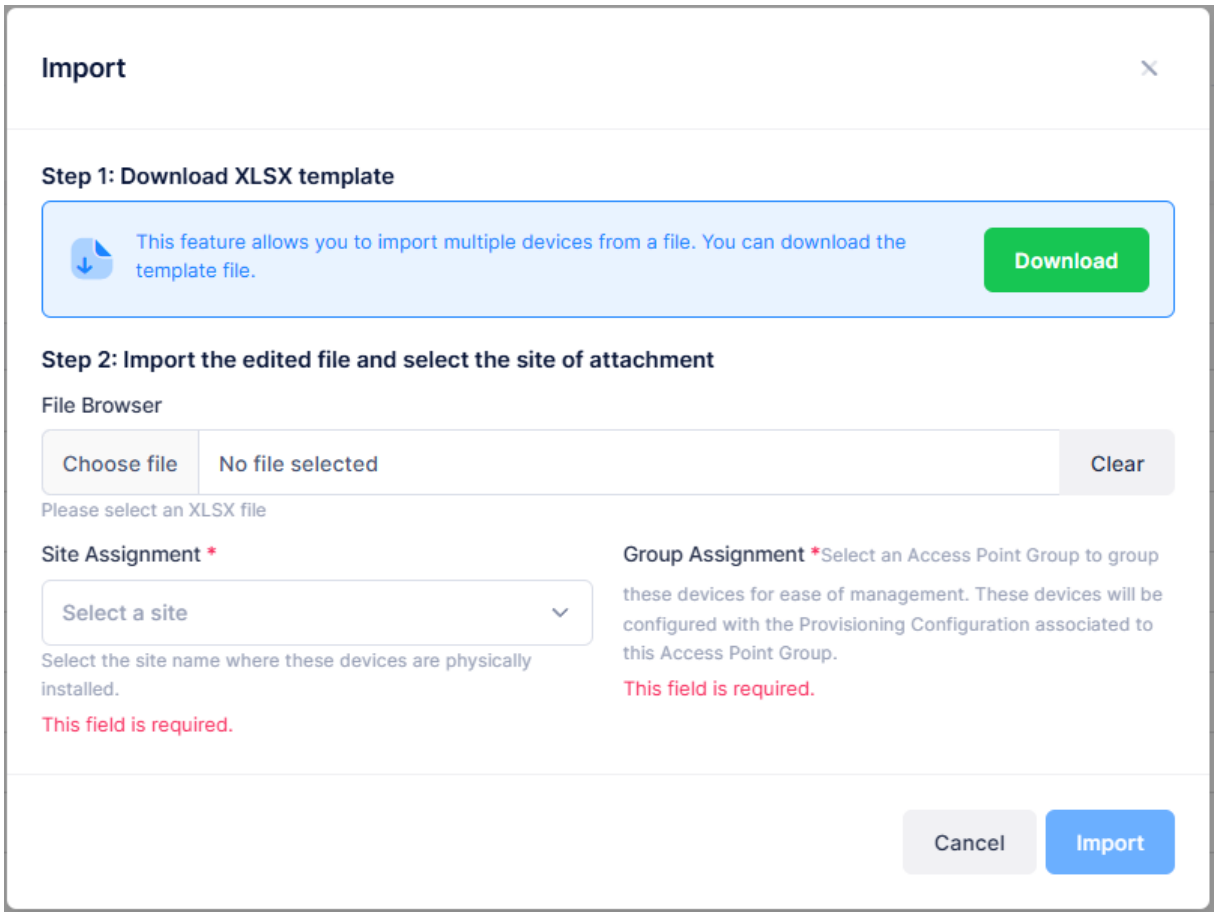
21 Oct 2025

4.1.1.3.4 Import Devices from an Excel Sheet

The Device List (see page 170) screen displays a list of devices that are known to an organization site. The list will be empty if no devices have been added to the site. There are three methods for adding a device to a site: import an OmniVista CSV file, (see page 200) import an Excel XLSX file, or manually add a device (see page 203).

To import devices from an existing Excel sheet (.xlxs), click on **Import from...** and select **XLSX template file**. An "Import" form will open on which you will complete the fields as described below to configure multiple devices to upload to the Device Catalog.





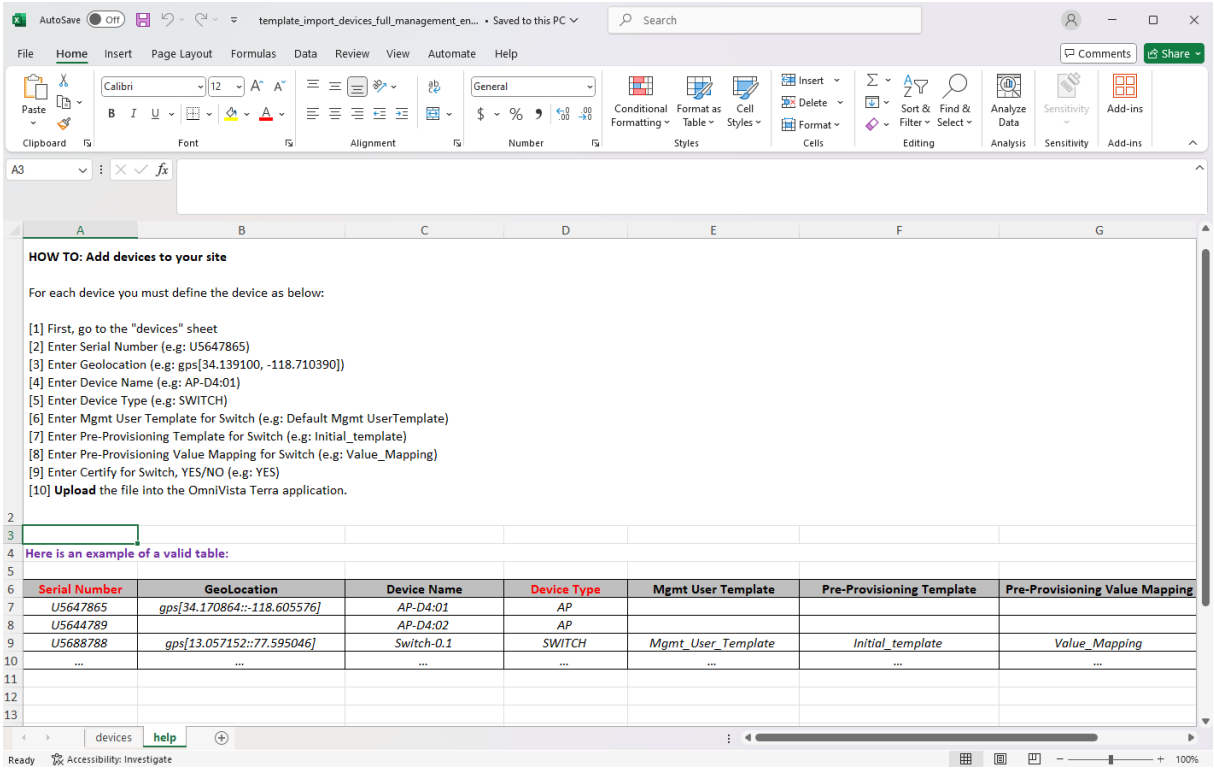
4.1.1.3.4.1 Step 1. Download XLSX Template

Click on **Download XLSX template** and specify where you would like to save the template file. When you open the template file, instructions are provided about how to define the devices to be added.

Consider the following when filling out and importing the template file:

- If the serial number for a device defined in the import template matches the serial number of a device already known in the Device Catalog, OmniVista Terra imports the serial number and overwrites the device details with the template device details.

The following sample template file is an example of the template provided for defining multiple devices to add to the Device Catalog:



Fill out the template with information for each device that you want to import into OmniVista Terra. Once the file is complete and saved, return to Step 3 on the Import form.

4.1.1.3.4.2 Step 2. Import the edited file and select the site of attachment

Complete the following fields to import the devices listed in the template file:

- **File Browser** - Click in this field to find and select the existing template file to import.
- **Site Assignment** - Click in this field to display a list of Organization Sites and select the site to which the devices defined in the template file will be imported.
- **Group Assignment** - Click on this field to select the Access Point Group to which the AP devices will be assigned. The provisioning configuration (see page 313) associated with this group will be applied to the imported devices.

> If the Access Point Group is associated with more SSIDs than the AP model can support, then you cannot add the AP to the group.

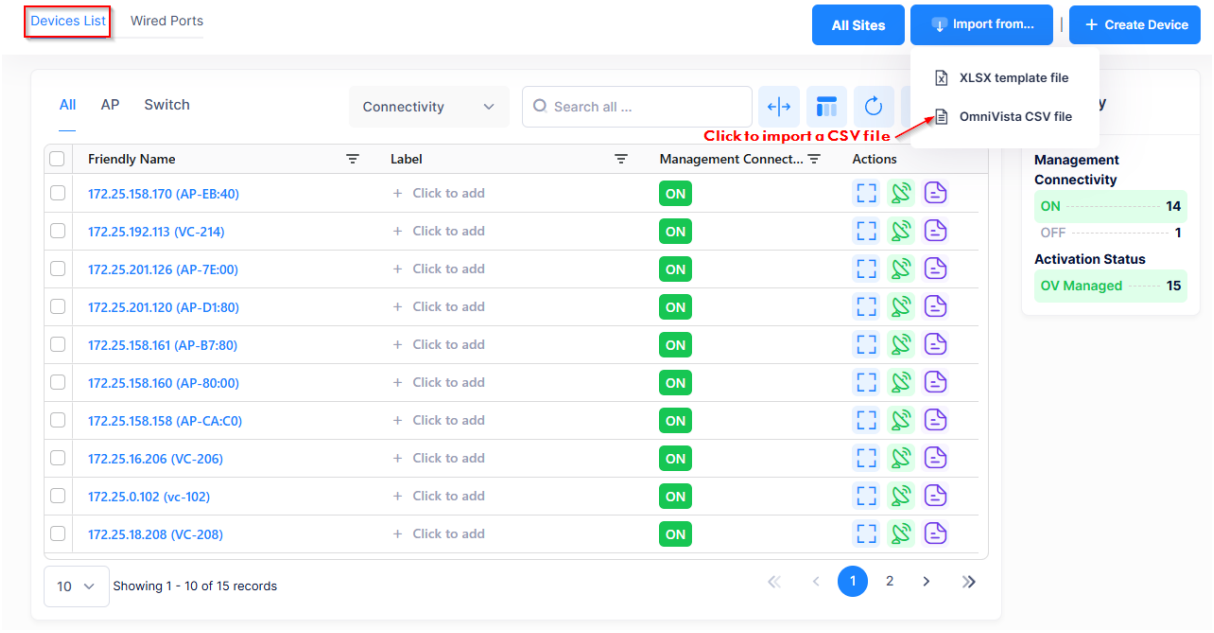
Once the Import form is complete, click on **Import**. The Device Catalog for the site is populated with the imported devices.

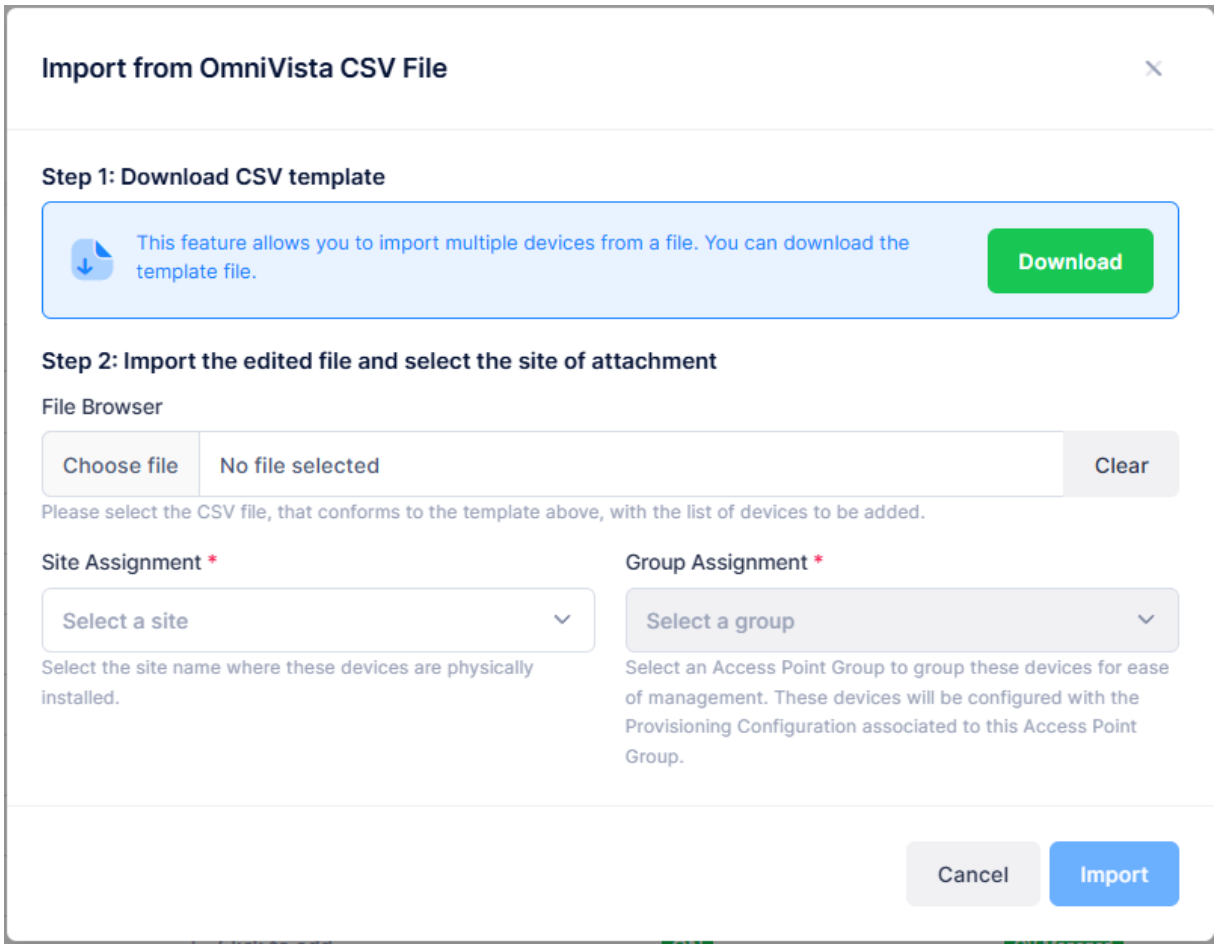
21 Oct 2025

4.1.1.3.5 Import Devices from an OmniVista CSV File

The Device List (see page 170) screen displays a list of devices that are known to an organization site. The list will be empty if no devices have been added to the site. There are three methods for adding a device to a site: import an OmniVista CSV file, import an Excel XLSX file (see page 197), or manually add a device (see page 203).

To import devices from an existing OmniVista .csv file, click on **Import from...** and select **OmniVista CSV file**. An “Import from OmniVista CSV file” form will open on which you will complete the fields as described below to configure multiple devices to upload to the Device Catalog.





Step 1: Download CSV template

Download the CSV template file and add device information based on the template instructions.

Consider the following when importing devices from an OmniVista CSV file:

- If the serial number for a device defined in the import file matches the serial number of a device already known in the Device Catalog, OmniVista Terra imports the serial number and overwrites the device details with the template device details.

Step 2: Import the edited file and select the site of attachment

Complete the following fields to import the devices listed in the CSV file.

- **File Browser** - Click in this field to find and select the existing CSV file to import.
- **Site Assignment** - Click in this field to display a list of Organization Sites and select the Site to which the devices defined in the CSV file will be imported.
- **Group Assignment** - Click on this field to select the Access Point Group to which the AP devices will be assigned. The provisioning configuration associated with this group will be applied to the imported devices.

If the Access Point Group is associated with more SSIDs than the AP model can support, then you cannot add the AP to the group.

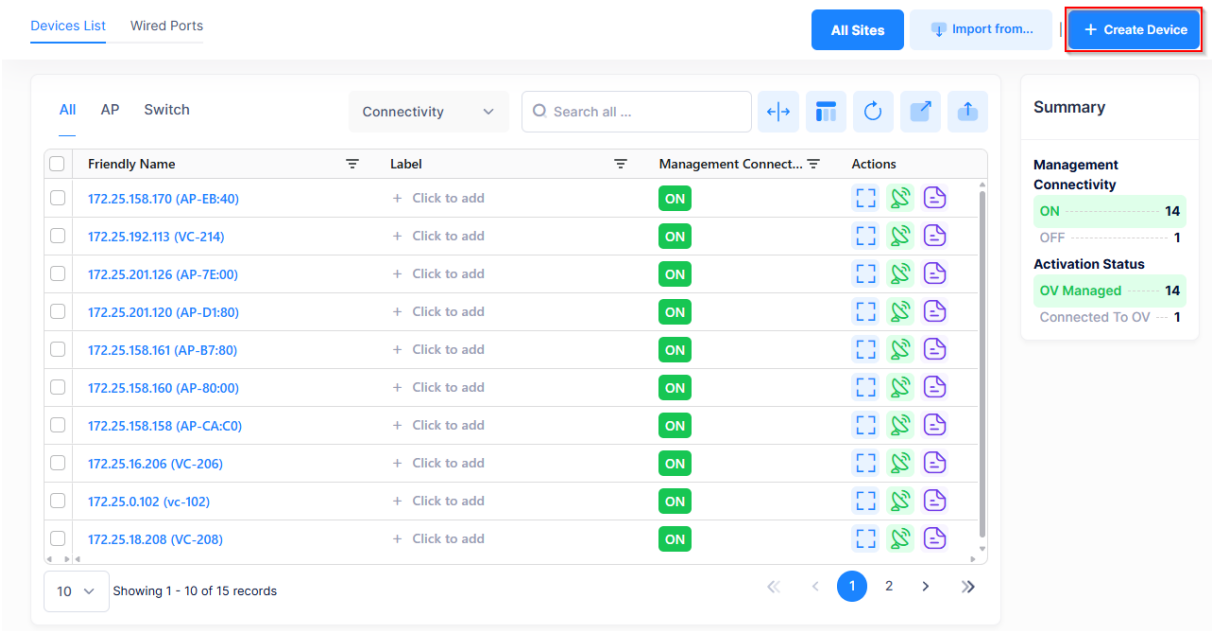
Click on **Import**. The Device Catalog list for the site is populated with the imported devices.

21 Oct 2025

4.1.1.3.6 Manually Add a Device

The Device List (see page 170) screen displays a list of devices that are known to an organization site. The list will be empty if no devices have been added to the site. There are three methods for adding a device to a site: import an OmniVista CSV file (see page 200), import an Excel XLSX file (see page 197), or manually add a device.

To manually add a single device to a specific Site, click **Create Device** on the Device List (see page 170) screen to bring up the Create Device form.



The Create Device form is used to declare a device that you want OmniVista Terra to manage by entering information to identify and describe the device in the Device Catalog.

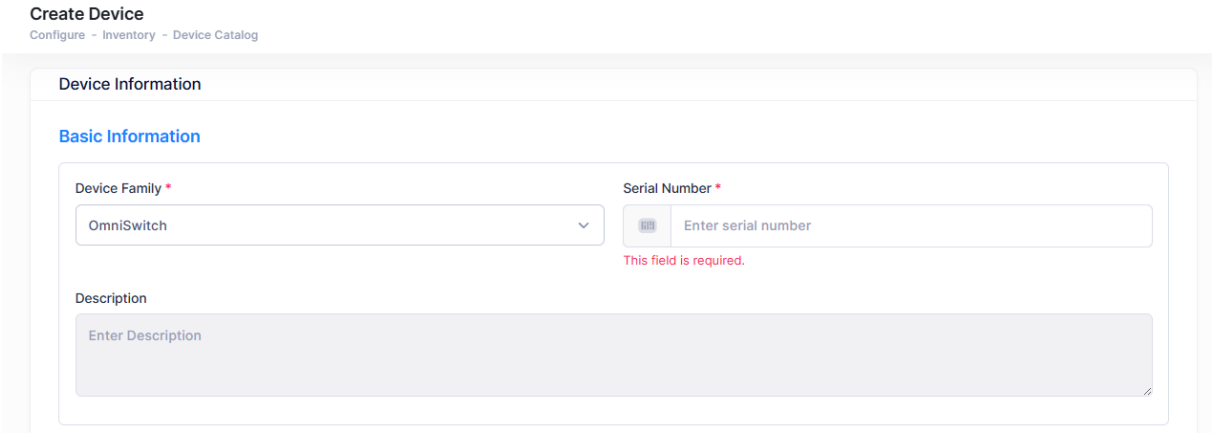
The Create Device form is divided into the following sections:

- Basic Information (see page 204)
- Software Information (see page 205)
- Assigned Site (see page 206)
- Added Labels (see page 207)
- Assign License (see page 207)
- Initial Configuration (Switch Only) (see page 208)
- Location in the Building (see page 209)
- Device Image (see page 209)

Complete the required fields and any optional fields in each section, as described below, then click on **Create Device**.

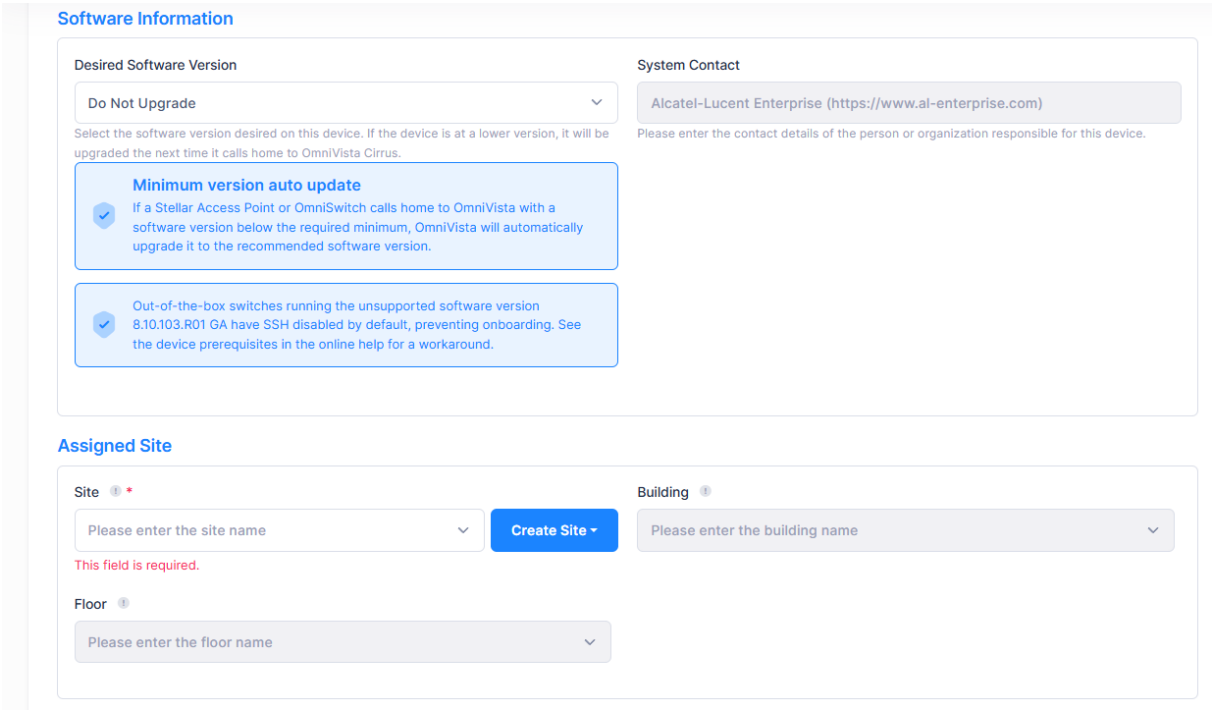
Click on **Create another** to return to the Create Device form to fill out for another device. If this box is not checked, the display returns to the Device Catalog screen.

4.1.1.3.6.1 Basic Information



- **Device Family** - Select the device family to which the device that you want to manage belongs (for example, Stellar APs or Switches).
- **Serial Number** - Enter the serial number of the device. Note the following when entering the serial number of the device that you want to manage:
  - Make sure the device is not already managed by another instance of OmniVista. If so, remove the device from the other instance, then add the device to OmniVista Terra.
  - When adding a Virtual Chassis (VC), enter the serial number of the switch that is designated as the Master chassis. Do not use the serial number of any other switch in the VC configuration.
- **Description** - Enter an optional description for the device. This field is configurable when adding an AP to the Device Catalog, but is not configurable when adding a switch to the Device Catalog. The description displayed for the switch is the same description displayed with the **show system** CLI command.

4.1.1.3.6.2 Software Information and Assigned Site



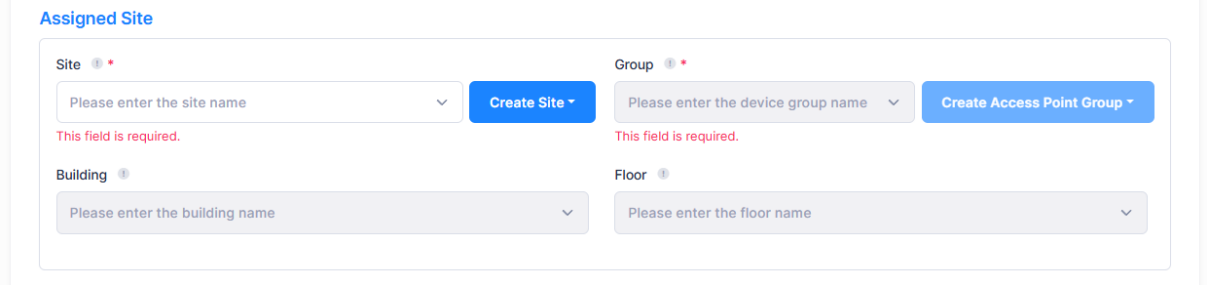
Software Information

- **Desired Software Version** - Select a specific software version for the device from the drop-down menu. This will trigger the device to automatically download and install the selected software version as part of the activation process. Note that the selected software version must be higher than the version currently installed on the device. Also note that if the device does not support the selected software version, the "Desired Software Version" field will be set to "Do Not Upgrade" after the device is validated.
  - **Do Not Upgrade** - Select "Do Not Upgrade" if you do not want to change the installed software on the device. If the device is part of an existing network, selecting “Do Not Upgrade” will leave your device running its current software version. If this is a new device, updating to the latest release is recommended. In general, you should only select a specific release if you understand the features of the specific release.

- Minimum Version Automatic Update. If a device calls home to OmniVista with a software version below the required minimum, OmniVista will automatically upgrade the device to the recommended software version.
- Out-of-the-box switches running the unsupported software version 8.10.103.R01 GA have SSH disabled by default, preventing onboarding. See the device prerequisites in the online help for a workaround.

- **System Contact** - The contact information for the device (for example, “My Company Inc https://www.mycompany.com”). This field is configurable when adding an AP to the Device Catalog, but is not configurable when adding a switch to the Device Catalog. The system contact displayed for the switch is the same contact displayed with the **show system** CLI command.

Assigned Site



- **Site** - Select the Organization Site where the device is physically located and installed. To select an existing Site, click on the Site name in the drop-down menu or click on **Create Site** to create a new Site to assign to the device.

  When you click on **Create Site**, a drop-down menu appears from which you can select how you want to access the Create Site screen (launce screen in a new browser tab or discard changes and launch screen in current browser tab). See Configure and Manage a Site (see page 72) for steps on how to define a site for an Organization.

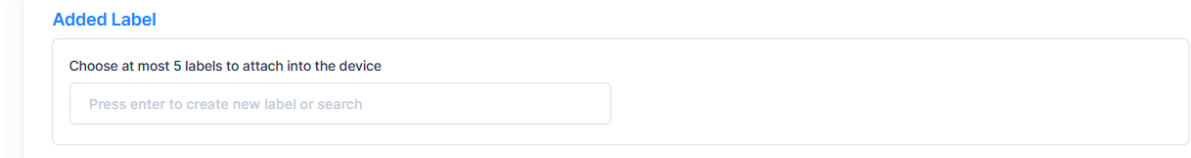
- **Group (AP only)** - The Access Point group from which the device will get its provisioning configuration. When you selected a Site for the device, a list of Access Point Groups associated with the Site is automatically provided in this field. Select one of the existing groups or the “Mgmt VLAN based automatic grouping” option from the drop-down list. You can also click on **Create Access Point Group** to create a new group for the Site.
  - **Mgmt VLAN based automatic grouping** - If you select this option, the AP device is automatically assigned to an AP Group that is associated with a Provisioning Configuration (see page 313) that specifies VLAN IDs for the Auto-Group VLANs attribute. The assignment is based on the AP management VLAN ID received by LLDP. If the management VLAN matches a VLAN ID specified for Auto-Group VLANs, the AP is assigned to the corresponding AP Group.

If the Extended SSID Scale option is enabled for the selected group, make sure that the serial number belongs to a Stellar AP model that supports up to 14 SSIDs. Otherwise, the AP will stay in “First Contact Pending” status.

When you click on **Create Access Point Group**, a drop-down menu appears from which you can select how you want to access the Create Access Point Group screen (launch screen in a new browser tab or discard changes and launch screen in current browser tab). See Configure and Manage Access Point Groups (see page 309) for more information.

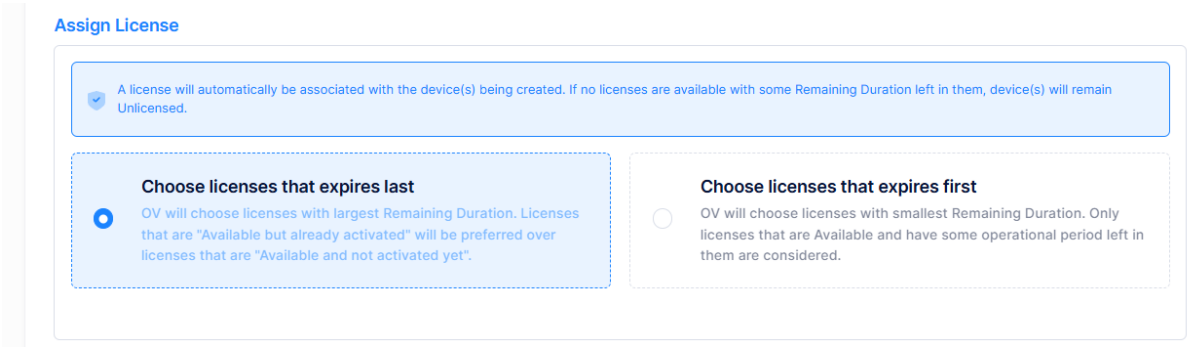
- **Building** - The name of the building at the Organization Site where the device is physically located. When you selected a Site for the device, a list of building names associated with the Site is automatically provided in this field. Select one of the existing building names from the drop-down menu. See Configure and Manage a Building (see page 83) for steps on how to define a building for a Site.
- **Floor** - The name of the floor in the building where the device is physically located. When you selected a building where the device is physically located, a list of floor names associated with that building is automatically provided in this field. Select one of the existing floor names from the drop-down menu. See Configure and Manage a Floor (see page 92) for steps on how to define a new floor for the building.

4.1.1.3.6.3 Added Label



Select up to five labels from the drop-down menu to assign to the device. Assigning labels to device(s) allows you to group managed devices together. All devices that have the same label belong to the same group. This also allows grouping of different device types. For example, if you assign the same label to Switches and to APs, both of those device types are included in the same group. See Performing Device Operations (see page 227) for more information about device labels.

4.1.1.3.6.4 **Assign License**



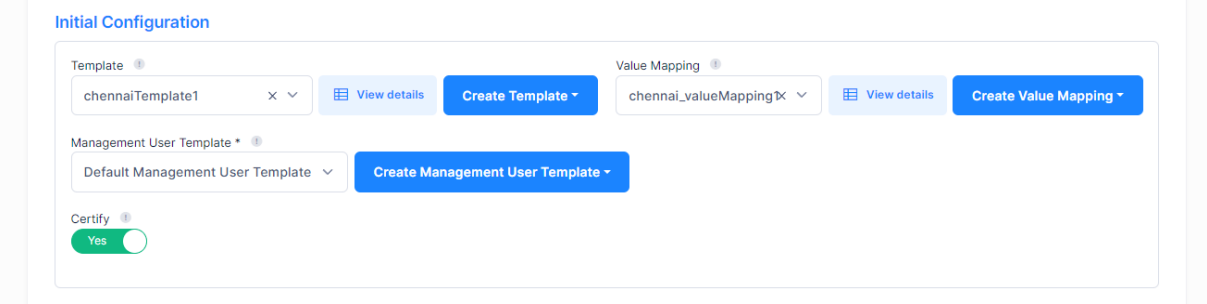
Assign License

Automatically assign a license to the device. Note that if there are no licenses available that have a Remaining Duration, the device will remain unlicensed. This section does not appear if the Organization is under a Trial License, as it applies only to paid license subscriptions. Select one of the following options to specify how OmniVista Terra will select licenses to assign to a device:

- **Choose licenses that expires last** - Licenses that have the most amount of Remaining Duration time are selected. Licenses that are “Available (Activated)” are preferred over licenses that are “Available (Not Activated).

- **Choose licenses that expires first** - Licenses that have the least amount of Remaining Duration time are selected. Only licenses that are “Available” and have some amount of time left until they expire are considered.

4.1.1.3.6.5 Initial Configuration (Switch Only)

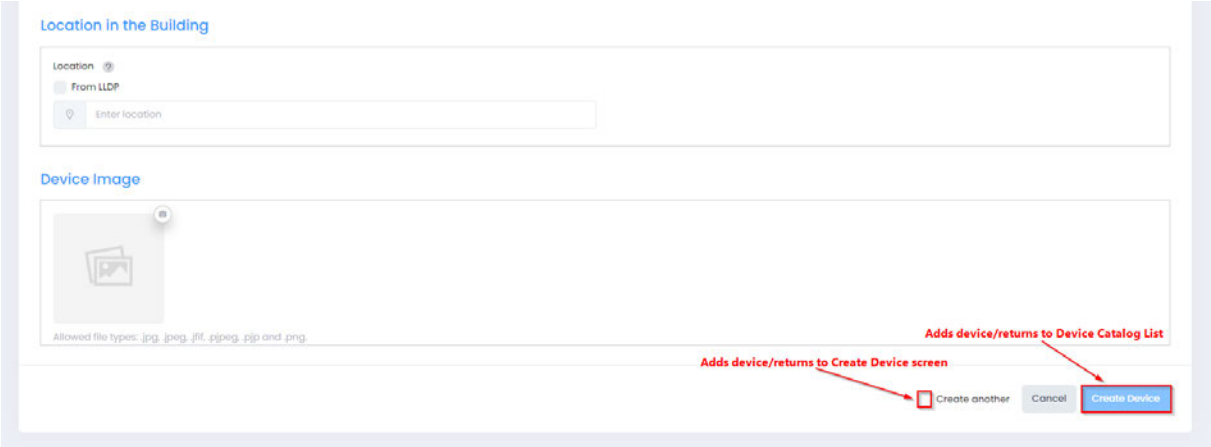


Initial Configuration

The Initial Configuration section of the Create Device form displays when you select **Switches** for the Device Family. This section does not appear when you select **Stellar AP**. The Initial Configuration is pushed to

- **Template** - Select an existing Configuration Template that you want to push to the Switch or click on **Create Template** to open the Create Template screen and create a new template. (see page 459)You can also click on **View Details** to view information about the selected template. The configuration template contains CLI commands that are applied before the Switch becomes managed. Note that you do not have to select a Configuration Template. For example, you may want to onboard a switch with an existing configuration but do not want to modify that configuration. If you do select a template to apply to the Switch, the template CLI commands are appended to the Switch configuration.
  - **Value Mapping** - If you use variables to create a dynamic Configuration Template, you must create Value Mappings to define the values of the variables in the template. Select an existing Value Mapping or click on **Create Value Mapping** to open the Create Value Mapping screen and create a new Value Mapping (see page 467). You can also click on **View Details** to view information about the selected mapping.
- **Management User Template** - Select an existing Management User Template or click on **Create Management User Template** to open the Create Management User screen and create a new template. (see page 472) The Management User Template contains CLI/FTP credentials that OmniVista Terra will use to connect with the switch. By default, the “Default Management User Template” is pushed to the Switch unless you select a different template.
- **Certify** - Save the configuration to the Certified Directory on the Switch. Note that this option is enabled by default. If you disable this option and the Switch reboots, the configuration is not saved. It is recommended that you leave this option enabled.

4.1.1.3.6.6 Location and Device Image



Location in the Building

This section does not appear when you select **OmniSwitch**.

- **Location** - Enter details about where a device is located within a Floor (for example, front desk, Rack-10). This option is not available if the From LDAP option is selected.
- **From LLDP** - When this option is selected, OmniVista will use LLDP to automatically add the location of the device.

Device Image

- Upload an image file (png, jpg, or jpeg) to associate with the device.

21 Oct 2025

4.1.1.3.7 Device Onboarding - FAQs/Troubleshooting

4.1.1.3.7.1 Provisioning fails when onboarding a switch with a memory threshold that is to low

When this issue occurs, usually on low-end switches such as an OmniSwitch 6360, check the Results Provisioning Information for the switch (Configure > LAN > CLI Based Provisioning > Results). If the Provisioning Status is "*Failed*" and the Last Provision Message is "*Failed to install the OmniVista agent on the switch, possibly due to insufficient device disk space or memory*", increase the memory threshold on the switch using the following CLI command:

```
health threshold memory (value)
```

For example, if the memory threshold on the switch is 54% but the required threshold for the OmniVista agent is 74% (or higher):

```
health threshold memory (80)
```

Note: You can directly issue the above CLI command on the switch, or use an Incremental Template (which takes affect the next time the switch calls home).

4.1.1.3.7.2 How to add serial numbers for a Virtual Chassis (VC) to the Device Catalog

The recommended method for adding serial numbers to a VC is as follows:

1. **Add the VC to the Device Catalog** - Add the serial number of the primary chassis for the VC. You can also add the serial number for each chassis in the VC.
2. **Create the VC in the Network** - Once the device is added to the Device Catalog, form the Virtual Chassis by connecting each participating chassis in the network.
3. **Ensure Correct Time and Internet Access** - Make sure the switch has the correct time and can resolve FQDNs over the Internet.
4. **Wait for the Call Home** - The VC should automatically call home based on the Time to Next Call Home (TNCH) value, which you can verify with the CLI command **show cloud-agent status**. You can also manually trigger the call home by disabling and enabling the Cloud Agent using the CLI command **cloud-agent admin-state disable/enable**.
5. **Device Catalog Entry** - Once managed, only one entry for the VC's serial number will appear in the Device Catalog. The "Number of Licenses Used" column reflects the total number of chassis in the VC. Clicking on **Additional Information** in the Device Catalog or the Topology Map will display detailed information about each chassis in the VC.
6. **Adding Additional Chassis** - You can add chassis to the VC in the network at a later time. The "Number of Licenses Used" will update after OmniVista Terra performs a periodic or manual Rediscovery. Similarly, you can remove a chassis from a VC at a later time, and the license count will be updated during the next Rediscovery operation. If adding another chassis to the VC causes the primary switch to return to a "Registered" state, release and then assign the device license for the primary switch.

4.1.1.3.7.3 How to use the Activation Status field in the Device Catalog List to troubleshoot problems adding/licensing devices

You can use the following list of commands to troubleshoot/resolve device problems based on the Activation Status.

Activation Status	Resolution
Unsupported Device Model	• The device is not supported in OmniVista Terra.
Waiting for First Contact	• If you are adding a Device to the Device Catalog and the device remains in this state (rather than moving to "Registered"), verify that you have met all of the Network and Device Prerequisites (see page 8). If necessary, make any needed configuration changes. Otherwise, restart the activation process (see page 196) on the device.
Registered	• If you are licensing a device and it remains in this state (rather than moving to "OV Managed"), restart the activation process (see page 196) on the device.
VPN Config Failed	• Device was unable to configure a secure transport channel for connecting to the OmniVista Terra Server. Wait for 30 minutes. The network device will automatically contact the OmniVista Terra Server again to check the configuration. If resolved, the activation process will continue. If the problem persists, contact Customer Support.

Provisioning Failed	• Device was unable to process the provisioning configuration sent by the Provisioning application for APs. Wait for 30 minutes for the network device to retry and contact the OmniVista Terra Server. If the problem persists, contact Customer Support.
	• Failed to open an SSH session to the device.
	  • Try to restart the device to make sure the maximum number of SSH sessions has not been exceeded. There may have been a connection timeout. Check the network connection and try again.
	• An exception occurred when applying the configuration to device.
	  • Check the network connection.
	  • Check the configuration template.
	• Connection is closed by a foreign host.
	  • Check the connection to device and try again.
	• Failed to open a connection to a device.
	  • Make sure the username or password are correct. Check your user configuration.
	• AP Country Code conflict. Check and update the APs Country Code (see page 213), if necessary.
	• AP License Conflict.
	  • If there are no licenses available for a registered AP, you must free up licenses by deleting an AP or purchase additional licenses before you can manage the AP.
	• AP Registration Information is Incorrect (e.g., IP Address, SysOid).
	  • Verify and update the information, if necessary.

Certificate Previously Issued	• A certificate was previously provided to this network device but it has contacted OmniVista Terra without it. Remove device and add again to Device Catalog; then, wait for 30 minutes or restart the activation process on the device. If the problem persists, contact Customer Support.

Failed to Get Certificate	• Device has contacted the OmniVista Terra Server and the server attempted to create a certificate to achieve a more secure communication but the attempt has failed. Wait for 30 minutes. The network device will automatically contact OmniVista Terra again. If resolved, the activation process will continue. If the problem persists, contact Customer Support.
Upgrade Failed	• Device software version upgrade has failed. OmniVista Terra will attempt to fix this internally; however, if the problem requires action outside of OmniVista Terra, the default admin of the OmniVista Terra Account will be contacted. If the problem persists for more than 24 hours, contact Customer Support.
Factory Reset Required	• The VPN profile was changed/updated. You must restart the Activation Process on the device (see page 196).

4.1.1.3.7.4 AP successfully registers with OmniVista Terra, but the Provisioning Configuration failed

An incorrect configuration can cause the Activation Status field for the AP to indicate “Provisioning Failed”:

- Country Code Conflict.
  - Wireless regulations vary by country, so APs are configured and shipped based on the country's regulations. The Country Code configured for the RF Profile used to manage these APs must match the country code for the APs it is managing. If they do not match, the APs will remain in an unmanageable state until the problem is resolved.
  - The AP Country Code conflicts with the Country Code in the RF Profile.
  - Steps to check the Country Code on AP:
    - Navigate to the Device Catalog List (see page 170).
    - Select the AP on the Device Catalog List, then click on **Actions** and choose SSH from the drop-down menu.
    - Input the username and password of AP and click on **Start Session**.
    - In the AP session, run the command: showsysinfo to check Country Code.
  - Steps to check the Country Code in the OmniVista Terra UI:
    - Navigate to the Device Catalog List (see page 170).
    - Select the AP on the Device Catalog List, then click on the Additional Information icon to check which RF Profile the AP is using.
    - If AP is using a specific RF Profile, navigate to the RF Profiles List (see page 331), select RF Profile name, and check the Country Code on the details page.

        - If AP is using RF Profile of AP Group, navigate to the Access Point Groups List (see page 309)to which AP belongs, check the provisioning name, then navigate to the Provisioning Configuration List (see page 313) to check RF name for the Provisioning Configuration.
- Auto Group VLAN enabled and OmniVista Terra does not find the VLAN that matches the AP.
    - Steps to check VLAN:
        - Navigate to the Provisioning Configuration List (see page 313).
        - Click the Additional Information icon to check Auto-Group VLANs in the Time section.
- RAP feature is enabled *and* AP Group does not have enough IP addresses from the IP Range in the Data VPN Server to allocate for the AP.
    - Steps to check IP range:
        - Navigate to the Provisioning Configuration List (see page 313).
        - Click the Additional Information icon to see data VPNs in the Data VPN settings section.
        - Navigate to Data VPN Settings (see page 414).
        - Check the IP Range for the data VPNs.
- Some related logs in AP to troubleshoot:
    - /tmp/log/wmaagent.log
      Check some content in the log related to registration flow as below:
      “Main Send to WMA msgtype=registration,message=...”
      “Main Receive from WMA msgtype=registration ,message=…”
      “Main Receive from WMA msgtype=preconfig ,message=…”
      “Main Send to WMA msgtype=preconfig,message=…”
- Logs in OmniVista Terra to check:
    - Organization user audit logs (see page 122).
    - Network device alerts (see page 948).
    - Network events (see page 981).

4.1.1.3.7.5 When attempting to register a Full Management AP by serial number, the error message “A device with this Serial Number is already declared as part of another Organization” displays.

Provide the Alcatel-Lucent Enterprise Technical Support team with the serial number and URL so they can verify their configuration in the cluster and do any clean up as necessary.

4.1.1.3.7.6 AP successfully registers with OmniVista Terra, but the AP cannot broadcast SSIDs

If the registered AP is unable to broadcast SSIDs:

Check to see if the SSID was successfully pushed to the AP.

1. Navigate to the Device Catalog List (see page 170) (**Configure > Inventory > Device Catalog**).

2. Select the AP on the Device Catalog List, then click on **Actions** and choose the SSH item from the drop-down menu.
3. Input the username and password of the selected AP and click on **Start Session**.
4. Run this command: cd /tmp/local_config
5. Run this command: cat wlanservice.conf to check the SSID

The SSID is configured as 6Ghz but some countries do not support 6Ghz. To check the SSID band:

1. Navigate to the SSIDs List (see page 347) (**Configure > WireLess > SSIDs**)
2. Select the SSID that you want to check, then click on Edit icon to open the Customize SSID screen.
3. Check the bands selected for the Allow Band attribute in the Basic Information section.

Some related AP logs and commands to troubleshoot:

- /tmp/log/wmaagent.log
- /tmp/log/wma.log
- sta_list

Logs in OmniVista Terra to check:

- Organization user audit logs (see page 123) (**Organization > Users > Audit Logs**)
- Network device alerts (see page 948)(**Monitor > Alerts**)
- Network events (see page 981)(**Monitor > Diagnostic Tools > Network Events > Events**)

4.1.1.3.7.7 The SSID is applied to AP from OmniVista Terra UI but the AP does not broadcast the SSID

If the registered AP is unable to broadcast SSIDs:

Check to see if the SSID was successfully pushed to the AP.

1. Navigate to the Device Catalog List (see page 170) (**Configure > Inventory > Device Catalog**).
2. Select the AP on the Device Catalog List, then click on **Actions** and choose the SSH item from the drop-down menu.
3. Input the username and password of the selected AP and click on **Start Session**.
4. Run this command: cd /tmp/local_config
5. Run this command: cat wlanservice.conf to check the SSID

The SSID is configured as 6Ghz but some countries do not support 6Ghz. To check the SSID band:

1. Navigate to the SSIDs List (see page 347) (**Configure > WireLess > SSIDs**)
2. Select the SSID that you want to check, then click on Edit icon to open the Customize SSID screen.
3. Check the bands selected for the Allow Band attribute in the Basic Information section.

Some related AP logs and commands to troubleshoot:

- /tmp/log/wmaagent.log

- /tmp/log/wma.log
- sta_list

Logs in OmniVista Terra to check:

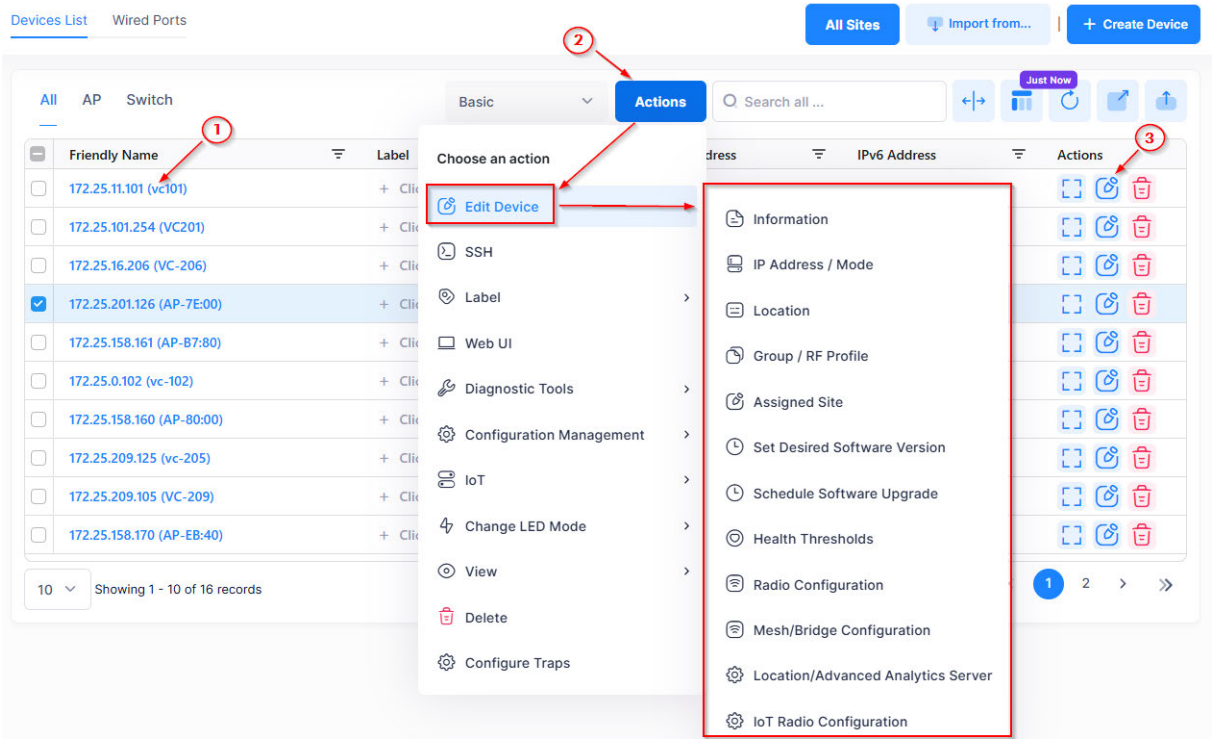
- Organization user audit logs (see page 123) (**Organization > Users > Audit Logs**)
- Network device alerts (see page 948) (**Monitor > Alerts**)
- Network events (see page 981)(**Monitor > Diagnostic Tools > Network Events > Events**)

21 Oct 2025

4.1.1.4 Edit Device Settings

You can edit the information for one or more devices. For example, if a device fails validation due to an incorrect serial number or MAC address, you can edit those fields. Note that not all fields are available when editing multiple devices.

The Device Catalog (see page 170) screen displays a list of all of the devices known to one or more Sites.



From this screen, you can use one of the following methods to edit the device information:

1. Click on the Friendly Name for the device to open the detailed Device Information screen (see page 217). From this screen, you can click on **Actions** and select **Edit Device**. If you're editing an Access Point, you can also set the LED mode for the Access Point device using **LED Mode** next to **Actions**.

2. Select a device that you want to edit by checking the box next to the device entry, then click on **Actions**. From the Actions drop-down menu, hover over **Edit Device** to display a drop-down list of configurable settings (see page 219) for the device.

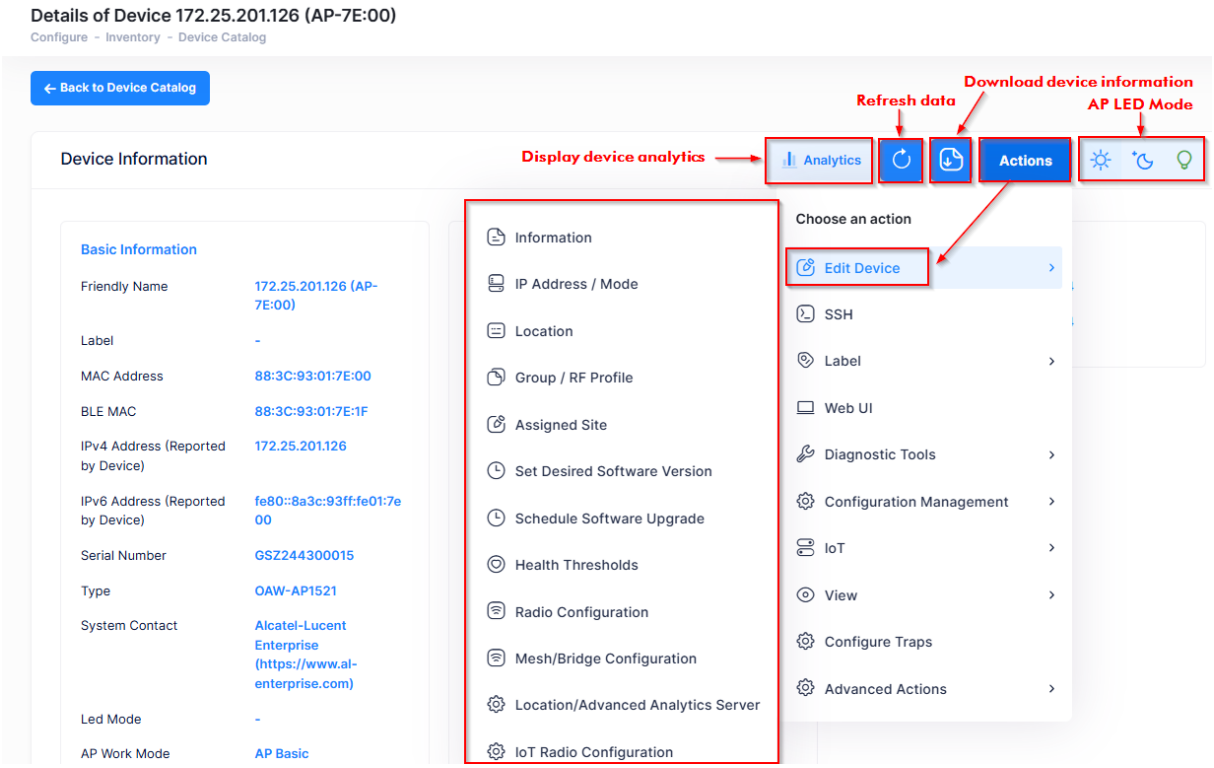
3. Under the "Actions" column, click on the Edit icon next to the device that you want to edit to access the Edit Device Information (see page 222) screen.

4.1.1.4.1 Detailed Device Information

The detailed Device Information screen displays all of the configuration information about a device. From this screen you can

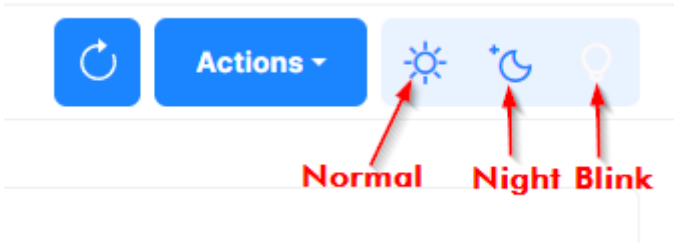
- Click on **Actions** and hover your cursor over **Edit Device** to display another drop-down menu of available settings (see page 219) you can edit for the device.
- Display Network Analytics for the device.
- Refresh the screen to update the information provided.

- Set the LED mode (see page 218) for the selected Access Point.



4.1.1.4.2 Setting the LED Mode for the Access Point

You can set the LED mode on an Access Point by clicking on one of the LED Mode buttons at the top of the detailed Device Information (see page 217) screen, next to **Actions**.



- **Normal Mode** (Default) **-** The LED displays in normal mode (Red/Green/Blue).
- **Night Mode -** The LED indicator is shut off.
- **Blink Mode -** LED alternately blinks Red/Green/Blue so that you can visually locate the AP(s).

4.1.1.4.2.1 LED Indicators

The LED light on the AP indicates the following conditions:

- RED (Flashing) - System abnormal, link down
- RED (Solid) - System startup

- RED and BLUE (Rotate Flashing) - OS upgrading
- BLUE (Solid) - System running, dual bands working
- GREEN (Flashing) - No SSID created
- GREEN (Solid) - System running, single band working
- RED, BLUE, and GREEN (Rotate Flashing) - System running (used to visually locate an AP).

4.1.1.4.3 Edit Device Settings

The Edit Device (**Actions - Edit Device**) drop-down menu provides the following list of device settings that you can edit for the selected device:

> Note that changing the RF profile for a selected device overrides the RF Profile assigned to the device through the Provisioning Configuration. The “Information”, “Group/RF Profile”, and “Assigned Site” settings all offer the option to change the RF Profile assignment for a device.

- **Information** - Opens the Edit Device screen (see page 222) from which you can change the information used to declare the device in OmniVista Terra.
- **IP Address/Mode** - Opens the Edit IP Mode/IP Address screen from which you can change how an AP obtains an IP address (DHCP or Static) or the IP address assigned to a Switch. Note that OmniVista Terra obtains and saves the IP address information reported by the device. When you make any changes to the IP address or mode, the changes are pushed directly to the device; however, the Edit IP Mode/IP Address screen may still display the previous IP address information until OmniVista receives the updated information from the device.
  - If you select an AP device, you can change how the AP obtains an IP address by editing the following fields:
    - **DHCP** - Obtain the IP address from a DHCP Server.
    - **Static** - Configure a static IP address by completing the following fields:
      - **IP Type** - Select IPv4 and/or IPv6.
      - **IP Address** - The IPv4/IPv6 address for the AP.
      - **Netmask** - The IPv4 address network mask for the AP.
      - **Subnet Prefix Length** - The length of the subnet prefix for the IPv6 address network mask.
      - **Default Gateway** - The default gateway used for AP forwarding.
      - **Preferred DNS** - The IP address of the DNS Server used by the AP.
      - **Alternate DNS** - The IP address of the alternate DNS Server used by the AP.
  - If you select a Switch, you can select an IP address to apply to the Switch. The IP mode (DHCP or Static) is not available for a Switch.
- **Location** - Opens the Edit Device Location screen from which you can specify the location of the device.

  - If you select an AP device and the “From LLDP” checkbox, OmniVista will use LLDP to automatically add the location; otherwise, enter a user-defined string for the location (for example, “Lab1/1/12”).
  - If you select a Switch, enter a user-defined string for the location (for example, “Lab1/1/14”). The LLDP option is not available for a Switch.
- **Group/RF Profile (AP only)** - Opens the Edit Group/RF Profile screen from which you can change the Access Point Group or RF Profile associated with the device.
  - **Group** - Change the Access Point Group (see page 309) associated with the device. Note that when assigning a Stellar Access Point to a different group , all current configuration of the Access Point will be lost. This would potentially impact the services (for example, SSIDs) currently offered by the Access Point. The Access Point will get the configuration associated with its new Access Point Group.
  - **RF Profile** - Change the RF Profile (see page 331) associated with the device. The RF Profile assigned at the device level takes precedence over the RF Profile assigned in the Provisioning Configuration.

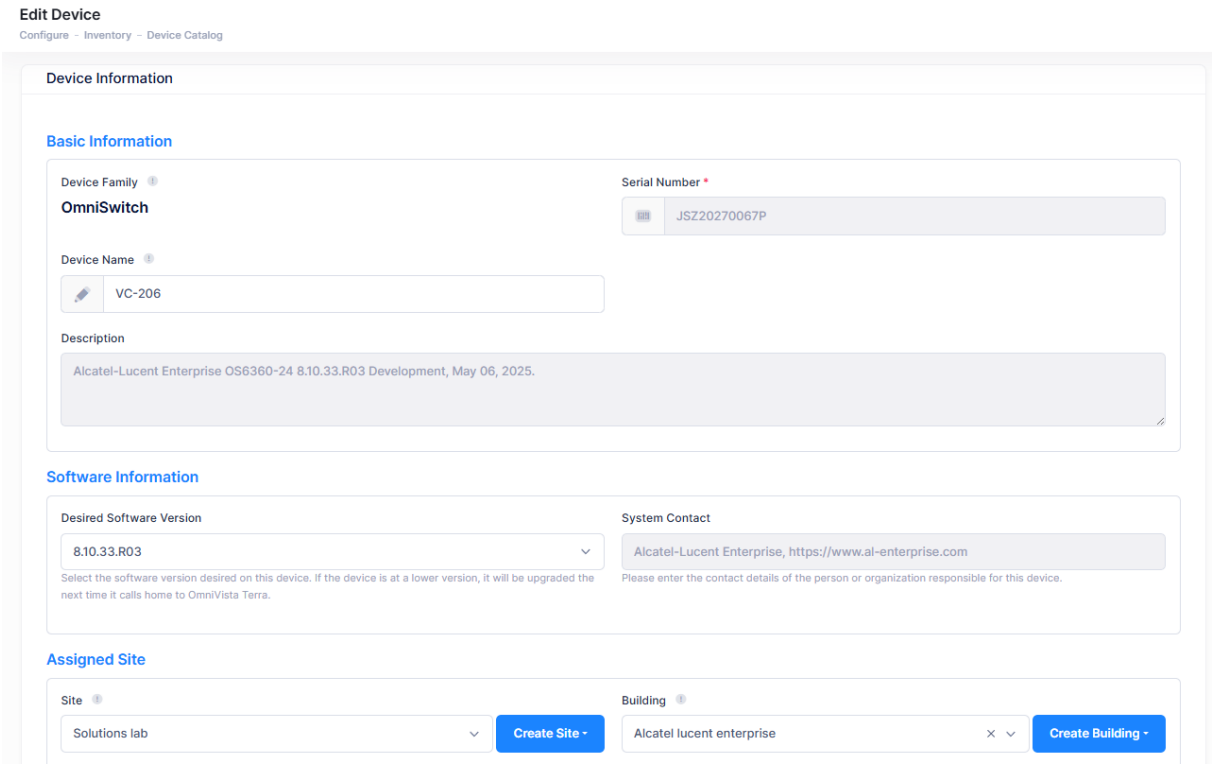
> If you want to change the RF Profile association for multiple APs, make sure that there is no conflict between the country code for the RF Profile and the selected AP devices. If there is a conflict, OmniVista Terra will reject the RF Profile update for all of the selected APs and display an error message indicating the APs that are causing the conflict. Otherwise, the RF Profile update is applied to all of the selected APs.

- **Assigned Site** - Opens an Edit Assigned Site Information screen in which you can change the location (Site, Group name, Building, Floor, and RF Profile) of the device. Note that when assigning a Stellar Access Point to a different Site or AP Group, all current configuration of the AP will be lost. This would potentially impact the services (for example: SSIDs) currently offered by the AP. The AP will get the configuration associated with its new Site or AP Group.
- **Discovery Manager Entry (Switch only)** - Opens the Edit Discovery Manager Entry popup screen from which you can edit the CLI/FTP Username and Password for a managed switch. The CLI/FTP User Name and Password fields enable you to inform OmniVista Terra of the device's CLI/FTP User Name and Password. A device's CLI/FTP User Name and Password cannot be configured from OmniVista, they must be configured directly on the device. If you do not define the CLI/FTP User Name and Password and you attempt to save, restore, or upgrade configuration files for a device, you will be individually prompted for the CLI/FTP User Name and Password of each individual device for which configuration files are being saved, restored, or upgraded. Also, OmniVista will be unable to auto-login to the device when establishing CLI Scripting sessions.
  - **CLI/FTP User Name** - The user name that OmniVista will use to establish CLI/FTP sessions with the managed devices. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored (see note below).

  - **CLI/FTP Password** - The password that OmniVista will use to establish CLI/FTP sessions with the managed devices. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored.
  - **Confirm CLI/FTP Password** - Re-enter the CLI/FTP password.
  - **Secondary Password** - The secondary CLI/FTP password, if applicable.
  - **Confirm Secondary Password -** Confirm the secondary CLI/FTP password, if applicable.
- **Set Desired Software Version** - Opens the Set Desired Software Version screen (see page 288) from which you can specify the software version that a device(s) will be update to on the next call home. This allows you to trigger an upgrade without waiting for a scheduled upgrade that is associated with the device.
- **Schedule Software Upgrade (AP only)** - Opens the Schedule Software Upgrade screen (see page 285) from which you can determine if the Access Point device is scheduled for a software update. You can also define or modify an upgrade schedule for the device.
- **Health Thresholds** - Opens the Edit Health Thresholds (see page 799) screen from which you can configure the CPU, memory, and flash threshold values for the device.
- **Radio Configuration (AP only)** - Opens the Edit Radio Configuration screen. On this screen, set **Use Private Config** to **On** to configure the radio band for the Access Point. Note that if you select the 6G band, APs that support 6G will accept the configuration; APs that do not support 6G will ignore the configuration.
- **Mesh/Bridge Configuration (AP only)** - Opens the Edit Mesh/Bridge Configuration screen from which you can configure the mesh configuration settings (see page 238) for the AP device. Note that updating the mesh configuration for the AP will affect the existing mesh network. During this time, the APs in mesh network will briefly lose connectivity and will re-establish a mesh network based on the new configuration.
- **Location/Advanced Analytics Server (AP only)** - Opens the Edit Location/Advanced Analytics screen from which you can configure the Location/Advanced Analytics Server options described below for the selected AP. Note that if you configure these options at the AP level, make sure that Advanced Analytics Server Profile and Wi-Fi RTLS Server Profile are selected in the AP Group (see page 309) to which the select AP belongs.
  - **Use Private Config** - Set to On to edit the following Location/Advanced Analytics Server options.
    - **OmniVista Terra Wi-Fi RTLS** - Enables/disables OmniVista Wi-Fi RTLS. If you enable OmniVista Terra Wi-Fi RTLS, then you should also enable OmniVista Terra Advanced Analytics.
    - **OmniVista Advanced Analytics** - Enables/disables OmniVista Advanced Analytics functionality.
- **IoT Radio Configuration (AP only)** - Opens the Edit IoT Radio Configuration screen from which you can configure BLE (if the Access Point supports this function). On this screen, set **Use Private Config** to **On** to configure BLE for the Access Point. Click here (see page 223)for more information.

4.1.1.4.4 Edit Device Information

The Edit Device Information screen displays the information for the device you selected from the Device Catalog list. Use this screen to change the information in any of the fields. When you are done editing any of the device information fields, as described below, click on **Save**.



Please read the information below about changing the Desired Software Version (see page 222) before you make any changes from the Edit Device Information screen.

Setting the Desired Software Version

Note the following when you change the Desired Software Version for the selected device from the Edit Device Information screen:

- If you select the **Upgrade as per AP Group's Schedule** option for the selected AP device, but there is no AP Group schedule, the message below is displayed. Click on **OK** to continue.

```
"Desired Software Version will be set to 'Do Not Upgrade' as there is no schedule for the associated AP Group. When the AP Group gets associated with a schedule, it will reflect in this device's information automatically."
```

- If a device-level schedule exists for the selected device, then the software version displayed in the “Desired Software Version” field is the one associated with the schedule. If you select another option for this field, the message below is displayed. Click **OK** to continue.

```
"This AP is part of schedule <schedule-name> and hence it will be upgraded to this version in the time window specified in that schedule. To upgrade the device on next call-home instead, navigate to 'Configure -> Inventory -> Scheduled Upgrades', Edit the schedule <schedule-name> and remove the AP from the selected devices list."
```

- If a device is a member of an AP Group for which a scheduled software update exists and you modify the “Desired Software Version” field, then the devices is removed from the schedule. The “Schedule Name” field for this device is set to empty and the following message is displayed for you to confirm whether you want the device to be updated per the associated AP Group schedule or on the next call home:

```
"This device is currently attached to schedule <schedule-name>. If you want software version to be upgraded during the time selected in that schedule, then click "Cancel" and just edit the schedule to change the Desired Software Version associated to this device. However, If you want the software version to be updated on the device at next call-home itself, then click "Ok". This option will remove the device from schedule <schedule-name>."
```

4.1.1.4.5 BLE Configuration

If an Access Point supports the IoT Radio function, the **IoT Radio Configuration** option will be activated on the Edit Device drop-down menu (see page 219). When you select this option, the Edit IoT Configuration screen opens. By default, the “Use Private Config” option on this screen is off and the BLE configuration is derived from the Access Point Group to which the Access Point belongs. If you want to configure private BLE parameters for a single Access Point, enable "Use Private Config" and specify the private settings. If the "Use Private Config" option is turned off at a later time, the private BLE configuration is removed from the AP and the AP Group settings are pushed to the AP or BLE Gateway.

To configure BLE for a single Access Point, set **Use Private Config** to **On**, set the **IoT Radio Mode** to **BLE**, complete the fields as described below, then click on **Save**.

- **Advertising**
  - **Advertising -** Enables/Disables the BLE advertising function for the AP. If enabled, the AP will broadcast BLE packets. If Advertising is enabled, the AP will broadcast BLE packets. BLE Advertising is optional for Asset Tracking. If disabled, the AP will detect surrounding BLE Tags/Beacons and will report information to the server for analysis.
  - **Emission Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)

- **Tx Power -** The transmit power used to broadcast BLE packets, in dBm. (Range = -20 - 10, Default = 4)
- **Tx Channel -** The transmit channel used to broadcast BLE packets. It is recommended that you use a different channel than the channel used for the WLAN.
- **Advertising Protocol -** Specify the BLE protocol used to define the broadcasting BLE beacon format.
  - **iBeacon -** Apple iBeacon format.
  - **Eddystone-URL -** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
  - **Eddystone-UID -** Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
    - **Namespace -** 20 characters containing 0-9a-f.
    - **Instance ID -** 12 characters containing 0-9a-f.

- **Scanning**
  - **Scanning -** Enables/Disables the Bluetooth beacon scanning function for the AP.
  - **Scanning Interval -** The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
  - **OUI Allowlist -** Specify the MAC OUI Allowlist to filter devices for BLE beacon broadcasting. Only those beacons broadcasting from the devices within the OUI Allowlist are valid and will be reported.

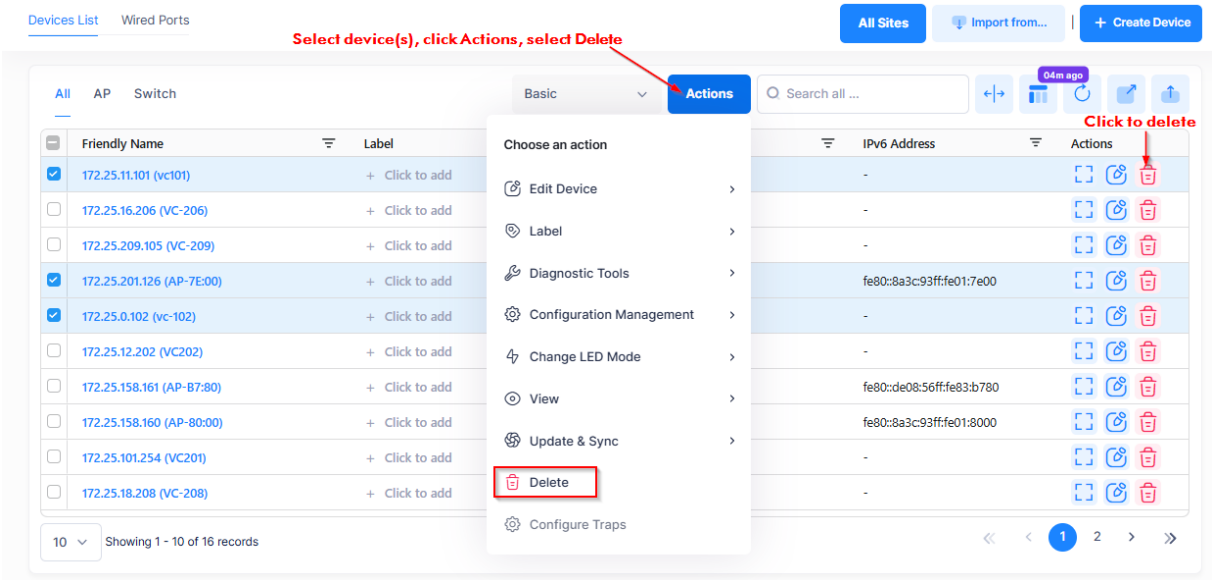
21 Oct 2025

4.1.1.5 Delete a Device

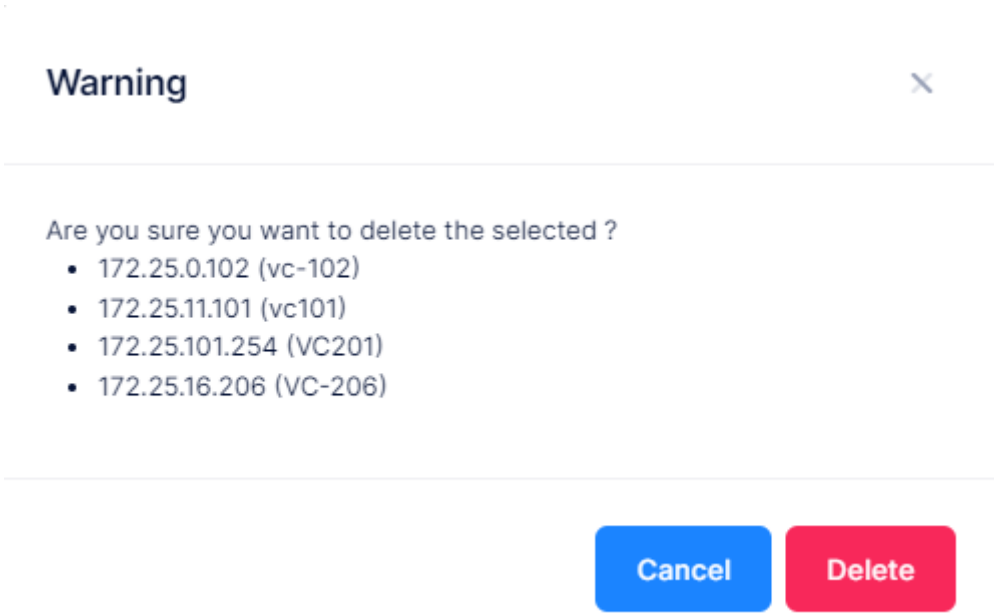
When you delete a device from the Device Catalog list, the device is no longer managed by OmniVista Terra.

You can delete one or more devices from the Device Catalog using one of the following options:

- To delete one or more devices, select the device(s) that you want to delete then click on **Actions** and select **Delete**. All the devices selected will be removed from the list.
- To delete just one device, click on the Delete icon under the “Actions” column next to the device that you want to delete. Note that the Delete icon is only available in the “Basic” Device Catalog (see page 170) view.



When you delete one or more devices, you are prompted to confirm your delete request.

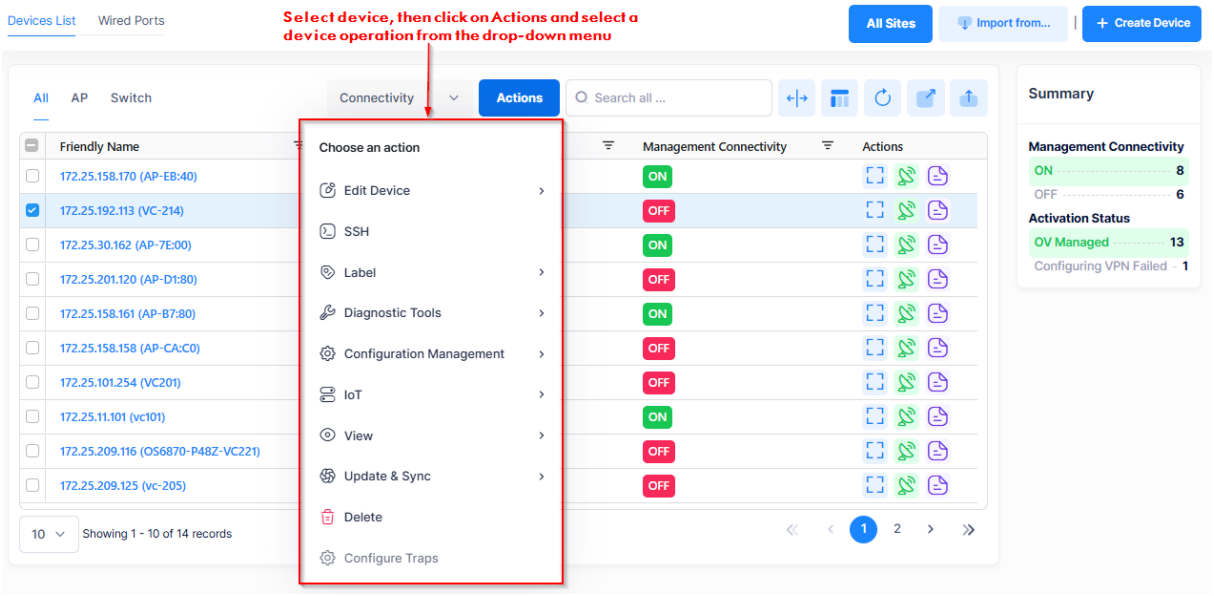


Click on **Delete** to confirm that the device(s) should be removed from the Device Catalog list.

21 Oct 2025

4.1.1.6 Perform Device Operations

In addition to performing actions, such as adding, editing or deleting devices, you can perform additional device operations by selecting a device(s) in the list, then clicking on **Actions** to select one of the operations described below. Note that the **Actions** button does not appear until you select a device.



> Not all operations are supported on all devices, and some operations can only be performed on a single device, not multiple devices. If an operation is not supported for the selected device(s), it will be grayed out or not included in the list.

- **Edit Device** - Edit the device settings (see page 217).
- **SSH** - Opens up an SSH or Telnet session with the selected device on the Terminal screen.
- **Label** - Assign one or more labels to the device. Assigning labels to device(s) allows you to group managed devices together. All devices that have the same label belong to the same group. This also allows grouping of different device types. For example, if you assign the same label to Switches and to APs, both of those device types are included in the same group.
- **Web UI (AP only)** - You can connect to individual Stellar APs using the Web UI Device Management Tool. The tool can be used to view and configure certain management parameters on an individual AP. Select an AP device in the catalog list, then click on **Actions** and select AP Web from the drop-down menu. The Login page for the Web UI Management Tool will appear. The password is set on the Provisioning Configuration Screen (see page 313) (AP Web configuration).
- **License** - Assign or release a license for the selected device(s). See the online help for Using the Device Catalog to Manage Device Licenses (see page 164) for more information.
- **Diagnostic Tools**

- **OmniVista Terra Agent (Switch only)** - When a Switch running AOS 8.9R1 or higher is added to the Device Catalog, OmniVista pushes the OmniVista Terra Agent (see page 232) to the Switch, then installs and starts the agent on the Switch. The following options allow you to manage the OmniVista Terra Agent on the Switch from the OmniVista UI:
  - **Upload Package File** - Upload the OmniVista Terra Agent package on the Switch. Note that after the Agent package is uploaded to the Switch, the running configuration should be saved (see page 229) before the Desired Software Version (see page 288) for the switch is set.
  - **Upload Configuration File** - Update the OmniVista Terra Agent Config and/or Monitoring files.
  - **Status** - View the status of the OmniVista Terra Agent that is running on the selected Switch. Use this screen to verify device information, agent version, status, and the last start or stop times of the Monitoring/Config agent components. After a package and/or configuration file updated, the agent is restarted. You can view the Status screen to check the agent status and start times.
  - **Restart Agent** - Manually restart the Config/Monitoring agent components.
- **Ping** - Immediately pings the selected device when you click on **Ping** in the Actions drop-down menu. OmniVista pings the device to determine reachability and manageability. The “Management Connectivity” field for the device will reflect the results of the ping for approximately two minutes (**On** = success, **Off** = failure). If after two minutes a message is received from the device, the Management Connectivity status updates to **On**. However, if the status is **Unknown**, then after approximately three minutes with no message from the device, the status changes to **Off**.
- **Reboot** - Manually reboots the selected device(s). The reboot operation is different depending on the device type. Note that the Reboot action is supported on Switches running AOS 8.9R4 or higher, and that if you select both Switch and AP devices,, only the Switches will be rebooted.
  - **Switch Device** - When you select a Switch(es) and click on **Reboot** from the **Actions** drop-down menu, you are prompted to select the switch directory that you want to reboot from (Working, Certified, or Other Directory) and when you want the reboot to occur (now, a specific number of minutes from now, or at a specific date and time). Note that when you reboot multiple devices, there is a minimum delay of 30 seconds before the devices reboot (even if you select the Reboot now option). If you select a large number of devices, the delay is equal to roundoff of (30 + (deviceCount/4), in seconds (e.g., if you select 1,000 devices, the delay is 280 seconds, or 4 minutes). The delay allows time to push the "Reboot" command to all devices.
  - **AP Device** - When you select an AP device(s) and click on Reboot from the Actions drop-down menu, you are prompted to confirm the reboot of the selected AP device(s). Click **OK** to continue. When a Stellar AP device is rebooted, the latest configuration available on OmniVista is downloaded to the device. If the device is unable to connect to OmniVista, the device will reboot with the latest saved local configuration.
- **Reset (AP only)** - You can reset an AP by selecting the AP(s), then click Actions and select **Reset** from the drop-down menu. The AP will reset to the factory default configuration and

reboot. When an AP is rebooted as part of a reset, the latest configuration available on OmniVista is downloaded to the AP. If the AP is unable to connect to OmniVista, the AP will come up with the factory default configuration.

- **Ping from device (AP only)** - Specify the host FQDN or IP address that you want to ping from the device.
- **Traceroute from device (AP only)** - Specify the host FQDN or IP address that you want to run a traceroute from the device.
- **Collect Support Info** - Collects log information from the device that you can then send to the Alcatel-Lucent Enterprise (ALE) team to troubleshoot problems. See the Collect Support Information (see page 1018) online help for more information.
- **Troubleshoot Device** - Opens the Device Troubleshooting (see page 970) screen for the selected device. From this screen, you can view a list of assigned commands previously issued to network devices, create troubleshooting commands to issue to network devices, edit and delete assigned commands.

- **Configuration Management**
  Note: All of the following Action options, except for “Save to Running”, apply only to switch configurations.
  - **Save to Running** - Saves the current running configuration to the current “working” directory of the selected device.
  - **Copy Running to Certified** - Copies the contents of the working/running directory to the certified directory of the selected switch.
  - **Copy Certified to Running** - If the selected switch is running in the working or a custom directory, this action copies the configuration of the certified directory to the working or custom directory.
    Note: If the selected switch is running in the certified directory, this action appears to work in the UI; however, it is not allowed on the switch. OmniVista will raise an Alert indicating that the action failed to apply the configuration.
  - **Instant Backup** - Triggers an immediate backup of the switch configuration.
  - **Configuration Backups** - Redirects to the Configuration Backups (see page 290) screen to display configuration backup files for the selected device.
  - **Mark as Golden Config** - Sets the current Running Configuration as the Golden Configuration (see page 248) for the switch. Once the Golden Configuration is set, a periodic audit function is automatically activated. When the audit is running, it will compare the Running Configuration to the Golden Configuration to detect any changes and will raise Alerts if OmniVista detects any deviations.
  - **View Device Configuration** - Redirects to the Device Detail screen where you can view and compare the Running Configuration and saved Golden Configuration for the switch. This option is available only when the Running Configuration has drifted from the Golden Configuration. The Summary panel on the Device List Configuration view provides a “Drift detected” (see page 252) counter that indicates the number of switches with a Running Configuration that is different from the Golden Configuration.

  - **Unmark as Golden Config** - Remove the Golden Configuration designation from the Running Configuration for the switch. Note that removing the Golden Configuration automatically disables the periodic auditing for the device(s).
  - **Resume Periodic Audit** - Restarts an activated periodic audit. When this option is greyed out, a periodic audit of the Running Configuration is currently running.
  - **Pause Periodic Audit** - Pause a periodic audit of the Running Configuration. By default, a periodic audit is performed once a day. You can set the time of day that the audit is performed by configuring the Audit Configuration setting on the Basic Settings screen (see page 130).
  - **Perform Audit** - Triggers an immediate audit of the Running Configuration.
- **Enable/Disable IoT**- The IoT feature provides a detailed, "real-time" view of all endpoint devices connected to Stellar AP or AOS switch devices (e.g., PCs, Tablets, Smartphones). IoT is disabled on devices by default. You can enable the IoT feature by selecting the device(s), then click on **Actions** and select **Enable IoT** from the drop-down menu. (Note that enabling or disabling IoT is not offered in the Actions drop-down menu if the device does not support IoT.) When IoT is enabled, OmniVista will begin collecting IoT information for endpoints connected to the selected devices. To view the IoT information collected, go to the IoT Devices screen (**Network > Access Records > IoT Devices**) under the “Monitor” section of the OmniVista Terra Menu (see page 45).
- **Change LED Mode (AP only)** - Select one of the following options to set the LED mode for the AP:
  - **Save as Normal Mode** - The LED displays in normal mode (Red/Green/Blue).
  - **Save as Night Mode** - The LED indicator is shut off.
  - **Save as Blink Mode** - LED alternately blinks Red/Green/Blue so that you can visually locate the AP(s).
- **View**
  - **Application Visibility (AP only)** - Redirects to the Application Visibility (see page 862) screen where you can view analytics for application/protocol flows based on Application Signatures that identify an associated application or protocol.
  - **Collect Support Info** - Redirects to the Collect Support Information (see page 1018) screen where you can collect log information from network devices for the Alcatel-Lucent Enterprise (ALE) team to troubleshoot problems.
  - **In Topology** - Displays the selected device in the network topology map.
  - **IoT Devices** - Redirects to the IoT Devices (see page 558) screen to display detailed information for all endpoint devices that are connected to the network (e.g., PCs, Tablets, Smartphones).
  - **Mesh Topology (AP only)** - Displays the Mesh topology for the organization. This option is available if the AP device is participating in a Mesh configuration. See the AP Mesh Configuration (see page 238) online help for more information.
  - **Neighbor APs** - Displays a list of neighbor APs to which the connected wireless client might roam. The list includes static and automatically-discovered neighbors. See the Managing Access Point Neighbors (see page 236) online help for more information.

    - **Traps** - Redirects to the Network Events (see page 981) screen to display trap notifications for the selected device(s).
    - **Wired Clients** - Redirects to the Wired Client Sessions (see page 837) screen to display sessions for the selected devices. Note that you can select up to 10 devices in the Device List. However, you cannot select both Switch and AP devices to display Wired Client Sessions.
    - **Wireless Clients (AP only)** - Redirects to the Wireless Client Sessions (see page 833) screen to display sessions for the selected AP devices. Note that you can select up to 10 APs in the Device List. However, you cannot select both AP and Switch devices to display Wireless Client Sessions. In addition, you cannot view wired clients connected to AP devices from the Device List; instead, go directly to the Clients screen (see page 826).
- **Update & Sync (Switch only)**
    - **Rediscover** - Triggers an immediate polling of the selected device(s) to update Switch information known to OmniVista Terra. For example, you may not want to wait until the next polling interval to update any changes to the Switch configuration (such as status, VLAN members, ports, IP address). When you click on **Rediscover** in the **Actions** drop-down menu, you are prompted to confirm the rediscovery of the selected device(s). Click **OK** to continue and a progress screen will appear. When the discovery is complete, the Device Catalog information for the device(s) is updated.
    - **Poll Links** - Triggers an immediate polling of the selected device(s) to discover links.
    - **Poll for Traps** - Triggers an immediate polling of the selected device(s) to update trap information.
- **Delete** - Deletes the selected device(s) from the Device List. Note that the device is then no longer managed by OmniVista Terra, but may still be up and running in the network.
- **Configure Traps** - Redirects to the Create Event Configuration (see page 1004) screen where you can configure the traps that you want the selected device to send to OmniVista Terra.
- **More Actions…** - Displays the Detailed Device Information (see page 217) screen for the selected device. This screen displays all of the configuration information about the device and allows you to perform actions on the device.
- **Advanced Actions** - This option is available on the Actions drop-down menu of the Detailed Device Information (see page 217) screen.
    - **Launch Heat Map** - Opens the Wi-Fi Heatmap screen which provides a visual representation of the wireless signal coverage and strength of Access Points connected to the network. See the Wi-Fi Heatmap (see page 943) online help for more information.

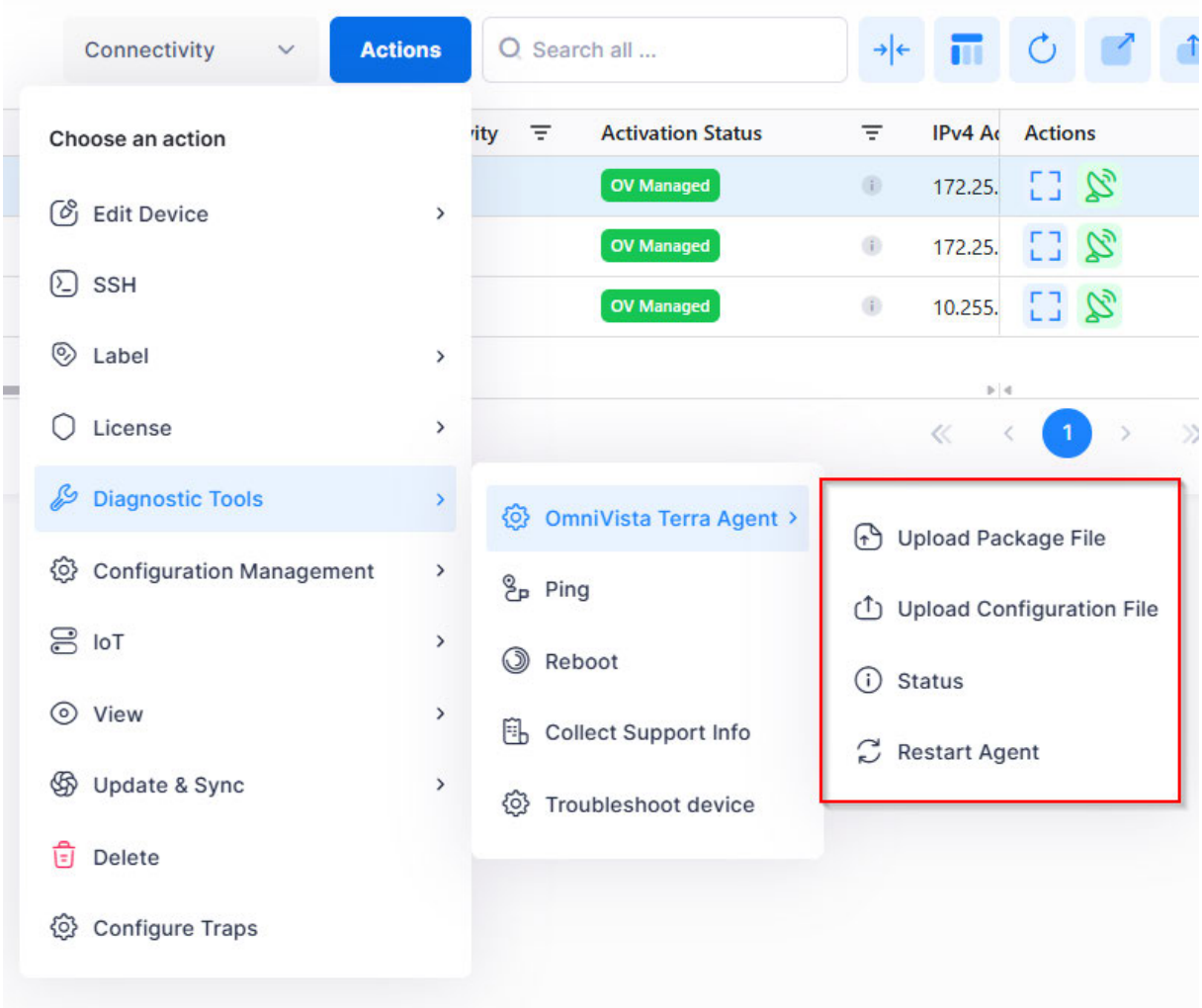
21 Oct 2025

4.1.1.6.1 OmniVista Terra Agent

The OmniVista Terra Agent is an independent package that OmniVista automatically downloads, installs, and starts on a switch when the switch is added to the Device Catalog. The package consists of a monitoring and configuration agent that interacts on a push-pull, on demand basis with OmniVista to manage switches.

> Note that if you change the Running directory on the switch, then you must force provision the switch to get the Agent to start.

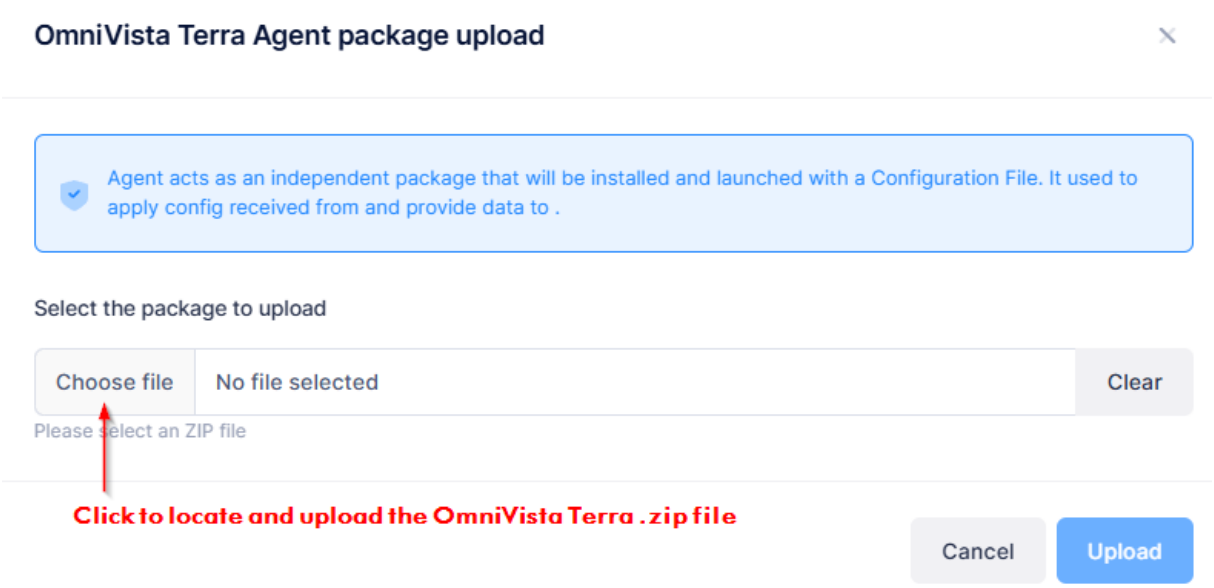
The OmniVista Terra Agent options under Diagnostic Tools (see page 227) in the Device Catalog allow you to manage the Agent on the switch from the OmniVista UI. To access these options, select one or more devices, then click on **Actions > Diagnostic Tools > OmniVista Terra Agent**.



Please coordinate with your Alcatel-Lucent Enterprise Technical Support representative before attempting to use the “Upload Package File” or “Upload Configuration File” options.

Upload Package File

Use this option to upload the OmniVista Terra Agent package on the switch. Click on the “Choose file” field to locate the OmniVista Terra Agent .zip file, then click on **Upload**.



After the Agent package is uploaded to the switch, the following message displays:

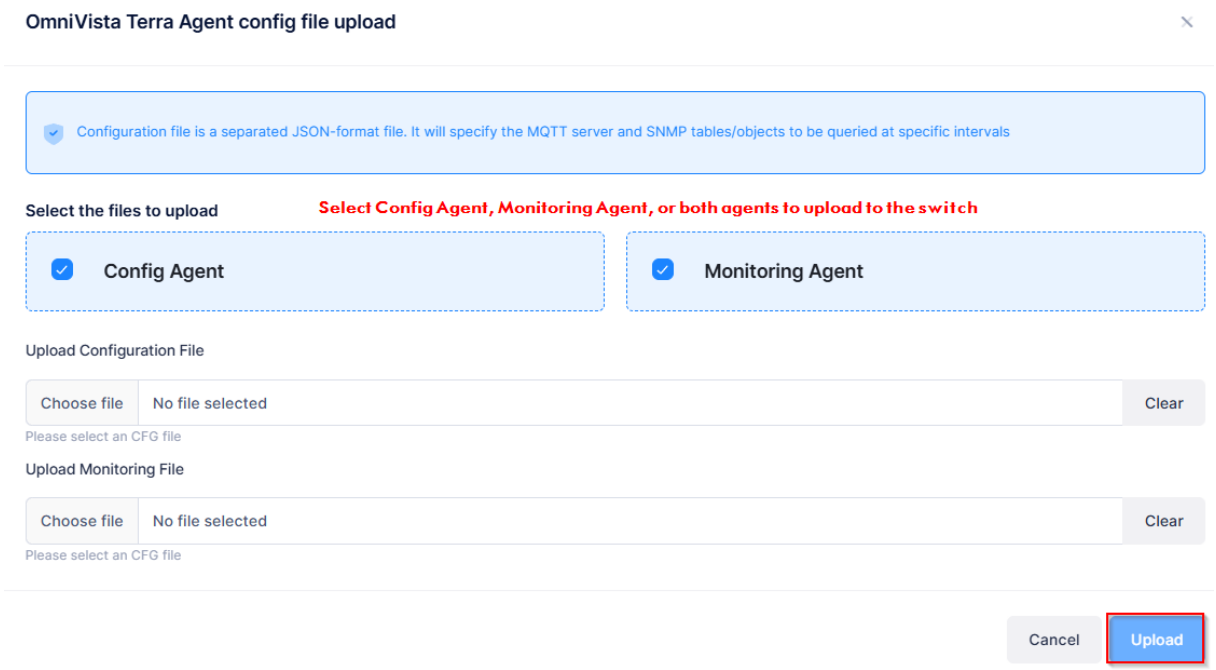
"The package upload request has been successfully sent to the device(s). Please check the agent status after few minutes."

The Agent is restarted after the package update. You can see the installed version, status, and start time on the OmniVista Terra Agent Status (see page 234) window.

Note: After the Agent package is uploaded to the switch, save the switch running configuration before setting the Desired Software Version (see page 288) for the switch.

Upload Configuration File

Use this option to update the OmniVista Terra Agent Configuration and/or Monitoring agent files. Select the Config Agent, Monitoring Agent, or both agents, then click on the appropriate “Choose File” field to locate the .cfg and click on **Upload**.



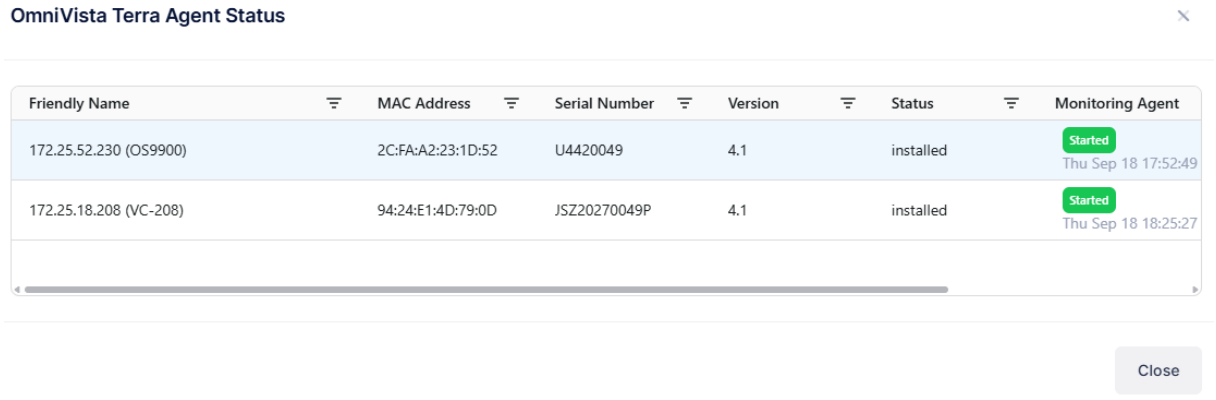
After the Config or Monitoring agent file is uploaded to the switch, the following message displays:

"The package upload request has been successfully sent to the device(s). Please check the agent status after few minutes."

The Agent is restarted after the package update. You can see the installed version, status, and start time on the OmniVista Terra Agent Status (see page 234) window.

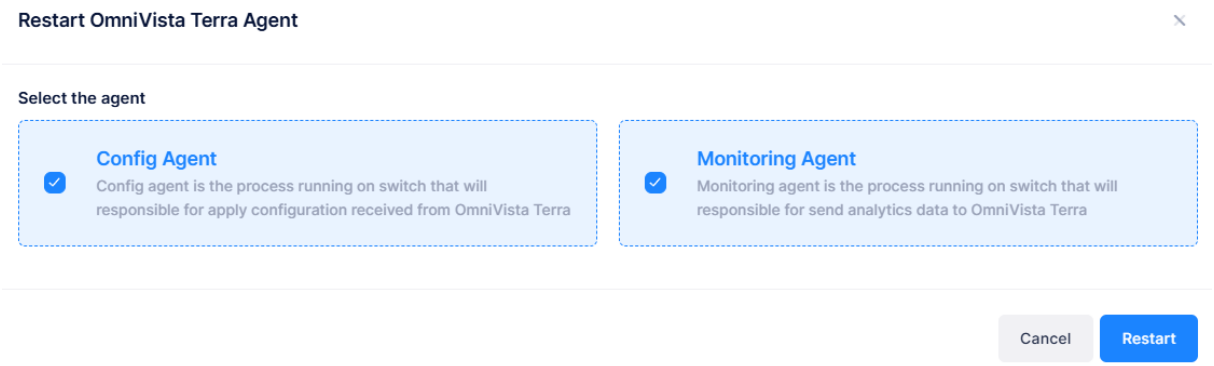
Status

Use this option to verify device information, agent version, status, and the last start or stop times of the Monitoring/Config agent components. After a package and/or configuration file update, the agent is restarted. You can view the Status screen to check the agent status and start times.



Restart Agent

Use this option to manually restart the Configuration and/or Monitoring agent components on the switch. Select the Config Agent, Monitoring Agent, or both agents, then click on **Restart**.



Based on which agent components you selected to restart, the following messages display:

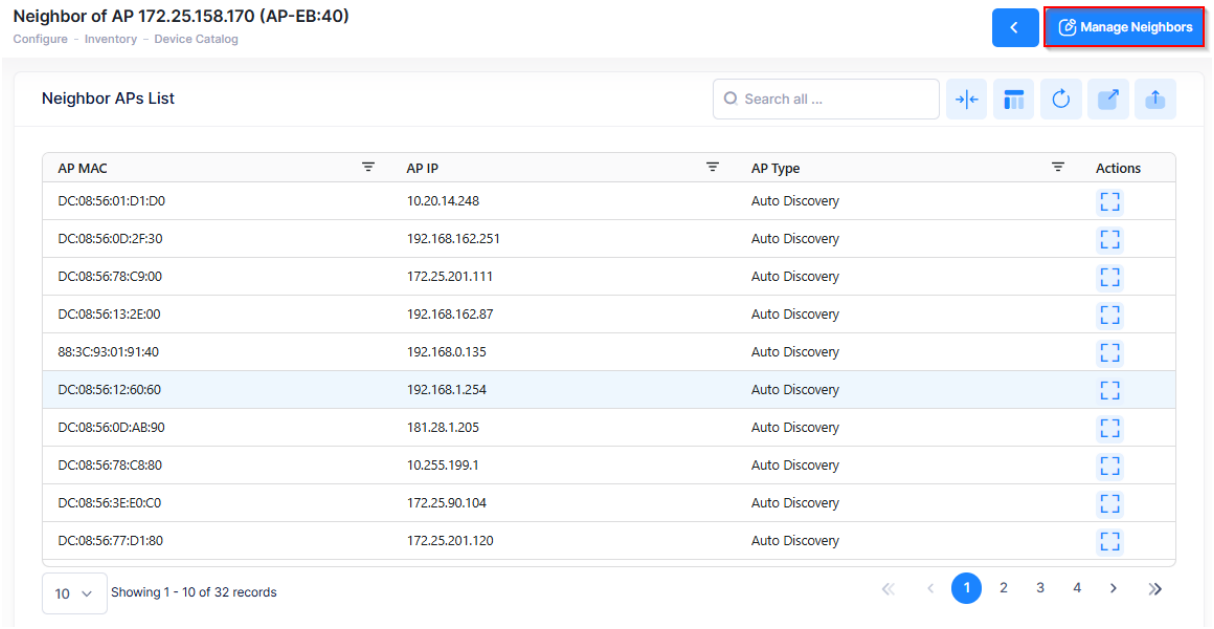
- **Monitoring Agent Message** - “Restart of monitoring agent request has been successfully sent to the device(s). Please check the agent status after few minutes.”
- **Config Agent Message** - “Restart of config agent request has been successfully sent to the device(s). Please check the agent status after few minutes.”
- **Both Agents Message** - “Restart of both config agent and monitoring agent request have been successfully sent to the device(s). Please check the agent status after few minutes.”

The Agent is restarted. You can see the installed version, status, and start time on the OmniVista Terra Agent Status (see page 234) window.

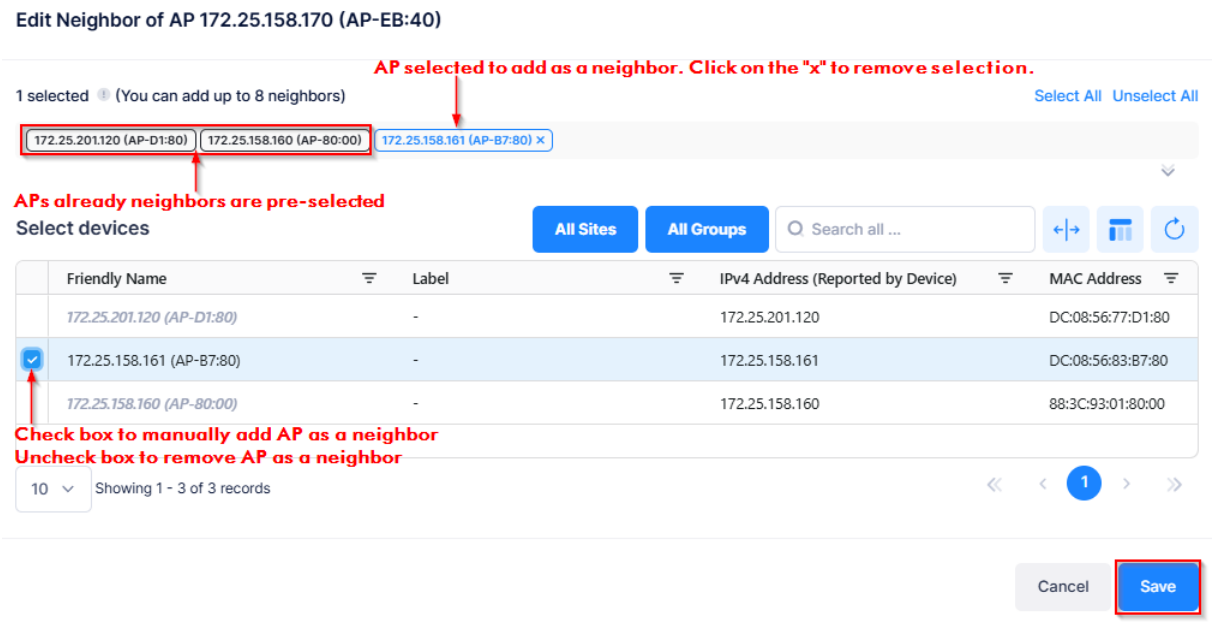
23 Sep 2025

4.1.1.6.2 Managing Access Point Neighbors

Identifying neighbor APs can help to improve network monitoring and optimization. When you select an AP device and click on the **Neighbor APs** option in the View (see page 230) drop-down menu, a list of neighbor APs retrieved from the selected AP is displayed.



The Neighbor APs List displays the AP MAC address, IP address, and AP Type (Auto Discovery or Static) for each of the neighboring APs. To add or remove static APs associated with the selected AP, click on **Manage Neighbors** to open the Edit Neighbor screen.



Use the Edit Neighbor screen to do the following:

- View APs that are already neighbors of the AP.
- View APs available to manually add as neighbors to the AP.

- Select an available AP on the list (APs with a checkbox are available) to add as a neighbor. You can click on **Select All** or **Unselect All** to select or unselect all of the available APs.
- Remove an AP that was manually added as a neighbor by unchecking the box or clicking on the “x” next to the AP entry, as shown above.

When you are done manually adding or removing AP neighbors, click on **Save**.

21 Oct 2025

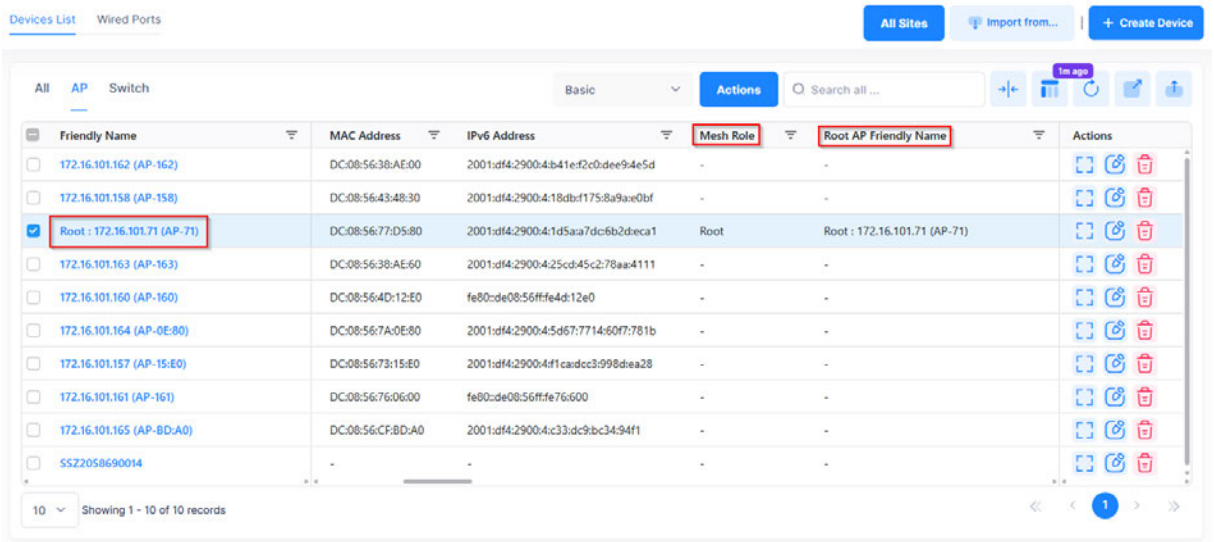
4.1.1.7 AP Mesh Configuration

Out-of-Box Mesh is primarily designed to improve mesh deployment efficiency. To enable it, the administrator must first log in to the AP's Express Mode of the intended Root AP and configure it as the Root using the Express Mode UI. Other leaf mesh points can then automatically join the mesh network without requiring manual configuration. For more details, refer to the Stellar AP User Guide.

By default, a Stellar AP in its factory configuration, when powered on without a wired uplink, will attempt to establish a mesh link automatically using its built-in configuration (Mesh SSID: [Stellar-MESH] and password on the 2.4 GHz band). Once an AP has been connected to a wired uplink, the out-of-box mesh function is permanently disabled. It can only be restored by resetting the AP to factory defaults.

The Device List (see page 170) of AP devices provides the following information to identify APs that are participating in a mesh configuration:

- If the Preferred Device Naming convention in the user preference settings (see page 26) is set to "Mesh Level: IP Address (System Name)", then the Friendly Name for the AP indicates the mesh level for the AP.
- The "Mesh Role" field indicates if the AP serves as the root of the mesh or is a repeater. If this field is blank, the AP is not participating in a mesh configuration.
- The "Root AP Friendly Name" field identifies the root AP for the mesh. The information in this field displays only for mesh APs.

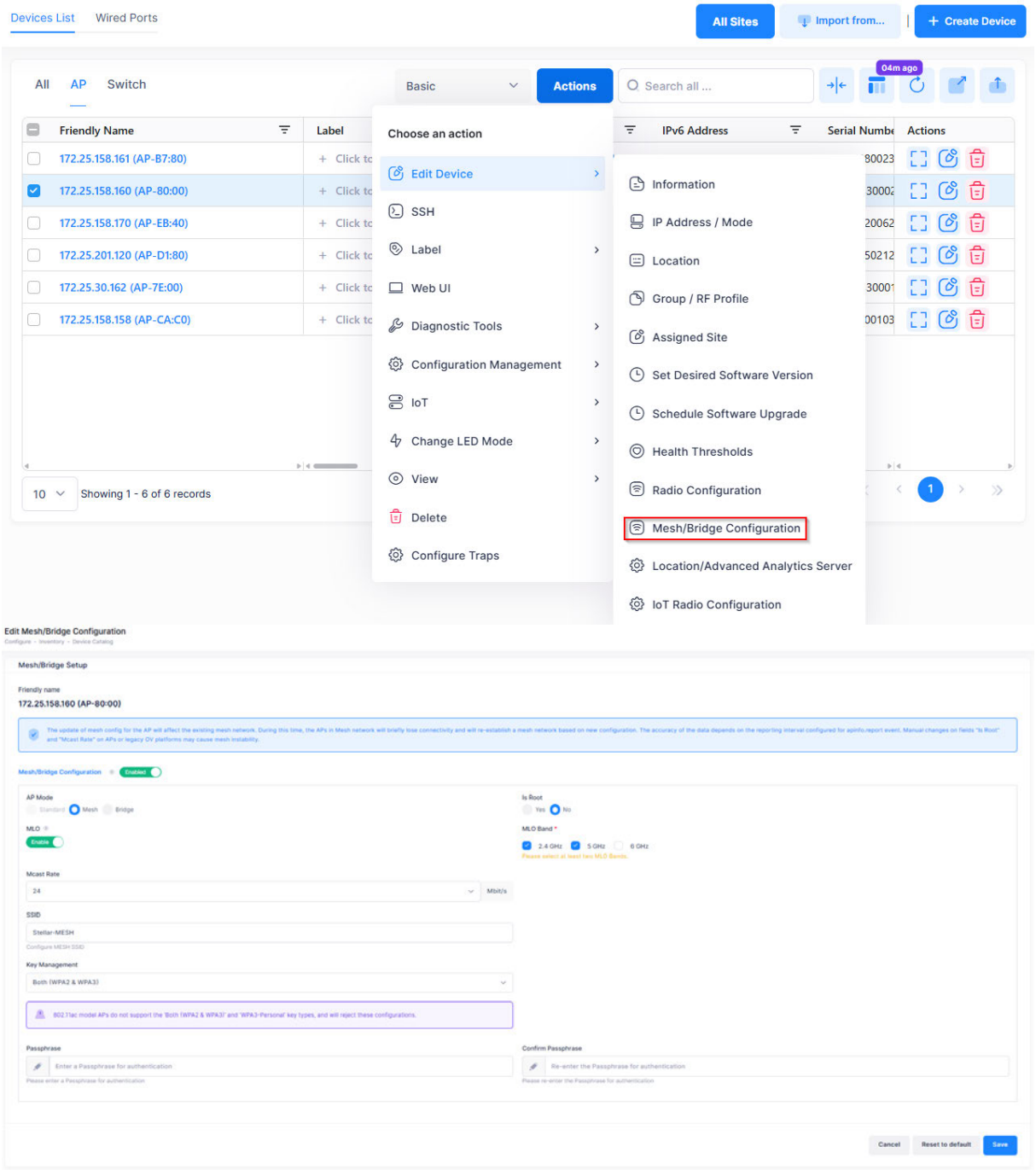


You can also use the Device Catalog List to configure the Mesh settings (see page 238) for an AP and view the Mesh topology (see page 241) for the Organization.

4.1.1.7.1 Configuring the AP Mesh/Bridge Settings

To configure the Mesh settings for a specific AP device, select an AP device from the the Device Catalog List (see page 170) then click on **Mesh/Bridge Configuration** from the **Actions - Edit Device** drop-down menu. The Edit Mesh/Bridge Configuration screen displays the mesh/bridge configuration for the selected AP device.

Note that if Management Connectivity for the device is “Off”, the Mesh/Bridge Configuration option is not available.



To configure the AP mode (mesh or bridge) for the device, enable the “Mesh/Bridge Configuration” option and complete the following fields:

- **AP Mode** - Select Mesh or Bridge for the AP mode.

  - Mesh APs provide network access for wireless clients and establishes a Mesh path to the Mesh root, which uses its wired interface to connect to the LAN network.
  - A Bridge AP is used to create a wireless bridge across two sites. It does not provide any network access directly for wireless clients.
- **Is Root** - Specify whether the device will be the root of the mesh or bridge connection (Yes or No).
- **MLO** - Enables/Disables MultiLink Operation (MLO) for the Mesh configuration. MLO allows Wi-Fi 7 capable APs (currently AP1511/AP1521) to simultaneously send and receive data between different frequency bands and channels. This option only appears on the Edit Mesh Configuration Screen for Wi-Fi 7 capable APs. By default, MLO is disabled and only the radio band is displayed. When MLO is enabled, the "Band" field changes to "MLO Band". Note that the MLO function also relies on the radio status and the radio Extremely High Throughput (EHT) setting. Make sure the corresponding radio and the radio EHT are enabled to activate MLO.
  - **MLO Band -** If MLO is enabled, select at least two of the radio bands to use for Mesh MLO.
- **Band** - If MLO is disabled, select the radio band for the Mesh network (2.4G, 5G, or 6G). Note that selecting the 6G option applies only to AP models that support 6GHz band.
- **Mcast Rate** - The Multicast rate that is applied to "Multicast Video Stream" to help reduce jitters in a Mesh environment. Select the rate to apply to Multicast traffic from the drop-down menu (6, 12, 24, 36, 48, or 54, Default = 24).
- **SSID** - Edit the name of the SSID for the Mesh network.
- **Key Management** - Select the type of encryption to use for the connections between Mesh/ Bridge APs from the drop-down list. Note that 11AC model APs do not support key type “Both(WPA2 & WPA3)”, “WPA3-personal” and will reject configuring these encryption key types.
  - Both(WPA & WPA2)
  - WPA2-Personal
  - Both(WPA2 & WPA3)
  - WPA3-Personal (Note that when 6G Band is selected, only this key type is available)
- **Passphrase** - Enter the passphrase for the Mesh network.
- **Confirm passphrase** - Re-enter the Mesh network passphrase.

When you are done configuring the Mesh/Bridge Configuration for the device, click **Save**. To reset the Mesh/Bridge Configuration back to the factory settings, click on **Restore to Default**.

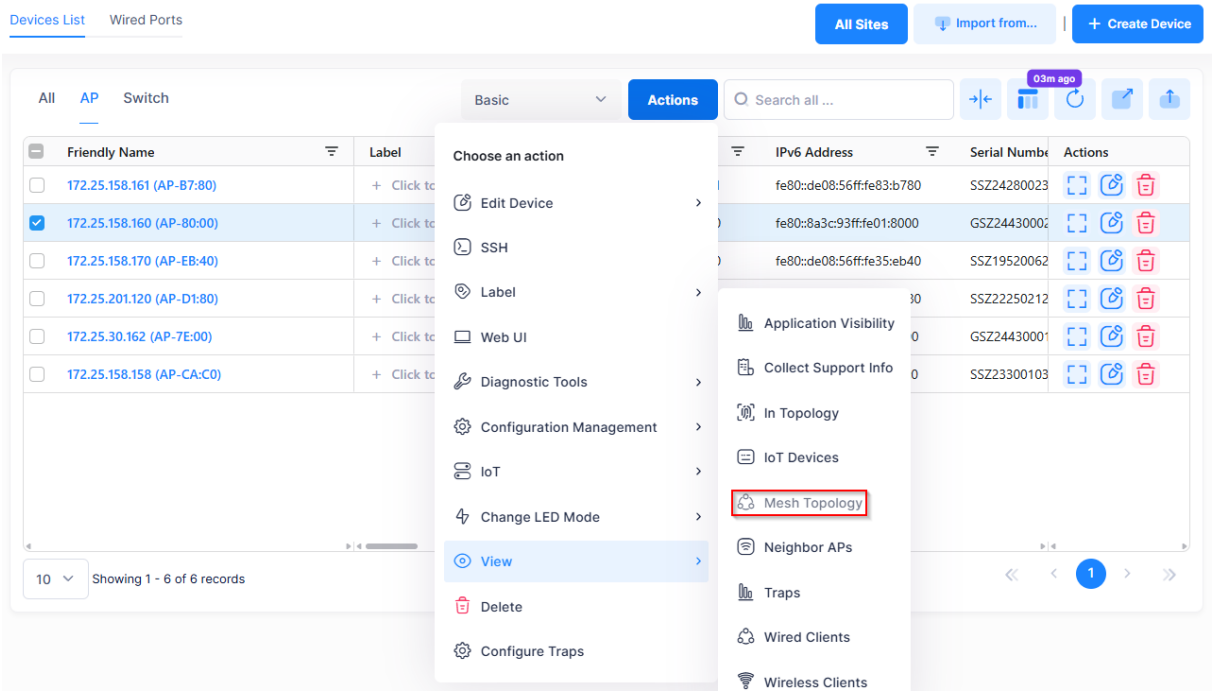
Note that updating the mesh configuration for the AP will affect the existing mesh network. During this time, the APs in mesh network will briefly lose connectivity and will re-establish a mesh network based on the new configuration.

Configuring the Mesh configuration for an AP is particularly useful for an out-of-the-box Mesh configuration. Out-of-the- box Mesh is a feature that helps you quickly set up a Mesh network without configuring the out-of-the-box APs. The out-of-box APs will establish a Mesh network with hardcoded settings. You only need to specify the Mesh root, then other APs will establish a Mesh configuration automatically.

4.1.1.7.2 Displaying the Mesh Topology

> The accuracy of the Mesh topology display depends on the reporting interval configured for the “apinfo.report” event in the OmniVista Terra Advanced Analytics (see page 388) engine profile.

To display the AP Mesh topology for the Organization, select an AP device from the Device List (see page 170), then click on **Mesh Topology** in the **Actions - View** drop-down menu. The Mesh Topology List screen opens.

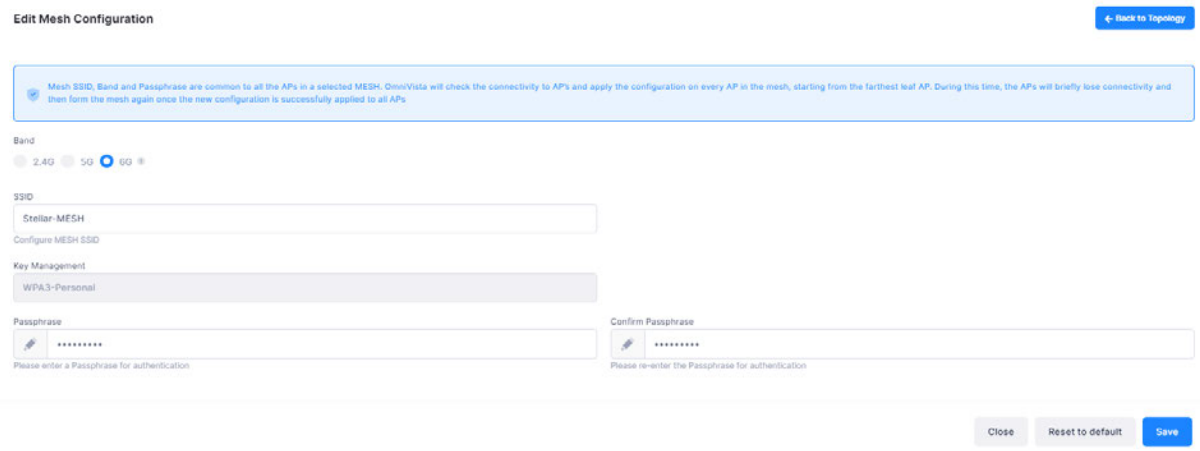


The Mesh Topology List displays all the AP devices participating in the Mesh configuration.

> QoE Analytics (see page 776) also includes data on the Mesh Network. For example, an authorization failure message displays in the QoE Successful Connects (see page 780) classifier when Leaf APs in a Mesh Network exchange a four-way handshake.

4.1.1.7.2.1 Editing Common Mesh Parameters

You can also edit the mesh SSID, band, and passphrase (common to all APs in the mesh) from the Mesh Topology List screen. To edit the common Mesh configuration parameters for the topology, click on **Edit Mesh Configuration** in the **Actions** drop-down menu. The Edit Mesh Configuration screen opens.



Modify the following common Mesh configuration parameters, as desired:

- **Band** - Select the radio band for the Mesh network (2.4G, 5G, or 6G). When selecting the 6G option, make sure that all of the APs in the Mesh network support the 6GHz band.
- **SSID** - Edit the name of the SSID for the Mesh network.
- **Mcast Rate** - This parameter is not configurable from the Edit Mesh Configuration (see page 242) screen, even though it is a common Mesh parameter. Instead, one of the following values is used for the common Multicast rate:
  - The Mcast Rate value specified when configuring the Mesh configuration through OmniVista Terra.
  - The default Mcast Rate value of 24, if another value was not configured through OmniVista Terra.
- **Key Management** - Select the type of encryption to use for the connections between Mesh/ Bridge APs from the drop-down list. Note that 11AC model APs do not support key type “Both(WPA2 & WPA3)”, “WPA3-personal” and will reject configuring these encryption key types.
  - Both(WPA & WPA2)
  - WPA2-Personal
  - Both(WPA2 & WPA3)
  - WPA3-Personal (Note that when 6G Band is selected, only this key type is available)
- **Passphrase** - Enter the passphrase for the Mesh network.
- **Confirm passphrase** - Re-enter the Mesh network passphrase.

When you are done changing any of the common Mesh parameters, click **Save**. The changes are applied to all AP devices in the Mesh. To reset the common Mesh parameters back to the factory settings, click on **Restore to Default**.

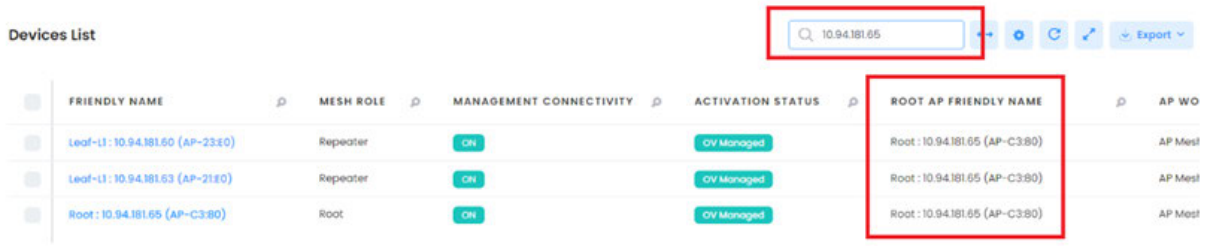
The Mesh SSID, Band, and Passphrase are common to all the APs in a selected Mesh. OmniVista Terra will check the connectivity to each AP and apply the configuration on every AP in the Mesh, starting from the farthest leaf AP. During this time, the APs will briefly lose connectivity and then form the Mesh again once the new configuration is successfully applied to all of the APs.

21 Oct 2025

4.1.1.7.3 AP Mesh - FAQs/Troubleshooting

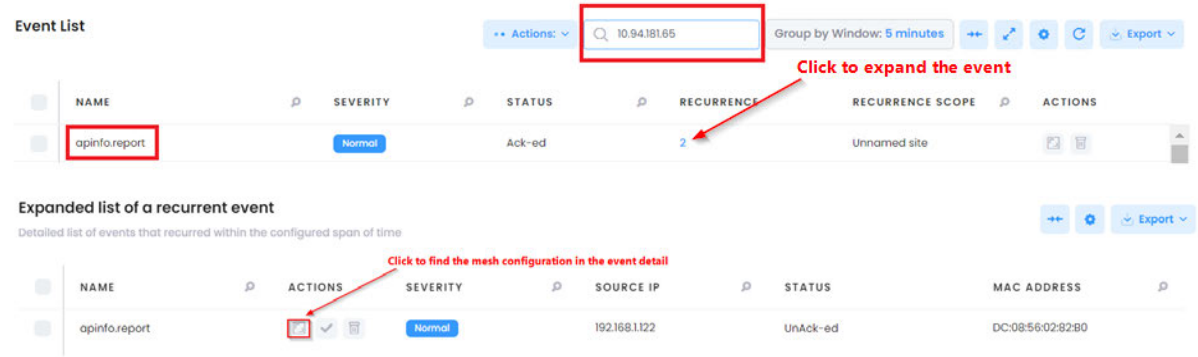
4.1.1.7.3.1 How can I view APs that are part of a specific mesh if there are multiple mesh configurations in my network?

The column “ROOT AP FRIENDLY NAME” in the Device Catalog List (see page 170) contains the information for the Root AP of the mesh network. In order to view a particular mesh, you can search for the specific Root AP either through “search all” or specifically searching through the “ROOT AP FRIENDLY NAME” column.



4.1.1.7.3.2 You changed the AP Mode from Standard to Mesh or updated the existing mesh configuration for an AP, but don’t see the latest changes.

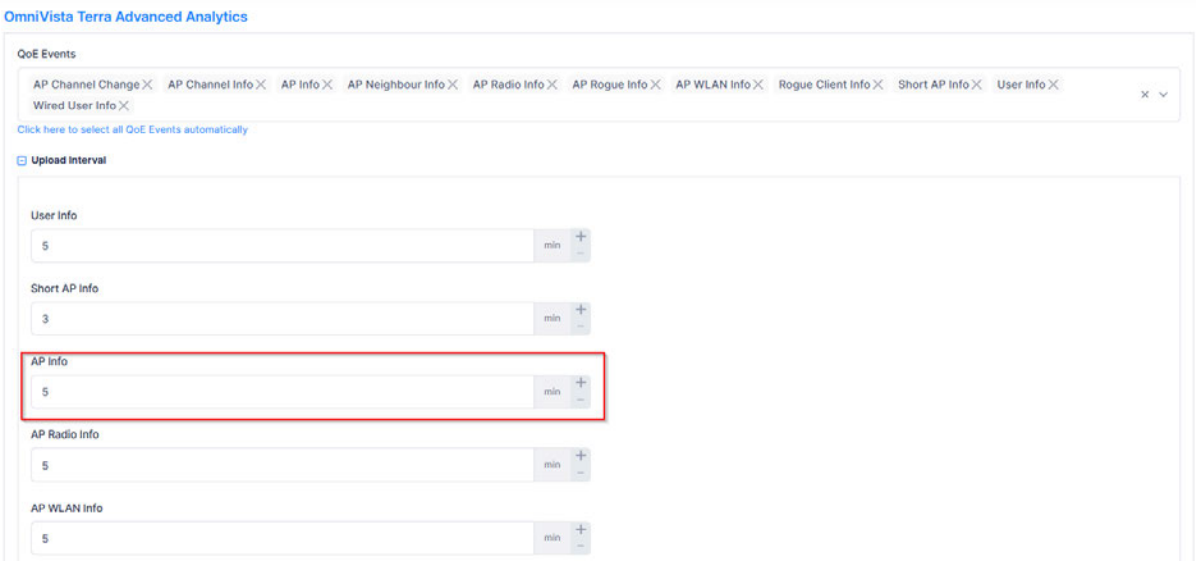
The accuracy of the information reported for the Friendly Name of the AP depends on the reporting interval of the “apinfo.report” event. Check the last received “apinfo.report” event from the QoE Analytics tab on the Events screen (**Diagnostic Tools** > **Events)**.



In the event detail, you can find the most recent Mesh configuration, as shown:

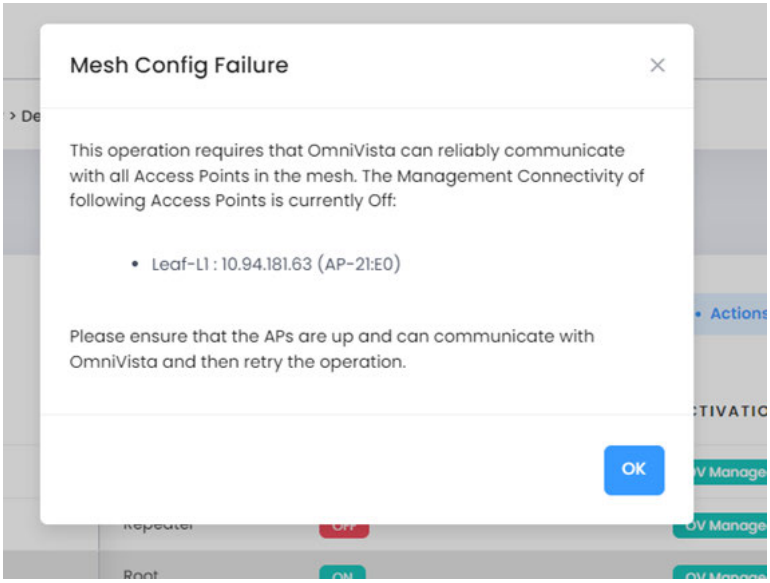

```
"mesh_mode": "Mesh",
"mesh_role": "Root",
"mesh_parent_node": "",
"mesh_ssid": "Stellar-MESH-101",
"mesh_band": "5G",
"bssids": [
 "dc:08:56:77:c3:a2"
],
```


To configure the time interval at which the “apinfo.report” event is sent, go to the OmniVista Terra Advanced Analytics Engine Type (see page 775) screen (**Wireless > Advanced > External Engines**).

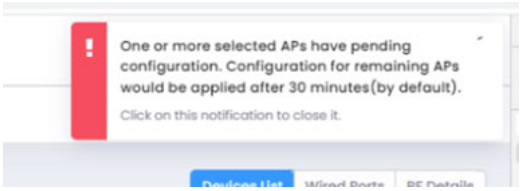


4.1.1.7.3.3 My AP became unreachable during a mesh configuration update for a mesh network.

If any AP is unreachable while performing a mesh configuration update for a mesh network, the below dialog box would appear with details of the AP(s) that are unreachable from OmniVista Terra. You can try applying the configuration again once all the APs in the network are reachable.



4.1.1.7.3.4 When I try to change the mesh configuration for a specific mesh, I receive an error message stating that one or more APs have a pending configuration.

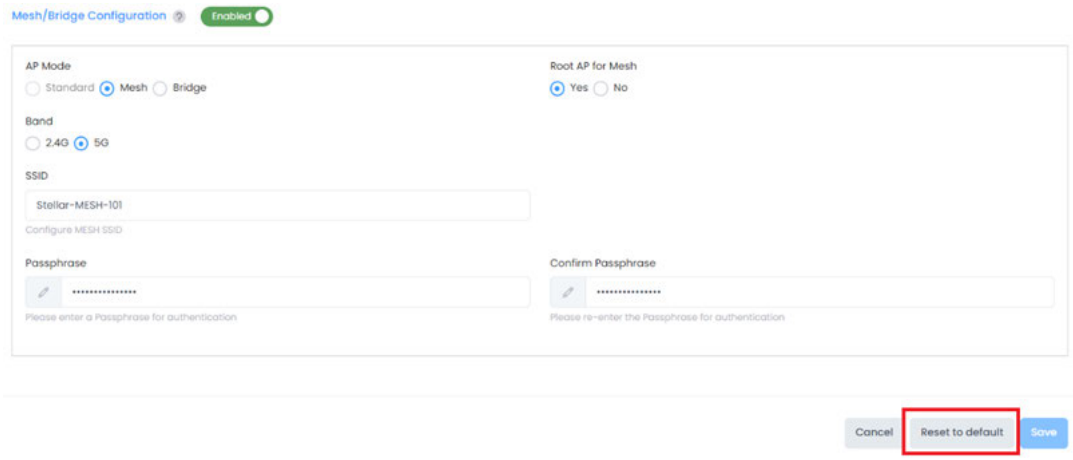


If you receive the above error message when attempting to change the configuration for a specific mesh, consider the following:

- Previously when a user applied a configuration to APs in a mesh network, a service crash might have occurred during the process which resulted in a configuration push interruption for a few APs.
- Ideally, this would take 30 minutes to push the configuration to remaining APs once the related service is up and running. It is recommended to wait for 60 minutes for the service to push the configuration to pending APs.
- In some cases, one or more pending APs might become unreachable due to various factors. So, the service retries this process for around 120 minutes. After this time period, configuration would be pushed to APs in the mesh that are reachable.
- If an AP becomes unreachable, the new configuration cannot be pushed to the AP. The AP will disconnect from the Mesh. When this happens, use Express UI to manually edit the AP mesh configuration to allow the AP to join the Mesh network again.

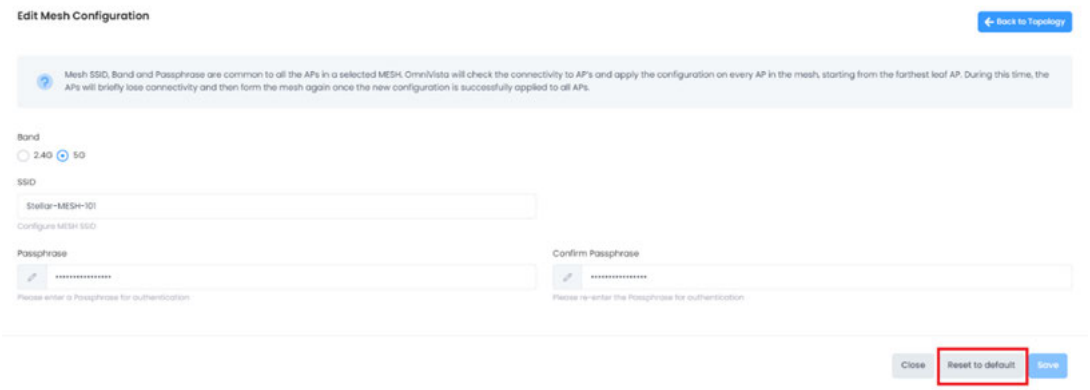
4.1.1.7.3.5 How can I reset the mesh configuration to the factory default for one or more AP(s)?

- To reset the mesh configuration for a specific AP back to the factory default settings, select the AP device from the the Device Catalog List (see page 170) then click on **Mesh/Bridge Configuration** from the **Actions - Edit Device** drop-down menu. When the following screen appears, click on **Restore to default**.



- To reset the mesh configuration for all APs in a specific mesh, select an AP device from the Device Catalog List (see page 170), then click on **Mesh Topology** in the **Actions** drop-down menu. The Mesh Topology List screen displays all the APs participating in the mesh. On this screen,

click on **Edit Mesh Configuration** in the **Actions** drop-down menu. When the following Edit Mesh Configuration screen appears, click on **Restore to default**.



4.1.1.7.3.6 How can I add a Cluster Mode AP to an existing Mesh network in OmniVista Terra?

If the AP is not added to OmniVista Terra and is in Cluster Mode, connect to the default AP Wi-Fi or access Express UI to edit the mesh configuration for the cluster AP (Band, SSID, Passphrase) to be the same as the existing configured Mesh network in OmniVista Terra.

Note: If the AP is connected to a switch port, disable Ethernet on the port while still keeping PoE service enabled on the switch to make sure the AP is UP by Mesh network:

→ lanpower port <portNum> admin-state enable

→ interface <portNum> admin-state disable

4.1.1.7.3.7 If the AP Root is not working, what should I do?

- You can set up another AP Mesh Root with the same existing Mesh configuration (Band, SSID, Passphrase), then the AP Leaves can successfully join the network with the new AP Mesh Root.
- For any reason, the Root AP needs to do a factory reset (hardware reset). After the AP is UP, AP Root UP must get all the Mesh configuration from OmniVista Terra before the factory reset, then the Mesh is successfully formed.

4.1.1.7.3.8 My AP Leaf became unreachable during a new Mesh configuration update and was disconnected from the Mesh network.

The Mesh configuration update process will continue for other AP Leafs until the Root AP. Manual intervention is required to edit the Mesh configuration for unreachable APs using the Express UI. After that, the APs will successfully join the Mesh network.

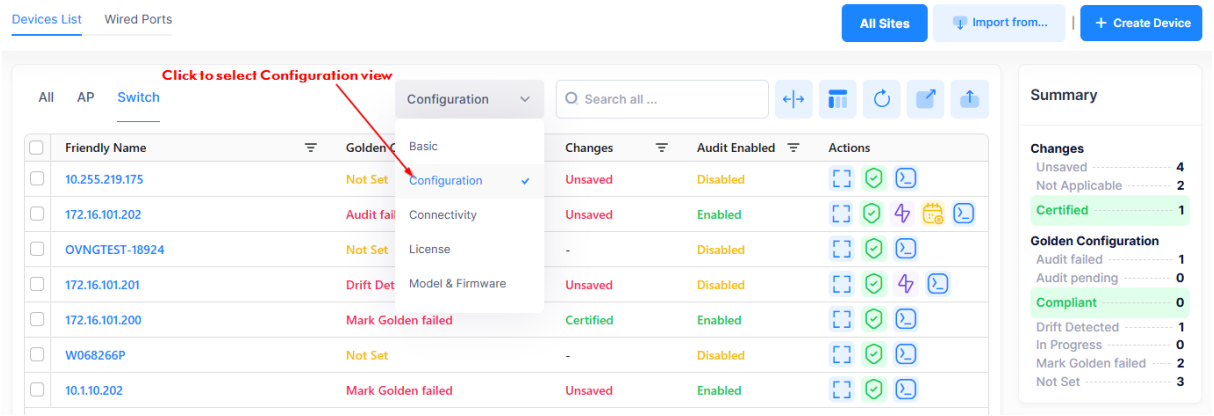
21 Oct 2025

4.1.1.8 Auditing the OmniSwitch Golden Configuration

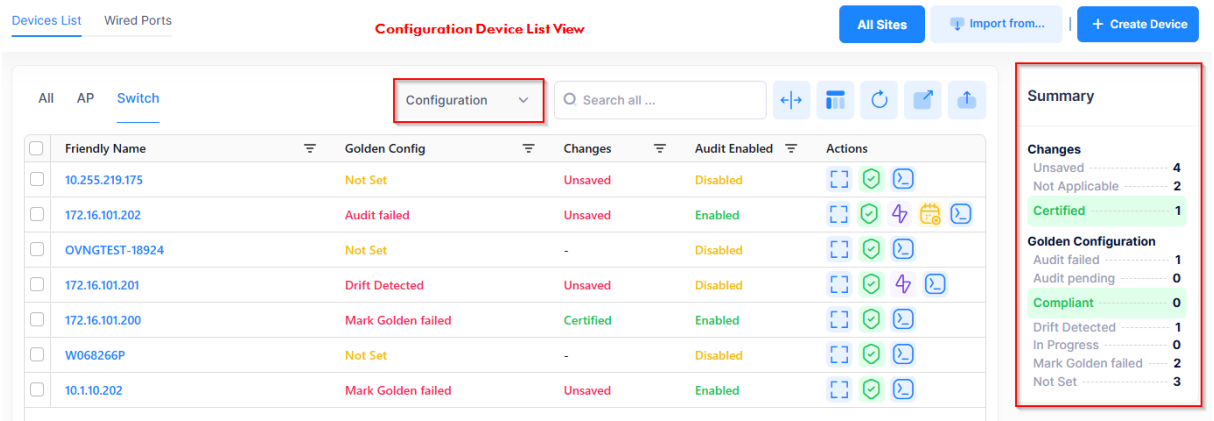
You can audit the Running Configuration of a switch by designating the configuration as a Golden Configuration. Once the Golden Configuration is set (see page 249), an automatic audit function will compare the Running Configuration to the Golden Configuration to detect any changes. If any differences are found during the audit, OmniVista Terra will raise alerts.

The Device List provides a dedicated "Configuration" view (see page 175)that allows you to view configuration information for your OmniSwitch devices, manage Golden Configuration settings, and perform auditing functions. In addition, a Summary panel (see page 251) displays statistics that you can use to analyze configuration changes and the Golden Configuration status.

By default, the "Connectivity" Device List view is selected. To select the "Configuration" view, click on **Configuration**.



The Device List view changes to the following Configuration view:



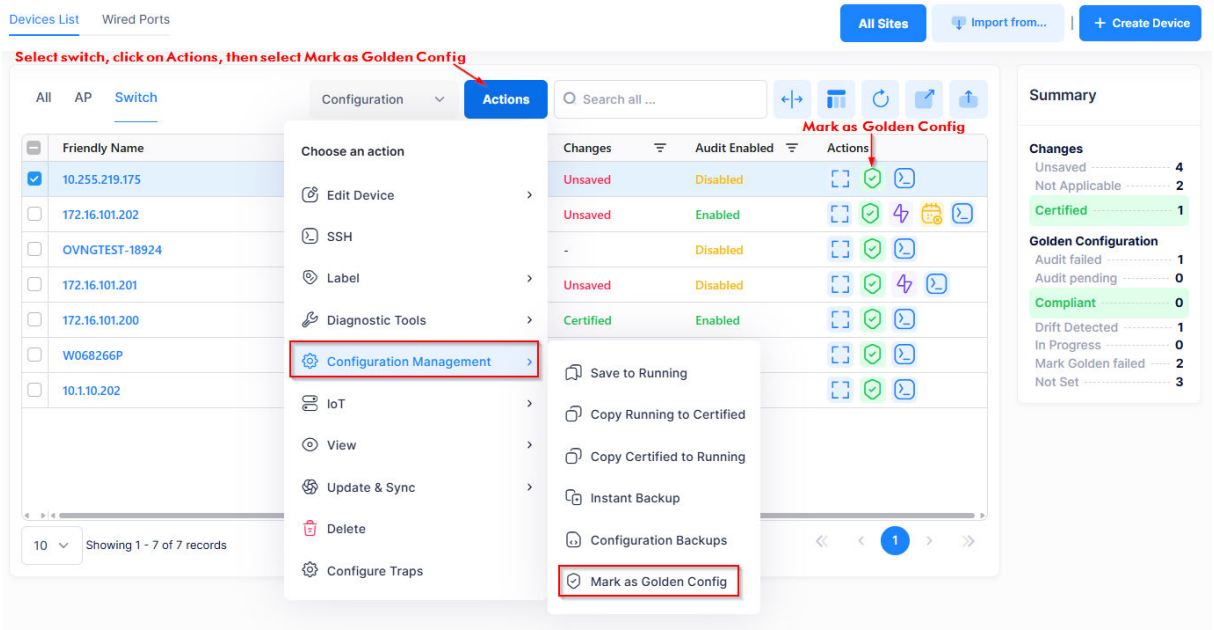
The Configuration view includes a list of switches known to the Organization with the following information:

- Whether or not a Golden Configuration is marked for each switch (see page 249).
- A Summary panel (see page 251) that provides Golden Configuration and Auditing statistics for all the switches.

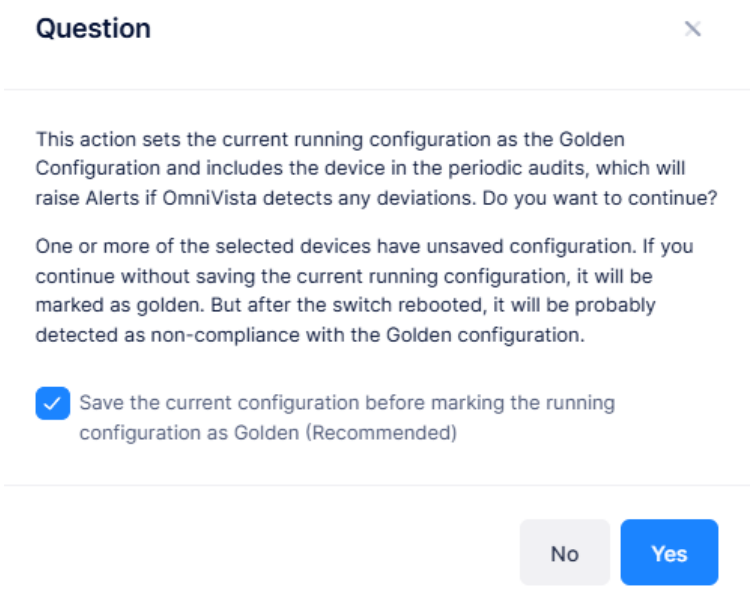
See the Device List Configuration View (see page 175) online help for more information.

4.1.1.8.1 Setting the Golden Configuration

To mark the Running Configuration as the Golden Configuration, select the switch, then click on **Actions** to select **Mark as Golden Config** from the Configuration Management menu. You can also click on the Mark as Golden Config icon under the “Actions” column next to the switch entry.



The following confirmation message appears to notify you of any selected devices with an unsaved configuration:

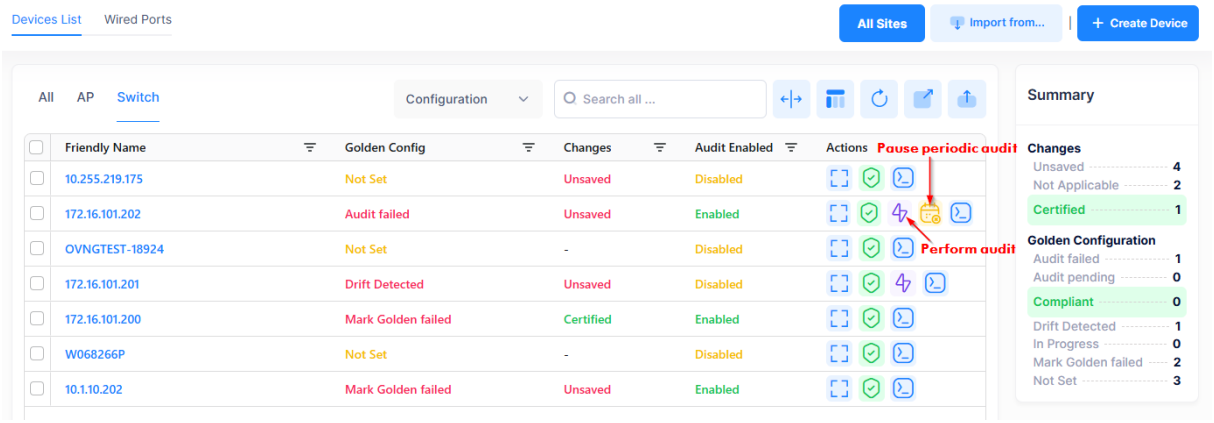


Saving the current configuration before marking the Running Configuration as the Golden Configuration is highly recommended. This option is enabled by default and performs a `write memory flash-synchro` CLI command on the switch to save and certify the current configuration.

Click **Yes** to mark the current Running Configuration as the Golden Configuration for the selected devices.

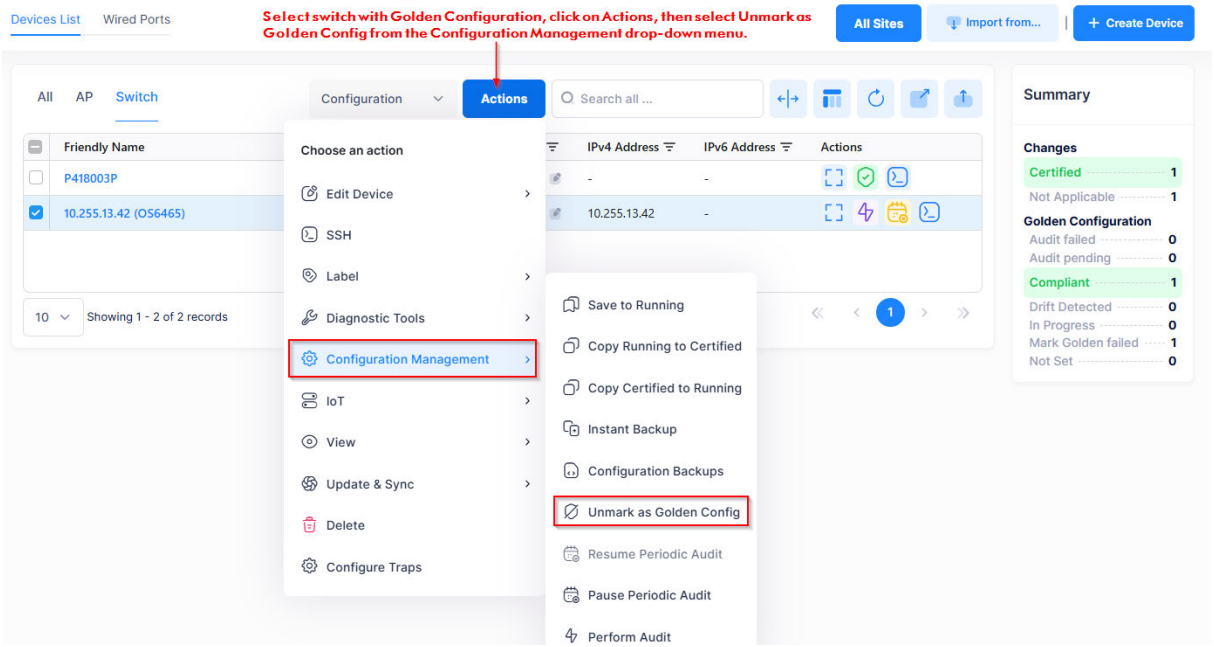
When the Golden Configuration is marked for a device, a periodic audit of the Running Configuration is automatically started and the following icons appear next to the device entry under the “Actions” column, as shown below.

- **Perform Audit** - Triggers an immediate audit.
- **Pause/Resume Periodic Audit** - Click to pause or resume the periodic audit. By default, a periodic audit is performed once a day. You can set the time of day that the audit is performed by configuring the Audit Configuration setting on the Basic Settings screen (see page 127).

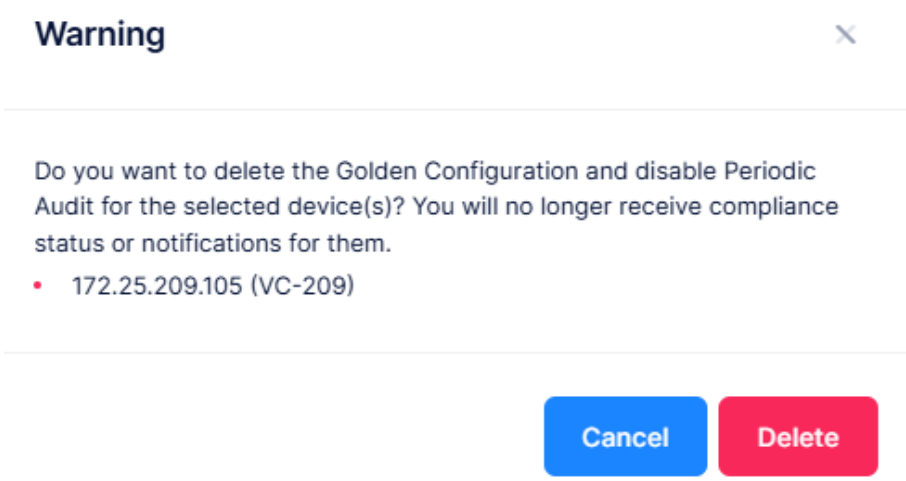


4.1.1.8.2 Removing a Golden Configuration

To remove a Golden Configuration designation for a switch, select the switch, then click on **Actions** to select **Unmark as Golden Config** from the Configuration Management menu.



The following warning message appears listing the device(s) that you have selected to remove the Golden Configuration:

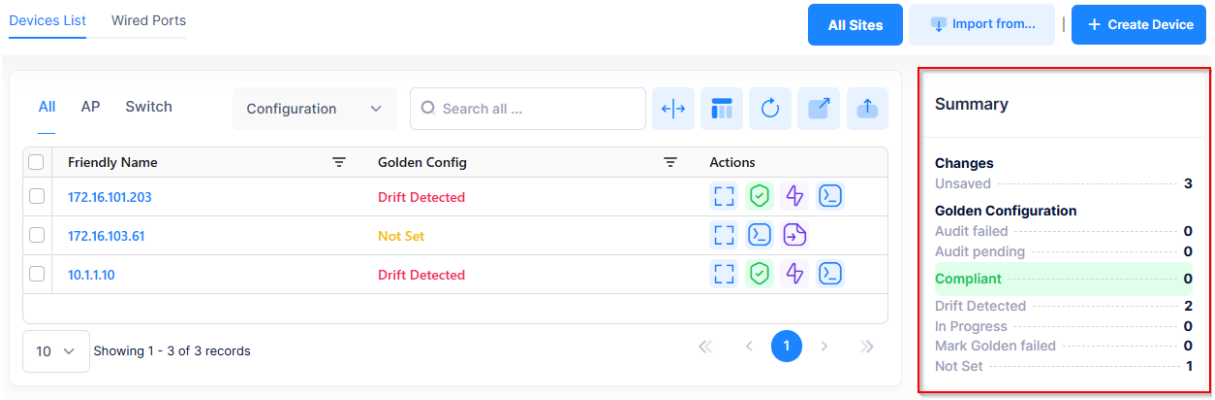


Click on **Delete** to confirm removing the Golden Configuration from the selected device(s). Note that removing the Golden Configuration automatically disables the periodic auditing for the device(s).

4.1.1.8.3 Configuration View Summary

The Summary panel located on the right side of the Configuration view screen, provides configuration statistics that are updated on the next automatic poll of the OmniSwitch.

> The OmniVista Terra polling interval is once an hour to collect switch information. If some information appears out of date, wait until the next polling interval.



The Configuration Summary panel provides the following information:

- **Changes** - Provides statistics for the number of changes to switch configurations.
  - **Certified** - The number of Running configurations that are saved to the Certified Directory on the switch.
  - **Unsaved** - The number of Running Configurations that are not saved.

  - **Uncertified** - The number of Running Configurations that are not saved to the Certified Directory on the switch.
  - **Not Applicable** - The number of devices that changes to the Running Configuration does not apply.
- **Golden Configuration** - The Golden Configuration statistics for all of the switch configurations.
  - **Audit failed** - The number of configuration audits that failed.
  - **Audit pending** - The number of periodic configuration audits that are pending.
  - **Compliant** - The number of managed switches with a set Golden Configuration that does not differ from the Running Configuration per the last periodic audit.
  - **Drift detected** - The number of switches where a difference was detected between the Golden Configuration and the Running Configuration. When a drift is detected, OmniVista raises an Alert. See Restoring a Drifted Configuration (see page 252) for more information.
  - **In Progress** - The number of Running Configurations where the marking as Golden is not yet completed.
  - **Mark Golden failed** - The number of configurations where the attempt to mark the Running Configuration as Golden failed.
  - **Not Set** - The number of configurations that do not have a Golden Configuration designated.

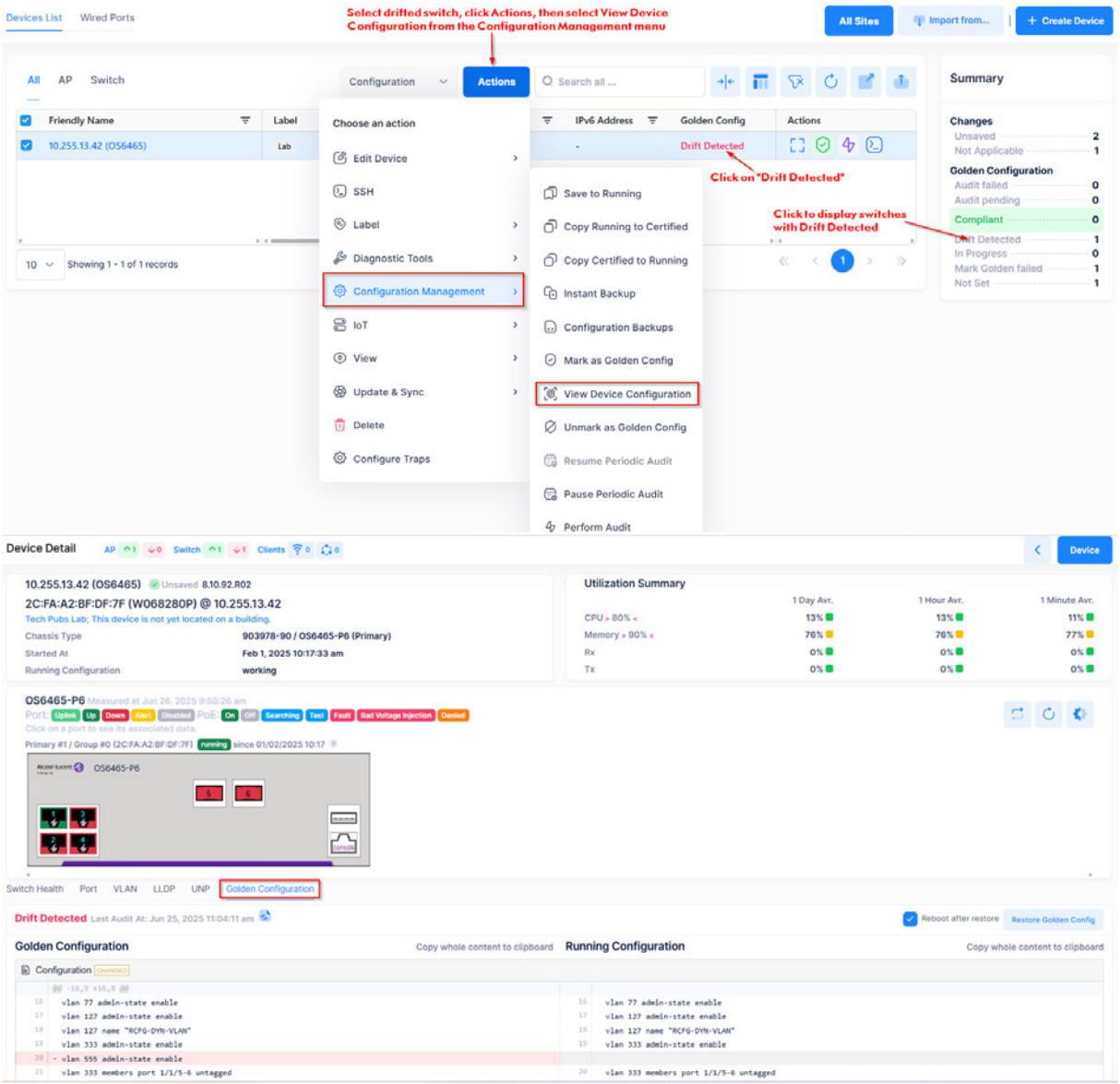
4.1.1.8.4 Restoring a Drifted Running Configuration

When a drift occurs between the Running Configuration and the saved Golden Configuration, you can view both configurations to compare the differences. In addition, you can restore the Golden Configuration and/or copy the Running and Golden Configuration contents.

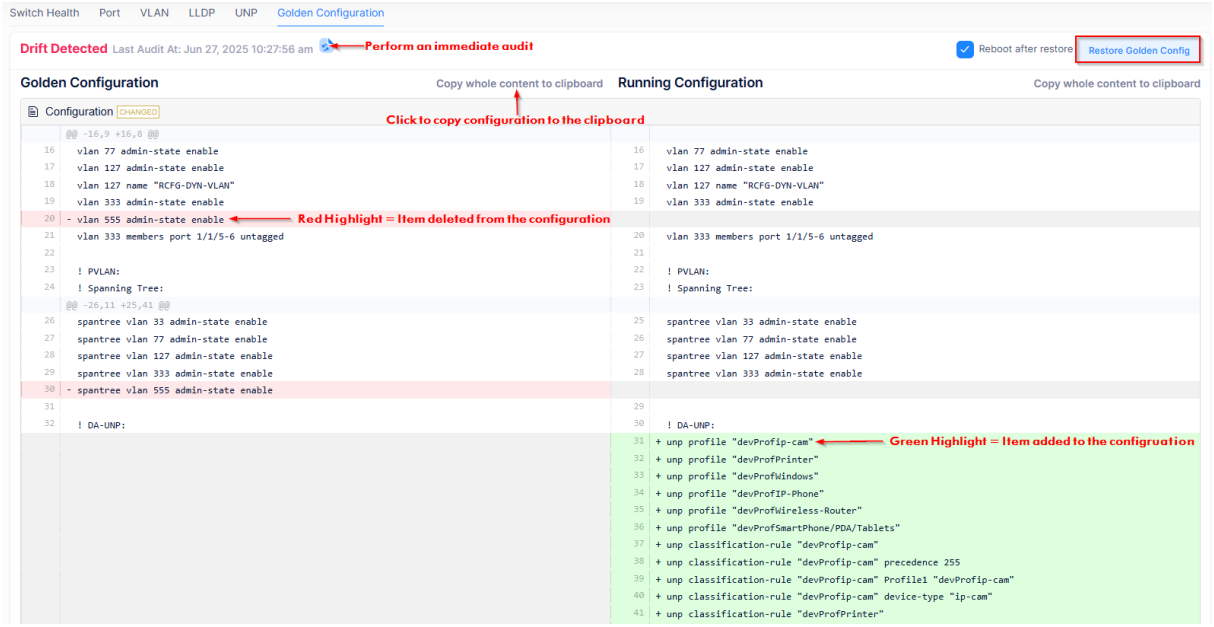
A drift counter is listed under the “Global Configuration” section of the Summary panel. Click on the “Drift Detected” link to display only those switches with a Running Configuration different from the Golden Configuration.

To view and compare the Running and Golden Configurations for a drifted switch, select the switch, click on **Actions** and select “View Device Configuration” from the Configuration Management menu or click on **Drift Detected** in the “Golden Config” field. You are then redirected to the Device Detail screen (see page 815) for the selected switch.

The “View Device Configuration” action is only available when a drift is detected for the selected switch.



The Device Detail screen displays a comparison between the saved Golden Configuration and the current Running Configuration. Objects removed are highlighted in red; objects added are highlighted in green. For example:



You can perform any of the following actions from the Golden Configuration tab on the Device Detail screen:

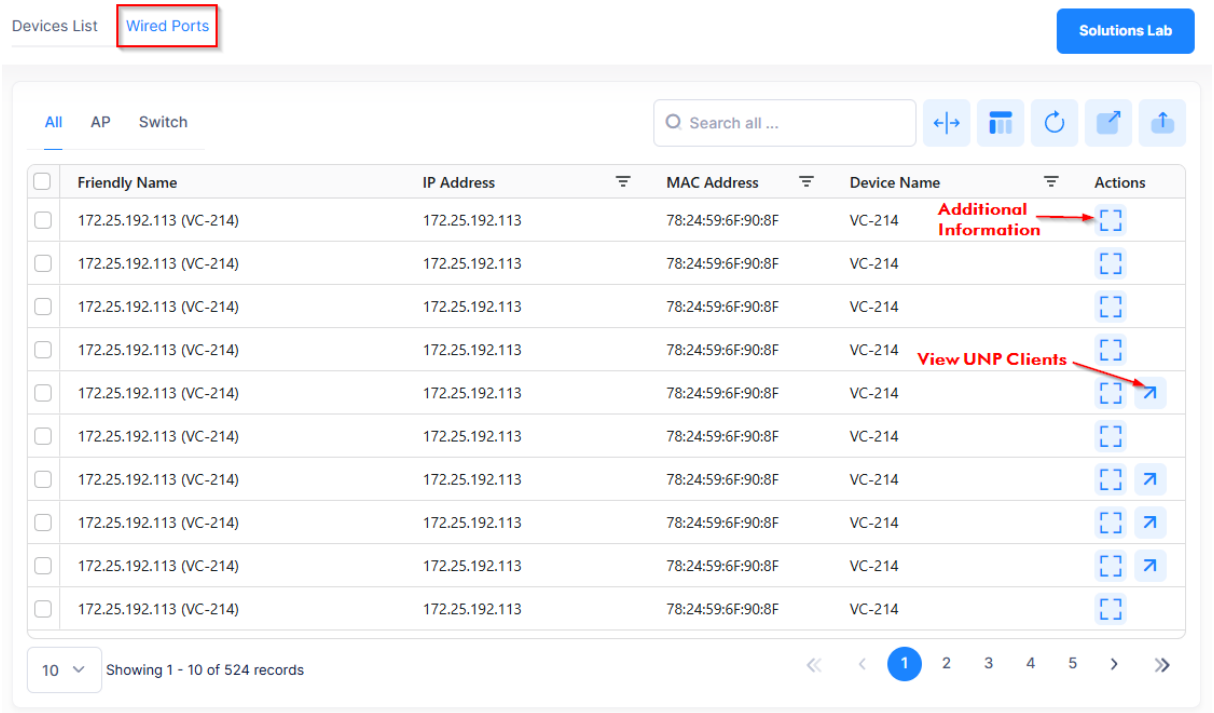
- View the differences between the saved Golden Configuration and the Running Configuration.
- Copy the Golden and/or Running Configuration to the clipboard.
- Determine the date and time the Drift was detected.
- Perform an immediate audit of the switch configuration.
- Click on **Restore Golden Config** to restore the Golden Configuration as the device configuration for the switch. By default, the “Reboot after restore” option is selected. Consider the following when you select this action:
  - **Restore Golden Configuration with the “Reboot after restore” option selected**
    The Golden Configuration is copied to the switch as the new Running Configuration and reloads the switch.
  - **Restore Golden Configuration with the “Reboot after restore” option is not selected**
    The Golden Configuration is copied to the vcboot.cfg of the switch as the new configuration file and the switch is not reloaded. The current Running Configuration for the switch remains.

21 Oct 2025

4.1.2 Wired Ports

Click on the **Wired Ports** tab on the Device Catalog (see page 169) screen to display information (see page 257) about wired ports on Switch and AP devices. Note that not all Stellar AP models support wired ports; only wired ports from AP models that have downlink wired ports are included in the display.

On the Wired Ports screen, you can select if you want to display all wired ports within the Organization, within a Site, within a specific Building, within a specific Floor, or on specific devices.



There are three Wired Ports lists available to view from this screen:

- **All** - Displays a list of wired ports on all devices (Access Points and Switches).
- **AP** - Displays a list of wired ports on Access Points.
- **Switch** - Displays a list of wired ports on Switches.

Click on **All** (default), **AP**, or **Switch** to view the related Wired Ports list.

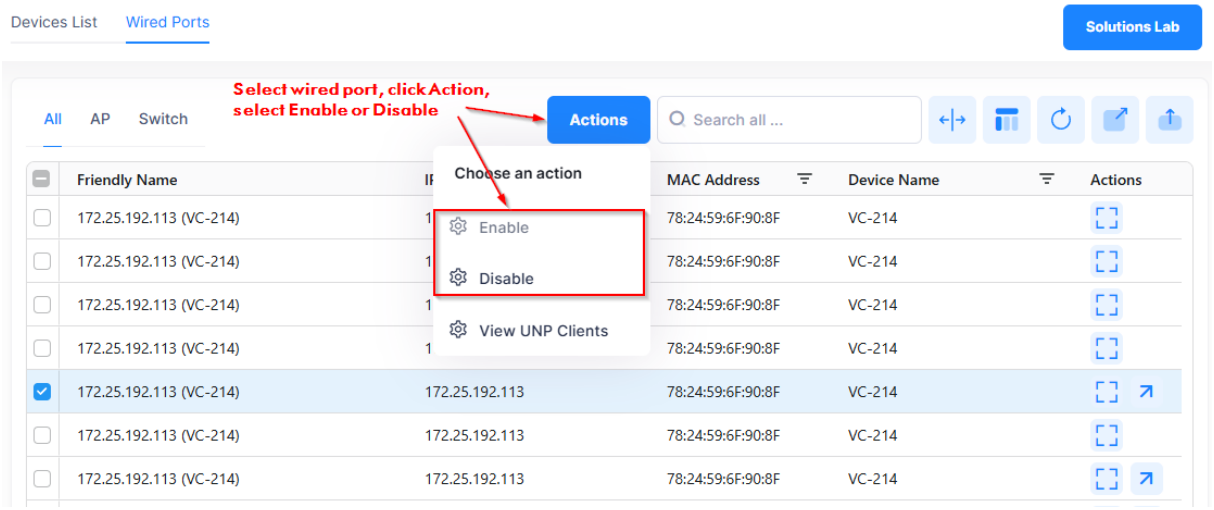
In addition to viewing wired ports, you can administratively enable/disable the port status (see page 255) and display UNP clients (see page 256) connected to a port.

Enabling/Disabling the Wired Port Status

To administratively enable or disable the wired port(s) status:

1. Select the wired port(s) that you want to administratively enable or disable.
2. Click on **Actions** and select **Enable** or **Disable** from the Actions drop-down menu. The administrative status of the wired port is changed to Up (enabled) or Down (disabled).

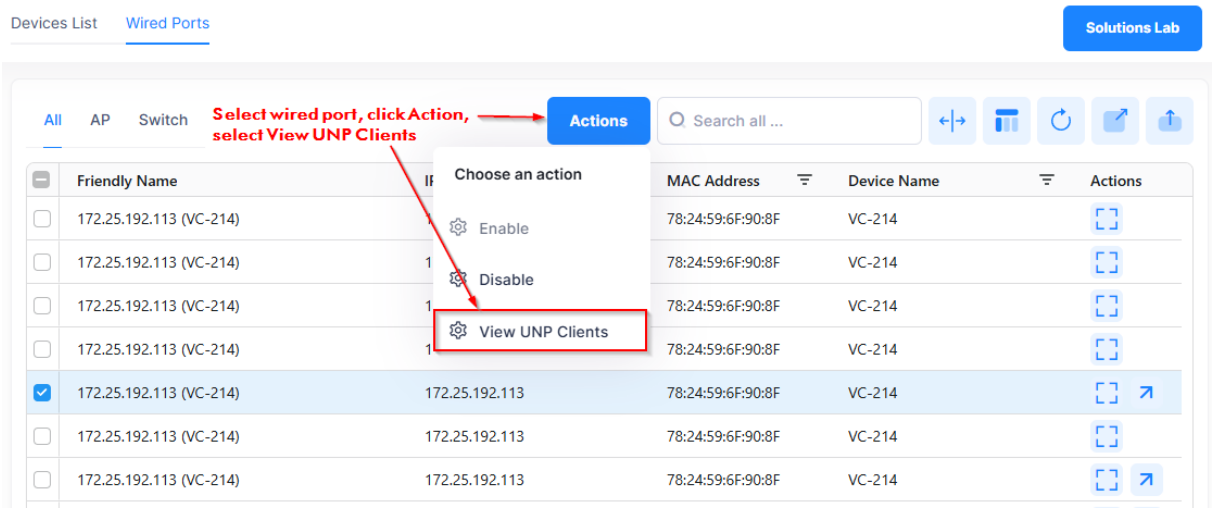
The “Admin Status” field for a wired port displays the current Up (enabled) or Down (disabled) administrative status for the port.



Displaying UNP Clients

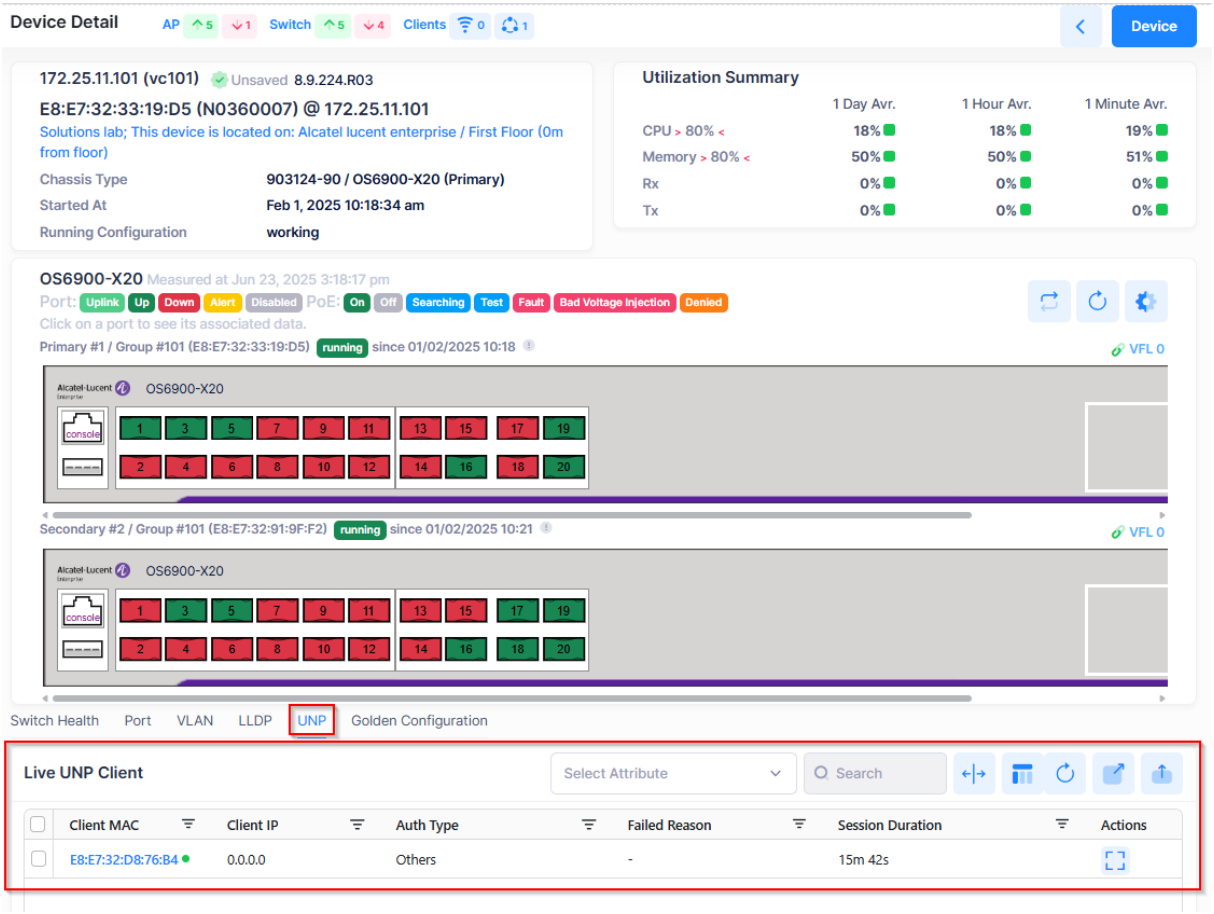
There are two methods for viewing UNP clients learned on wired UNP ports:

- Click on the View UNP Clients icon next to the wired UNP port.
- Select a wired UNP port, then click on **Actions** and select **View UNP Clients** from the Actions drop-down menu.



The View UNP Clients icon only appears next to wired UNP ports. This icon does not appear if the wired port is not configured as a UNP port.

When you click on View UNP Clients, the Device Detail screen for the device is displayed showing Live UNP Client list. For example:



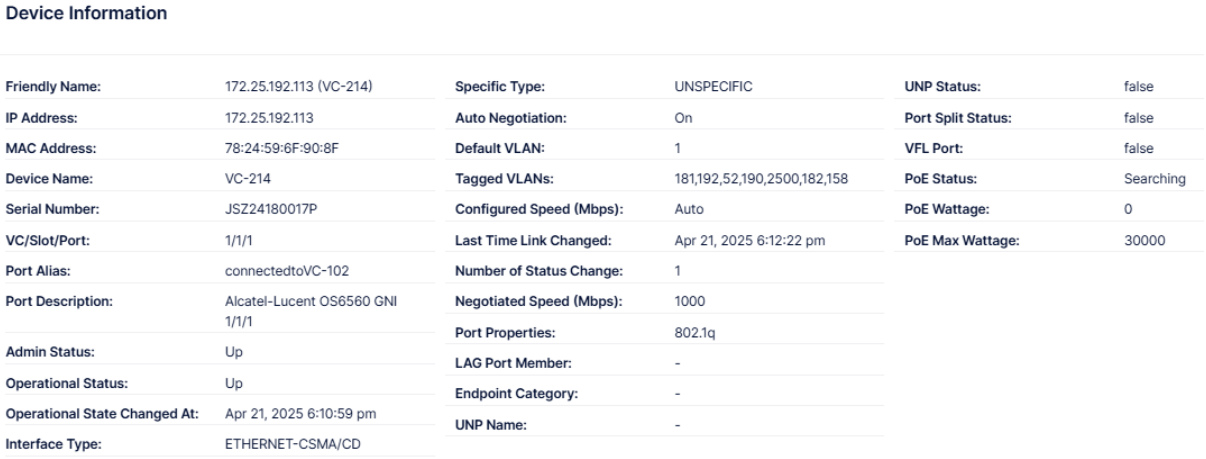
4.1.2.1 Displaying Wired Ports Information

Click the Additional Information icon next to a Wired Port entry to display the Device Information screen. The information displayed on this screen is defined below.

> The OmniVista Terra polling interval is once an hour to collect wired port information. If some information appears out of date, wait until the next polling interval.

Note that the information displayed for Switch Wired Ports (see page 258) and AP Wired Ports (see page 259) may differ.

4.1.2.1.1 Switch Wired Port Information



- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26) By default, the Friendly Name is set to IP Address (System Name).
- **IP Address** - The IP address of the device.
- **MAC Address** - The MAC address of the device.
- **Device Name** - The name of the device model.
- **Serial Number** - The serial number of the device model.
- **VC/slot/port** - The chassis/slot/port number on the device.
- **Port Alias** - The user-defined alias for the port.
- **Port Description -** A detailed description of the interface (for example, Alcatel-Lucent OS6900 QNI 1/1A).
- **Admin Status -** The administrative status of the port (Up/Down). When the admin status of a port is "Up", the port can receive and transmit data as long as a cable is connected and no physical or operational problems exist. When the admin status of a port is "Down", the port will not transmit or receive data even if a cable is connected and the physical connection is operational. Note that physical or operational problems may cause a port to be nonfunctional even when its admin status is enabled.
- **Operational Status -** The operational status of the port (Up/Down/Unknown). If the operational status of a port is "Up", the admin status of the port is "Up" and a cable is connected to the port and transmitting data.
  Note: If an interface's Admin Status is "Down", its Operational Status will also be "Down". When the Admin Status is changed to up, the interface's Operational Status will change to "Up" if the interface is ready to transmit and receive packets; or the Operational Status will change to "Dormant" if the interface is waiting for external actions; or the Operational Status will remain "Down" if there is a fault that prevents it from going "Up".
- **Operational State Changed At -** The date and time the operational status of the port last changed (from "Up" to "Down" or "Down" to "Up").
- **Interface Type -** The port type (for example, Ethernet-CSMA/CD).
- **Specific Type -** Detailed information about the port type (e.g., LAG, Stack).

- **Auto Negotiation -** Auto Negotiation status on the port (On = Enabled, Blank = Disabled).
- **Default VLAN -** The default VLAN assigned to the port.
- **Tagged VLANs** - The 802.1Q-tagged VLANs assigned to the port.
- **Configured Speed (Mbps) -** The configured interface line speed, in Mbps. If the port is set to "Auto", the switch automatically sets the line speed to match the attached device.
- **Last Time Link Changed -** The last time the configuration for the interface was changed.
- **Number of Status Changes -** The total number of times the configuration of the interface has changed.
- **Negotiated Speed (Mbps)** - The actual speed of the port.
- **Port Properties -** The port configuration properties (e.g., UNP, Mobile, LLDP).
- **LAG Port Member -** The Link Aggregation Port(s) on the device, if applicable.
- **Endpoint Category -** The IoT Category of the endpoint connected to the port, if applicable.
- **UNP Name -** The Access Role Profile assigned to the port, if applicable.
- **UNP Status -** Indicates whether or not UNP is Enabled/Disabled on the port.
- **Port Split Status -** The split port status of the switch (Auto, 40GB, or 4 x 10GB). If the port is on a non-supported device, the field will display "False".
- **VFL Port -** Indicates whether or not the port is a VFL port (True/False)
- **PoE Status -** The administrative status of PoE on the port (True = Enabled, False = Disabled). If the device/port does not support PoE, the field will display "False".
- **PoE Wattage -** The amount of PoE power being used by the device, in milliwatts, if applicable.
- **PoE Max Wattage -** The maximum amount of power, in milliwatts, available to the port, if applicable

4.1.2.1.2 AP Wired Port Information

Device Information

Friendly Name:	10.255.230.1 (AP-4F:20)	**Interface Type:**	ETHERNET-CSMA/CD	**UNP Name:**	-
IP Address:	10.255.230.1	**Specific Type:**	-	**UNP Status:**	false
MAC Address:	DC:08:56:4A:4F:20	**Auto Negotiation:**	On	**Port Split Status:**	false
Device Name:	AP-4F:20	**Default VLAN:**	-	**VFL Port:**	false
Serial Number:	SSZ204500816	**Tagged VLANs:**	-	**PoE Status:**	-
VC/Slot/Port:	Eth2	**Configured Speed (Mbps):**	Auto	**PoE Wattage:**	0
Port Alias:	-	**Last Time Link Changed:**	-	**PoE Max Wattage:**	-
Port Description:	OAW-AP1311 LAN	**Number of Status Change:**	-		
Admin Status:	Down	**Negotiated Speed (Mbps):**	0		
Port Changed:	0	**Port Properties:**	-		
Operational Status:	Down	**LAG Port Member:**	-		
Operational State Changed At:	-	**Endpoint Category:**	-		

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26) By default, the Friendly Name is set to IP Address (System Name).
- **IP Address** - The IP address of the device.

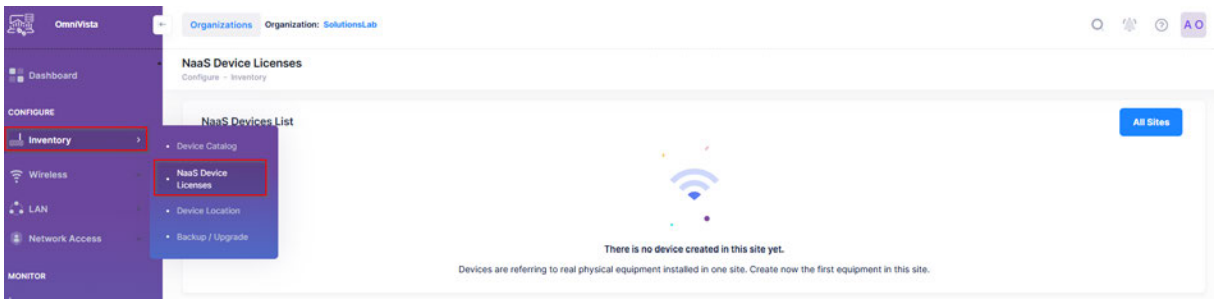
- **MAC Address** - The MAC address of the device.
- **Device Name** - The name of the device model.
- **Serial Number** - The serial number of the AP model.
- **VC/slot/port** - The wired port number on the AP device (for example, ETH4).
- **Port Alias** - The user-defined alias for the port.
- **Port Description -** A detailed description of the interface (for example, OAW-AP1301H LAN4).
- **Admin Status -** The administrative status of the port (Up/Down). When the admin status of a port is "Up", the port can receive and transmit data as long as a cable is connected and no physical or operational problems exist. When the admin status of a port is "Down", the port will not transmit or receive data even if a cable is connected and the physical connection is operational. Note that physical or operational problems may cause a port to be nonfunctional even when its admin status is enabled.
- **Port Changed** - The total number of times the configuration of the interface has changed.
- **Operational Status -** The operational status of the port (Up/Down/Unknown). If the operational status of a port is "Up", the admin status of the port is "Up" and a cable is connected to the port and transmitting data.
  Note: If an interface's Admin Status is "Down", its Operational Status will also be "Down". When the Admin Status is changed to up, the interface's Operational Status will change to "Up" if the interface is ready to transmit and receive packets; or the Operational Status will change to "Dormant" if the interface is waiting for external actions; or the Operational Status will remain "Down" if there is a fault that prevents it from going "Up".
- **Operational State Changed At -** The date and time the operational status of the port last changed (from "Up" to "Down" or "Down" to "Up").
- **Interface Type -** The port type (for example, Ethernet-CSMA/CD).
- **Specific Type -** Detailed information about the port type (e.g., LAG, Stack).
- **Auto Negotiation -** Auto Negotiation status on the port (On = Enabled, Blank = Disabled).
- **Default VLAN -** The default VLAN to which the port is assigned.
- **Tagged VLANs** - 802.1Q-tagged VLANs assigned to the port.
- **Configured Speed (Mbps) -** The configured interface line speed, in Mbps. If the port is set to "Auto", the switch automatically sets the line speed to match the attached device.
- **Last Time Link Changed -** The last time the configuration for the interface was changed.
- **Number of Status Changes -** The total number of times the configuration of the interface has changed.
- **Negotiated Speed (Mbps)** - The actual speed of the port.
- **Port Properties -** The port configuration properties (e.g., 802.Q, LAG).
- **LAG Port Member -** The Link Aggregation Port(s) on the device, if applicable.
- **Endpoint Category -** The IoT Category of the endpoint connected to the port, if applicable.
- **UNP Name -** The Access Role Profile assigned to the port, if applicable.
- **UNP Status -** Indicates whether or not UNP is Enabled/Disabled on the port.
- **Port Split Status -** The split port status of the switch (Auto, 40GB, or 4 x 10GB). If the port is on a non-supported device, the field will display "False".

- **VFL Port -** Indicates whether or not the port is a VFL port (True/False)
- **PoE Status -** The administrative status of PoE on the port (True = Enabled, False = Disabled). If the device/port does not support PoE, the field will display "False".
- **PoE Wattage -** The amount of PoE power being used by the device, in milliwatts, if applicable.

21 Oct 2025

4.2 NaaS Device Licenses

The Inventory NaaS Device Licenses screen displays the Network as a Service (NaaS) device licensing information for Access Points. Use this screen to determine and monitor the status of the Device License Mode for each device.



A device interacts with a designated License Activation Server to obtain a Device License (NaaS, CAPEX, or CAPEX Undecided). OmniVista Terra obtains the Device License information when a device is added to the Device Catalog and associated with an OmniVista Terra Management License.

There is a difference between a Device License and an OmniVista Terra Management License. A Device License can be NaaS or CAPEX. A license key is pushed to the device to enable or disable certain features on the device. The licensed features are applied to the device, even if the device is not managed by OmniVista Terra. The type of Device License determines the license mode for the device:

- If a NaaS license is received, the device operates in the NaaS Device License mode. The licensed features are tied to a subscription-based model with an end date, which can be renewed.
- If a CAPEX license is received, the device operates in the CAPEX Device License Mode. There is no end date (no subscription) for the licensed features. The license is permanent and never expires.

The NaaS Device Licenses screen only lists devices that have obtained a NaaS or CAPEX Device License. The following Device License information is displayed for each licensed device:

- **Friendly Name -** The user-defined name of the device.
- **IP Address (v4) -** The IP address of the device.
- **MAC Address -** The MAC address of the device.
- **Serial Number -** The serial number of the device.
- **Management Mode** - Whether the device is configurable (Full Management) or the device is only reporting Advanced Analytics data (Analytics Only).
- **Site Name** - The name of the Organization Site to which the device belongs.
- **Access Point Group** - The name of the Access Point (AP) Group to which the AP device belongs within the Organization.
- **Management Features on Device -** The status of the Management Feature License (Licensed, Not Licensed, In Grace Period, or Expired (see page 264)). This feature license allows management

capabilities on the device. Note that when this license expires, a 30-day Grace Period is triggered during which a configuration change can be applied to the device. However, after the 30-day Grace Period expires, the device goes into a degraded mode during which a configuration change is not allowed.

- **Upgrade Features on Device -** The status of the Upgrade Feature License (Licensed, Not Licensed, or Expired (see page 264)). This feature allows software upgrades on the device. If this license is "Expired", OmniVista Terra will return a failed update message if an attempt is made to upgrade the device. There is no Grace Period triggered when this feature license expires.
- **Other Features on Device -** The status of all other licensed features (Licensed, Not Licensed, In Grace Period, or Expired (see page 264)), except the Management and Upgrade licensed features. Click on a device entry to display licensing details (see page 263) for these additional features.
- **Device License Mode -** The Device License mode.
  - **NaaS -** The licensed device participates in the NaaS subscription-based model. Licensed features have a end date.
  - **CAPEX -** The licensed device does not participate in the NaaS subscription-based model. Licensed features do not have an end date; the license never expires.
  - **CAPEX Undecided** - The device has not yet obtained a license.

> If the device is reported as a CAPEX or CAPEX UNDECIDED device, the "Management Feature on Device", "Upgrade Feature on Device", and "Other Features on Device" fields will be blank.

4.2.1 Device License Details

If a device is licensed for features other than the Management or Upgrade features, the following information is displayed for each additional licensed feature when you click on the Additional information icon next to the device entry under the Actions column:

- **Feature Name -** The name of the feature licensed for the device.
  - **Essentials -** The default license for the device that licenses the use of basic features.
  - **Advanced -** The basic features license plus the Data Center and 10G feature licenses.
- **Expiry date -** The date on which the feature license expires.
- **Days Left for Expiry -** The remaining amount of time until the License expires or the remaining Grace Period time if the License has expired.
- **Status -** The status of the licensed feature (Licensed, Not Licensed, In Grace Period, or Expired (see page 264)).

4.2.2 Device License Status

- **Licensed -** The feature is licensed, and the license expires on the given date. For example, "Licensed (until June 20, 2022)".
- **Not Licensed** - The feature is not licensed for the device.
- **In Grace Period -** The NaaS feature license has expired and is in a grace period. The grace period duration depends on the feature. When the grace period ends, the status of the licensed feature changes to “Expired” (see page 263)and the feature goes into a “degraded” mode of operation (feature stops working). If there is no grace period for the feature, the license status bypasses “In Grace Period” and goes directly from “Licensed” to “Expired” status.

> Note that the end of the grace period is calculated based on the number of days the device is active. If a NaaS feature license expires and the device is not active, the grace period will not start until the device is active again. For example, if a device is inactive after the license expires and then goes active after 15 days, the 30-day grace period starts after the 15 days and ends 45 calendar days after the license expires.

- **Expired -** The NaaS feature license has expired. A feature goes from "Licensed” status to “In Grace Period” status (see page 263) when it reaches the Expiry date. During the grace period, the feature will continue to work. Only after the grace period ends, does the feature status change to “Expired”. When the feature licensed has Expired, the feature goes into a “degraded” mode of operation (feature stops working). For example, if the Management feature reaches its Expiry Date, the status of the Management feature changes to “In Grace Period”. During the grace period, the device can continue to be managed. At the end of the grace period, the status of the Management feature changes to “Expired” and the feature goes into a “degraded” mode where it can no longer be managed.

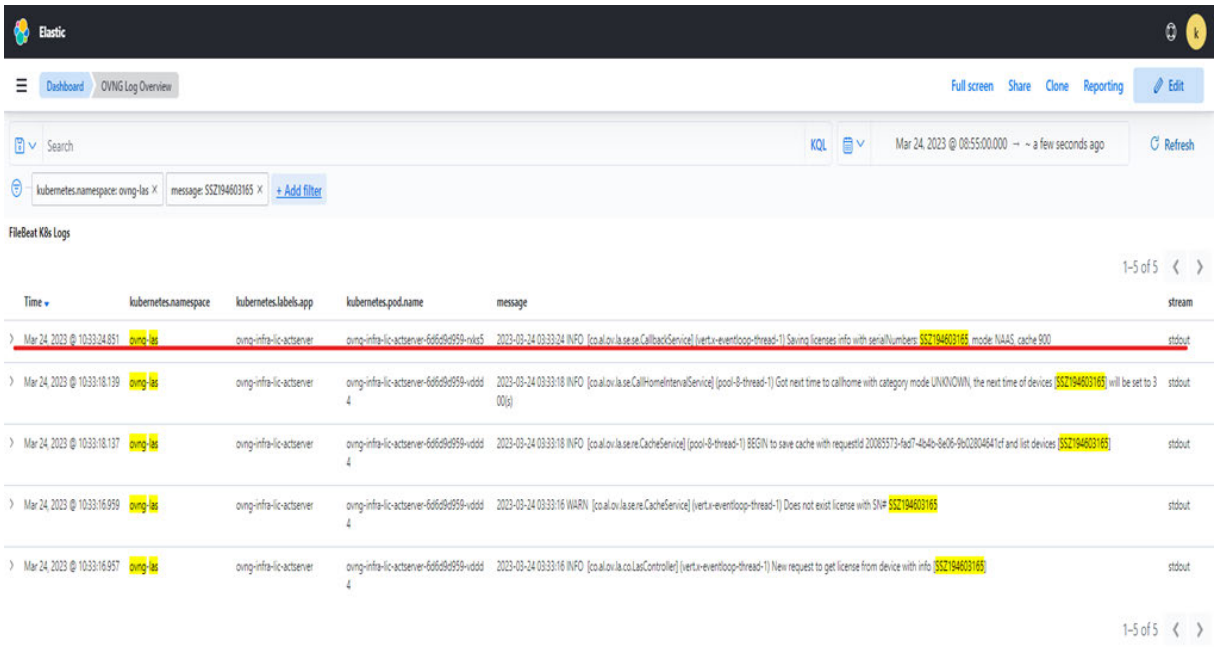
> Note that some features may have a grace period (e.g., 30 days) and some features may not have a grace period. For example, the Upgrade feature might not have a grace period. If there is no grace period and the Upgrade feature license reaches its Expiry date, the feature goes directly into an “Expired” state and immediately reaches the “degraded” mode.

21 Oct 2025

4.2.3 NaaS License Management - FAQs/Troubleshooting

4.2.3.1 Device has NaaS license info, but the NaaS Device License mode is “CAPEX”

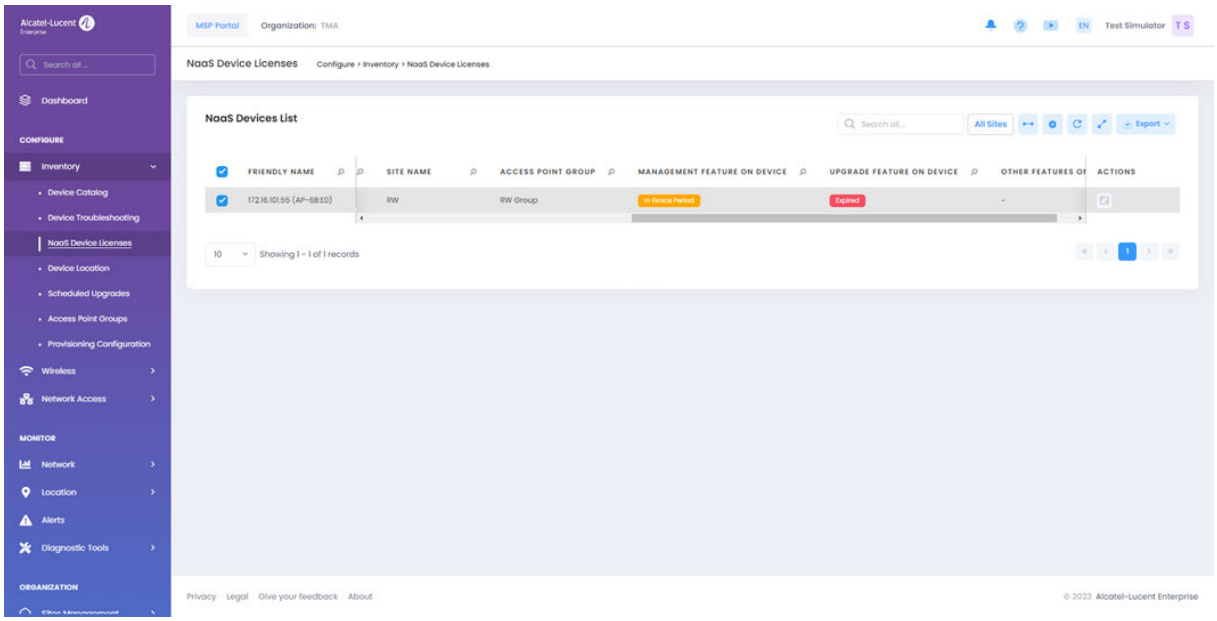
Check the NaaS mode value response from Service Manager. (Refer to How to Search Log Messages in Wazuh (see page 267).)



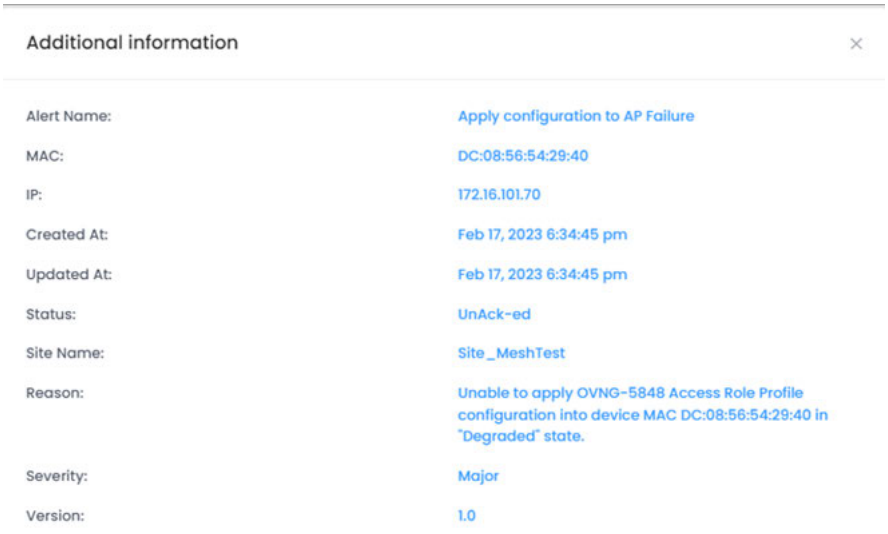
4.2.3.2 Cannot apply a configuration to an AP device

Check the following to determine why you cannot apply a configuration to an AP:

- Check the NaaS Device Licenses (see page 262) screen to see if the Management Feature License has expired for the AP device.



- Check the Alerts screen to see if an “Apply configuration to AP Failure” alert was received because the device is in the Degraded state.



4.2.3.3 Cannot upgrade an AP device

- Check the NaaS Device Licenses (see page 262) screen to see if the Management Feature License has expired for the AP device.
- Check the Alerts screen to see if the upgrade failed because the device is in the Degraded state.

4.2.3.4 A new NaaS device license is activated for the device, but it does not effect. The device still shows the old NaaS license

Devices call the License Activation Server (LAS) periodically to get a new license. LAS itself also caches the NaaS license for a period time. Wait for 900 seconds (maybe more, based on the expiry time configuration) to get a new value from the Service Manager.

4.2.3.5 NaaS Device License mode is “UNKNOWN”

The first request to the License Activation Server always responds with “UNKNOWN” mode, and Service Manager will call a webhook to update NaaS license in LAS. Wait for the next LAS call home.

4.2.3.6 The device does not automatically change the mode “NAAS” after call home to NaaS

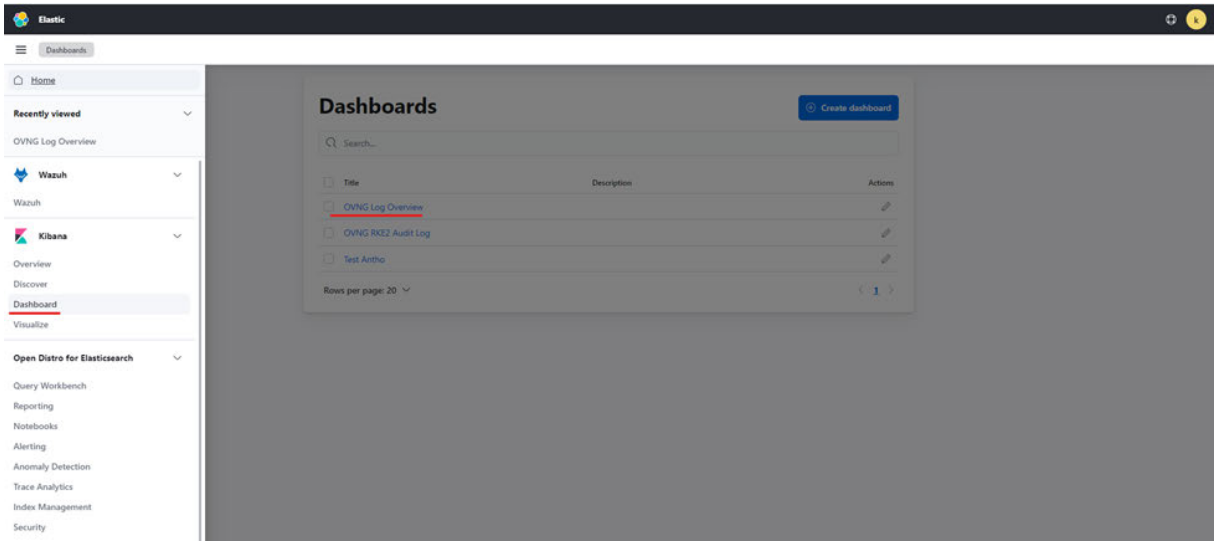
Restart wmaagent by executing the cmd /etc/init.d/wmaagent restart

4.2.3.7 AP device troubleshooting commands

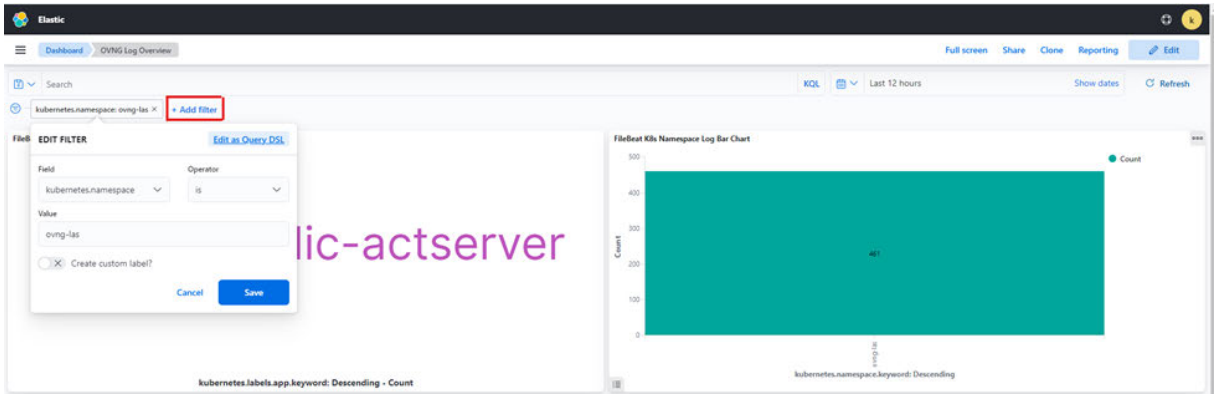
- Check License Activation Server (LAS) connection information
  cat /tmp/dhcp_ocloud_info
- Verify license, response from LAS
  cat /tmp/log/license_client.log
- View NaaS information
  + AP: ubus call ap_manage getapbasicinfo

4.2.3.8 How to search log messages in Wazuh

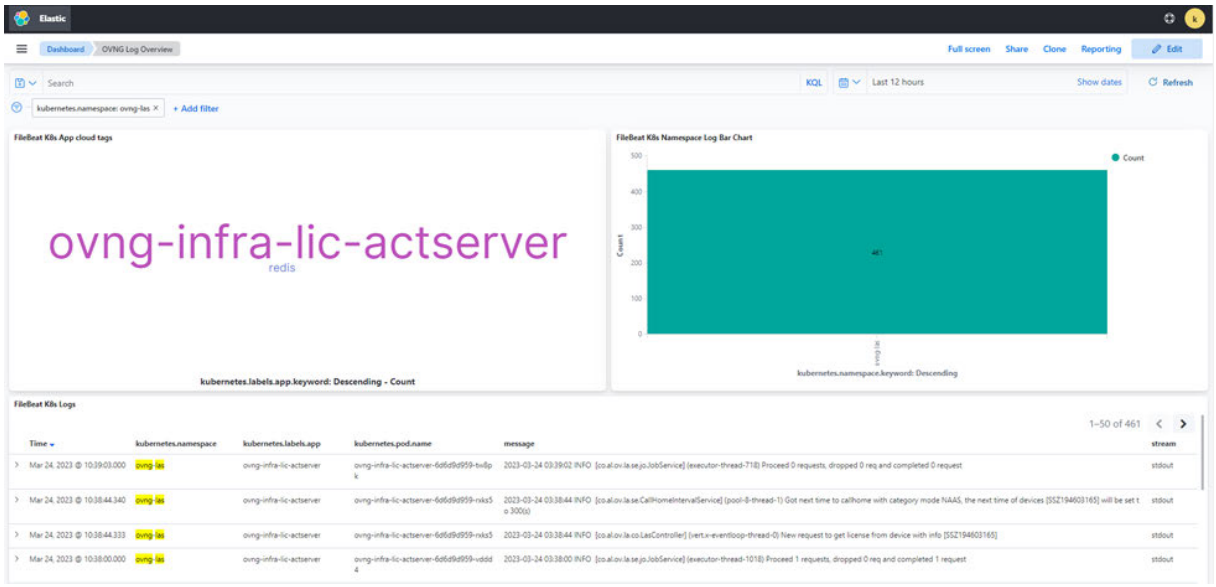
- Access the Wazuh page and login with your OmniVista Terra account. For example, the Wazuh log server for sqa-eu cluster: https://wazuh-sqa-eu.ovng.dev.myovcloud.com/ If you don’t have permission, please contact your Alcatel-Lucent Enterprise representative.
- On the left menu, click on **Dashboard** and select **OVNG Log Overview** on the right panel.



- To filer the log for License Actserver, click **Add filter** and input data:
  Field: **kubernetes.namespace**
  Operator: **is**
  Value: **ovng-las**
  Click **Save** to filter the log.

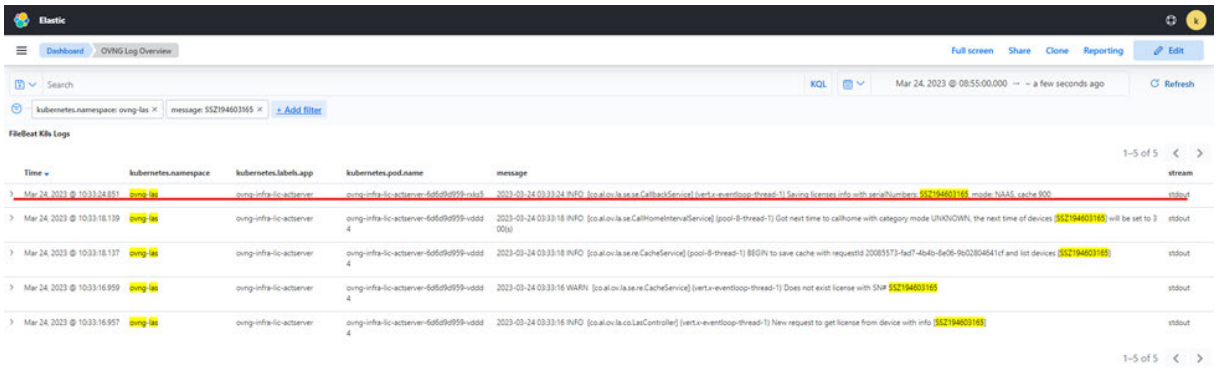


- All logs will be display in section “FileBeat K8s Logs” as shown below:



- Wazuh also provides a time range tool in the top-right corner that you can use to filter.

- To find if any keywords exist in the logs, you can add more filters with metadata:
  Field: **message**
  Operator: **is**
  Value: *your_keyword_here*
  For example, to check the device license mode returning from Switch Manager callback with device serial number SSZ194603165, click **Add filter** and input the following:
  Field: **message**
  Operator: **is**
  Value: **SSZ194603165**


Elastic
Dashboard
OVNG Log Overview
Full screen
Share
Clone
Reporting
Edit
Search
KQL
Mar 24, 2023 @ 08:55:00.000 → a few seconds ago
Refresh
kubernetes.namespace: ovng-las
message: SSZ194603165
+ Add filter
FileBeat K8s Logs
1–5 of 5
Time
kubernetes.namespace
kubernetes.labels.app
kubernetes.pod.name
message
stream
Mar 24, 2023 @ 10:33:24.851
ovng-las
ovng-infra-lic-actserver
ovng-infra-lic-actserver-6d6d9d959-nks5
2023-03-24 03:33:24 INFO [co.al.ov.la.se.se.CallbackService] (vert.x-eventloop-thread-1) Saving licenses info with serialNumbers: SSZ194603165, mode: NAAS, cache 900
stdout
Mar 24, 2023 @ 10:33:18.139
ovng-las
ovng-infra-lic-actserver
ovng-infra-lic-actserver-6d6d9d959-vddd4
2023-03-24 03:33:18 INFO [co.al.ov.la.se.CallHomeIntervalService] (pool-8-thread-1) Got next time to callhome with category mode UNKNOWN, the next time of devices SSZ194603165 will be set to 3 00(s)
stdout
Mar 24, 2023 @ 10:33:18.137
ovng-las
ovng-infra-lic-actserver
ovng-infra-lic-actserver-6d6d9d959-vddd4
2023-03-24 03:33:18 INFO [co.al.ov.la.se.re.CacheService] (pool-8-thread-1) BEGIN to save cache with requestId 20085573-fad7-4b4b-8e06-9b02804641cf and list devices SSZ194603165
stdout
Mar 24, 2023 @ 10:33:16.959
ovng-las
ovng-infra-lic-actserver
ovng-infra-lic-actserver-6d6d9d959-vddd4
2023-03-24 03:33:16 WARN [co.al.ov.la.se.re.CacheService] (vert.x-eventloop-thread-1) Does not exist license with SN# SSZ194603165
stdout
Mar 24, 2023 @ 10:33:16.957
ovng-las
ovng-infra-lic-actserver
ovng-infra-lic-actserver-6d6d9d959-vddd4
2023-03-24 03:33:16 INFO [co.al.ov.la.co.LasController] (vert.x-eventloop-thread-1) New request to get license from device with info SSZ194603165
stdout
1–5 of 5

21 Oct 2025

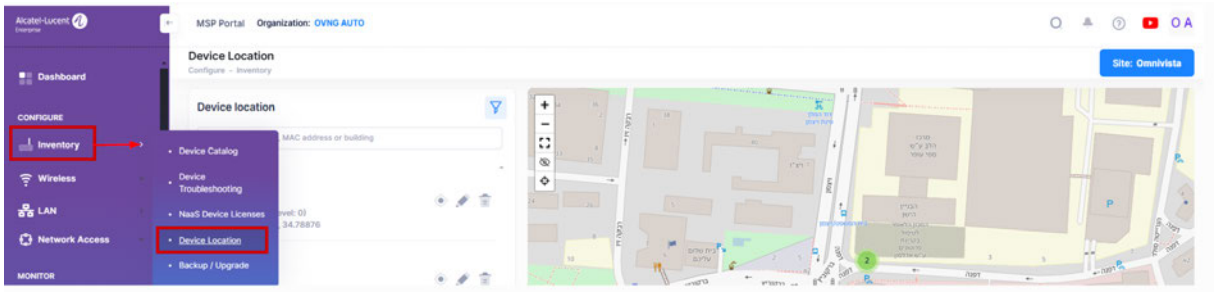
4.3 Locate a Device on a Floorplan

> The Device Location feature will be enabled only when you will have declared at least one Building on your Site and one Floor in one of the Buildings.

From the OmniVista Terra Menu (see page 45), go to the Device Location screen and click on **Inventory > Device Location**.

This page is divided into two sections:

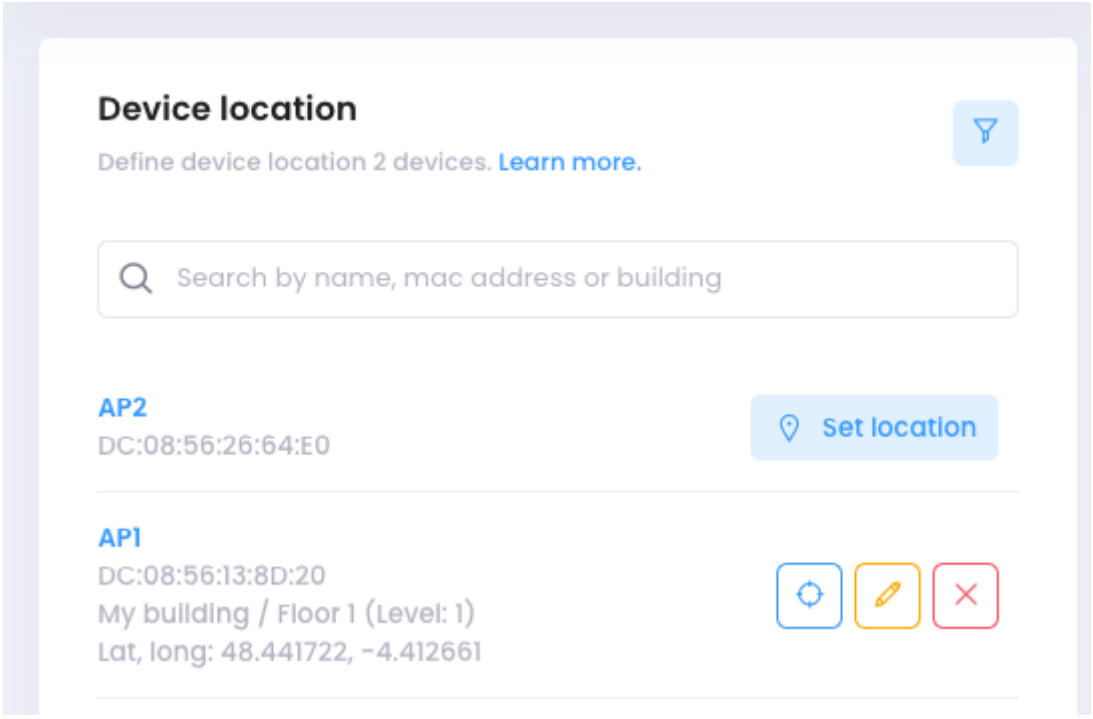
- **Device List**: On the left, all devices declared on your site are displayed. You can search for a specific device by entering the device name or MAC Address.
- **Floor plan**: This is the floor plan of the current selected Building/Floor. You can switch to a different floorplan by selecting another entry from the bottom right dropdown on the floorplan.



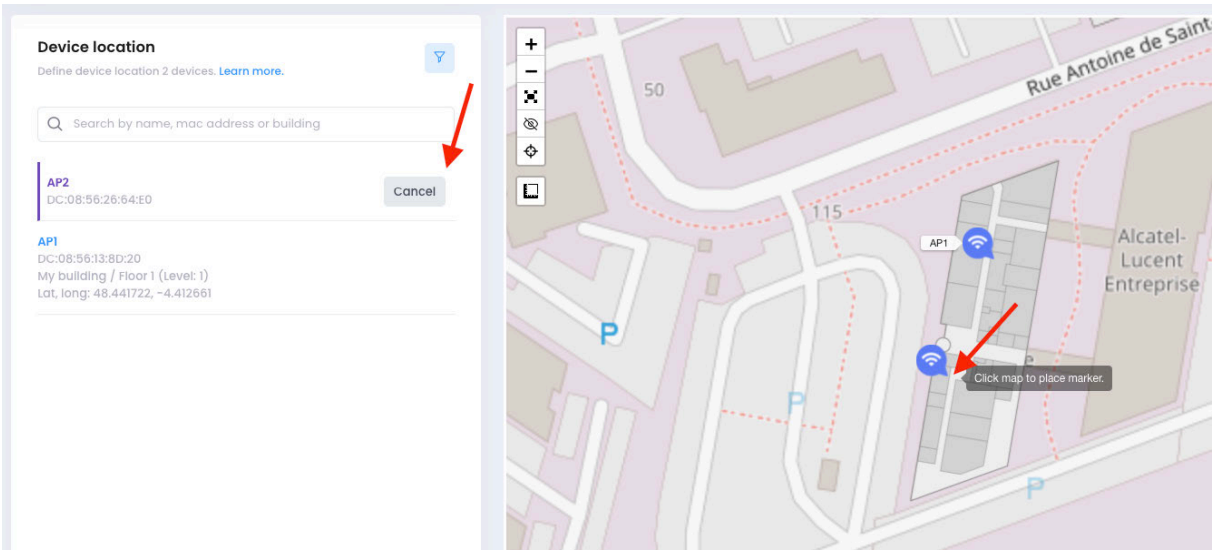
4.3.1 Locate a Device on the Floorplan

The **Set Location** button will be displayed for all devices not yet located on a floor plan.

Click on **Set Location** to start the process.

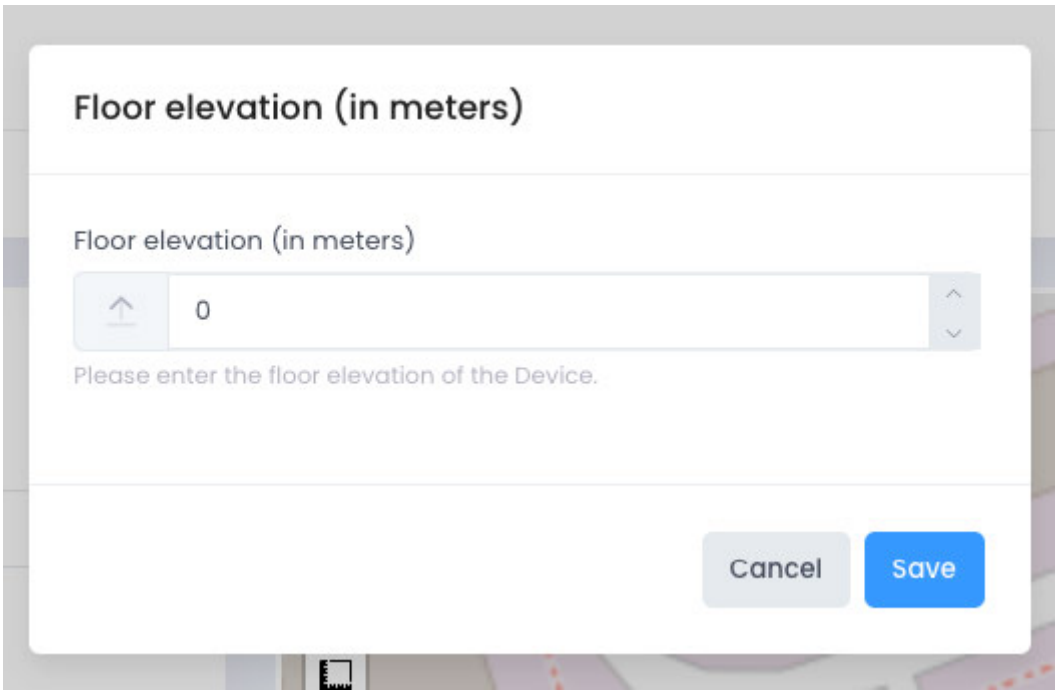


The **Set location** button is then automatically replaced by a **Cancel** button, which allows you to cancel the current initiated process.



Once you clicked on **Set Location**, move your mouse to the right on the floorplan. You will see that a Gateway Pointer is now attached to your mouse. Simply move and zoom to the desired location and click on the map to validate the position.

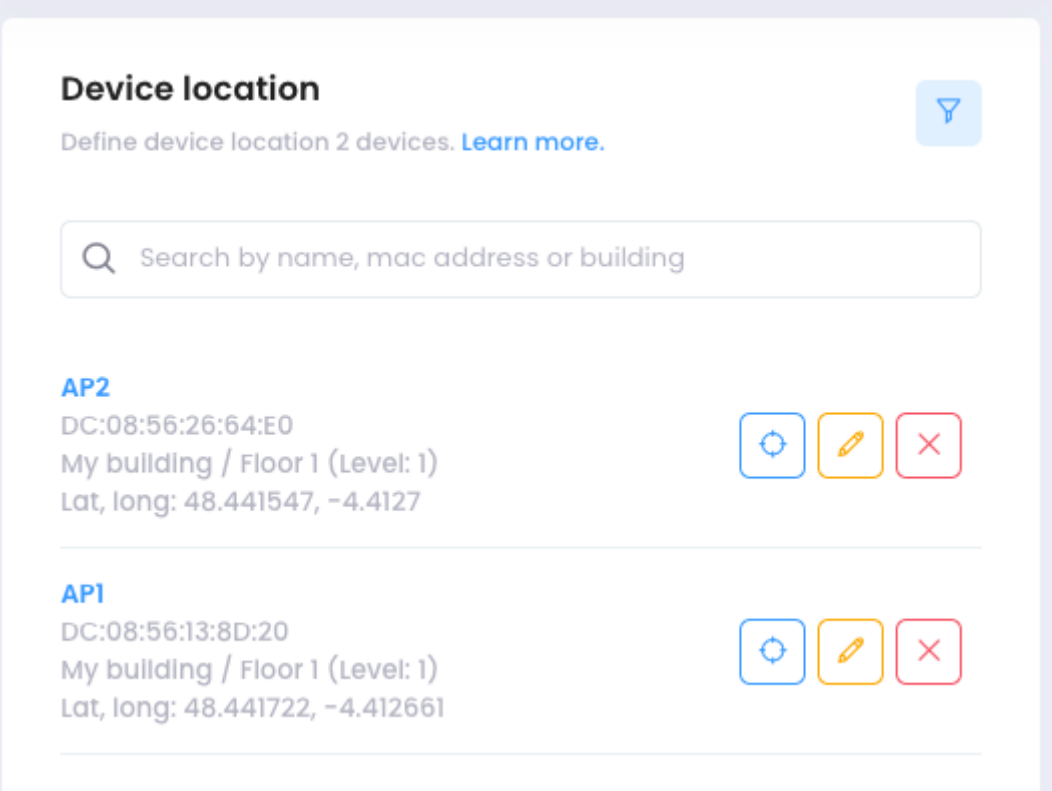
A modal window will appear automatically asking you to enter the Device elevation (in meters) from the floor.



Click on **Save** to apply your changes.

Your device is now located on your floorplan. On the left, three buttons are now attached to the located Device:

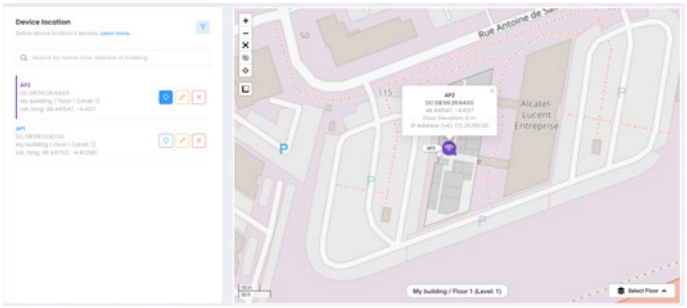
- **Highlight Device**: Click to highlight this device on the map.
- **Edit Device Location**: Click to change the current Device location.
- **Remove Device Location**: Click to completely remove the Device Location.



4.3.2 Highlight a Device on the Floorplan

Click on **Highlight Device** on the device you want to locate on the map.

A zoom is automatically performed on the map, and a tooltip is displayed on the top of the highlighted device. The marker turns purple to make it easier to locate the device on the map.

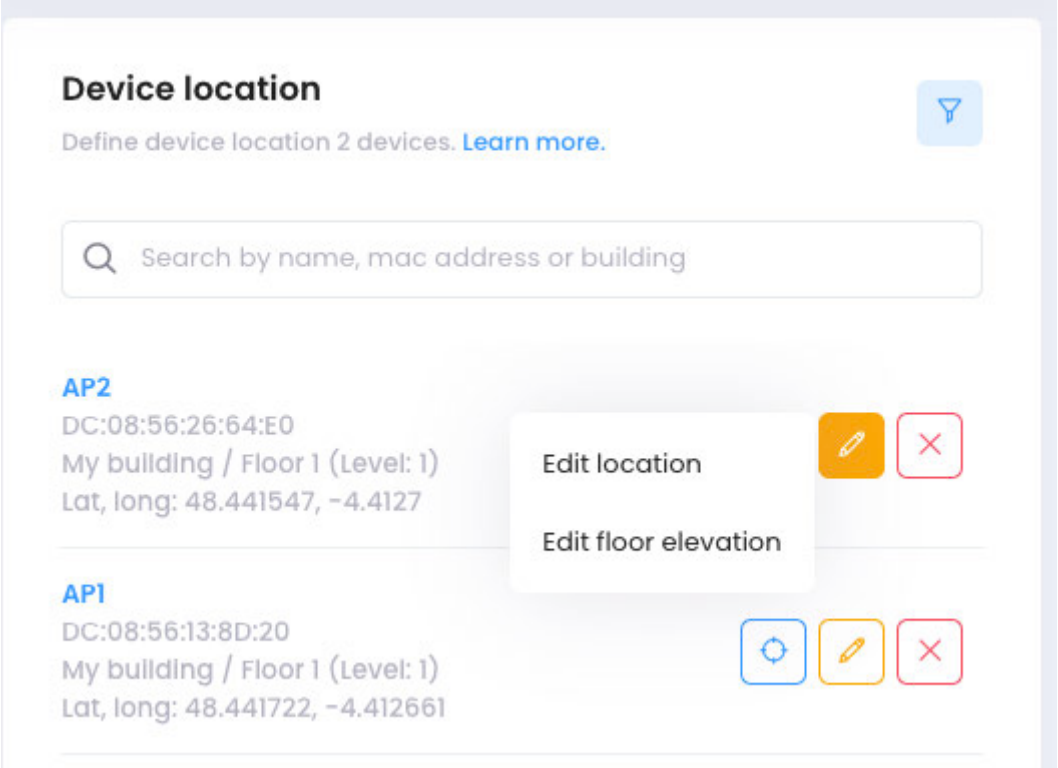


4.3.3 Edit Device Location

Click on **Edit Device Location** on the device for which you want to edit the location.

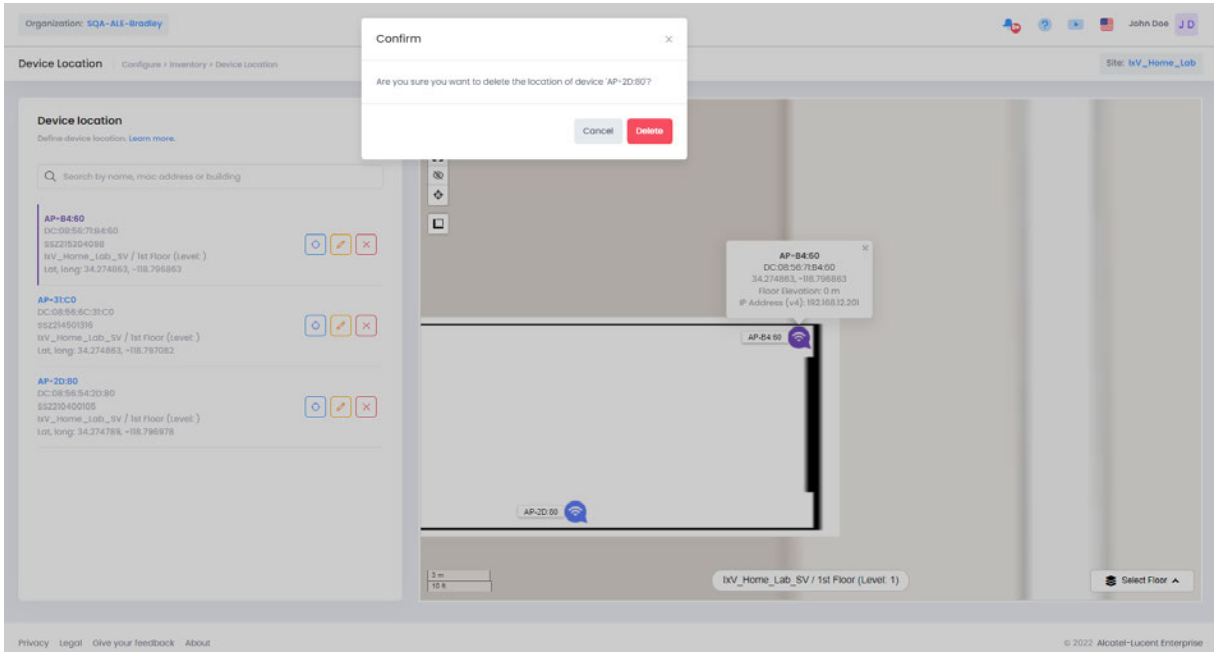
Then, select one of the following options:

- **Edit Location**: Click here if you want to change the current device location on the floorplan
- **Edit floor elevation**: Click here if you want to update the floor elevation without changing his location.



4.3.4 Remove Device Location

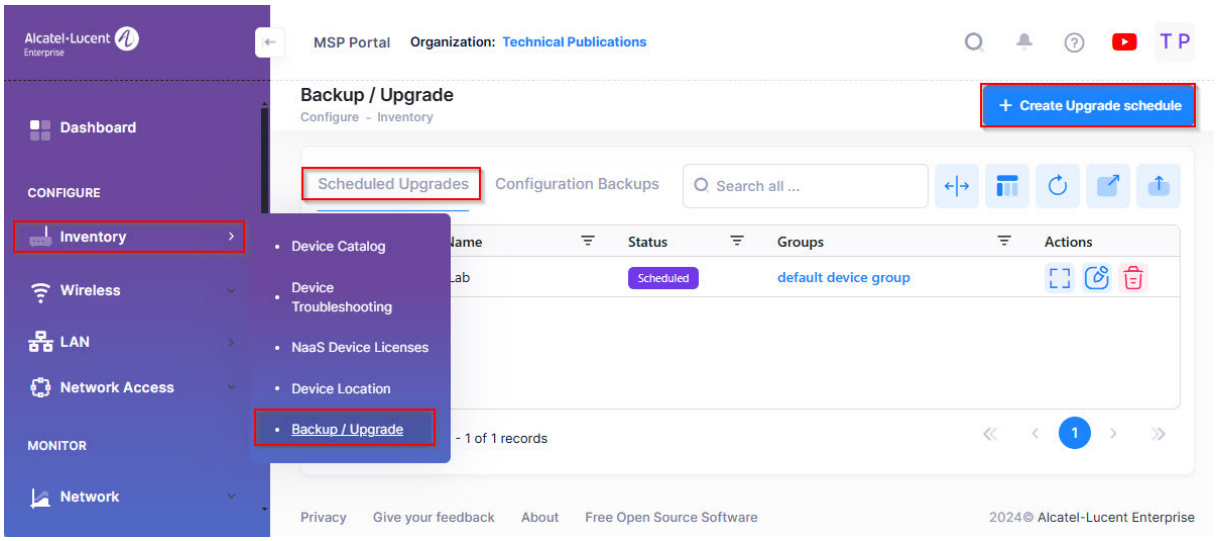
Click on **Remove Device Location** on the device for which you want to remove from the location. A modal window is displayed asking you to confirm your action.



4.4 Schedule a Device Software Update

The Scheduled Upgrades tab on the Inventory Backup/Upgrade screen is used to schedule automatic software updates for your network Access Point devices. The Scheduled Upgrade feature enables you to schedule automatic updates to specific network devices during specific time windows (e.g., non-business hours) to ensure minimal network disruption. You can create (see page 276), edit (see page 277), execute (see page 277), activate (see page 277), deactivate (see page 278) and delete (see page 278)scheduled updates. Configured scheduled updates are displayed in the Scheduled Upgrades List (see page 279).

To configure and manage automatic software update schedules, navigate to the Scheduled Upgrades screen by clicking on **Inventory > Backup/Upgrade** and selecting the **Scheduled Upgrades** tab under the “Configure” section of the OmniVista Terra Menu (see page 45).



Note that scheduled updates can also be configured from the Device Catalog (see page 169) screen (**Inventory > Device Catalog**) by selecting a device(s) in the Device Catalog List and clicking on **Actions**. From the Actions drop-down menu, select the **Edit Device > Schedule Software Upgrade** option.

Important Note: It is recommended that you schedule software updates on devices so that they do not adversely affect network performance. For example, stagger updates for different devices in different time windows during non-busy hours.

4.4.1 Updating the Device to the Desired Software

Use on of the following methods to create a scheduled software update or initiate a software update without waiting for a scheduled time:

- Schedule a Device Software Update from the Scheduled Upgrades List (see page 281).
- Schedule a Device Software Update from the Device Catalog Screen. (see page 285)
- Initiate a Device Software Update from the Device Catalog Screen. (see page 288)

4.4.2 Editing a Scheduled Upgrade

Select a scheduled upgrade in the Scheduled Upgrades List, then click on **Actions** and select **Edit** from the drop-down menu. You can also click on the Edit icon under the “Actions” column for the scheduled upgrade entry. The Edit Scheduled Upgrade screen opens. Edit the fields as described in Schedule a Device Upgrade from the Scheduled Upgrades List (see page 281), then click on **Save** to retain changes to the scheduled upgrade.

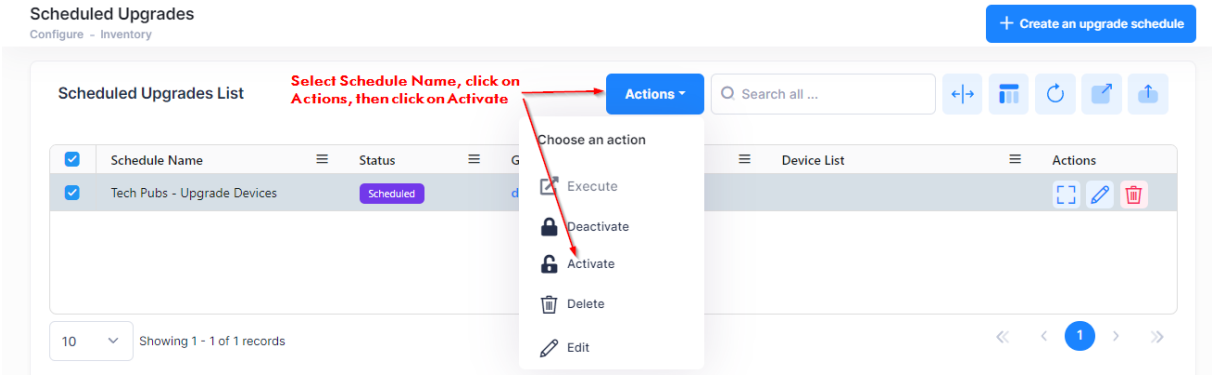
4.4.3 Execute a Scheduled Upgrade

Select a Schedule Name that you want to execute in the Scheduled Upgrades List, then click on **Actions** and select **Execute** from the drop-down menu.

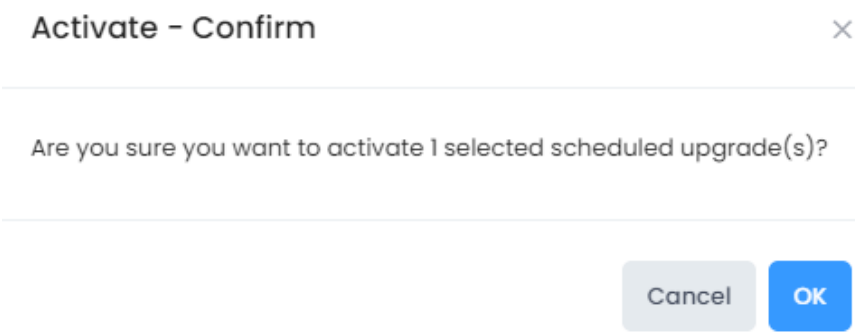
Click on **OK** to confirm that you want to execute the Scheduled Upgrade(s) from the List.

4.4.4 Activate a Scheduled Upgrade

Select a Schedule Name that you want to activate in the Scheduled Upgrades List, then click on **Actions** and select **Activate** from the drop-down menu.



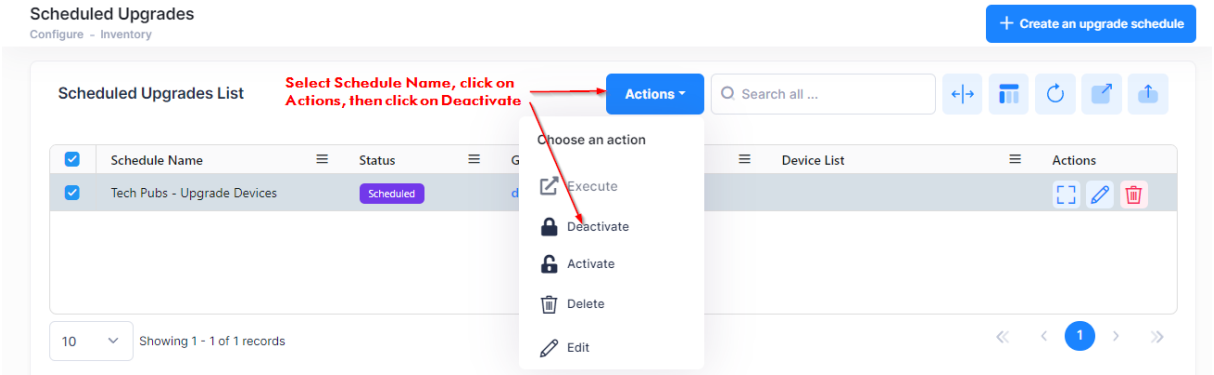
When you select the Scheduled Upgrade that you want to activate, the following confirmation prompt appears:



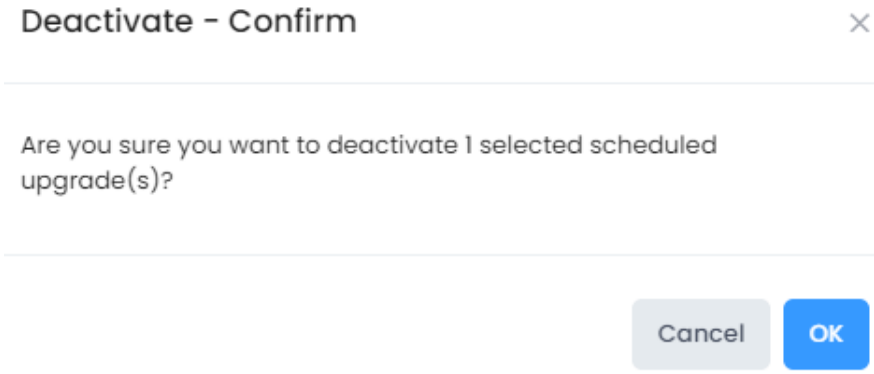
Click on **OK** to confirm that you want to activate the Scheduled Upgrade(s) from the List .

4.4.5 Deactivate a Scheduled Upgrade

Select a Schedule Name that you want to deactivate in the Scheduled Upgrades List, then click on **Actions** and select **Deactivate** from the drop-down menu..



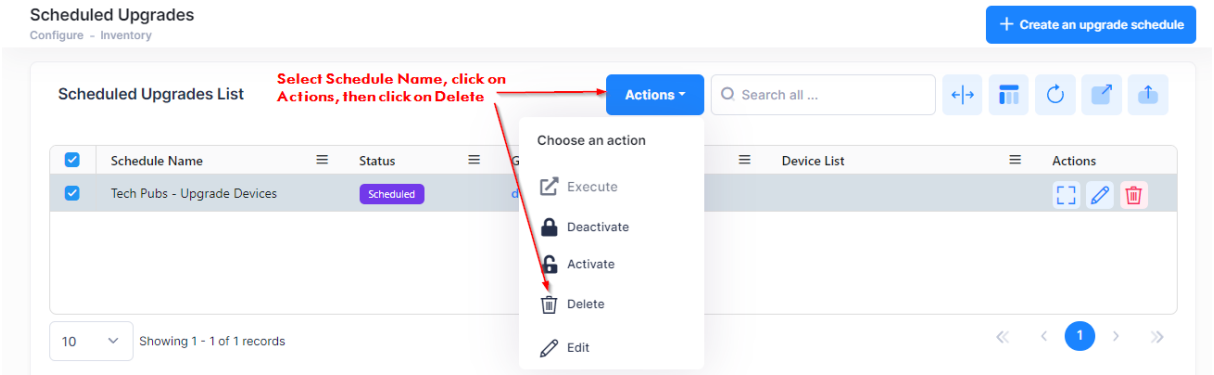
When you select the Scheduled Upgrade that you want to deactivate, the following confirmation prompt appears:



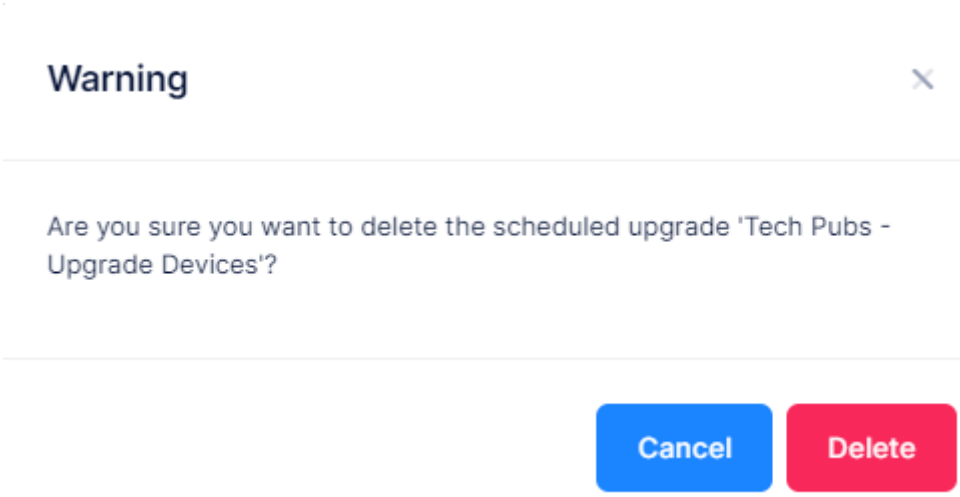
Click on **OK** to confirm that you want to deactivate the Scheduled Upgrade(s) from the List.

4.4.6 Deleting a Scheduled Upgrade

Select a Schedule Name(s) that you want to delete in the Scheduled Upgrades List, then click on **Actions** and select **Delete** from the drop-down menu. You can also click on the Delete icon under the “Actions” column for the scheduled upgrade entry.



When you select the Scheduled Upgrade you want to delete, the following confirmation prompt appears:



Click on **Delete** to remove the Scheduled Upgrade(s) from the List.

After deleting a Scheduled Upgrade, the Desired Version of scheduled devices will change to “Do Not Upgrade” in Device Catalog.

4.4.7 Scheduled Upgrade List

The Scheduled Upgrade List provides information on all scheduled upgrades.

- **Schedule Name -** User-configured name for the scheduled upgrade.
- **Status -** The status of the schedule upgrade.
  - **Scheduled -** The upgrade is scheduled to occur in the future. Note that if some of the devices in a Scheduled Upgrade were not upgraded during the configured time window, the status will change from "Upgrading" back to "Scheduled" until the next recurrence of the upgrade.
  - **Upgrading -** The upgrade is taking place within the configure time window.

  - **Disabled -** The scheduled upgrade was disabled when the time setting expired.
- **Groups** - The Access Point Groups selected for upgrade.
- **Devices List -**The devices being upgraded. Click on the devices in the column to view a full list of devices and additional information on each device, including the upgrade status of each device.
- **Start Date -** The date and time the upgrade is scheduled to start.
- **End Date -** The date and time the upgrade is scheduled to end.
- **Last Update Date -** The date and time the scheduled upgrade took place.

21 Oct 2025

4.4.8 Schedule an Upgrade from the Scheduled Upgrades List

The Create an Upgrade Schedule screen is used to define the schedule, the AP devices, and the software version to be used for the upgrade. To access this screen, click on **Create an upgrade schedule**.

The Create an Upgrade Schedule screen provides the following step-by-step process for configuring a scheduled upgrade:

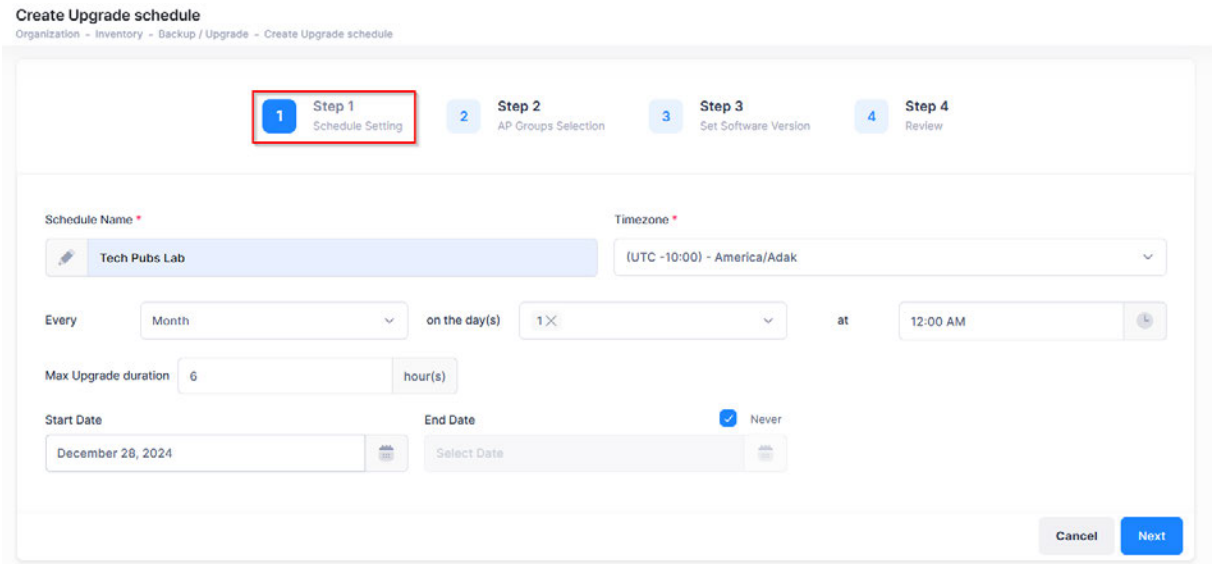
Step 1. **Schedule Setting** (see page 281) - Assign a name, timezone, the time to begin the upgrade, and the frequency at which the automatic upgrade is performed.

Step 2. **AP Groups Selection** (see page 282) - Select the devices to automatically upgrade.

Step 3. **Set Software Version** (see page 283) - Specify the software version to use for the upgrade.

Step 4. **Review** (see page 284) - Review all the configured schedule parameters before creating the scheduled update.

4.4.8.1 Step 1. Schedule Setting

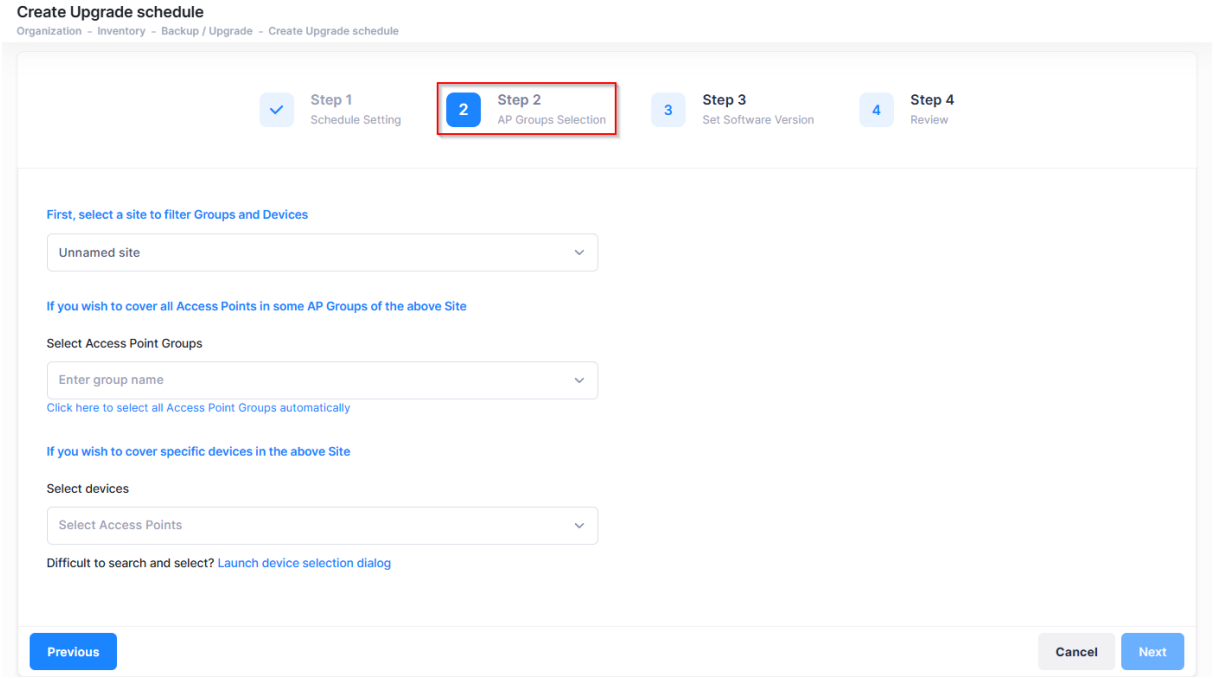


Complete the Schedule Setting fields as described below and click on **Next** to move to the next tab (Step 2).

- **Schedule Name** - User-configured name for the schedule name.
- **Timezone** - The timezone in which the device resides.
- **Every/at** - Select the frequency (Day, Week, Month) and the time at which the upgrade will occur.
- **Max Upgrade Duration** - The maximum time interval during which the upgrade will be performed. For example, if the upgrade is scheduled to start at 12:00 AM every day and the Max Upgrade Duration attribute is set is 6 hours, devices will start getting upgraded only between 12 AM to 6 AM. If a device in the schedule has not been updated when the time interval expires, it will not be upgraded during that scheduled upgrade, but will be upgraded during the next recurrence. Those devices that have already been upgraded will be skipped.

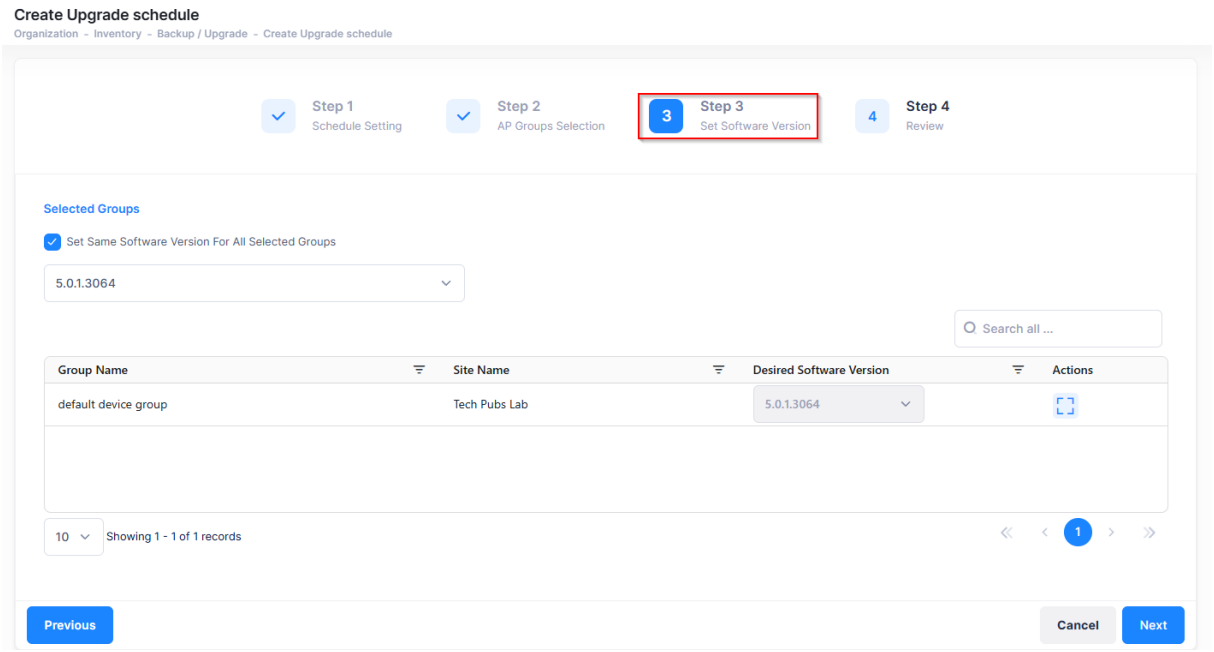
- **Start Date** - Select the start date for the scheduled upgrade. The scheduled update will begin on the start date at the configured frequency and time.
- **End Date** - Select “Never” to continue the upgrade schedule indefinitely or enter a date on which the upgrade schedule will end.

4.4.8.2 Step 2. AP Groups Selection



Select a Site from which AP Groups and/or devices can be selected, then select the AP Groups and/or devices to which the update schedule is applied. To pick devices from a list of devices, click on “Launch device selection dialog”. A Device Selection window opens from which you can select the devices for upgrade. Once devices are selected, click on **Next** to move to the next tab (Step 3).

4.4.8.3 Step 3. Set Software Version



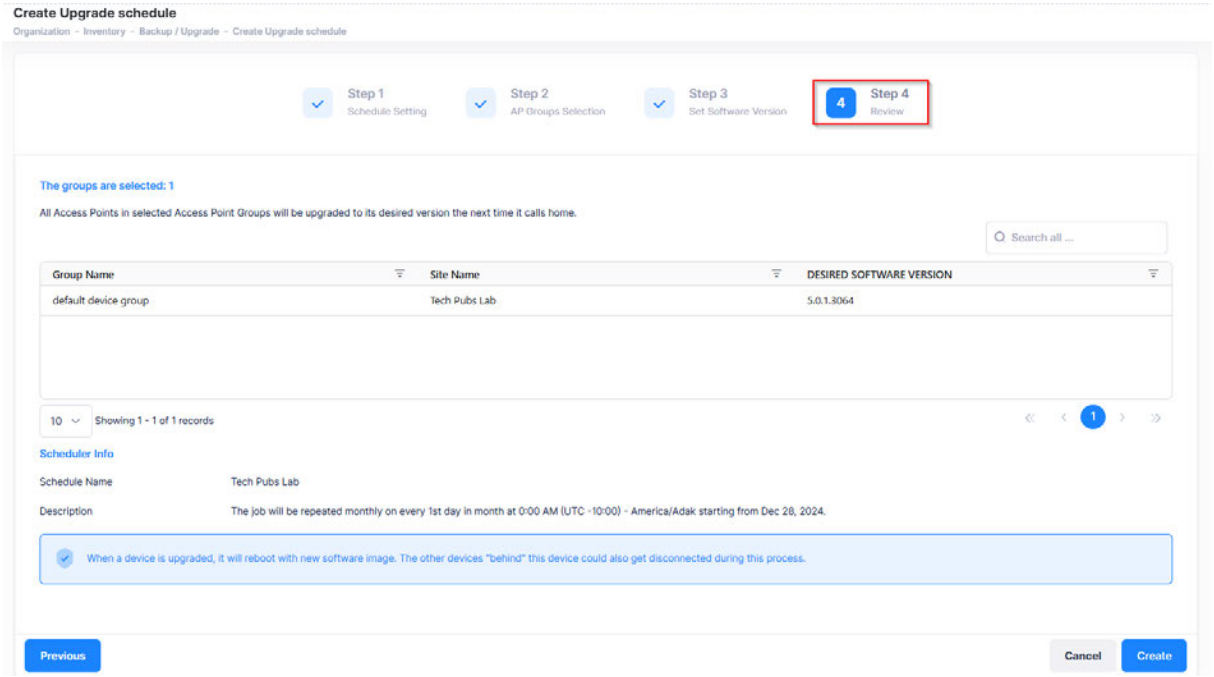
This screen displays the AP Groups that were selected for the upgrade schedule. Use this screen to specify the software version to which the devices will be upgraded. To remove a device from the Selected Access Points list, click on “X” under the “Actions” column.

- **Set Same Software Version for all Selected Groups (same models only)** - Select an upgrade software version to upgrade all selected AP groups to that software version. The selected access points groups must use the same base software. If not, the "Do Not Upgrade" will be your only option.
- **Set a Different Software Version for each Access Point Group** - Make sure the “Set Same Software Version for all Selected Groups” option is not checked. Under the "Desired Software Version" column, select the upgrade software version for each access point group.

> You CANNOT set “Do Not Upgrade” for any AP Group or device while creating scheduled upgrade.

After setting the software upgrade version, click on **Next** to move to the next tab (Step 4).

4.4.8.4 Step 4. Review



Review the groups and schedule information that you have configured and click on **Create**. A device will be upgraded to the desired software version the next time the device calls home.

> When a device is upgraded, it will reboot with a new software image. The other devices "behind" this device could also be disconnected during this process.

21 Oct 2025

4.4.9 Schedule an Upgrade from the Device Catalog Screen

Scheduled upgrades can be configured from the Device Catalog (see page 169) screen (**Configure > Inventory > Device Catalog**) by selecting one or more AP devices in the Device List and clicking on **Actions**. From the Actions drop-down menu, select **Edit Device - Schedule Software Upgrade** to open the Schedule Software Upgrade screen.

Similar to the Create an Upgrade Schedule (see page 281) screen, the Schedule Software Upgrade screen provides the following step-by-step process for configuring an upgrade schedule for selected devices:

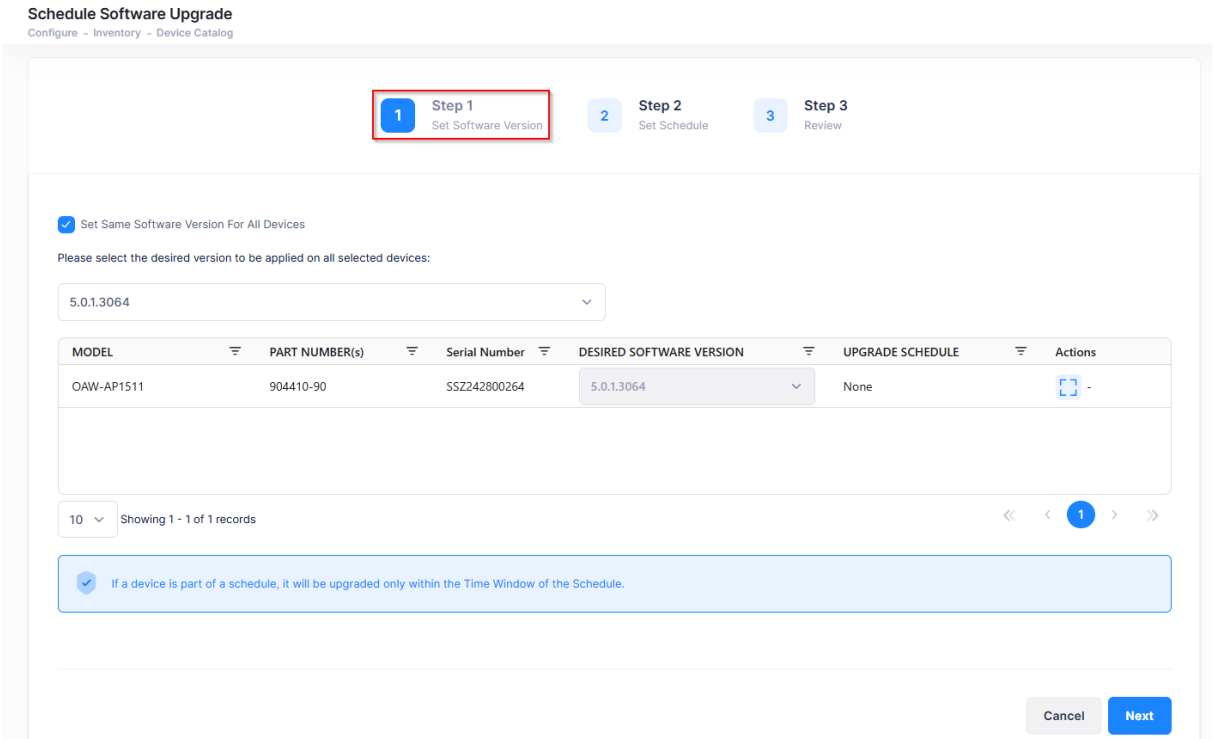
Step 1. Set Software Version (see page 285) - Specify the software version to use for the upgrade.

Step 2. Set Schedule (see page 286) - Select an existing schedule or create a new schedule for upgrading the device.

Step 3. Review (see page 287) - Review the configured schedule parameters before saving the desired settings.

> Use **Next** and **Previous** to navigate between the tabs.

4.4.9.1 Step 1. Set Software Version



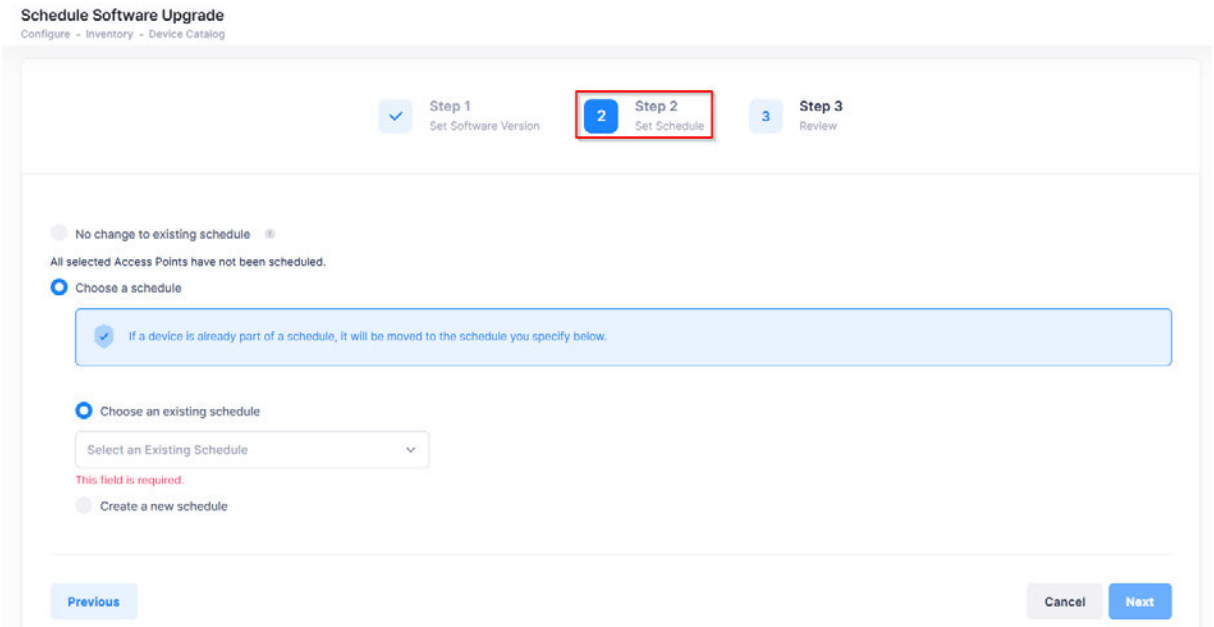
This screen displays the device(s) that were selected for the upgrade schedule. Use this screen to specify the software version to which the devices will be upgraded.

- **Set Same Software Version for All Devices (same models only)** - Select an upgrade software version to upgrade all devices to that software version. The devices must use the same base software. If not, the "Do Not Upgrade" will be your only option.
- **Set a Different Software Version for each Device** - Make sure the “Set Same Software Version for all Devices” option is not checked. Under the "Desired Software Version" column, select the upgrade software version for each device.

> If a device is part of a schedule, it will be upgraded only within the Time Window of the Schedule.

After setting the software upgrade version, click on **Next** to move to the next tab (Step 2).

4.4.9.2 Step 2. Set Schedule

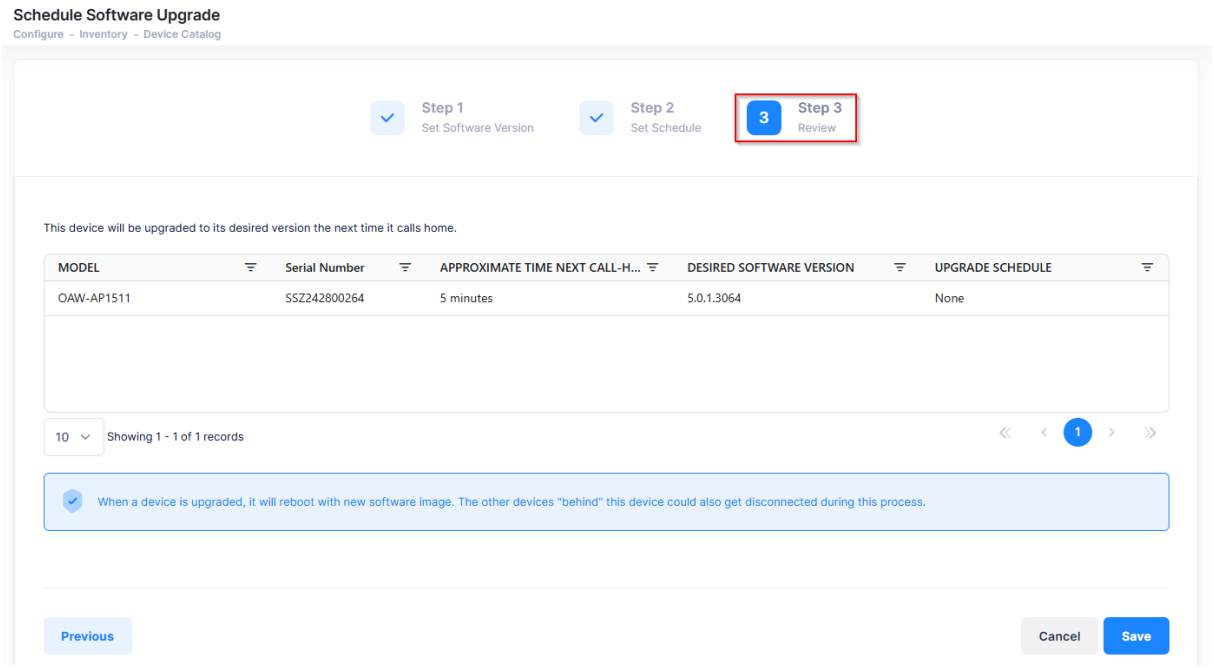


Specify the upgrade schedule by selecting one of the following options on the Set Schedule tab:

- **No change to existing schedule** - Select this option if the device is already included in a schedule. The device will be upgraded based on the time window of that schedule. (If the Access Point is not set in a scheduler, it will upgrade in the next time call home).
- **Choose a schedule** - Select a schedule that already exists or create a new schedule. Note that if a device is already included in an existing schedule, it will be moved to the schedule you specify with one of the following options:
  - **Choose an existing schedule** - Select an existing schedule from the drop-down menu.
  - **Create a new schedule** - Select this option to define a new schedule. Enter a schedule name, timezone, update frequency, update duration, and start/end date.

After setting the upgrade schedule, click on **Next** to move to the next tab (Step 3).

4.4.9.3 Step 3. Review



Review the selected device(s) and schedule that you configured. After reviewing the schedule parameters, click on **Save** to return to the Device Catalog List. A device will be upgraded to the desired software version the next time the device calls home.

- If you created a new upgrade schedule for the device, it will appear on the Review tab and is saved to the Scheduled Upgrades List (see page 276).
- If you specified a different upgrade schedule for the device, the device is added to the selected devices for that scheduled upgrade.

21 Oct 2025

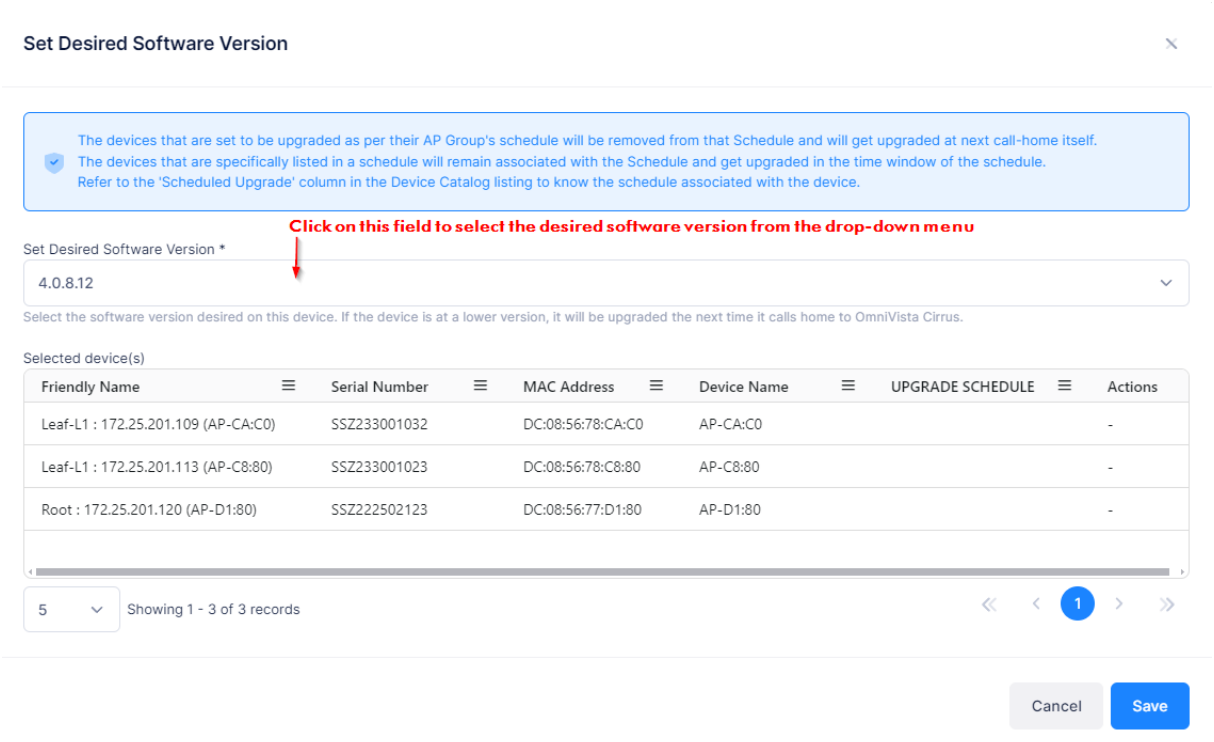
4.4.10 Set the Desired Software Version

The following options allow you to specify the desired software version for a device(s) directly from the Device Catalog List (see page 170):

- Select a single device (AP or Switch), then click on **Edit Device - Information** from the Actions drop-down menu. This opens the Edit Device Information screen (see page 222) where you can set the desired software version for the device. The device is updated to the specified software version the next time the device calls home.
- Select one or more devices (AP only), then click on **Edit - Schedule Software Upgrade** from the Actions drop-down menu. This opens the Schedule Software Upgrade screen (see page 285) where you can set the desired software version for the device(s). The device is updated to the specified software version according to the schedule associated with the device.
- Select one or more devices (AP or Switch), then click on **Edit - Set Desired Software Version** from the Actions drop-down menu. This option allows you to trigger a software upgrade the next time the selected device(s) call home, instead of waiting for a scheduled upgrade that is associated with the device.

4.4.10.1 Using the Set Desired Software Version Option

To use the “Set Desired Software Version” option, select the device(s) you wish to upgrade and click on **Actions**. From the Actions drop-down menu, click on **Edit Device - Set Desired Software Version**. The following Set Desired Software Version screen opens:



This screen displays the device(s) that you selected from the Device Catalog List. Use this screen to specify the software version to which the devices will be upgraded.

- **Set Desired Software Version** - click on this field to select one of the following options from the drop-down menu:
  - **Do Not Upgrade** - Do not upgrade the software on the device. If the device is part of an existing network, selecting “Do Not Upgrade” will leave your device running its current software version.
  - **Upgrade per AP Group schedule** - Upgrade the device based on the upgrade schedule for the AP Group to which the device belongs.
  - **Available software versions** - Select one of the available software versions listed.

Note the following about using the “Set Desired Software Version” option:

- The devices that are set to be upgraded per their AP Group's schedule will be removed from that Schedule and will be upgraded at the next call-home.
- The devices that are specifically listed in a schedule will remain associated with the Schedule and get upgraded during the time window of the schedule.
- Refer to the 'Scheduled Upgrade' column in the Device Catalog listing to know the schedule associated with the device.

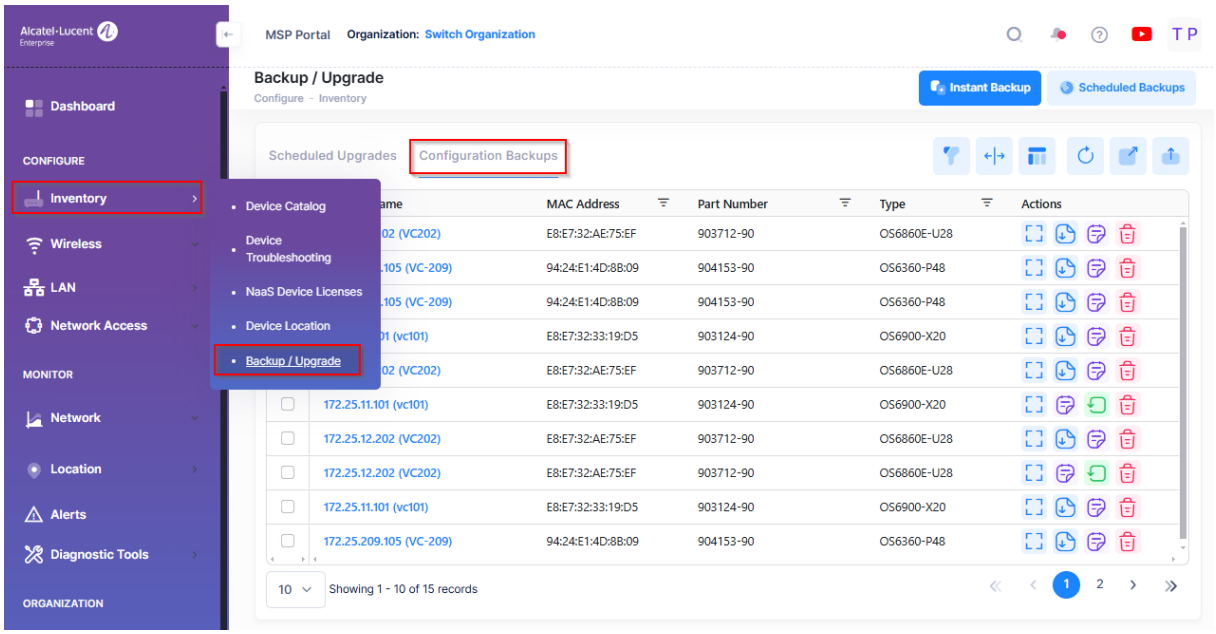
21 Oct 2025

4.5 Managing Switch Configuration Backups

The Configuration Backups tab on the Inventory Backup/Upgrade screen displays (see page 293)a list of all switch configuration backups that currently exist in OmniVista Terra. From this screen, you can perform any of the following actions:

- Backup switch configuration files (see page 290) - Perform immediate or create scheduled backups.
- Download configuration backups (see page 291) - Download a configuration backup to view on your local system.
- Delete configuration backups (see page 291) - Deletes selected backups from OmniVista Terra.
- View configuration backup files (see page 292) - View the files that are included in a specific configuration backup.
- Display configuration backup information (see page 293) - View basic information about a configuration backup. You can also customize the display to show the last backup created per device first or only backups with a specific scope (Site, Switch, Floor).

To configure and manage switch configuration backups, navigate to the Configuration Backups screen by clicking on **Inventory > Backup/Upgrade** and selecting the **Configuration Backups** tab under the "Configure" section of the OmniVista Terra Menu (see page 45).



Note that the Configuration Backups tab is also accessible from the Device Catalog (see page 169) screen (**Inventory > Device Catalog**) by selecting a switch device(s) in the Device Catalog List and clicking on **Actions**. From the Actions drop-down menu, select the **Configuration Management > Configuration Backups** option.

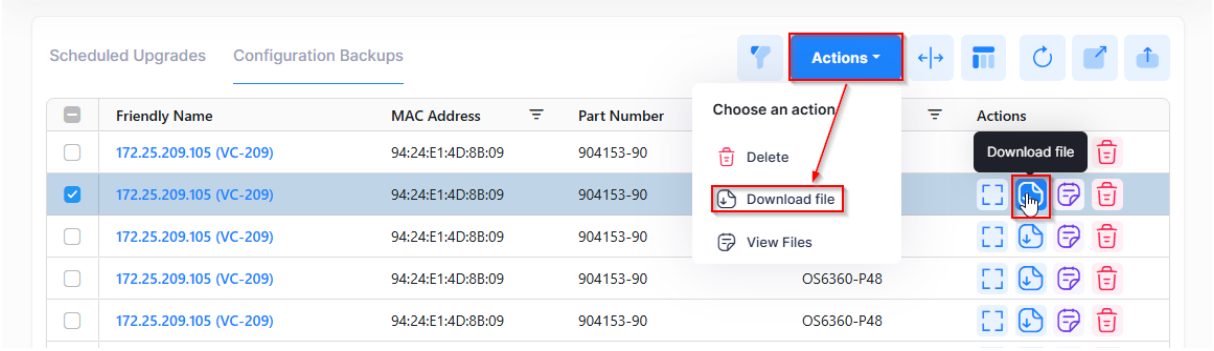
4.5.1 Performing a Backup

There are two ways to perform a configuration backup:

- Trigger an instant backup (see page 296) from the Configuration Backups tab, the Device Catalog screen, or the Topology screen.
- Use the Scheduled Backups (see page 300) on the Configuration Backups tab to schedule backups.

4.5.2 Downloading a Configuration Backup

To download the contents of a configuration backup, select the backup file entry, click on **Actions**, then select **Download file** from the drop-down menu. You can also click the Download icon under the “Actions” column for the configuration backup file entry.

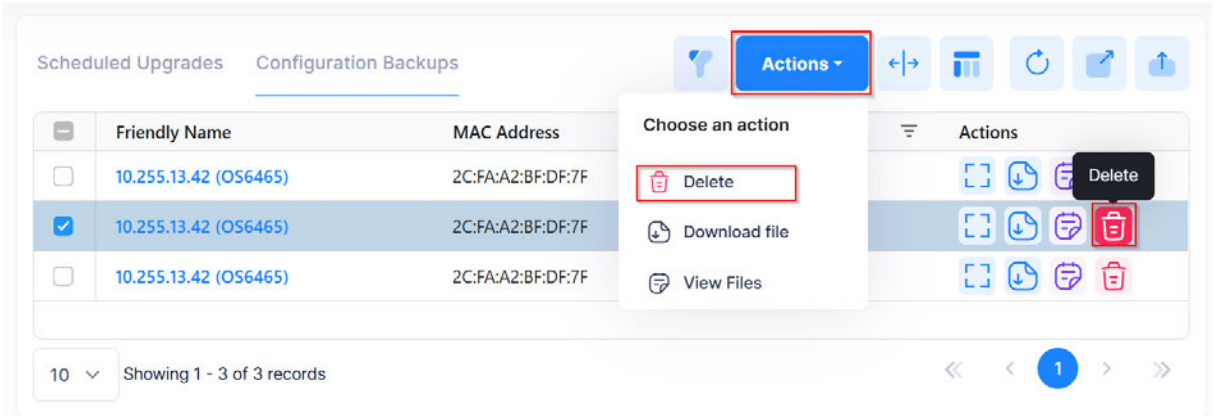


When you perform a backup file download, you are prompted to specify where on your system you would like to save the backup file. Once the downloaded file is saved, you can view the contents of the backup.

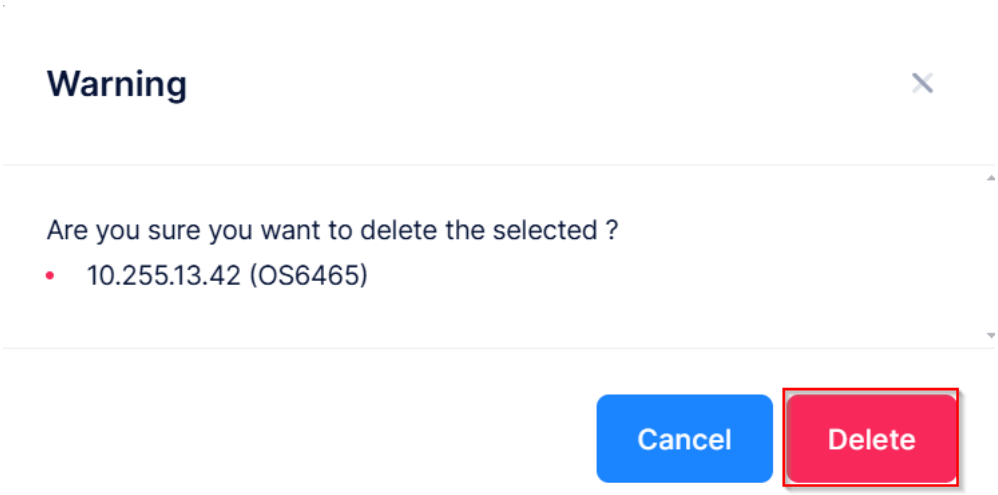
> If the configuration backup partially failed (“Status” field shows “Partial Success” or “Failed”), the download option is not available. Instead you will see an option to “Retry” the backup again.

4.5.3 Deleting a Configuration Backup

To delete a configuration backup, select the backup file entry, click on **Actions**, then select **Delete** from the drop-down menu. You can also click the Delete icon under the “Actions” column for the configuration backup file entry.



When you select the backup file that you want to delete, the following confirmation popup appears.



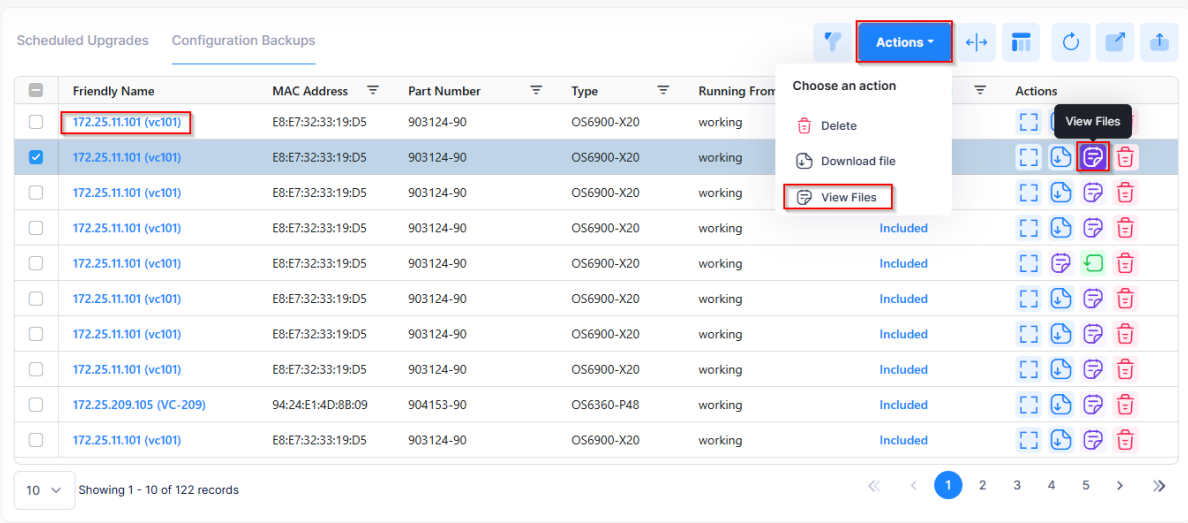
Click on **Delete** to remove the backup file from the Configuration Backups list.

> When a device is deleted from the Device Catalog, all configuration backups for that device are also deleted.

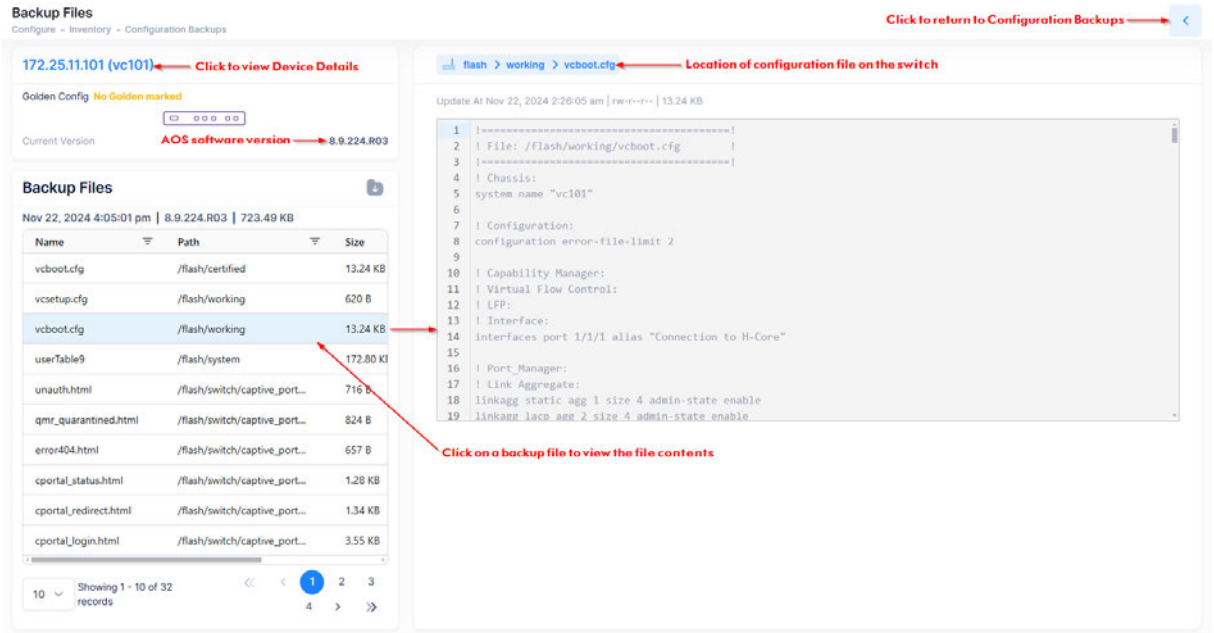
4.5.4 Viewing Configuration Backup Files

The Configuration Backups list provides the following methods for viewing the contents of configuration backups:

- Click on the Friendly Name of the device.
- Select the device, then click on **Actions** and select **View Files** from the drop-down menu.
- Click on the View Files icon under the “Actions” column next to the configuration backup entry.



When you select one of the above options, the Backup Files screen for the selected device appears.



The Backup Files screen includes provides the following information:

- **IP Address** - The IP address of the device, which is a link to the Device Details page for the device.
- **Golden Config** - Whether the configuration backup is a Golden Configuration for the device.
- **Current Version** - The AOS software version for the switch device (for example, 8.9.224.R03).
- **Backup Files** - The configuration files that were included in the configuration backup. Click on any one configuration file to see the contents of the file, as shown above. Note that the file contents is not configurable at this time.

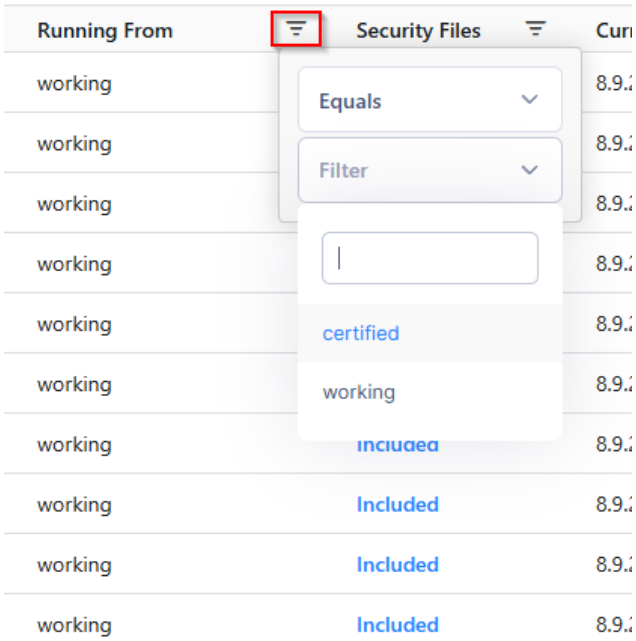
4.5.5 Display Backup Information

The Configuration Backups table displays the following basic information for each backup:

- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings (see page 26). By default, the Friendly Name is set to IP Address (System Name).
- **MAC Address** - The device MAC address.
- **Part Number** - The part number for the device.
- **Type** - The model number for the device (for example, OS6900-X20).
- **Running From** - The directory from which the switch is running (for example, “working”).
- **Security Files** - Whether security files on the switch were included in the backup (“Included” or “Excluded”).
- **Current Software Version** - The software version of the backup files (for example, 8.9.224.R03)
- **Status** - Indicates if the backup was successful, partially successful, or failed. If partially successful, a Retry icon appears in the “Actions” column that you can click to try the backup again.

- **Failed Reason** - If the backup failed, displays the reason for the failure (for example, invalid credentials)
- **Description** - The user-configured description for the backup, if one was entered for the backup.
- **Created At** - The date and time the backup was initiated.
- **# Files** - The number of files that were included in the backup.
- **Size** - The size, in bytes, of the backup file.

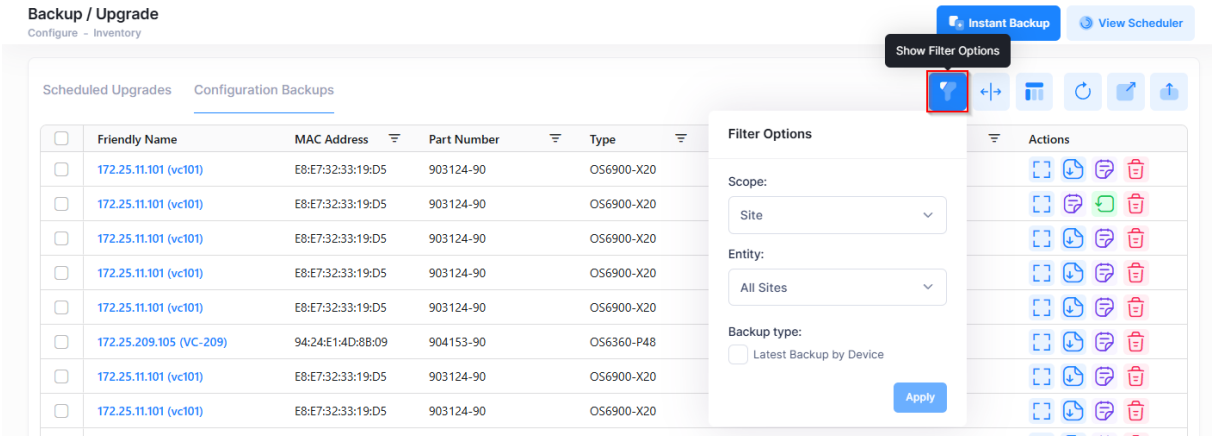
You can search for information in a specific column by clicking on the Search icon at the top of the column and entering search criteria. Delete the search criteria to return to the previous display. For example, you can select to search for “working” in the “Running From” column.



Note that each column in the Configuration Backups table has search criteria specific to the column field values.

4.5.5.1 Customizing the Configuration Backups Display

By default, information about all backups is displayed. To change the display to show customized views of the configuration backups, click on Show Filter Options and select the filters as described below:



- **Filter Options**:
  - **Scope** - Select Site (the default), Floor, or Switch.
  - **Entity** - Based on the scope selected, select one of the following entities from the drop-down list:
    - **Site** - Select All Sites (the default) or an individual site. Displays only backups for the selected Site.
    - **Floor** - Select a floor. Displays only backups for devices associated with the selected floor.
    - **Switch** - Select a switch. Displays only backups for the selected switch.
  - **Backup Type**
    - **Latest Backup by Device** - Select this option to display the latest backup per device.

After you have selected the filters to customize the display, click **Apply**. The Configuration Backups display will change according to the filters you applied. For example:

- By default, “Site” is selected for the Scope and “All Sites” is selected as the Entity and the Backup Type is not selected, so all backups for all devices within the Organizations are listed.
- If you change the filters to “Floor” for Scope and select a floor for the Entity, only backups for devices assigned to the selected floor are displayed.

21 Oct 2025

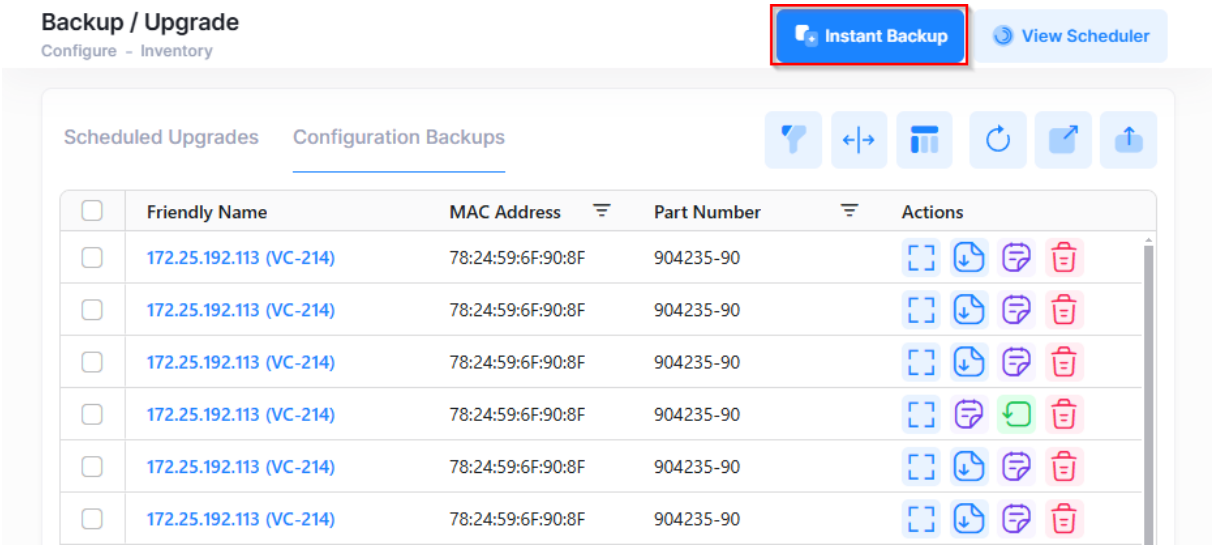
4.5.6 Perform an Instant Backup

You can trigger an immediate configuration backup on selected devices without having to wait for a scheduled backup time. There are two methods for performing an immediate configuration backup:

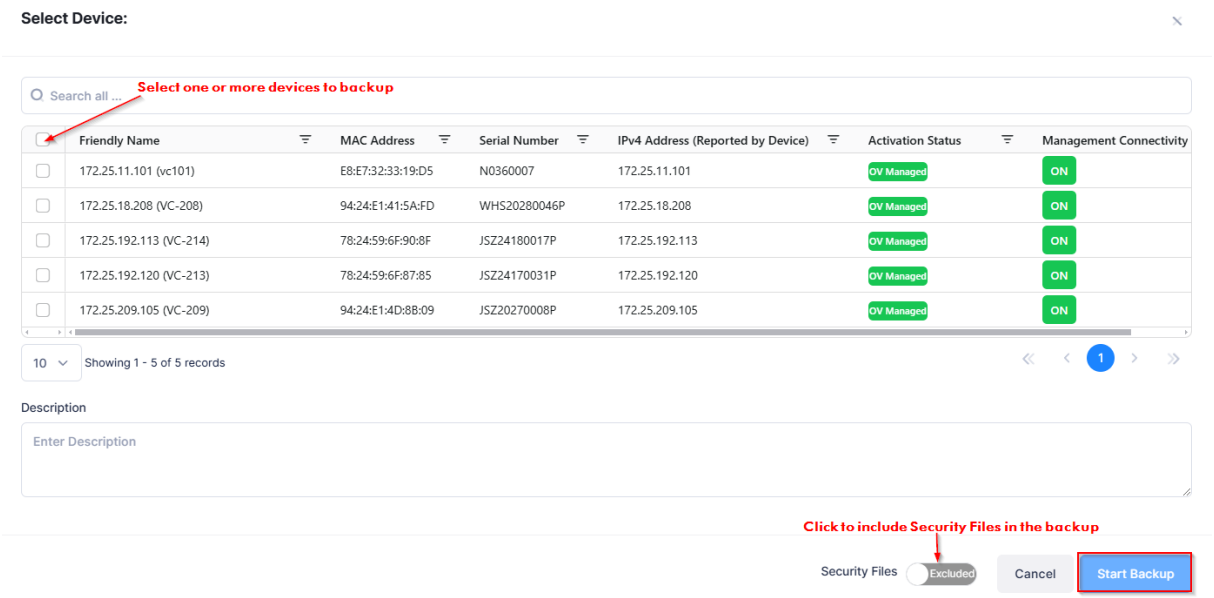
- On the Configuration Backups screen (see page 296), click on **Instant Backup**.
- On the Device Catalog screen (see page 297), select switch devices to back up and click on the **Instant Backup** option from the “Configuration Management” drop-down menu.

4.5.6.1 Instant Backup from the Configuration Backups Tab

To trigger an immediate backup, click **Instant Backup** on the Configuration Backups Tab.



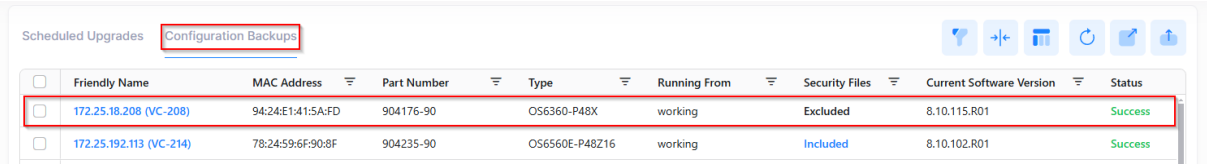
The following Select Device screen appears.



Select one or more devices to include in the Instant Backup, then complete the following and click **Start Backup**.

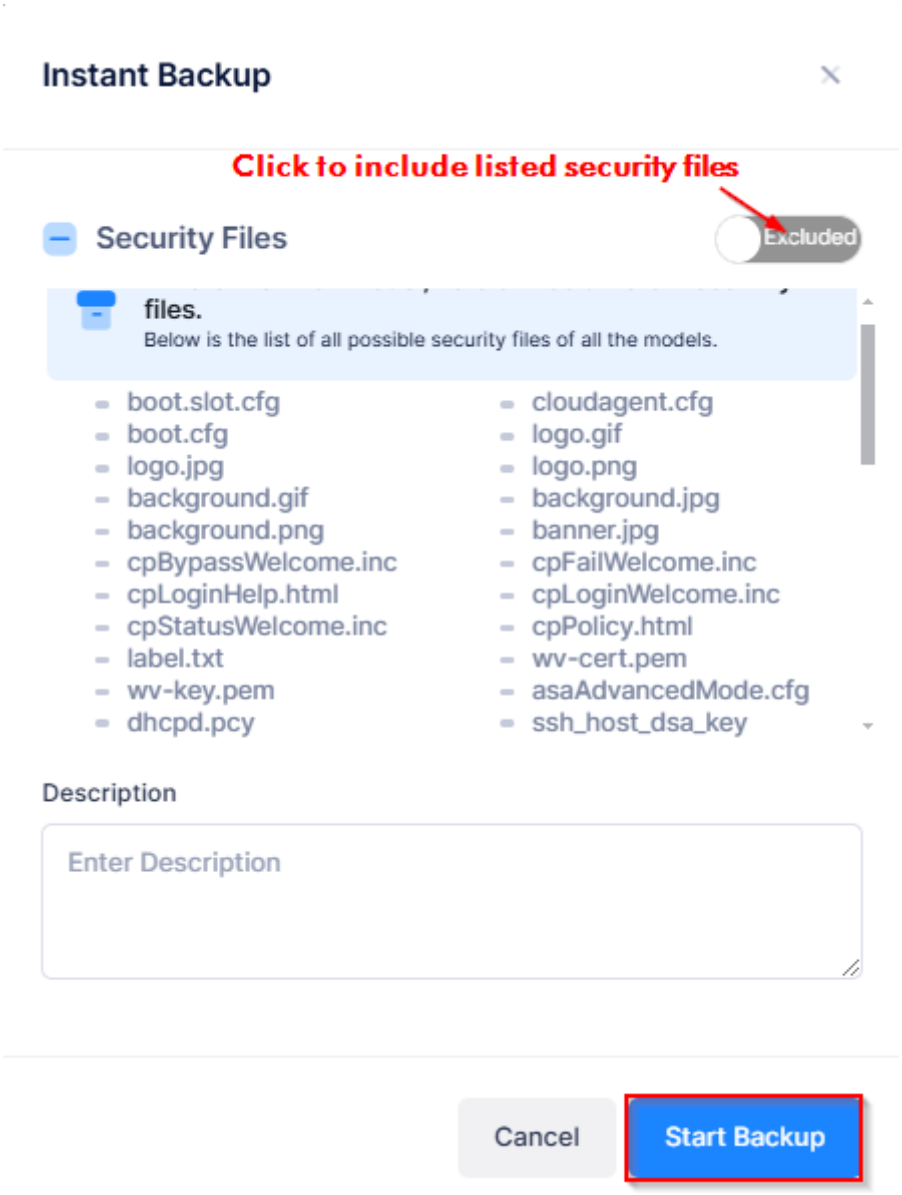
- **Description** - Enter an optional description for the backup.
- **Security Files** - Include or exclude switch security files in the backup. You do not have the option to select directories for a configuration backup since all configuration-related files in all directories are backed up. However, you can exclude security files from the backup for security reasons. By default, security files are excluded from the backup. If you want to include security files in the backup, set the Security Files slider to “Included”.

A configuration backup entry for the selected device(s) appears in the Configuration Backups list once the instant backup is triggered. The “Status” field will indicate the backup is “In Progress”. When complete, the “Status” field will change to “Success”. Refer to Displaying Configuration Backup Information for more details about Configuration Backup field values.



4.5.6.2 Instant Backup from the Device Catalog Screen

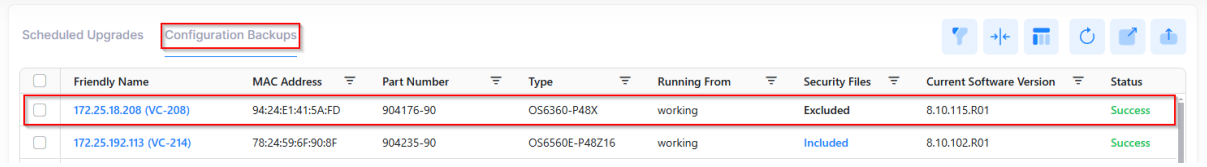
To trigger an immediate backup from the Device Catalog (see page 170) screen (**Configure > Inventory > Device Catalog**), select switch device(s) and click on **Actions**. From the Actions drop-down menu, select **Configuration Management - Instant Backup** to open the Instant Backup screen.



Complete the following on the Instant Backup popup screen, then click **Start Backup**.

- **Security Files** - Include or exclude switch security files in the backup. You do not have the option to select directories for a configuration backup since all configuration-related files in all directories are backed up. However, you can exclude security files from the backup for security reasons. By default, security files are excluded from the backup. If you want to include security files in the backup, set the Security Files slider to “Included”.
- **Description** - Enter an optional description for the backup.

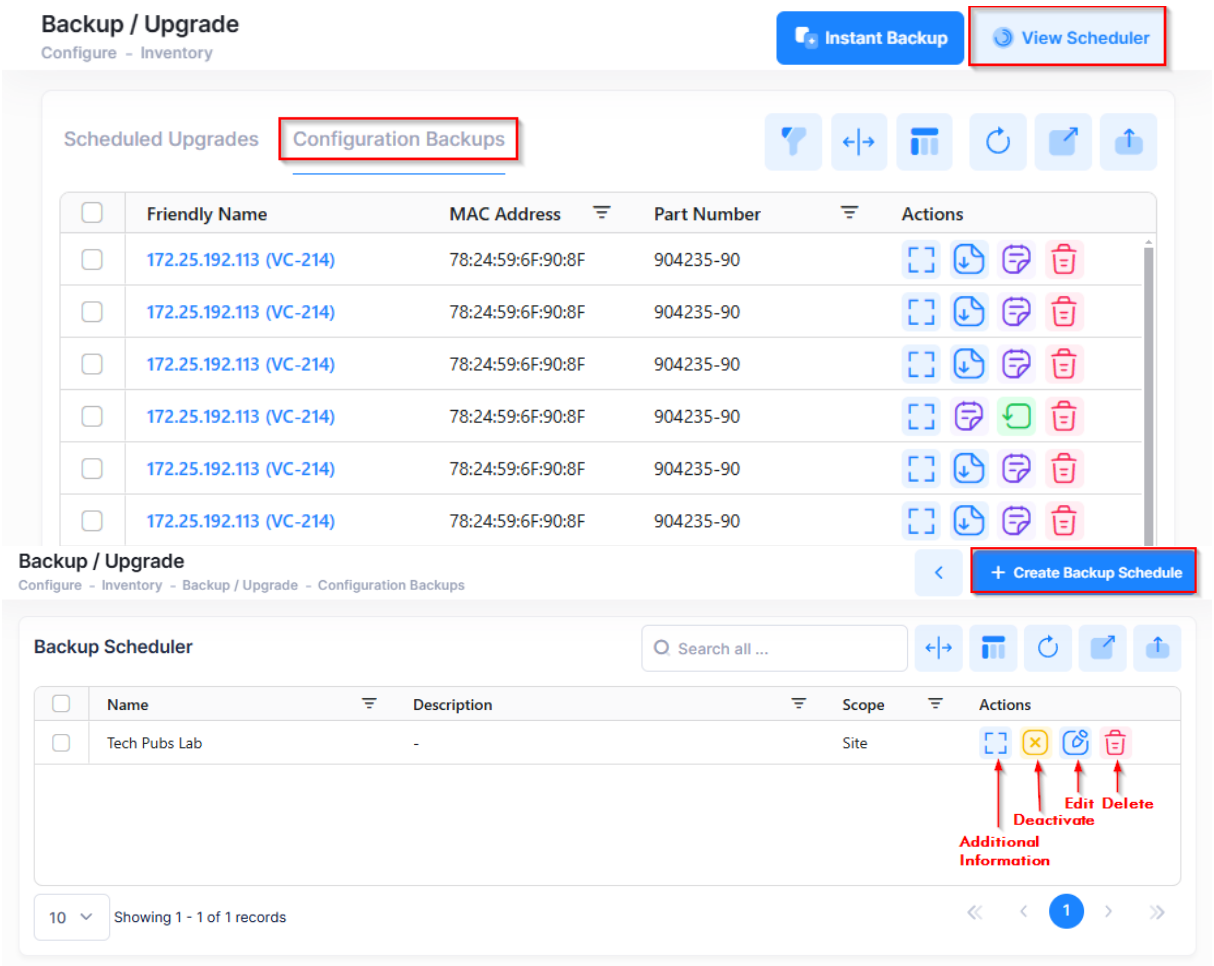
A configuration backup entry for the selected device(s) appears in the Configuration Backups list once the instant backup is triggered. The “Status” field will indicate the backup is “In Progress”. When complete, the “Status” field will change to “Success”. Refer to Displaying Configuration Backup Information for more details about Configuration Backup field values.


Scheduled Upgrades
Configuration Backups
Friendly Name
MAC Address
Part Number
Type
Running From
Security Files
Current Software Version
Status
172.25.18.208 (VC-208)
94:24:E1:41:5A:FD
904176-90
OS6360-P48X
working
Excluded
8.10.115.R01
Success
172.25.192.113 (VC-214)
78:24:59:6F:90:8F
904235-90
OS6560E-P48Z16
working
Included
8.10.102.R01
Success

21 Oct 2025

4.5.7 Schedule a Configuration Backup

The Backup Scheduler screen displays information about configuration backup schedules, and is used to create (see page 300), edit, activate, deactivate, and delete scheduled backups. This screen is accessible from the Configuration Backups (see page 290) tab by clicking on **View Scheduler**, as shown below.

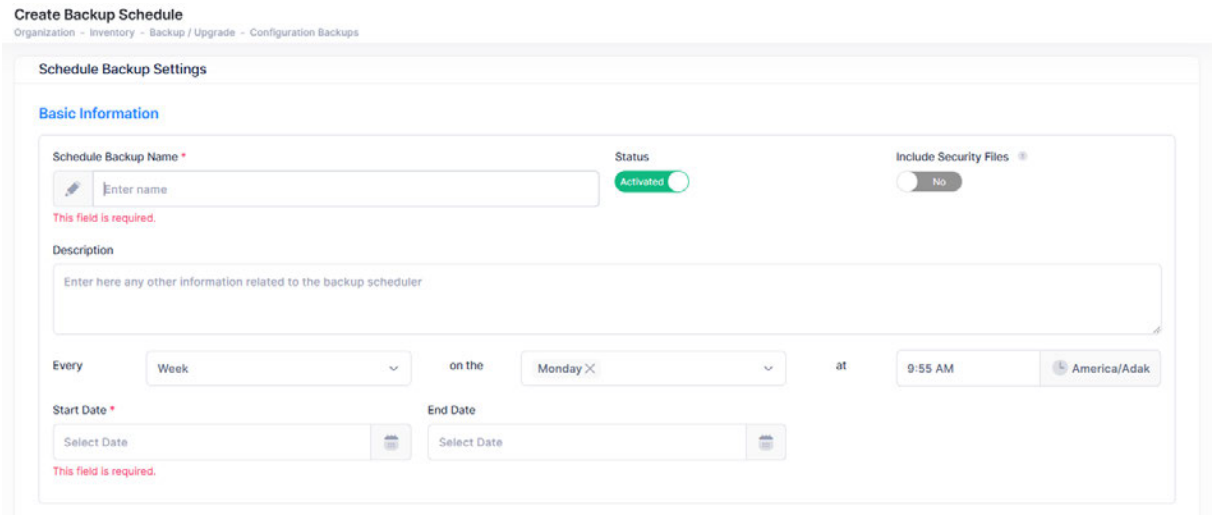


4.5.7.1 Creating a Backup Schedule

The Create Backup Schedule screen is used to configure regular backup schedules for switch device(s). To access this screen, click **Create Backup Schedule** on the Backup Schedular screen.

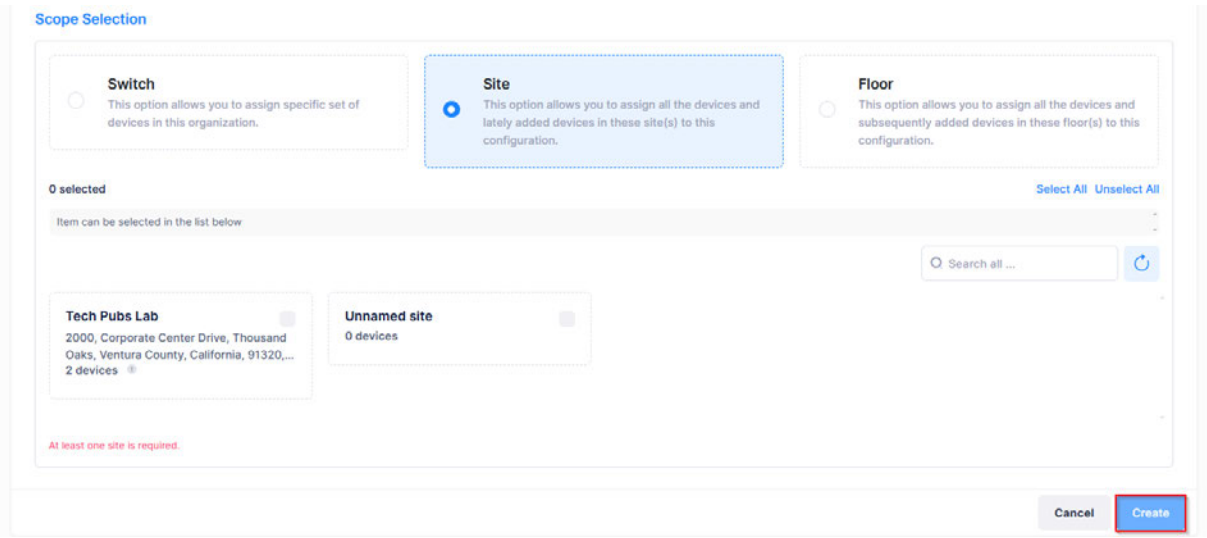
Complete the fields as described below to create a scheduled backup, then click **Create**. The new scheduled backup will appear in the Backup Scheduler list.

4.5.7.1.1 Basic Information



- **Scheduled Backup Name** - Enter the name to assign to the scheduled backup.
- **Status** - Activate (the default) or Deactivate the scheduled backup.
- **Include Security Files** - Include (Yes) or exclude (No) switch security files in the backup. You do not have the option to select directories for a configuration backup since all configuration-related files in all directories are backed up. However, you can exclude security files from the backup for security reasons. By default, security files are excluded from the backup. If you want to include security files in the backup, set the Security Files slider to “Yes”.
- **Description** - Enter an optional description for the scheduled backup.
- **Every/at** - Select the frequency (Day, Week, Month) and the time at which the backup will occur. (**Note:** The scheduler uses the Organization time zone therefore, changing the time zone in Organization Settings will affect the backup trigger time.)
- **Start Date** - Select the start date for the scheduled backup. The backup will begin on the start date at the configured frequency and time.
- **End Date** - Select a date on which the backup will end.

4.5.7.1.2 Scope Selection

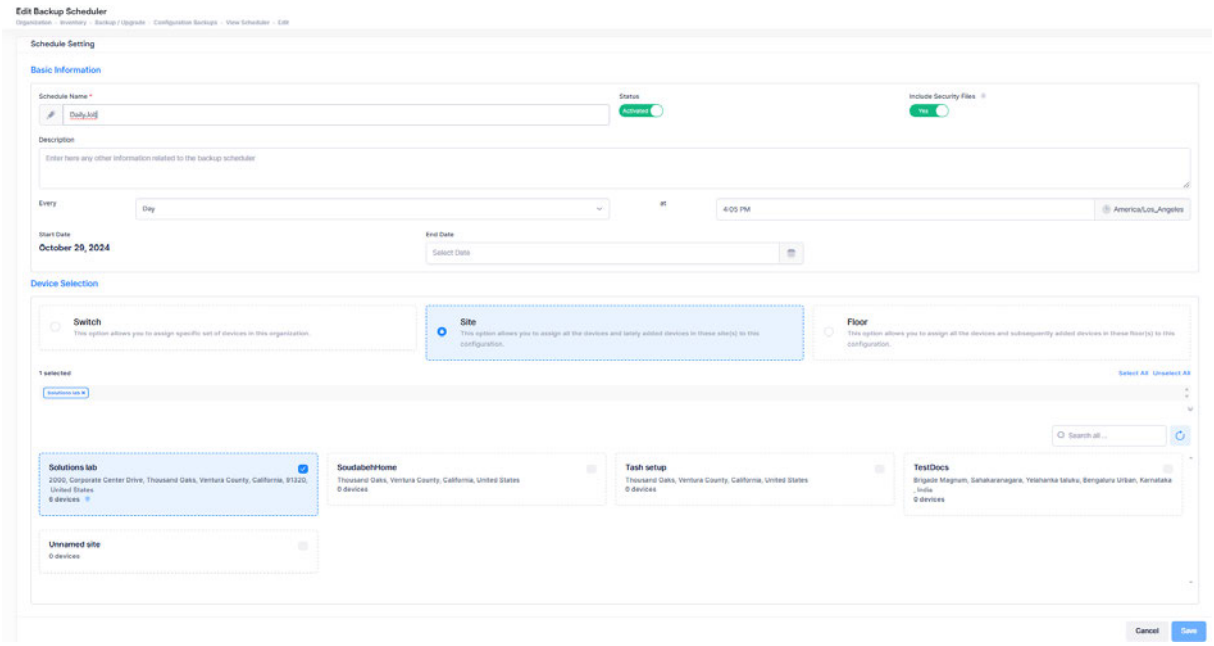


The Scope Selection section is where you can designate the devices to backup by selecting one of the following options:

- **Switch** - Assign specific switch devices in the Organization to the scheduled backup. The selected switches are backed up according to the backup schedule.
- **Site** - Assign an Organization Site to the scheduled backup. All switch devices associated with the Site are backed up according to the backup schedule. Any devices that are added to the Site are also included in the backup schedule assigned to the Site.
- **Floor** - Assign Organization Floors to the scheduled backup. All switch devices associated with the selected Floors are backed up according to the backup schedule. Any devices that are added to any of the selected Floor are also included in the backup schedule assigned to the Site.

4.5.7.2 Editing a Backup Schedule

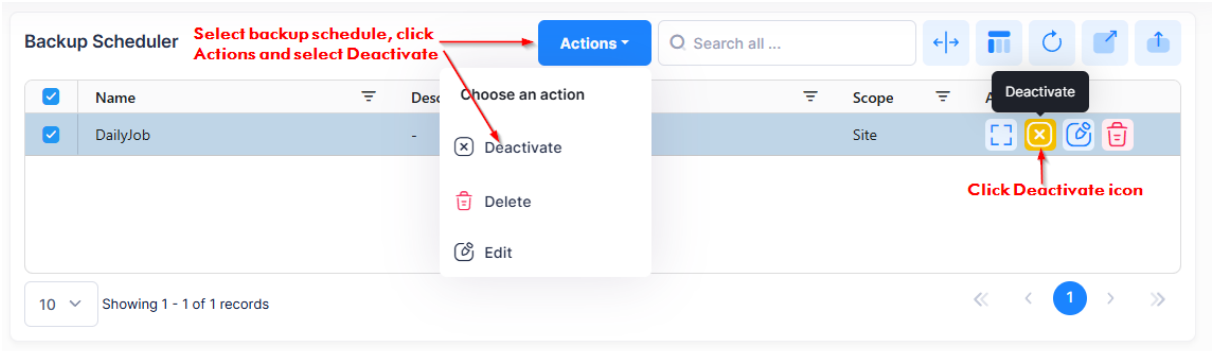
Select a backup schedule in the Backup Scheduler list, then click on **Actions** and select **Edit** from the drop-down menu. You can also click on the Edit icon under the “Actions” column for the backup schedule entry. The Edit Backup Scheduler screen opens.



Edit the fields as described in Creating a Backup Schedule (see page 300), then click on **Save** to retain changes to the scheduled upgrade.

4.5.7.3 Deactivating a Backup Schedule

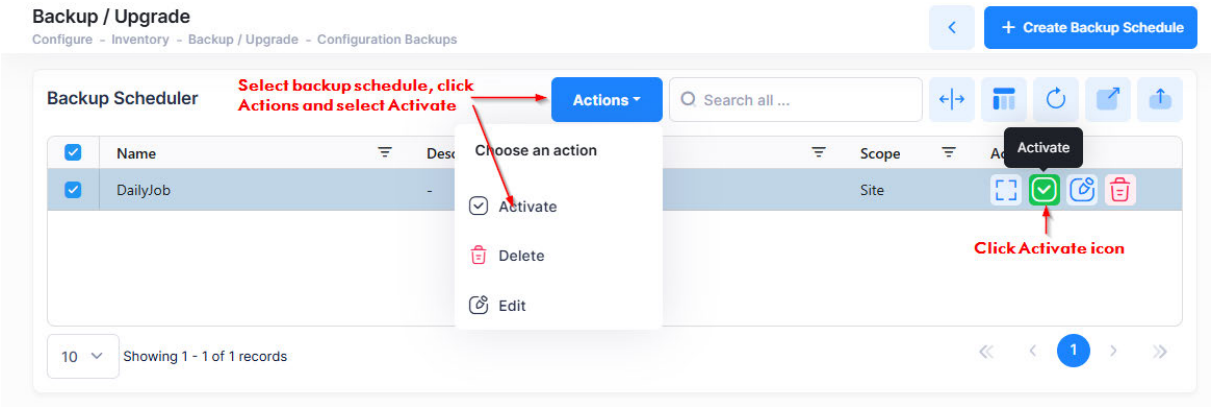
Select a backup schedule in the Backup Scheduler list, then click on **Actions** and select **Deactivate** from the drop-down menu. You can also click on the Deactivate icon under the “Actions” column for the backup schedule entry.



When you deactivate a backup schedule, there is no warning message and the “Deactivate” option and icon change to “Activate”.

4.5.7.4 Activating a Backup Schedule

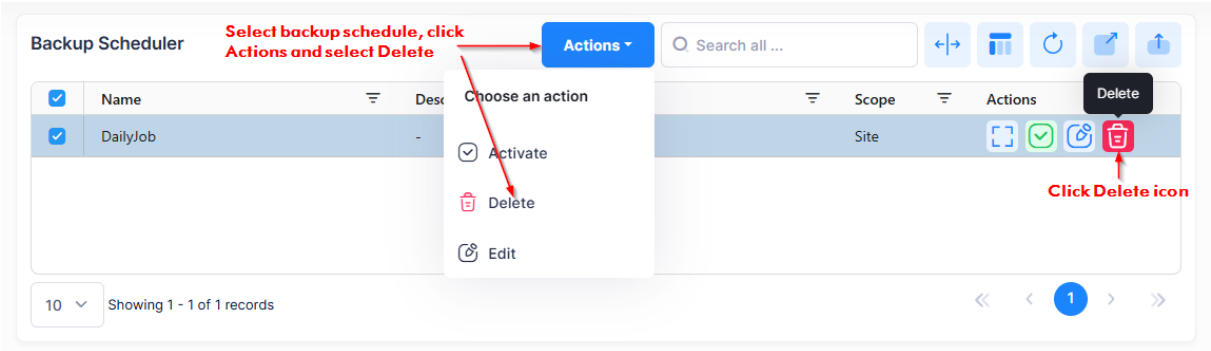
Select a backup schedule in the Backup Scheduler list, then click on **Actions** and select **Activate** from the drop-down menu. You can also click on the Activate icon under the “Actions” column for the backup schedule entry.



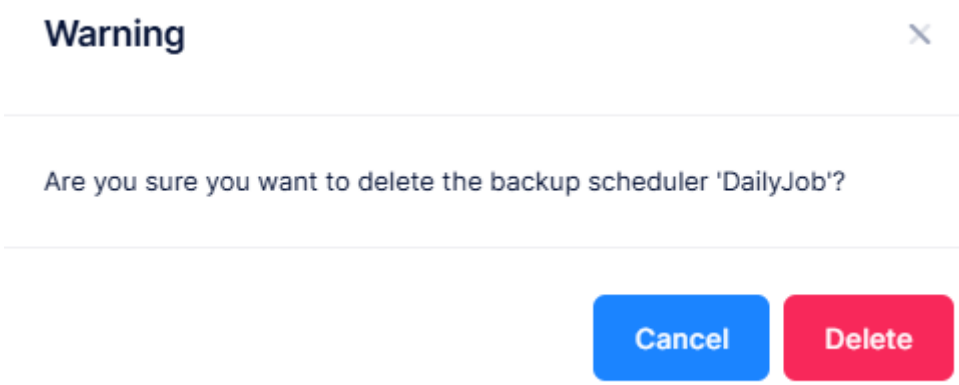
When you activate a backup schedule, the “Activate” option and icon change to “Deactivate”, as shown here (see page 303).

4.5.7.5 Deleting a Backup Schedule

Select a backup schedule in the Backup Scheduler list, then click on **Actions** and select **Delete** from the drop-down menu. You can also click on the Delete icon under the “Actions” column for the backup schedule entry.



When you select the backup schedule that you want to delete, the following confirmation popup appears.



Click on **Delete** to remove the backup schedule from the Backup Scheduler list.

- If all sites or devices in the Backup Scheduler are deleted, the scheduler is deleted immediately.
- If all floors in the Backup Scheduler are deleted, the scheduler will be deleted the next day.

21 Oct 2025

5 Configure WLAN Network Management

The OmniVista Terra Wireless LAN (WLAN) group of applications are used to configure wireless networks, policies to prevent attacks on Stellar AP Series Wireless Devices, and Radio Frequency (RF) profiles for devices. It is also used to configure External Engines and UPAM server certificates.

To access the WLAN group of applications, click on the **Wireless** option under the “Configure” section of the OmniVista Terra Menu (see page 45). When you click on the **Wireless** option, the following list of applications is provided to assist with configuring WLAN network management:

- **Profile**
  - **Access Point Groups** (see page 309) - Displays information about configured Access Point (AP) Groups. This screen is also used to create, edit, or delete AP Groups.
  - **Provisioning Configuration** (see page 313) - Displays information about Provisioning Configurations that are assigned to AP Groups.
  - **RF Profiles** (see page 331) - The RF Profiles application is used to create wireless RF Profiles for Stellar APs and AP Groups.
- **SSIDs** (see page 347) - The SSIDs application is used to configure wireless networks. The SSIDs option simplifies wireless network configuration with one-step provisioning, including SSID setup as well as authentication and policy configuration.
- **WIPS** (see page 376)- The Wireless Intrusion Protections System (WIPS) application is used to monitor the wireless radio spectrum for the presence of unsafe access points and clients, and is used to configure policies to classify rogue APs/wireless attacks and take countermeasures to mitigate the impact of foreign intrusions.
- **Advanced**
  - **External Engines** (see page 388) - The External Engines application is used to declare server configurations for Aeroscout, Stellar Asset Tracking, Wifi RTLS, and Advanced Analytics. OmniVista Terra can integrate with an Aeroscout, OmniVista Terra WiFi RTLS, and OmniAccess Stellar Asset Tracking Server to provide Location Based Services (LBS); OmniVista Advanced Analytics to provide advanced analytics data to OmniVista Terra and above installations. BLE Location Service is a pre-configured service dedicated to OmniAccess Stellar Asset Tracking.
  - **Certificates** (see page 394)- The Certificates application is used to configure/upload a Web Server/External Portal Server Certificate File. This Certificate File is used to establish a secure connection between OmniVista Terra and APs when using the Web UI Device Management Tool as well as a secure connection to an External Portal Server. This application is also used to upload a Local LDAP Certificate File, which is used to establish a secure connection between an AP and a Local LDAP Server.
  - **External Captive Portal** (see page 409) - The External Captive Portal Configuration file is used to provide secure communication between APs and an External Captive Portal Server. The management of external configuration files is done through Access Role Profiles. When the Captive Portal option for the Access Role Profile is set to “External”, you can specify the name of an External Captive Portal Configuration file to use. Traffic assigned to the profile will be redirected to the External Captive Portal Server identified in the configuration file.

- **Data VPN Settings** (see page 414) - The Data VPN Settings application is used to create Data VPN Server profiles. Data VPN Servers allow devices to access remote functionality.

21 Oct 2025

5.1 Profile

- **Access Point Groups** (see page 309) - Displays information about configured Access Point (AP) Groups. This screen is also used to create, edit, or delete AP Groups. Stellar AP Series devices are managed by AP Group. OmniVista does not manage individual APs. You must first add APs to AP Groups. The attributes configured for the AP Group are applied to all APs in the group. Specifying an AP Group is required when adding an AP to the Device Catalog.
- **Provisioning Configuration** (see page 313) - Displays information about Provisioning Configurations that are assigned to AP Groups. Access Points that are members of an AP Group utilize the Provisioning Configuration associated with the group to boot up and get a basic configuration. Specifying a Provisioning Configuration is required when creating an AP Group.
- **RF Profiles** (see page 331) - The RF Profiles application is used to create wireless RF Profiles for Stellar APs and AP Groups. RF Profiles enable the user to ensure that transmit power and operating frequencies meet the requirements of global regulatory agencies and individual countries. A user can also use the profiles to adjust the wireless parameters and functions according to real network environment to improve the user experience of wireless network.

21 Oct 2025

5.1.1 Access Point Groups

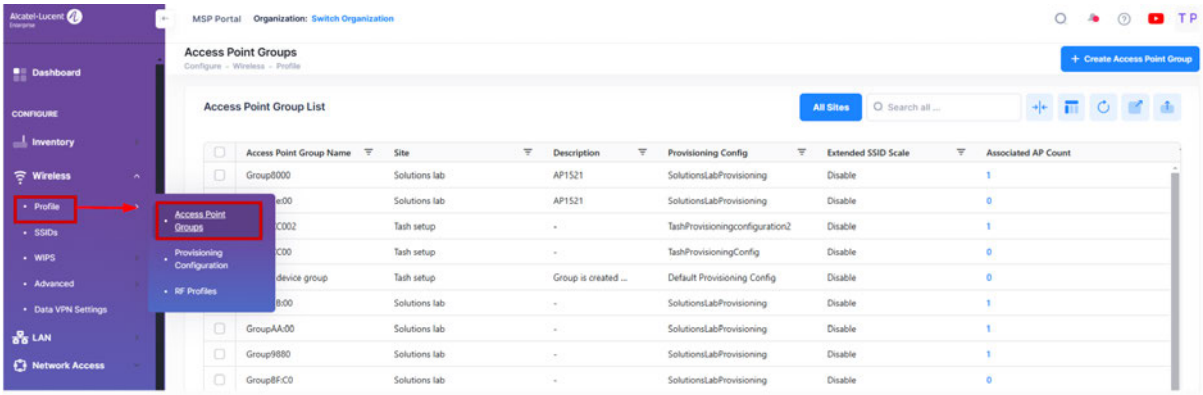
The Access Point Groups screen displays information (see page 312) about configured Access Point (AP) Groups. The screen is also used to create (see page 309), edit (see page 311), and delete (see page 311)AP Groups. Stellar AP Series devices are managed by AP Group. OmniVista does not manage individual APs. You must first add APs to AP Groups. The attributes configured for the AP Group are applied to all APs in the group.

Once an AP(s) are assigned to a group, you configure the APs in OmniVista by applying the configuration to the AP Group. In OmniVista applications (e.g., Scheduled Upgrades, Provisioning), rather than presenting the user with individual APs when applying a configuration, OmniVista presents the user with the option of applying a configuration to AP Groups. Any configuration applied to an AP Group is applied to all APs in the group.

If an AP Group contains a mix of AP models and some models do not support certain features, OmniVista Terra will skip applying a configuration to the AP models that do not support the specific feature. For example, AP12XX models may not support all AWOS 5.0.3 features, so this model is skipped when OmniVista Terra applies any 5.0.3 features not supported on the AP12XX.

Verify the features that are supported for your AP models when assigning models to an AP Group.

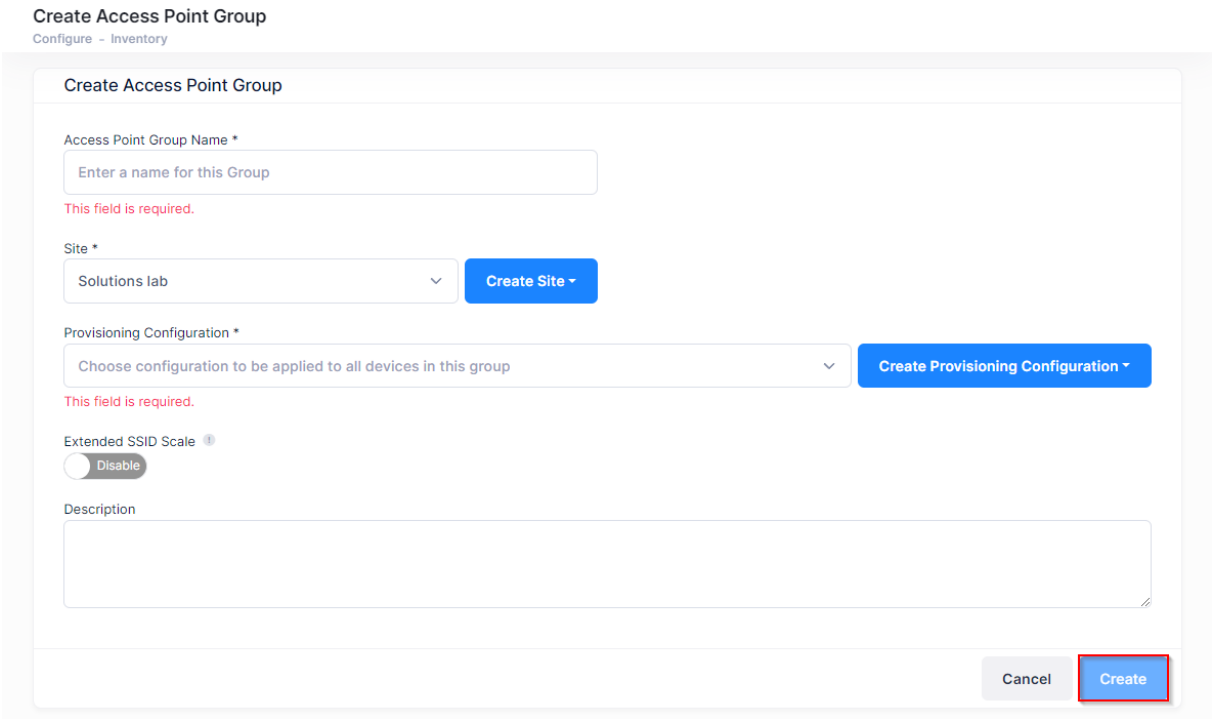
To manage AP Groups, navigate to the Access Point Groups screen by clicking on **Wireless > Profile > Access Point Groups** under the “Configure” section of the OmniVista Terra Menu (see page 45).



5.1.1.1 Creating an Access Point Group

An AP Group must be specified at the time an AP device is added to the Inventory Device Catalog (see page 170). There is a pre-configured default AP Group (“default device group”) designated for each Site within an Organization. You can select the default group or create a new AP group. Note that an AP can belong to only one AP Group at a time.

Click on **Create Access Point Group** on the Access Point Groups List screen. The Create Access Point Group screen opens.



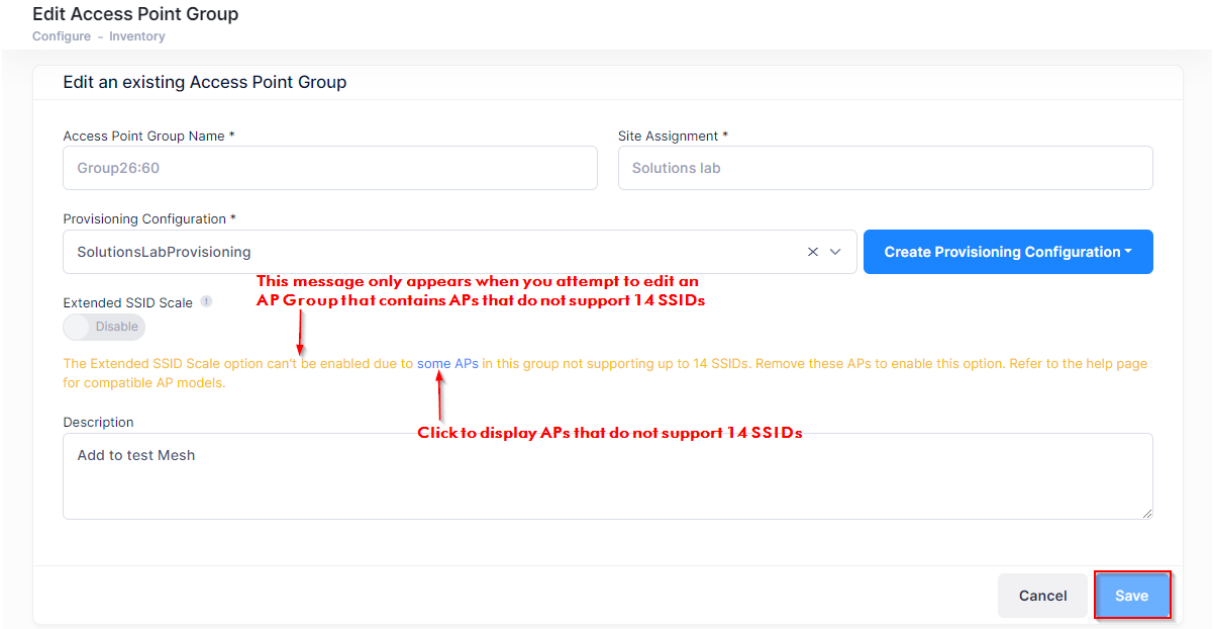
Complete the fields as described below to configure an AP Group. When you are finished, click on **Create**.

- **Access Point Group Name** (Required) - Enter a unique name for the group (up to 64 characters).
- **Site** (Required) - Select the Organization Site to which the AP Group will be assigned or click on **Create Site** to add a new Site to assign to the AP Group (see the Create a Site (see page 73) online help).
- **Provisioning Configuration** (Required) - You can select the “Default Provisioning Config” or one of the other provisioning configurations presented from the drop-down menu. To create a new configuration, click on **Create Provisioning Configuration** (see the Provisioning Configuration (see page 313) online help).
- **Extended SSID Scale** - Enable/Disable extending the number of SSIDs that can be assigned to the AP Group to 14. When enabled (On), only Stellar AP models that support up to 14 SSIDs can join the AP Group. When disabled (Off), any AP model can join the group, but the limit is 7 SSIDs per AP Group
  - Stellar AP models that support up to 14 SSIDs: AP1201, AP1321, AP 1322, AP1261, AP1361D, AP1362, AP1301H, AP1331, AP1351, AP1451, AP1411, AP1431, AP1201BG, AP1511, AP1521.
  - Note that the Extended SSID Scale status does not apply to 6GHz networks, which have a limit of 4 SSIDs per AP Group.
- **Description -** Enter an optional description for the group.

5.1.1.2 Editing an Access Point Group

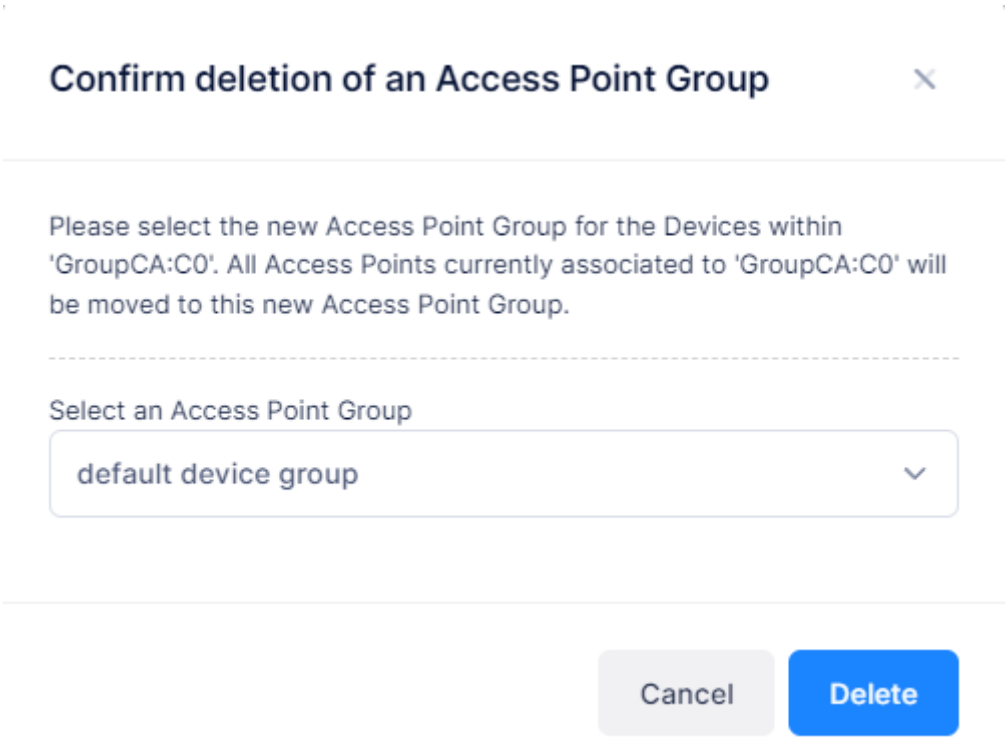
Select an AP Group in the AP Group List and click on the Edit icon under the “Actions” column or select Edit from the **Actions** drop-down menu to bring up the Edit Access Point Group screen. Edit the fields as described above (see page 309)and click on **Save**.

- The “default device group” cannot be edited.
- You cannot enable the Extended SSID Scale status for an AP Group that contains APs that do not support up to 14 SSIDs. Remove any such APs from the AP Group before enabling the Extended SSID Scale status.



5.1.1.3 Deleting an Access Point Group

Select an AP Group(s) in the AP Group List and click on the Delete icon under the “Actions” column or select Edit from the **Actions** drop-down menu. The following confirmation prompt appears:



Click on the “Select an Access Point Group” field to select the AP Group to which the APs that belong to the deleted group will be moved. This field defaults to “default device group”. Click on **Delete** to confirm removing the AP Group and moving associated APs to the selected group.

> You cannot delete the Default AP Group (“default device group”).

5.1.1.4 Access Point Group List

The Access Point Group List displays the following information for each Access Point Group:

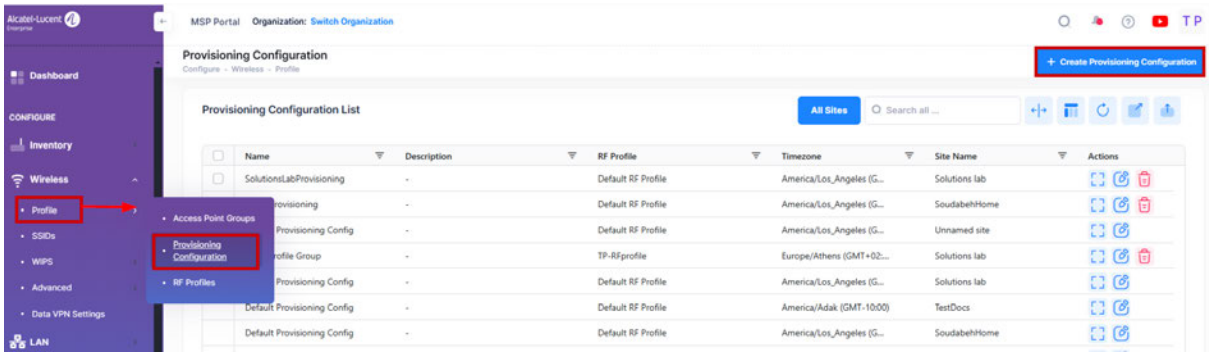
- **Access Point Group Name** - The unique name assigned to the AP Group.
- **Site** - The Organization Site to which the AP Group is assigned.
- **Description** - The optional description for the AP Group.
- **Provisioning Configuration** - The name of the Provisioning Configuration assigned to the AP Group.
- **Created At** - The date and time the AP Group was created.
- **Updated At** - The date and time the AP Group was last updated.
- **Extended SSID Scale** - The Extended SSID Scale status for the AP Group (Enable or Disable).
- **Associated AP Count** - The number of Access Points assigned to the AP Group.

5.1.2 Provisioning Configuration

A Provisioning Configuration contains the necessary settings an Access Point device requires to boot up and get a basic configuration. It is a site-level entity, meaning that two Provisioning Configurations for the same Site cannot have the same name. However, two different Sites can each have a Provisioning Configuration with the same name.

The Provisioning Configuration is applied to Access Points by assigning the configuration to an Access Point (AP) Group (see page 309). All Access Point members of the AP Group will utilize the associated Provisioning Configuration.

To manage Provisioning Configurations, navigate to the Provisioning Configuration List screen by clicking on **Wireless > Profile > Provisioning Configuration** under the "Configure" section of the OmniVista Terra Menu (see page 45). This screen displays information (see page 326) about existing Provisioning Configurations and is also used to create (see page 313), edit (see page 325), and delete (see page 325)a Provisioning Configuration.



5.1.2.1 Creating a Provisioning Configuration

A Provisioning Configuration must be specified at the time an AP Group is created. There is a pre-configured default configuration ("Default Provisioning Config") designated for each Site within an Organization. You can select the default configuration or create a new one.

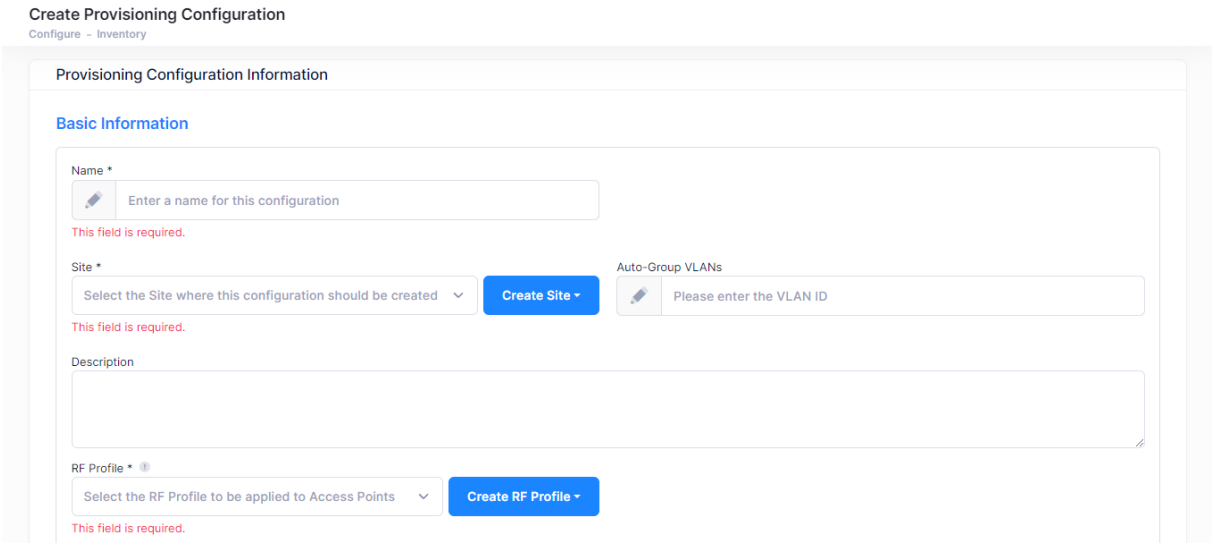
Click on **Create Provisioning Configuration** to open the Create Provisioning Configuration screen. Complete the fields for each of the following sections of the screen as described below.

- **Basic Information** (see page 314) - Configure identifying information for the Provisioning Configuration, such as name and description, as well as the Organization Site, associated Auto-Group VLANs, and an RF Profile.
- **Time** (see page 315)- Sets the timezone and defines an NTP server list.
- **802.1X Supplicant on AP Management Port** (see page 315) - Specifies if AP Group member devices will act as 802.1X clients.
- **SSH and AP Web** (see page 317) - Configure parameters for SSH login and web management.
- **Client Behavior Tracking** (see page 318) - Configures parameters to upload a Client Behavior Log File to an FTP Server and to upload Client Behavior Syslog messages to a remote Syslog Server.
- **Certificate** (see page 319)- Specify the certificates to establish secure communication with the AP.
- **Redirection Settings** (see page 319) - Proxy port number and/or FQDN/IP address used for redirection to UPAM or CPPM servers.

- **SNMP Setting** (see page 320) - Configure SNMP and Trap settings to allow third-party SNMP-based platforms to monitor APs in a Site using SNMP.
- **IoT Radio Configuration** (see page 321) - Configures the IoT Radio Mode for the AP.
- **IoT/Location/Advanced Analytics Server** (see page 322) - Set the external engine profile for the AP. If the location service is enabled, APs in the Site will report IoT/wireless scanning data/ advanced analytics data to the selected servers.
- **Data VPN Settings** (see page 323) - Select the VPN Server to use for the Data VPN Tunnel.
- **Event Configuration** (see page 323) - Select the event configurations to send to OmniVista Terra.
- **Miscellaneous** (see page 323)- Configure miscellaneous settings, such as a Captive Portal virtual IP address, Called Station ID, IPv6 L3 Forwarding, and IGMP Snooping.
- **Syslog** (see page 324)- Enable/disable logging of AP events to remote Syslog Servers.
- **Post Mortem Dump** (see page 324) - Enable/disable Post Mortem Dump (PMD) of AP information.

When you are finished completing the necessary sections, click on **Create**.

Click on **Create another** checkbox to return to the Create Provisioning Configuration screen to complete for another configuration. If this box is not checked, the display returns to the Provisioning Configuration List screen.

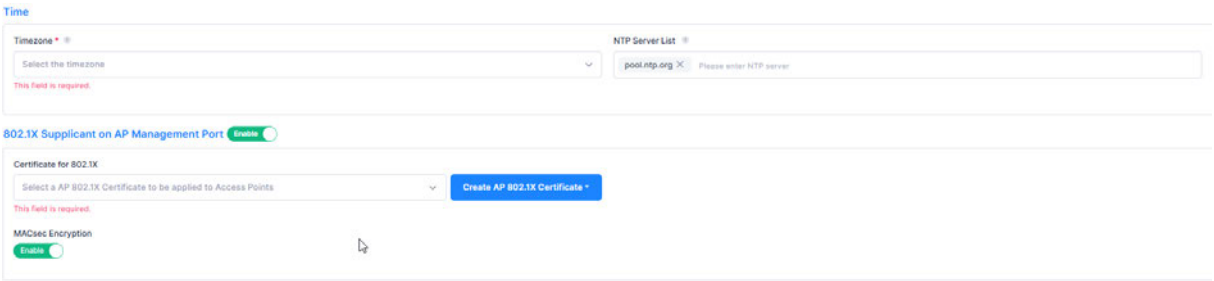


Basic Information

- **Name** (Required) - Enter a unique name for the Provisioning Configuration (up to 64 characters).
- **Site** (Required) - Select an existing Organization Site from the drop-down list or click on **Create Site** button to open the Create Site page and create a new Site (see the Create a Site (see page 73) online help) . The Provisioning Configuration is assigned to the specified Site.
- **Auto-Group VLANs** - A list of VLAN IDs to allow automatic grouping of APs during initial registration. Separate each VLAN ID entry with a comma (for example, 10, 20, 25-30). Based on the AP management VLAN ID received by LLDP, the AP can automatically be assigned to the corresponding AP Group. This option is used when an AP device is added to the Device

Catalog (see page 170) with the “Mgmt VLAN based automatic grouping” option selected for the Site AP Group.

- **Description** - Enter an optional description for the Provisioning Configuration.
- **RF Profile** (Required) - Select an existing RF Profile from the drop-down list or click on **Create RF Profile** button to open the Create RF Profile screen and create a new profile (see the RF Profiles (see page 331) online help) . The RF Profile contains the wireless attributes that are applied to all APs in the AP Group. When editing an existing Provision Configuration to change the specified RF profile, consider the following:
  - Changing the RF Profile is not allowed for a Provisioning Configuration that is associated with one or more APs when the current RF Profile country code is one of US/JP/ME but the new RF Profile country code does not match the current country code.
  - Changing the RF Profile is not allowed for a Provisioning Configuration that is associated with one or more APs when the country code for the new RF Profile is one of US/JP/ME but the current RF Profile country code does not match the new RF Profile country code.
  - An RF Profile assigned at the device level through the Device Catalog List (see page 170) takes precedence over the RF Profile assigned through the Provisioning Configuration.



- **Time**
  - **Timezone** (Required) - The timezone to be set on the APs.
  - **NTP Server List** - Enter the NTP Server for this Site. This sets the server list for all APs in the AP Group.
- **802.1X Supplicant on AP Management Port** - Enables/Disables APs in the AP Group to act as 802.1X clients (see AP Device as an 802.1X Client (see page 328) for more information). If enabled:
  - **Certificate for 802.1X** - Select the "Built-in Certificate" or a custom 802.1X client certificate from the drop-down list or click on **Create AP 802.1X Certificate** to open the Create AP 802.1X Certificate screen and create a new 802.1X certificate (see the Certificates (see page 394) online help).
- **MACsec Encryption -** Enable/Disable MACsec encryption. MACsec encrypts Ethernet frames on a LAN link. Two devices (called SecY entities) exchange keys via MKA (MACsec Key Agreement, IEEE 802.1X/802.1AE) and then establish Secure Associations (SAs) to encrypt/decrypt traffic. Passive and Assertive encryption refers to how a MACsec-capable port behaves during link negotiation when the other side may or may not support MACsec.
  - Passive (Default): The port prefers MACsec but will allow the link to come up in plaintext mode if the peer does not support MACsec or key negotiation fails.
  - Assertive: If the peer doesn’t support MACsec or fails to complete key negotiation, the link will not pass traffic.

In AWOS 5.0.3 GA the MACsec functionality is supported on the AP1321 and AP1361 only.

Only specific OmniSwitch models and ports support MACsec. Ensure your AP is connected to a port that supports MACsec. Refer to the AOS documentation for the OmniSwitch model you are using for more details.

To configure an AP to establish a MACsec connection with an OmniSwitch follow the steps below:

1. Authenticate the AP as an 802.1X supplicant to the OmniSwitch without MACsec.
2. Enable MACsec on the AP.
3. Enable MACsec with Dynamic RADIUS mode on the interface port of the OmniSwitch where the AP is connected.

MACsec with Dynamic RADIUS is not supported over Linkagg.

If a Stellar AP is acting as an 802.1x client to a switch port and MACsec is enabled on the switch port; the MACsec link does not work and the AP remains disconnected. Rebooting the AP after enabling MACsec fixes the issue.

For troubleshooting MACsec perform the following:

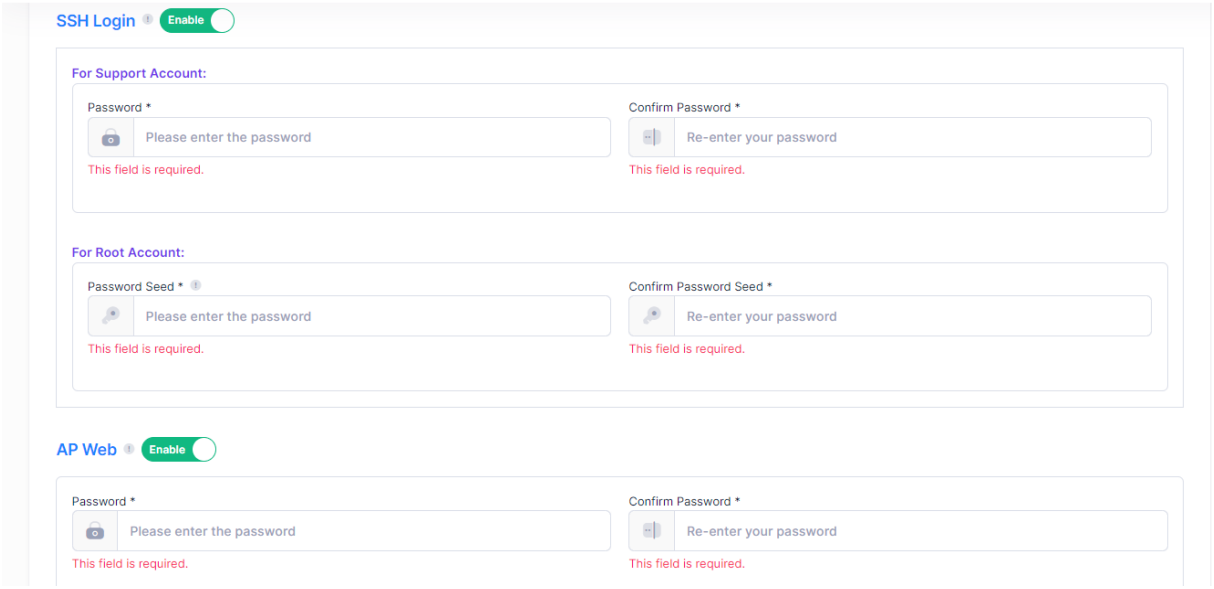
AP - If MACsec is not established successfully the AP may be out of the network.

1. Access the AP via the console port.
2. Check the /tmp/log/wpa.log for 802.1X Authentication and MACsec establishment process.

OmniSwitch:

1. Check the result of 802.1X authentication using the **show unp user details** command. A successful 802.1x authentication must be established for MACsec to work properly.
2. Checking the MACsec operational status using the **show interfaces macsec dynamic** command.
3. Restart the 802.1X authentication and MACsec using the **interface c/s/p admin-state disable** and **interface c/s/p admin-state enable** commands.

Note that out-of-the-box APs have a "Built-in Certificate" that is common to all APs. It is recommended that you use a custom 802.1X client certificate to improve network security. See AP Security Recommendations (see page 329) for more information.

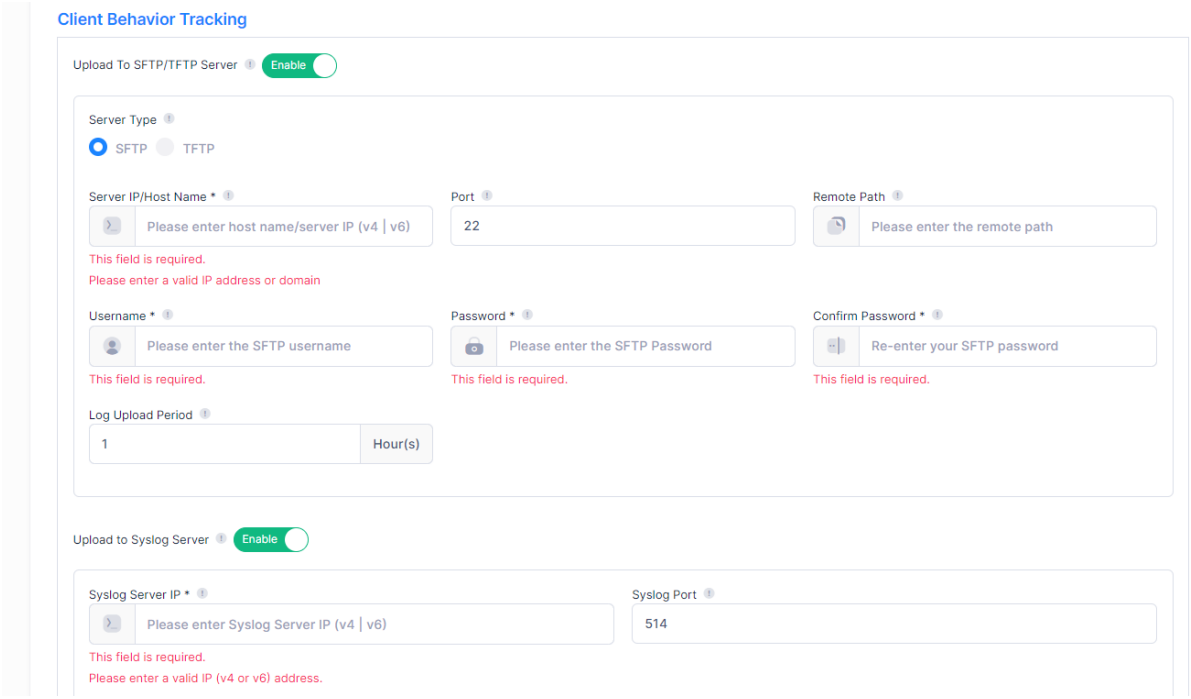


SSH

- **SSH Login** - Enables/Disables SSH login for APs in the AP Group. If enabled:
  - **For Support Account -** The SSH password used for an SSH connection to the AP.
    - **Password -** Enter a password that will be required to access an AP through SSH.
    - **Confirm Password -** Confirm the password.
  - **For Root Account -** Configuring a Root Account Password Seed adds a second layer of security for AP access. When you configure a Password Seed, the Root Password is derived from a character string composed of two parts: the Password Seed and the Fixed Root Password. The Password Seed can be changed on demand.
    - **Password Seed -** Enter a Root Account Password Seed for the APs in the AP Group.
    - **Confirm Password Seed -** Re-enter the Password Seed.

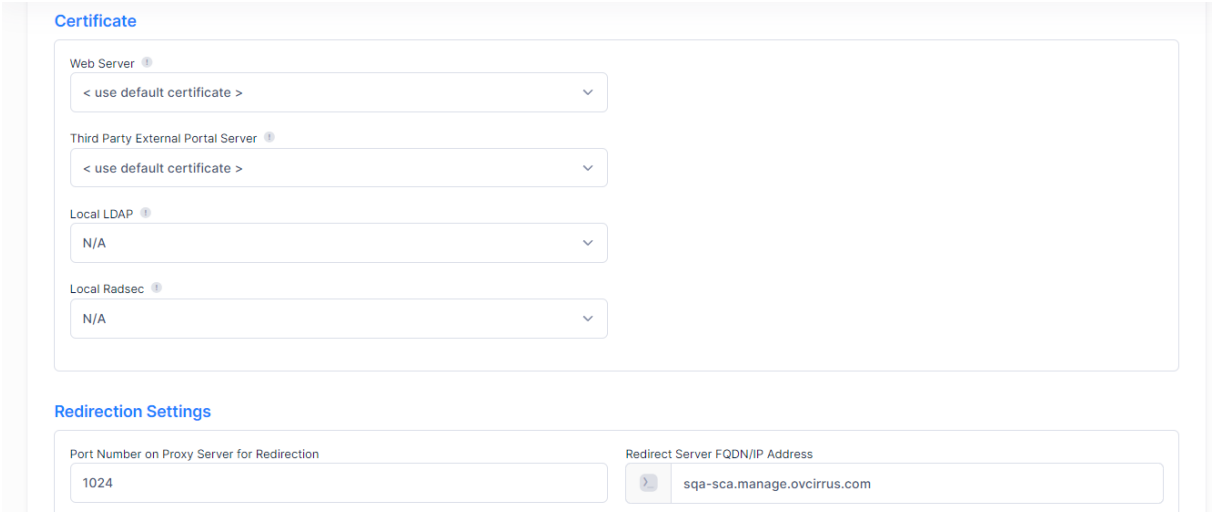
AP Web

- **AP Web** - Enables/Disables web management of APs in the AP Group. If enabled:
  - **Password** - Enter a password that will be required to access an AP through the Web Management UI.
  - **Confirm Password** - Re-enter the password.



Client Behavior Tracking

- **Upload To SFTP/TFTP Server -** Enables/Disables uploading of a Client Behavior Log File to an FTP Server. If enabled, enter:
  - **Server Type -** FTP Server type (SFTP/TFTP).
  - **Sever IP/Host Name -** IP address or Host name of the FTP Server.
  - **Port -** FTP port number.
  - **Remote Path -** File path on the FTP Server storing the Client Behavior Log.
  - **Username (SFTP Server only) -** User name used to access the SFTP Server.
  - **Password (SFTP Server only) -** Password used to access the SFTP Server.
  - **Confirm Password (SFTP Server only) -** Re-enter the password used to access the SFTP Server.
  - **Log Upload Period -** Frequency for uploading the Client Behavior Log to the FTP Server, in hours (Range = 1 - 24, Default = 1).
- **Upload to Syslog Server -** Enables/Disables uploading of Client Behavior Syslog messages to a remote Syslog Server. If enabled, enter the following information:
  - **Syslog Server IP -** IP address of the Syslog Server.
  - **Syslog Port -** Syslog Port number.

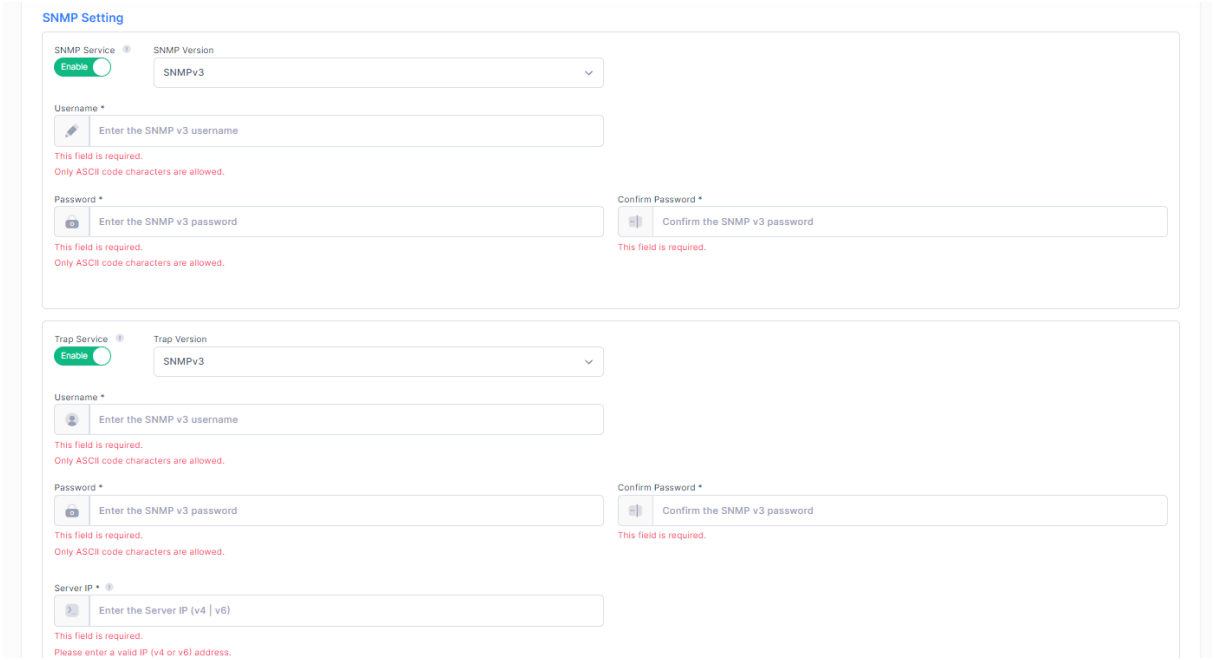


Certificate

- **Web Server -** The Certificate used for communication between the AP Web Server and browser. Make sure your Web Server certificate's Common Name (CN) is 'mywifi.al-enterprise.com' and that the certificate is in Unix format.
- **Third Party External Portal Server -** The Certificate used to communicate with a third-party portal server. Make sure your Web Server certificate's Common Name (CN) is NOT 'mywifi.al-enterprise.com' and that the certificate is in Unix format.
- **Local LDAP -** The certificate used for secure communication between the AP and an LDAP Server if the user authentication source is the local LDAP Server.
- **Local RadSec** - The Certificate used for secure communication between the AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS).

Redirection Settings

- **Port Number on Proxy Server for Redirection** - The HTTP proxy port number to use for redirection to UPAM or the CPPM Server.
- **Redirect Server FQDN/IP Address** - The FQDN/IP address used for redirection of HTTP traffic to UPAM or the CPPM Server. Specify the address that is associated with the dynamic URL returned from UPAM or the CPPM Server.



SNMP Setting

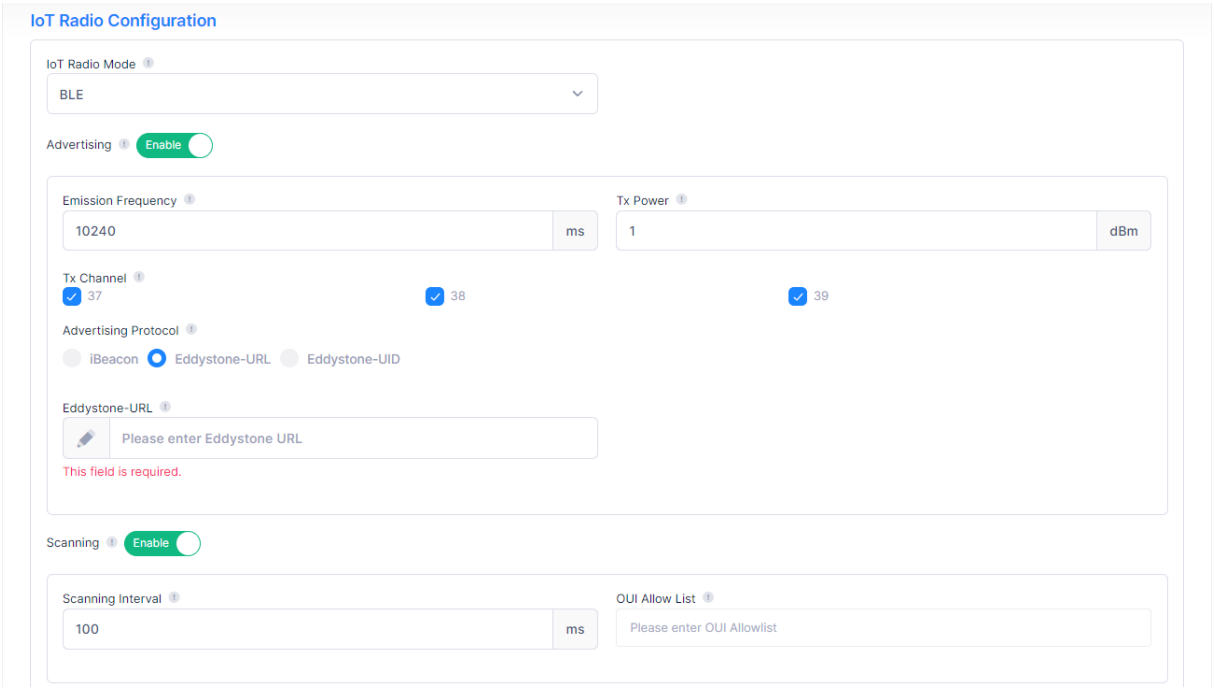
This option allows third-party SNMP-based platforms to monitor APs in a Site using SNMP. OmniVista Terra does not use SNMP to manage Stellar APs. With defined SNMP MIBs, an Administrator can monitor APs, configured services, and wireless clients and their traffic utilization.

When using SNMPv3, Stellar APs support only SHA authentication protocol and AES privacy protocol.

- **SNMP Service -** Enables/Disables (On/Off) the SNMP Service on APs in the AP Group.
  - **Version -** The SNMP version. Select v3 or v2c. (Default = v3)
    - **v3 -** When SNMP v3 is selected, complete the following:
      - **Username -** The user account name.
      - **Password -** The password for the user account.
      - **Confirm -** Confirm the specified password.
    - **v2c** - When SNMP v2c is selected, complete the following field:
      - **Read Community -** The credential used for communication between the network management system and APs.
- **Trap Service -** Enables/Disables (On/Off) SNMP Trap Service on APs in the AP Group.
  - **Version -** The SNMP version. Select v3 or v2c. (Default = v3)
    - **v3 -** When SNMP v3 is selected, complete the following fields:
      - **Username -** The user account name.
      - **Password -** The password for the user account.
      - **Confirm -** Confirm the specified password.

- **Server IP -** The server to which AP trap messages are sent. This is the IP address of the network management server you are using. It is not recommended that you use the OmniVista Terra Server IP address to avoid the posting of duplicate traps in OmniVista.

- **v2c** - When SNMP v2c is selected, complete the following fields:
  - **Community -** The credential used for communication between the network management system and APs.
  - **Server IP -** The server to which AP trap messages are sent. This is the IP address of the network management server you are using. It is not recommended that you use the OmniVista Server IP address to avoid the posting of duplicate traps in OmniVista.



IoT Radio Configuration

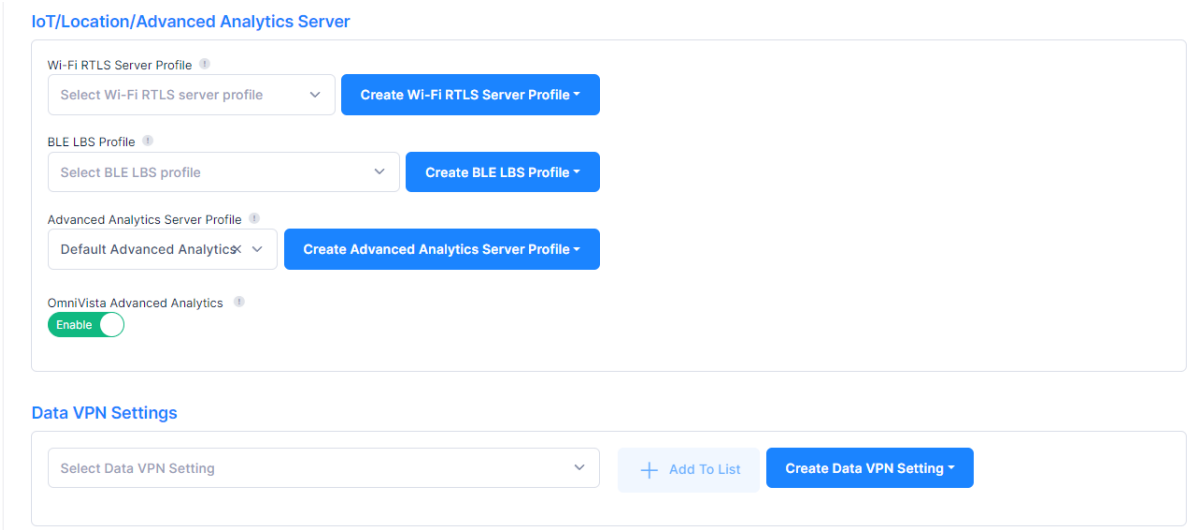
- **IoT Radio Mode -** Select **BLE** to configure the IoT Radio Mode. If an AP in the AP Group supports BLE Beaconing, the BLE configuration (below) will be applied to the AP(s).

BLE Configuration

This option is used to enable/disable BLE Beaconing for APs in the AP Group. BLE Beaconing is used by the Location Service to deliver location services like way-finding, geo-location, geo-notification, and geo-fencing.

- **Advertising -** Enables/Disables the BLE advertising function for the AP. If Advertising is enabled, the AP will broadcast BLE packets. If disabled, the AP will detect surrounding BLE Tags/ Beacons and will report information to the server for analysis. Note that BLE Advertising **must** be enabled for Stellar Asset Tracking.
  - **Emission Frequency** - The time circle during which the BLE packets will be broadcast, in milliseconds. (Range = 20 - 9,000,000, Default = 200)

- **Tx Power -** The transmit power used to broadcast BLE packets, in dBm. (Range = -20 - 19, Default = 4)
- **Tx Channel -** The transmit channel used to broadcast BLE packets. It is recommended that you use a different channel than the channel used for the WLAN.
- **Advertising Protocol -** Specify the BLE protocol used to define the broadcasting BLE beacon format.
  - **iBeacon -** Apple iBeacon format. Note that you **must** select iBeacon for Stellar Asset Tracking.
  - **Eddystone-URL -** Google Eddystone format. A compressed URL that, once parsed and decompressed, is directly usable by the client.
  - **Eddystone-UID -** Google Eddystone format. A unique static ID with a 10-byte Namespace component and a 6-byte Instance component.
    - **Namespace -** 20 characters containing 0-9a-f.
- **Scanning -** Enables/Disables the Bluetooth beacon scanning function for the AP. Note that BLE Scanning **must** be enabled for Stellar Asset Tracking.
  - **Scanning Interval -** The Bluetooth scanning interval for the AP, in milliseconds. (Range = 4 -10240, Default = 100)
  - **OUI Allow List -** Specify the MAC OUI allow list to filter devices for BLE beacon broadcasting. Only those beacons broadcasting from the devices within the OUI Allow List are valid and will be reported.



IoT/Location/Advanced Analytics Server

This option is used to set an IoT/Location/Advanced Analytics Server Profile for APs in the AP Group. If the location service is enabled, APs in the group will report IoT/wireless scanning data/advanced analytics data to the selected servers.

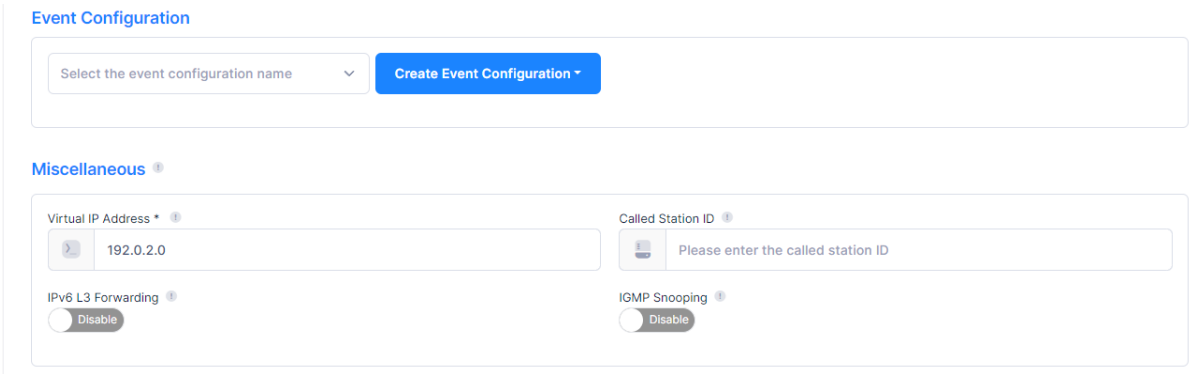
> The option to set an IoT/Location/Advanced Analytics Server Profile applies only to Access Points running AWOS 4.0.6 or higher.

- **Wi-Fi RTLS Server Profile -** Select a Wi-Fi RTLS Server Profile for APs. A default AeroScout Location profile with AeroScout engine type is provided or select a profile with the OmniVista Terra WiFi RTLS engine type. To create a new server profile, click **Create Wi-Fi RTLS Server Profile** to open the Create External Engine (see page 388) screen and add a new profile.
- **BLE LBS Profile** - Select a BLE Location Based Server Profile. The BLE Location profile is a Stellar Location Engine used for OmniAccess Stellar Asset Tracking. To create a new server profile, click **Create BLE LBS Profile** to open the Create External Engine (see page 388) screen and add a new profile.
- **Advanced Analytics Server Profile** - Select an advanced analytics profile with an OmniVista Terra Advanced Analytics engine type. A “Default Advanced Analytics” profile with OmniVista Terra Advanced Analytics engine type is provided to send advanced analytics data to OmniVista Terra 10 and above. To create a new server profile, click **Create Advanced Analytics Server Profile** to open the Create External Engine (see page 388) screen and add a new profile.
- **OmniVista Advanced Analytics** - Enables/disables the OmniVista Advanced Analytics functionality.

> OmniVista Advanced Analytics is enabled by default. Note that if you disable this functionality, the AP will not send QoE events to OmniVista Terra.

Data VPN Settings

- **Data VPN Server(s)** - Select the VPN Server to use for the Data VPN Tunnel. The user traffic will be carried in the data VPN tunnel between the APs and selected VPN Server. To create a new Data VPN Server, click **Create Data VPN Setting** to open the Create Data VPN Setting (see page 414) screen and add a new VPN Server.

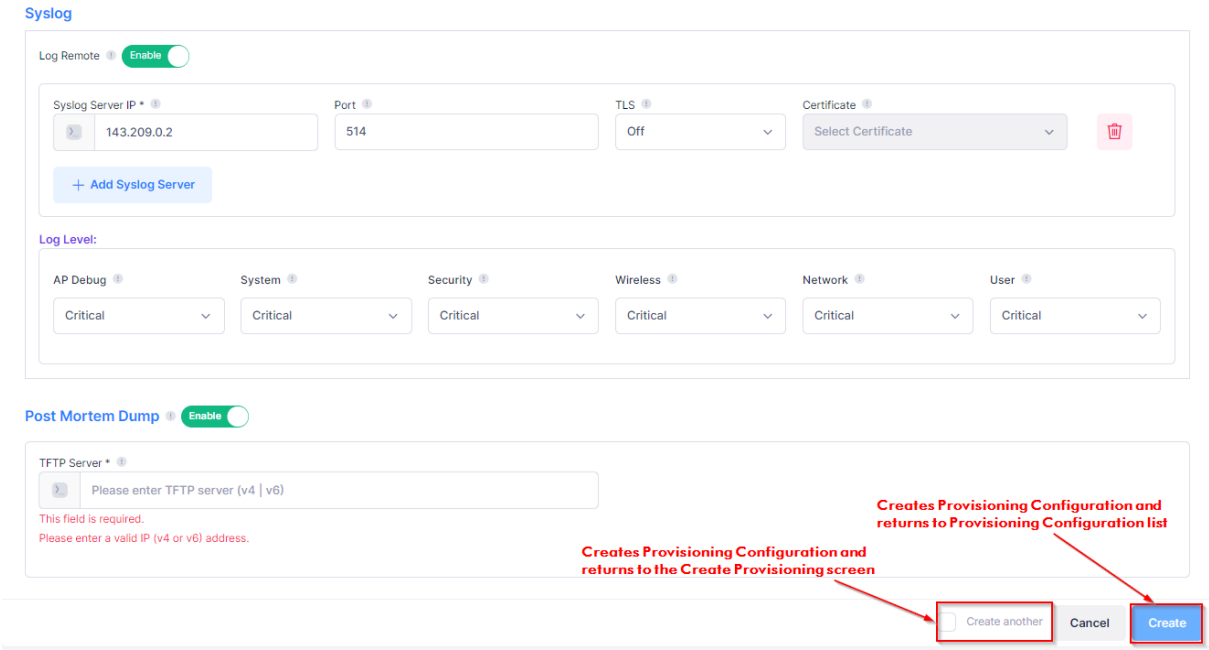


Event Configuration

- **Event Configuration Name** - Select the event configurations that you want devices to send to OmniVista Terra. To create a new event configuration, click **Create Event Configuration** to open the Create Event Configuration (see page 1004) screen and add a new event configuration.

Miscellaneous

- **Virtual IP Address -** The virtual IP address used for Captive Portal redirection in the AP. You can customize the virtual IP address according to your network deployment to avoid exposing the AP management interface. Be careful not to specify an IP address that is already in use in your network.
- **Called Station ID** - RADIUS attribute. Define what to pass in Called-Station-ID RADIUS attribute that is exchanged between the NAS client (Access Point) and RADIUS Server. By default, the format of Called Station ID" is: <AP-MAC-ADDRESS>:<SSID>. Example "00-10-A4-23-19-C0:guest". But in some special scenarios, administrators may need to change this default depending on how their RADIUS servers function. Note that, when UPAM is used as the RADIUS server and an Access Policy is configured with "SSID" attribute as the Mapping Condition, UPAM assumes the standard format of <AP-MAC-ADDRESS>:<SSID> to extract "SSID" value from this "Called-Station-ID" attribute . So, whenever this attribute is specified with a different value, UPAM Access Policy might need to be modified accordingly.
- **IPv6 L3 Forwarding -** Enables/Disables the IPv6 service on APs. Once enabled, IPv6 packets received by APs will be handled at the application level and forwarded on Layer 3. By default, the IPv6 service is disabled.
- **IGMP Snooping** - Enables/Disables the IGMP Snooping function on the APs.



Syslog

Use this option to enable logging of AP events to remote Syslog Servers. Specify the Syslog Server IP address and Syslog port to which an AP device will send events. Syslog Server (IP 143.209.0.2, port 514) is provided by default. To add an additional server, click on the **Add Syslog Server** button. Note that you can specify up to four Syslog Servers.

- **Log Remote -** Enable/Disable remote logging of AP events. When enabled, complete the following fields for each Syslog Server that will receive the AP events.
  - **Syslog Server IP** - The IP address of the remote Syslog Server.
  - **Port** - The port used to connect to the remote Syslog Server.

- **TLS** - Enable/Disable (On/Off) the use of the Transport Layer Security encryption method for remote logging of AP events.
  - **Certificate** - If TLS is enabled (On), select a Syslog Over TLS Certificate (see page 682).
- **Log Level -** Select a log level for events. This sets the log level for all APs in the AP Group. Note that the AP Debug, System, Security, Wireless, Network, and User log levels must be equal to or higher than the AP Debug log level.

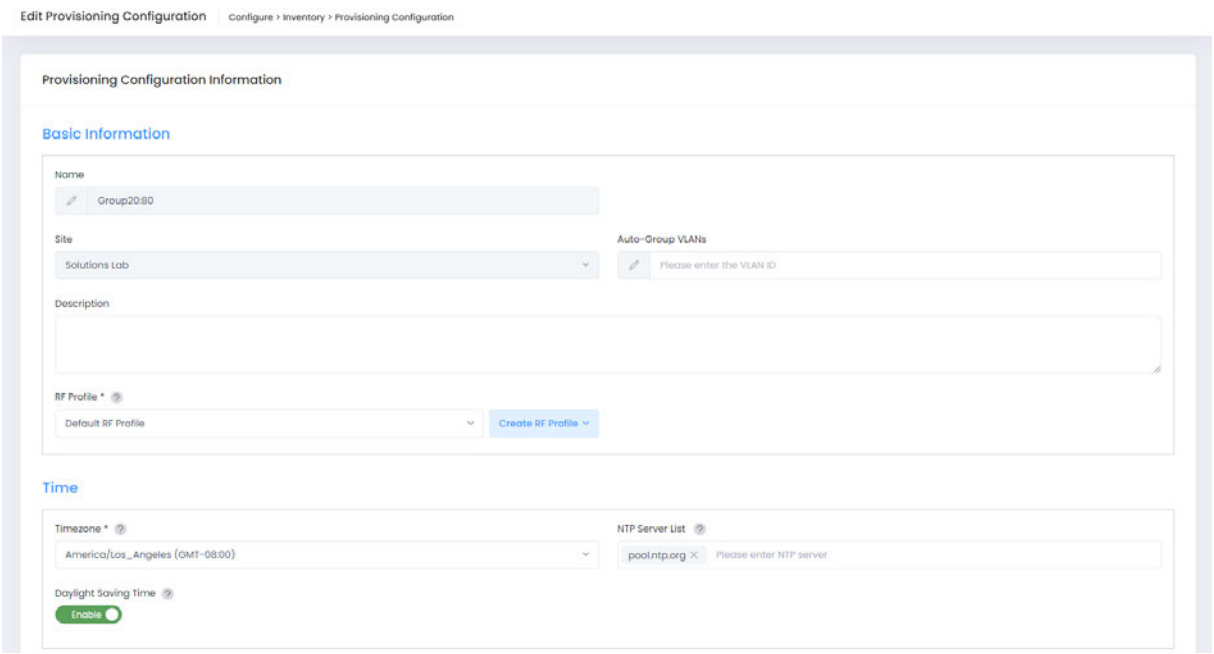
Post Mortem Dump

- **PMD -** Enables/Disables Post Mortem Dump (PMD) of information for APs in the AP Group.
- **TFTP Server -** The IP address of the TFTP Server used for PMD.

5.1.2.2 Editing a Provisioning Configuration

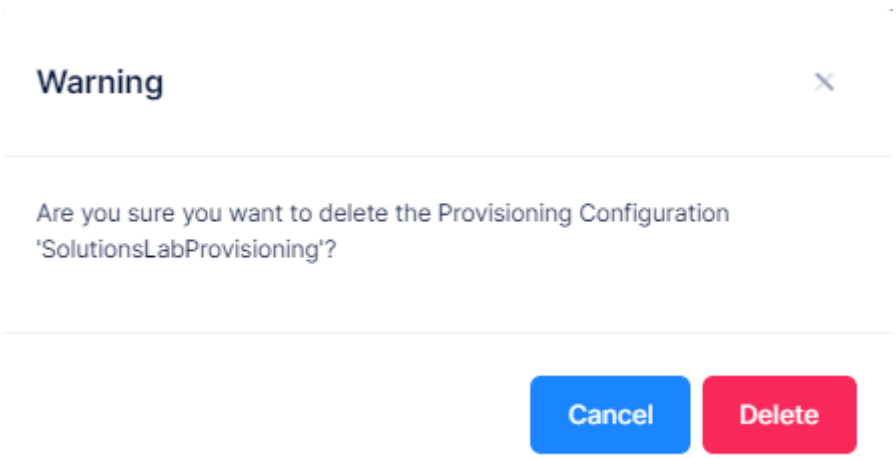
Select a Provisioning Configuration in the Provisioning Configuration List and click on the Edit icon under the “Actions” column or select Edit from the **Actions** drop-down menu to bring up the Edit Provisioning Configuration screen. Edit the fields as described above (see page 313)and click on **Save**.

> You can edit the “Default Provisioning Config”, except for the “Name”, “Site”, “Auto-Group VLANs”, and “Description” fields.



5.1.2.3 Deleting a Provisioning Configuration

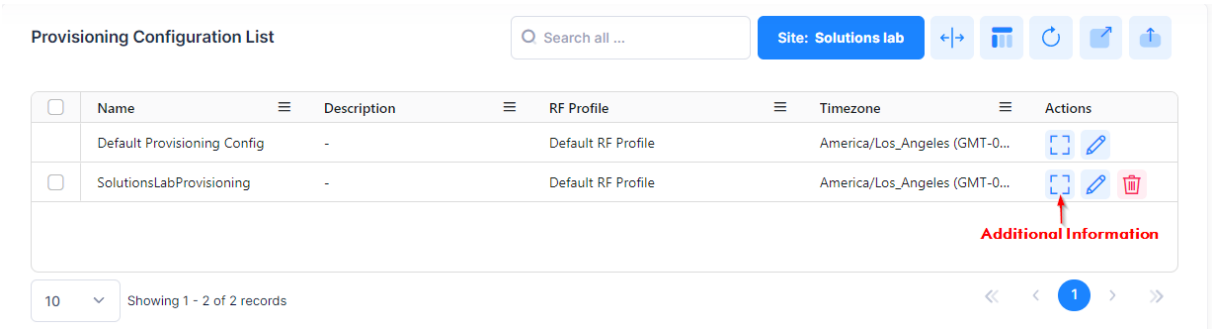
Select a Provisioning Configuration in the Provisioning Configuration List and click on the Delete icon under the “Actions” column or select Delete from the **Actions** drop-down menu. The following confirmation prompt appears:

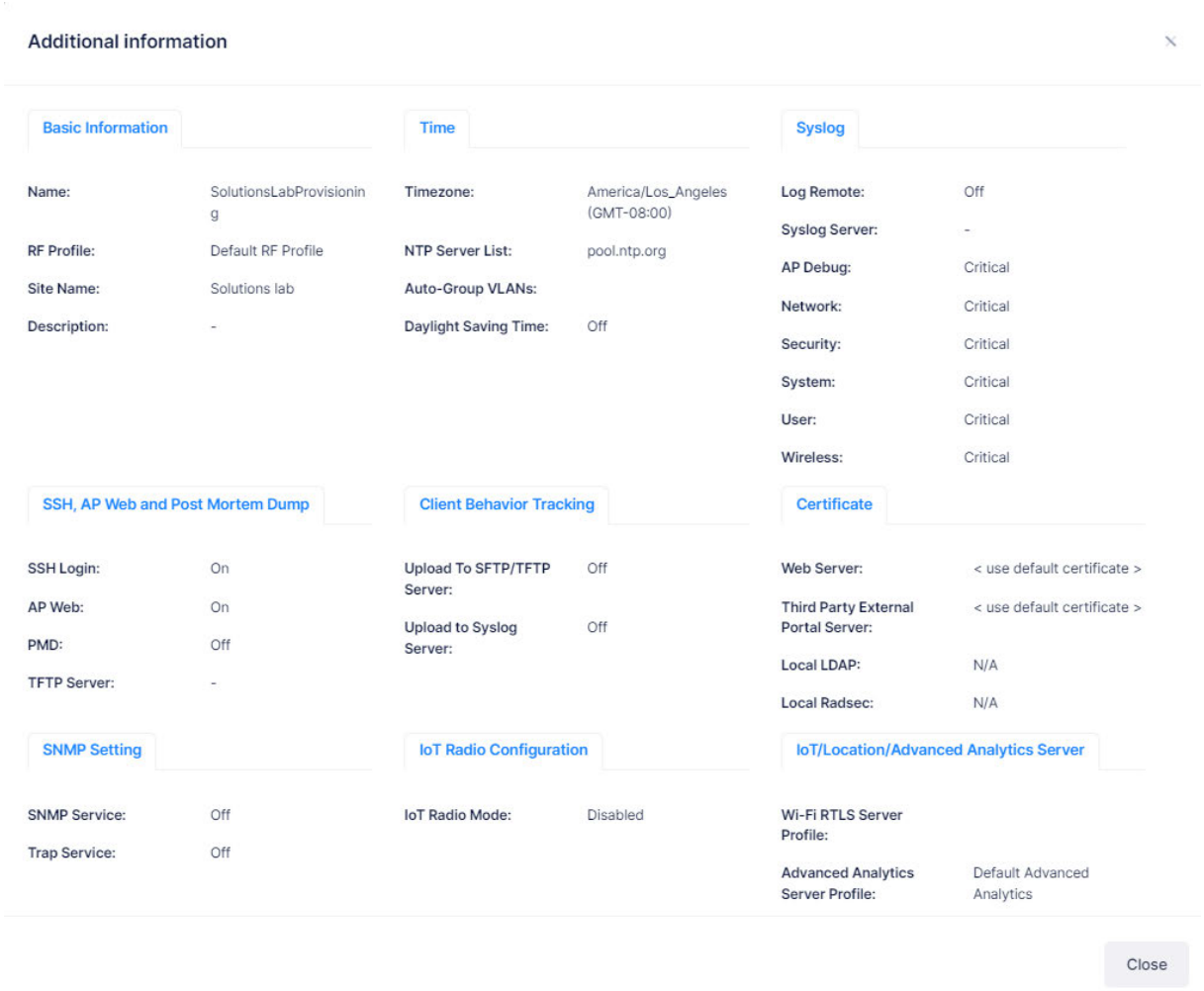


You cannot delete the ”Default Provisioning Config” or a Provisioning Configuration that is associated with an Access Point Group.

5.1.2.4 Display Additional Information

Click the icon in the “Actions” column next to the Provisioning Configuration List entry to display the Additional Information screen.




Additional information
Basic Information
Name: SolutionsLabProvisioning
RF Profile: Default RF Profile
Site Name: Solutions lab
Description: -
Time
Timezone: America/Los_Angeles (GMT-08:00)
NTP Server List: pool.ntp.org
Auto-Group VLANs:
Daylight Saving Time: Off
Syslog
Log Remote: Off
Syslog Server: -
AP Debug: Critical
Network: Critical
Security: Critical
System: Critical
User: Critical
Wireless: Critical
SSH, AP Web and Post Mortem Dump
SSH Login: On
AP Web: On
PMD: Off
TFTP Server: -
Client Behavior Tracking
Upload To SFTP/TFTP Server: Off
Upload to Syslog Server: Off
Certificate
Web Server: < use default certificate >
Third Party External Portal Server: < use default certificate >
Local LDAP: N/A
Local Radsec: N/A
SNMP Setting
SNMP Service: Off
Trap Service: Off
IoT Radio Configuration
IoT Radio Mode: Disabled
IoT/Location/Advanced Analytics Server
Wi-Fi RTLS Server Profile:
Advanced Analytics Server Profile: Default Advanced Analytics
Close

21 Oct 2025

5.1.2.5 AP Device as an 802.1X Client

When an 802.1X (supplicant) device is connected to a Unified Network Port (UNP) port on which 802.1X authentication is enabled, the switch will attempt to authenticate the device using 802.1X EAP frames. If after a configurable amount of time the device does not respond to the EAP frames sent by the switch, the device is identified as a non-802.1X (non-supplicant) device and undergoes MAC address authentication.

When a Stellar AP is connected to an OmniSwitch UNP port on which the AP Mode and 802.1X authentication is enabled, the switch starts to send EAP frames to the AP device. If the AP device does not respond to the EAP frames, the switch will identify the AP as a non-supplicant and will attempt to authenticate the AP with other methods. To ensure that the switch will identify the AP device as a supplicant (802.1X client), enable 802.1X functionality for the Provisioning Configuration (see page 313) associated with the AP Group to which the AP belongs and specify an 802.1X client certificate to install on the APs in the group. A built-in 802.1X client certificate is provided by default or you can generate and upload a custom client certificate.

Notes:

- OAW-AP1101 does not support the AP 802.1X client feature due to low flash size. All other APs, including other low-end APs (OAW-AP1201H, OAW-AP1201L, OAW-AP1201HL), support this feature.
- When an AP is operating as an 802.1X client, the AP does not support untagged WLAN/SSID/client and cannot participate in a Mesh deployment.

5.1.2.5.1 802.1X Authentication Use Cases

The following use case examples document the steps for configuring 802.1X authentication for the AP.

5.1.2.5.1.1 OmniVista UPAM 802.1X Server with Built-In Certificate on the AP

1. Enable 802.1X Supplicant functionality for the AP Group.
2. Select the Built-In Certificate from the drop-down menu.

5.1.2.5.1.2 OmniVista UPAM 802.1X Server with a Custom Client Certificate on the AP

1. Generate the client certificate (Cert, Private Key, CA cert) externally.
2. Import the client certificate into the UPAM database in OmniVista.
   a. Import the client certificate from the Wireless - Certificate (see page 682) screen and assign the certificate a name.
3. Push the custom client certificate to the APs.
   a. Enable 802.1X Supplicant functionality for the AP Group.
   b. Select the custom certificate name that was imported in Step 2(a).

5.1.2.5.1.3 Use an External Radius 802.1x Server with Built-In Certificate on the AP

1. This is the CA used to validate the AP as an 802.1x client. Import this CA into the external Radius server.
2. Push the built-in certificate to the APs.
    a. Enable 802.1X Supplicant functionality for the AP Group.
    b. Select the Built-in Certificate.

5.1.2.5.1.4 Use an External RADIUS 802.1X Server with a Custom Client Certificate on the AP

1. Generate the client certificate (Cert, Private Key, CA cert) externally.
2. Import the client CA certificate into the external RADIUS server database so the RADIUS server will trust the AP.
3. Push the custom client certificate to the APs.
    a. Import the client certificate from Wireless - Certificate (see page 682) screen and assign the certificate a name.
    b. Enable 802.1X Supplicant functionality for the Provisioning Configuration associated with the AP Group.
    c. Select the custom certificate name that was imported in Step 3(a).

5.1.2.5.1.5 802.1X Authentication with Username (AP MAC Address)

An 802.1X (supplicant) AP device can undergo certificate-based (see use cases above) or username-based 802.1X authentication. For username-based authentication, the user/pass = AP MAC address is configured in the UPAM database. When the AP MAC address attempting to authenticate matches the configured user/pass MAC address, UPAM returns a UNP profile/VLAN ID to the switch. This is often done when the user wants to assign a different VLAN based on the authentication result.

Note that when configuring username-based 802.1X authentication, the 802.1X Supplicant option for the Provisioning Configuration associated with the AP Group should be set to "Disabled" and Secure Mode is enabled on the switch port. This will ensure that the switch will learn the AP MAC address and perform the 802.1X authentication according to the configuration (Access Auth Profile) on the switch.

5.1.2.5.2 AP Security Recommendations

- Do not rely on the Default Client Certificate on APs and the Default Server Certificate on UPAM. It is recommended that you install Custom Client Certificates on APs/AP Groups and a Custom Server Certificate on UPAM for improved security.
- It is recommended that you set up an 802.1X Failure Policy on the switch port depending on whether you want the AP (and its clients) to have connectivity to the network even if the AP fails 802.1X authentication; or if you want the AP (and its clients) to be completely blocked from network access if the AP fails 802.1X authentication.

To learn about 802.1X authentication failures where AP is the client, check your RADIUS Server's Authentication Records.

21 Oct 2025

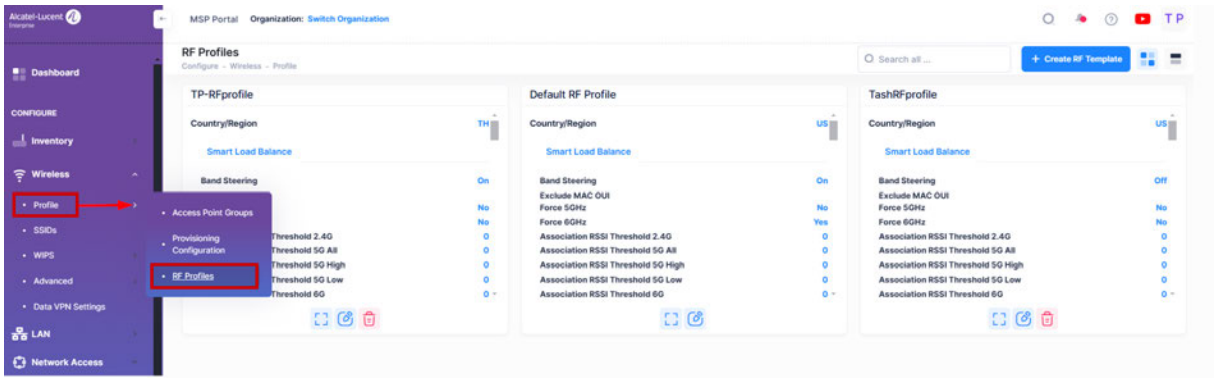
5.1.3 RF Profiles

The Radio Frequency (RF) Profiles application is used to define a wireless RF configuration for Stellar Access Points. An Access Point retrieves the RF Profile to use from the AP Group (see page 309) to which the AP belongs. Each AP Group is associated with a Provisioning Configuration (see page 313). Access Points that are members of the AP Group utilize the Provisioning Configuration to boot up and get a basic configuration. The associated Provisioning Configuration is where the name of the RF Profile to use is defined.

RF Profiles enable the user to ensure that transmit power and operating frequencies meet the requirements of global regulatory agencies and individual countries. A user can also use the profiles to adjust the wireless parameters and functions according to real network environment to improve the user experience of wireless network.

> An RF Profile is an Organization-level entity. An RF Profile is created in an Organization with a name that is unique across the entire Organization. You can not create two RF Profiles with the same name in the same Organization.

To manage the RF Profile configuration, navigate to the RF Profiles screen by clicking on **Wireless >Profile > RF Profiles** under the “Configure” section of the OmniVista Terra Menu (see page 45). The RF Profiles screen displays.

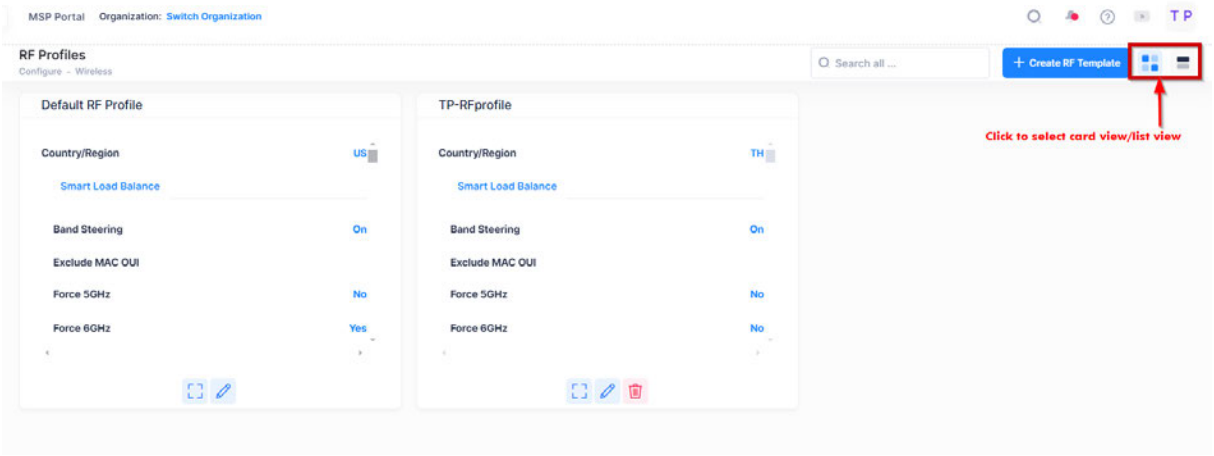


The RF Profiles screen displays information (see page 334) about all of the configured RF Profiles and is used to complete the following tasks:

- Customize the RF Profiles Display (see page 332) - Change how the profile information is displayed (card view, where each profile has its own widget; or list view, where the profiles are presented in a list format).
- Create an RF Profile (see page 339) - Create a new RF Profile that defines an RF configuration for Access Points.
- Edit an RF Profile (see page 333) - Modify the RF configuration for an existing profile.
- Delete an RF Profile (see page 333) - Delete an RF Profile configuration.

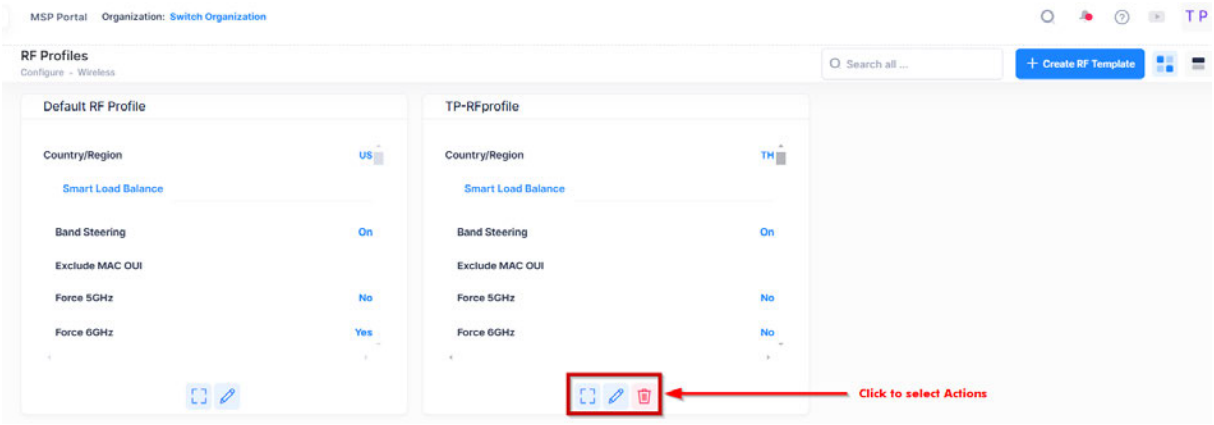
5.1.3.1 Customize the RF Profiles Display

You can specify that each RF Profile is displayed as its own widget (see page 332)(card view) or display each profile in a list format. To select which format you want to use, click on the **Change View** icon in the upper-right corner and select **Card View** or **List View** from the drop-down menu.



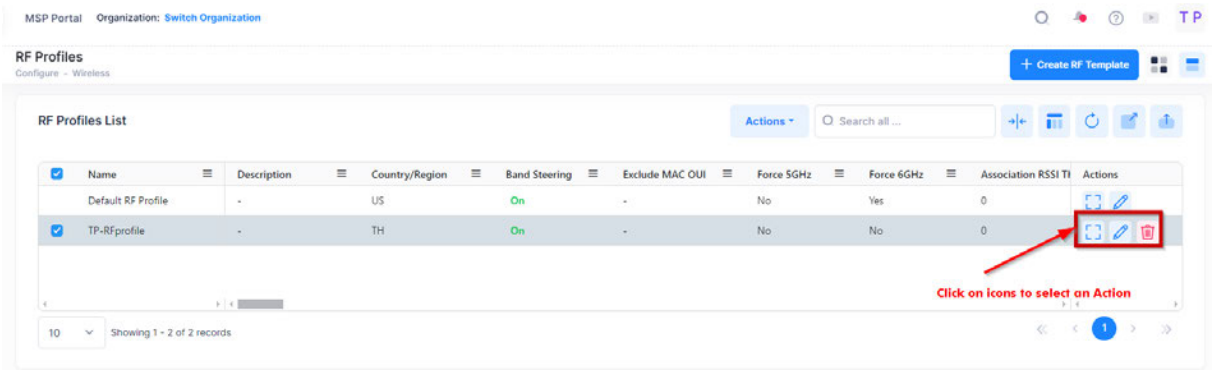
5.1.3.1.1 Display RF Profiles as Widgets

When you select the **Card View** display option, each profile will be presented in a Widget format, as shown above. Within each Widget you can scroll up or down to view all the configuration attributes. In the top-right corner of each Widget, there is an Actions icon that you can click on to display a drop-down menu with options to display details (see page 331), edit (see page 331), or delete (see page 331) the RF Profile.



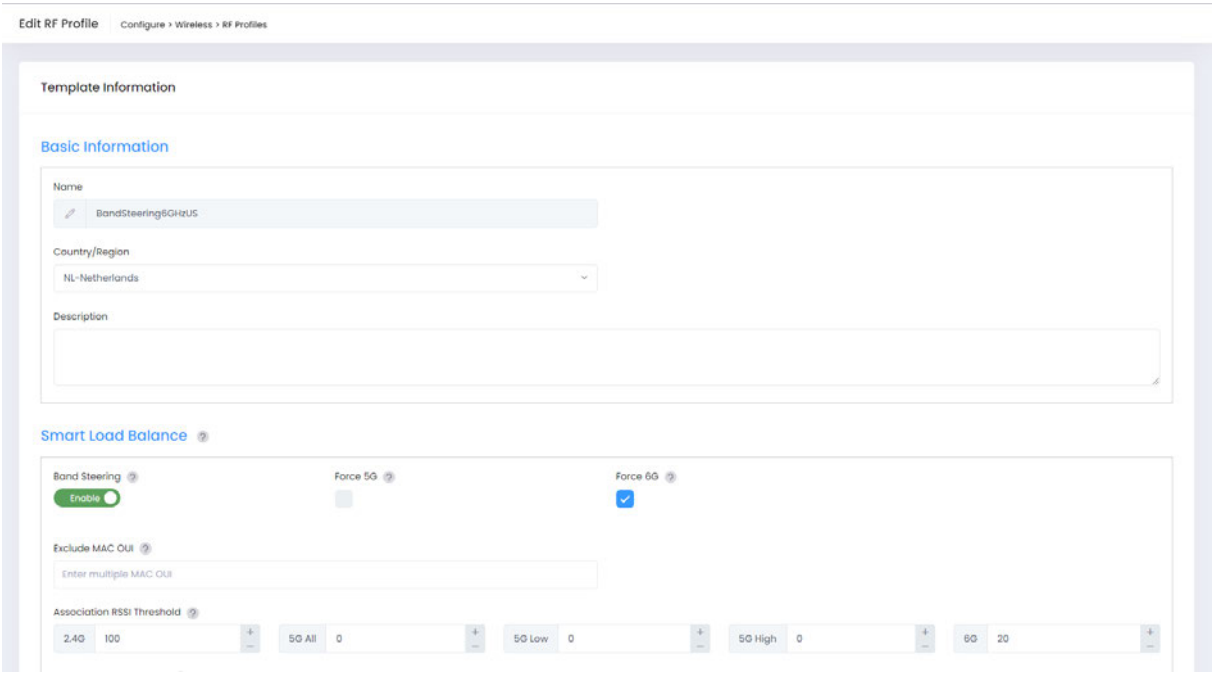
5.1.3.1.2 Display RF Profile in a List Format

When you select the List View display option, each profile is presented in a list format, as shown below. There is an Actions column that provides icons that you can click on to display details (see page 334), edit (see page 333), or delete (see page 333)the RF Profile.



5.1.3.2 Editing an RF Profile Configuration

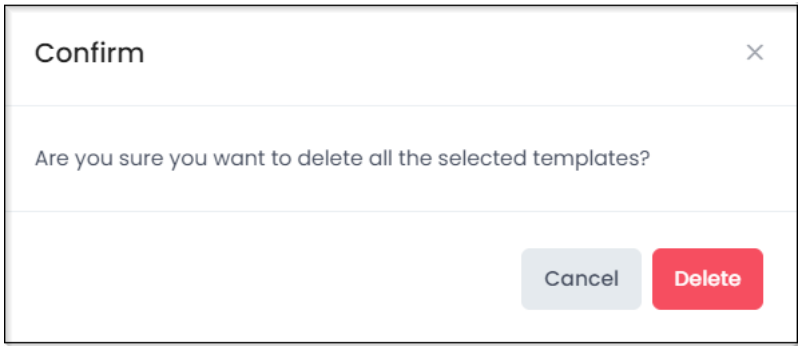
Select an RF Profile to edit by clicking on the Edit option on the Actions drop-down menu (card view (see page 332)) or the Edit icon under the Actions column (list view (see page 332)). You can also select the “Default RF Profile” to edit, if desired. The Edit RF Profile screen appears.



Edit the RF Profile configuration as described here (see page 339)and click the **Save** button. Note that you cannot edit the RF Profile name. The updated profile configuration is applied to all APs linked to the RF Profile through an AP Group (see page 309) or the Device Catalog (see page 170).

5.1.3.3 Deleting an RF Profile Configuration

Select an RF Profile to delete by clicking on the Delete option on the Actions drop-down menu (card view (see page 331)) or the Delete icon under the Actions column (list view (see page 331)). When the Confirmation Prompt appears, click on **Delete** to delete the profile.



You cannot delete the “Default RF Profile” or an RF Profile that is associated with a Provisioning Configuration or an Access Point Group.

5.1.3.4 RF Profile Information

Basic Information

- **Name -** The RF Profile name.
- **Description -** Optional RF Profile description.
- **Country/Region -** The Country Code for the profile. A Country Code is a short alphabetic or numeric geographical code that represent a country or dependent area and is used data processing and communications. The wireless transmitting power and operating frequencies (channels) vary by country/region. Select the country code where the APs are located.

Smart Load Balance

- **Band Steering** - The administrative status of Band Steering for the profile (On/Off).
- **Exclude MAC OUI** - The MAC address OUI that is excluded for band-steering.
- **Force 5Ghz** - The administrative status of the "Force 5GHz" feature (On/Off).
- **Force 6Ghz** - The administrative status of the "Force 6GHz" feature (On/Off).
- **Association RSSI Threshold 2.4G -** The RSSI setting for 2.4G radio.
- **Association RSSI Threshold 5G All -** The Association RSSI setting for 5G radio.
- **Association RSSI Threshold 5G High -** The Association RSSI setting for 5.2G band radio.
- **Association RSSI Threshold5G Low -** The Association RSSI setting for 5.8G band radio.
- **Association RSSI Threshold 6G** - The Association RSSI setting for 6G radio.
- **Roaming RSSI Threshold 2.4G -** The Roaming RSSI setting for 5G radio.
- **Roaming RSSI Threshold 5G All -** The Roaming RSSI setting for 5G radio.
- **Roaming RSSI Threshold 5G Low -** The Roaming RSSI setting for 5.8G band radio.
- **Roaming RSSI Threshold 5G High -** The Roaming RSSI setting for 5.2G band radio.
- **Roaming RSSI Threshold 6G -** The Roaming RSSI setting for 6G radio.

- **Dynamic Load Balance -** The administrative status of Dynamic Load Balancing for the profile (On/Off). If enabled, this feature performs client load balancing among APs in a group or groups in the same wireless network.
- **Airtime Fairness 2G -** The administrative status of the Airtime Fairness feature for 2G band radio (On/Off).
- **Airtime Fairness 5G** - The administrative status of the Airtime Fairness feature for 5G band radio (On/Off).

Per Band Info

- **Default Settings -** Indicates whether or not Band Settings are customized, the Default setting = "Off". If the Default Band Settings are being used, Default setting = "On".
- **2.4G -** Indicates whether or not the 2.4G Band Settings are configured for the profile (On/Off).
  - **Channel Setting -** The 2.4G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel Width -** The 2.4G Channel Width setting for the profile.
  - **Power Setting -** The 2.4G Power setting for the profile.
  - **Minimum Tx Power 2.4G -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 2.4G -** The maximum transmit power for auto power setting, if configured.
  - **External Antennas Gain -** The gain value of 2.4G band for the external antennas used by the APs mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 2.4G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 2.4G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 2.4G radio.
  - **Beacon Interval -** The 2.4G radio Beacon Interval.
- **5G All -** Indicates whether or not the 5G Band Settings are configured for the profile (On/Off).
  - **Channel Setting -** The 5G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 5G Channel Width setting for the profile.
  - **Power Setting -** The 5G Power setting for the profile.

  - **Minimum Tx Power 5G All -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 5G All -** The maximum transmit power for auto power setting, if configured.
  - **External Antennas Gain -** The gain value of 5G band for the external antennas used by the APs mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 5G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 5G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 5G radio.
  - **Beacon Interval -** The 5G radio Beacon Interval.
- **5G High -** Indicates whether or not the 5.8G Band Settings are configured for the profile (On/Off).
  - **Channel Setting -** The 5.8G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 5.8G Channel Width setting for the profile.
  - **Power Setting -** The 5.8G Power setting for the profile.
  - **Minimum Tx Power 5G High -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 5G High -** The maximum transmit power for auto power setting, if configured.
  - **External Antennas Gain -** Configure the gain value of 5.8G band for the external antennas used by AP1232(s) mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 5.8G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 5.8G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 5.8G radio.
  - **Beacon Interval -** The 5.8G radio Beacon Interval.
- **5G Low -** Indicates whether or not the 5.8G Band Settings are configured for the profile (On/Off).
  - **Channel Setting -** The 5.2G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.

  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 5.2G Channel Width setting for the profile.
  - **Power Setting -** The 5.2G Power setting for the profile.
  - **Minimum Tx Power 5G Low -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 5G Low -** The maximum transmit power for auto power setting, if configured.
  - **External Antennas Gain -** Configure the gain value of 5G band for the external antennas used by the APs mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 5.2G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 5.2G radio.
  - **High Efficiency -** The administrative status of the "High Efficiency" feature for 5.2G radio.
  - **Beacon Interval -** The 5.2G radio Beacon Interval.
- **6G -** Indicates whether or not the 6G Band Settings are configured for the profile (On/Off).
  - **Channel Setting -** The 6G Channel setting for the profile.
  - **Client Aware -** Client Aware Feature administrative status (On/Off)
  - **Channel DRM -** The Channel DRM administrative status (On/Off).
  - **CSA -** Channel Switch Announcement administrative status (On/Off).
  - **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel.
  - **Channel List -** If enabled, the available channel(s) that can be selected by DRM.
  - **Channel Width -** The 6G Channel Width setting for the profile.
  - **Power Setting -** The 6G Power setting for the profile.
  - **Minimum Tx Power 6G Low -** The minimum transmit power for auto power setting, if configured.
  - **Maximum Tx Power 6G Low -** The maximum transmit power for auto power setting, if configured.
  - **External Antennas Gain -** Configure the gain value of 6G band for the external antennas used by the APs mapping to this RF profile.
  - **Short Guard Interval -** The administrative status of the Short Guard Interval feature for 6G radio.
  - **MU-MIMO -** The administrative status of the MU-MIMO feature for 6G radio.
  - **Beacon Interval -** The 6G radio Beacon Interval.

Background Scanning

- **Background Scanning -** The administrative status of Background Scanning for the profile (On/Off). Background Scanning is used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks.

- **Scanning Channel -** Specify the channel(s) on which the wireless background scanning is executed. For a highly-sensitive packet delay use case, it is recommended that you enable background scanning only for the Working Channel.
- **Scanning Duration -** The Background Scanning duration in milliseconds. During the specified duration, APs examine the radio frequency through all channels on both the 2.4G band and 5G band.
- **Scanning Interval -** The Background Scanning interval, in seconds.
- **Voice and Video Awareness -** The administrative status of Voice and Video Awareness (On/Off). Background scanning must be aware of existing traffic on APs. If there is an ongoing voice/video service, scanning should not be performed to ensure uninterrupted traffic; and scanning should resume there is no active voice/video session.

Assigned Devices

- **Sites** - The Organization Sites to which the RF Profile is applied to selected groups within those Sites.
- **Assigned Groups and Devices** - The groups within the selected Sites to which the RF Profile is applied to the devices that belong to the group.

21 Oct 2025

5.1.3.5 Creating an RF Profile Configuration

There is a pre-configured RF Profile (“Default RF Profile”) designated for the Organization. You can select the default profile or create a new RF Profile. The Create RF Profile screen is used to define a wireless RF configuration for Stellar Access Points. To access this screen, click on **Create RF Template** button in the upper-right corner of the RF Profiles (see page 331) screen.

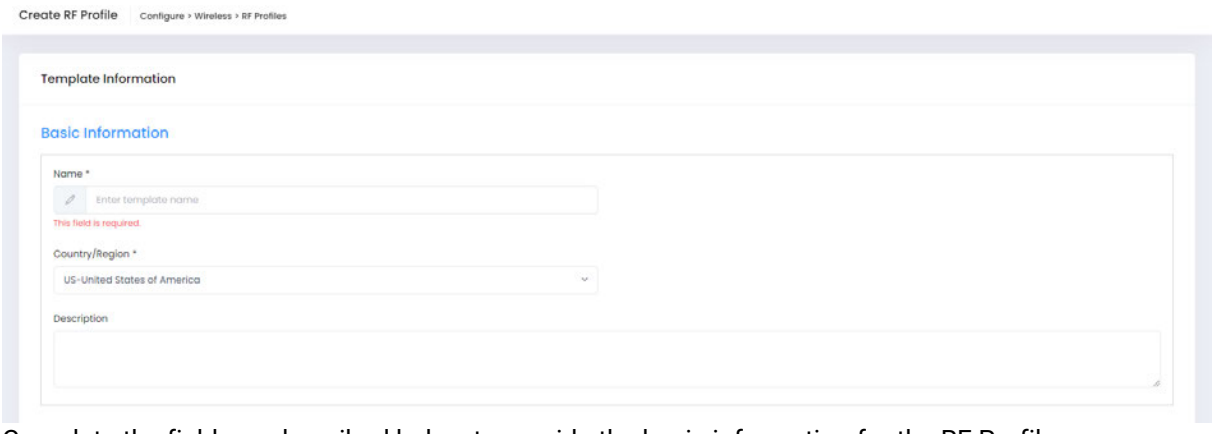
The Create RF Profile screen defines the following attributes for an RF Profile configuration:

- Basic Information (see page 339) - Configures identifying information for the RF Profile (for example, a profile name, county/region code, and optional description).
- Smart Load Balance (SLB) (see page 340) - Configures the SLB feature to improve the user experience when accessing wireless connectivity by guiding a user's client device to connect to a free wireless channel or AP and denying access to APs with a weak signal.
- Background Scanning (see page 342) - Used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks.
- Radio Settings (see page 342) - Configures the radio band options for specific AP models.
- Per Band Info (see page 343) - Configures the wireless setting for each radio band on an AP, such as working channel, transmit power, and short guard interval of the radio.

After configuring the sections of the Create RF Profile screen as described below, click on **Save**.

> Click on **Create another** checkbox to return to the Create RF Profile screen to complete for another configuration. If this box is not checked, the display returns to the RF Profile List screen.

5.1.3.5.1 Basic Information

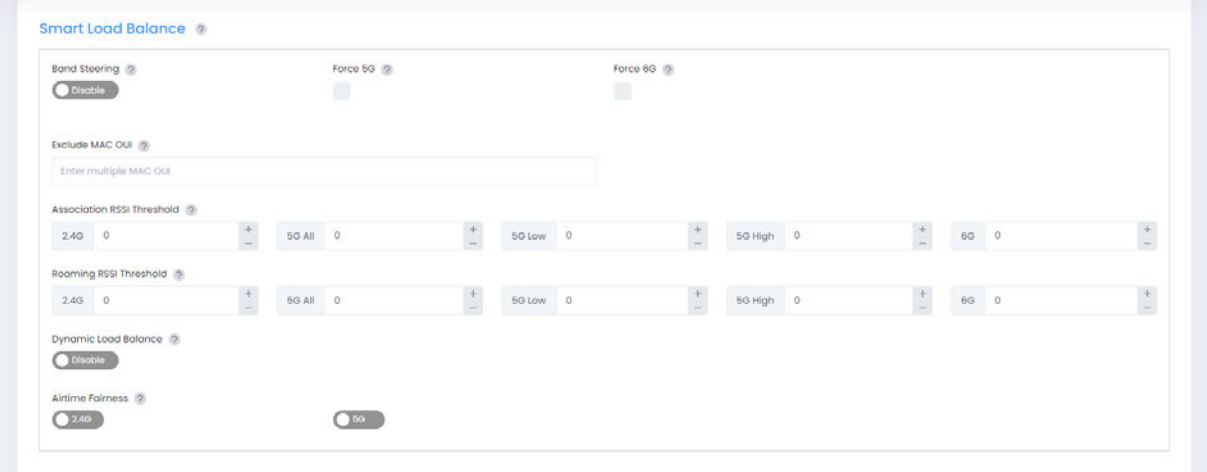


Complete the fields as described below to provide the basic information for the RF Profile:

- **Name** - The name to assign to the RF Profile.
- **Country/Region** - Select a Country Code. A Country Code is a short alphabetic or numeric geographical code that represents a country or dependent area and is used for data processing and communications. The wireless transmitting power and operating frequencies (channels) vary by country/region. Select the country code where the APs are located.

- **Description** - An optional description for the RF Profile.

5.1.3.5.2 Smart Load Balance

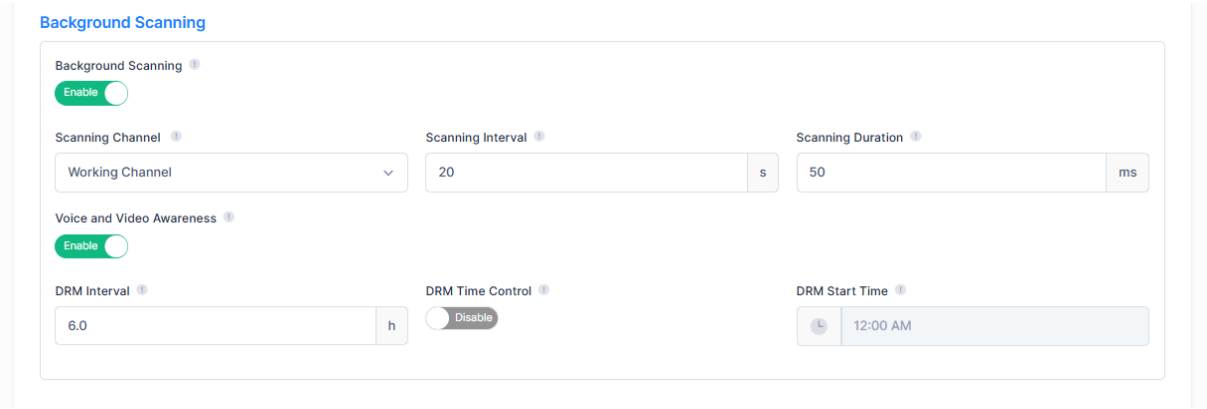


Smart Load Balance (SLB) is a feature that improves the user experience when accessing wireless connectivity by guiding a user's client device to connect to a free wireless channel or AP and denying access to APs with weak signal. Smart Load Balance includes:

- **Band Steering -** Enables/Disables Band Steering. Band Steering controls the behavior of dual band clients according to the utilization of a wireless channel and users connected to the AP, and guides a client accessing the network to the optimal AP.
- **Force 5G/Force 6G** - Dual-band wireless clients are directed to the appropriate AP radio based on the following Force 5GHz and Force6GHz settings:
  - Force 5G is disabled and Force 6G is enabled:
    - If a client supports 6G, then client is forced to connect to the 6G radio of the AP.
    - If a client supports 2.4G and 5G but not 6G, the client is not forced to connect to 5G.
  - Force 5G is enabled and Force 6G is enabled:
    - If a client supports 2.4G, 5G, and 6G, the AP will prevent the client from connecting to the 2.4G radio. The client will then try to connect to the 5G or 6G radio, which the AP will allow.
    - If a client supports 2.4G and 5G but not 6G, the AP will prevent the client from connecting to the 2.4G radio. The client will then try to connect to the 5G radio, which the AP will allow.
  - Force 5G is enabled and Force 6G is disabled:
    - If a client supports 2.4G, 5G, and 6G, the client is forced to connect to the 5G radio and not allowed to connect the 2.4G radio. If the AP supports 6G, then the client can try to connect to the 6G radio, which the AP will allow.
- **Exclude MAC OUI -** Excludes MAC OUI for band-steering. If Band Steering is enabled, enter a MAC OUI for a client. The client will not utilize Band Steering and will be allowed to connect to the wireless band. This setting may be preferable for certain legacy and latency sensitive clients (e.g., scanners, MIPT Phones).

- **Association RSSI Threshold -** Used to set thresholds to optimize connectivity when associating with an AP by forbidding client access to networks with a weak wireless signal (RSSI). Clients with an RSSI value lower than the Association RSSI Threshold will not be allowed to connect to the AP. By default, RSSI threshold is disabled (0). RSSI threshold can be applied to 2.4G band, 5G band, or 6G band separately. RSSI Threshold is recommended to be deployed in a high density scenario. By default, Association RSSI is disabled (0).
    - The 5G High and 5G Low settings are exclusively used to set the 5.8G radio and 5.2G radio on Stellar AP-1230 series. The 5G All setting is used to set the full band 5G radio on other AP series.
- **Roaming RSSI Threshold -** Used to set thresholds to optimize connectivity when roaming by forbidding client access to networks with a weak wireless signal (RSSI). The ability to define a Roaming RSSI Threshold helps to improve the client experience in harsh RF environments. Roaming RSSI can be applied to 2.4G band, 5G band, and 6G band separately and is used in conjunction with the 802.11k and 802.11v protocols. By default, Roaming RSSI is disabled (0).
    - When 802.11k and 802.11v functionality is enabled on the AP, clients that support these protocols will be informed on which AP to roam to when the threshold is breached. The client will then decide whether or not to roam to another AP.
    - Clients that do not support 802.11k or 802.11v will be dropped if their RSSI value is less than the Roaming RSSI Threshold.
    - If both 802.11k and 802.11v functionality is not enabled on the AP, then all of the clients will be treated as non-802.11k or non-802.11v clients and will be dropped if their RSSI value is less than the Roaming RSSI Threshold.
    - The 5G High and 5G Low settings are exclusively used to set the 5.8G radio and 5.2G radio on Stellar AP-1230 series. The 5G All setting is used to set the full band 5G radio on other AP Series.
- **Dynamic Load Balance -** Enables/disables client load balancing among APs in a group or groups in the same wireless network. The client information, such as client number, is synchronized in the wireless network so that an AP can know the load of its neighbor AP and decide whether or not to permit client access.
- **Airtime Fairness -** Enables/Disables the Airtime Fairness feature on 2.4G and/or 5G bands. The Airtime Fairness feature provides equal access to all wireless clients, regardless of client type, capability (802.11ac or 802.11n or 802.11a or 802.11g or 802.11b), thus delivering uniform performance to all clients. This feature prevents the clients from monopolizing resources. It is disabled by default. You must reboot the AP after the function enabled to make it take effect.

5.1.3.5.3 Background Scanning

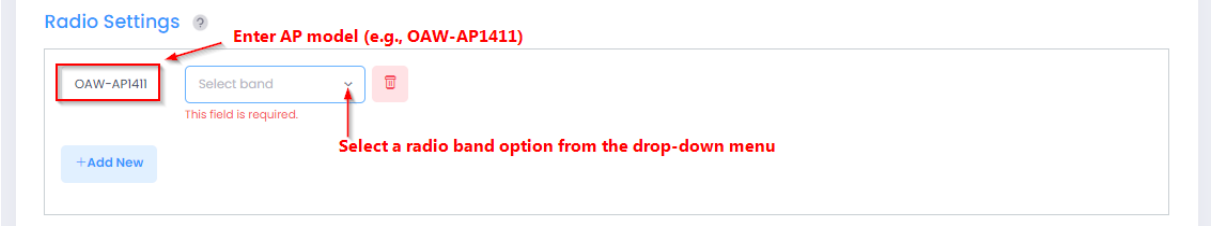


Configure the Background Scanning settings as described below:

- **Background Scanning -** Enables/Disables Background Scanning. Background Scanning is used to examine the radio frequency environment in which the wireless network is operating, discover neighbor APs, and identify interference and attacks. Background scanning is the basis of some advanced features such as: MIPS, RDA (ACS/APC) etc. If you want these advanced functions to be utilized, make sure it is enabled. By default, background scanning is enabled.
- **Scanning Channel -** Specify the channel(s) on which the wireless background scanning is executed. For a highly-sensitive packet delay use case, it is recommended that you enable background scanning only for the Working Channel.
- **Scanning Interval -** The Background Scanning interval, in seconds. (Default = 20)
- **Scanning Duration -** The Background Scanning duration in milliseconds. During the specified duration, APs examine the radio frequency through all channels on both the 2.4G band, 5G band, and 6G band. (Default = 50)
- **Voice and Video Awareness -** Enables/Disables Voice and Video Awareness. Background scanning must be aware of existing traffic on APs. If there is an ongoing voice/video service, scanning should not be performed to ensure uninterrupted traffic; and scanning should resume there is no active voice/video session.
- **DRM Interval** - If DRM Time Control is disabled (Off), specify a time interval for DRM channel selection. (Range = 0.5 hour - 12 hours, Default = 6 hours)
- **DRM Time Control** - Enables/Disables DRM Time Control. Enable to specify a start time for DRM automatic channel selection. When disabled, channel selection occurs at the specified DRM Interval (Default = 6 hours).
- **DRM Start Time** - If DRM Time Control is enabled (On), specify any hour of the day between 0 - 23 hours. Note that DFS radar detection change will take effect immediately.

5.1.3.5.4 Radio Settings

Configures the radio band options for specific AP models. For example, the AP-1411 is a dual-radio, tri-band (2.4G, 5G, 6G) Access Point with configurable radio options.

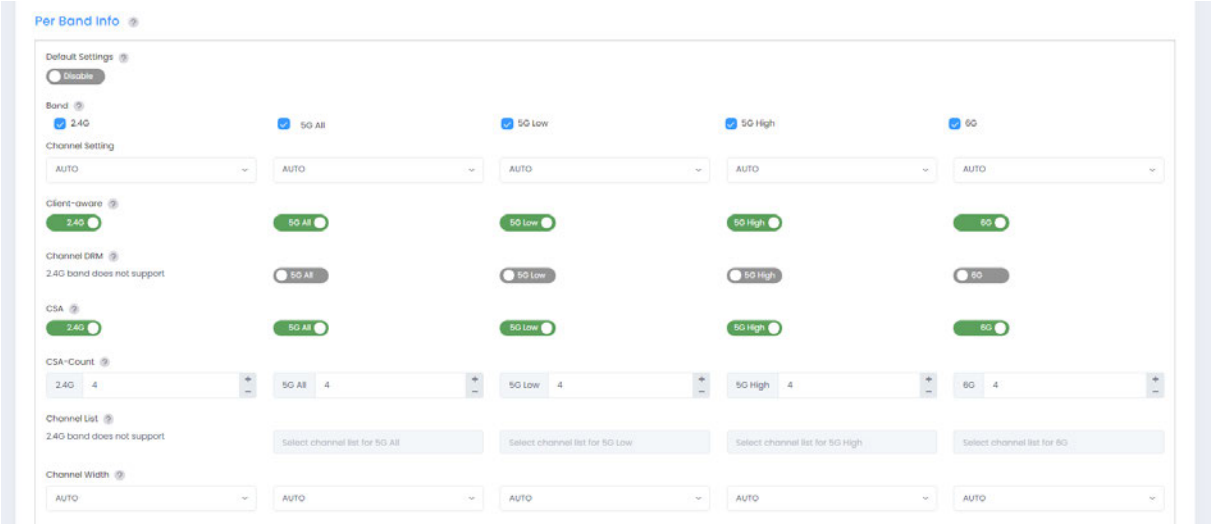


Enter the AP model number (must start with “OAW-AP”) and select one of the following bands from the drop-down menu:

- 2.4G, 5G Full
- 2.4G, 6G
- 5G Full, 6G

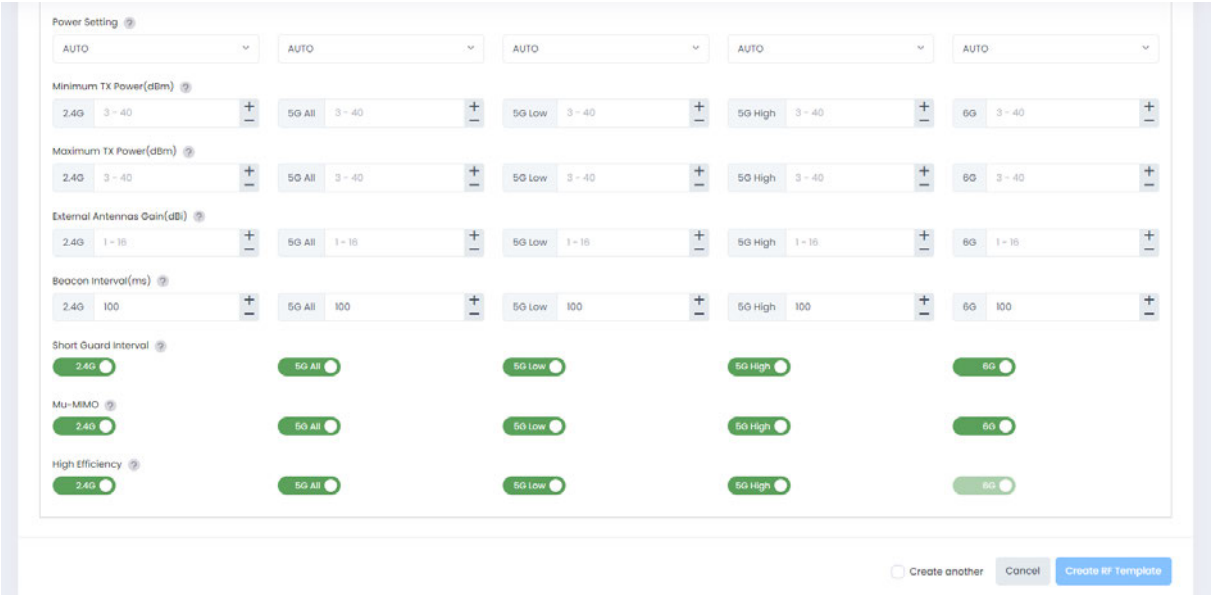
5.1.3.5.5 Per-Band Info

Configure the wireless setting for each radio band on an AP, such as working channel, transmit power, and short guard interval of the radio.



- **Default Setting -** Enables/Disables Band Default Settings. Disable to set custom bandwidth settings. Enable to reset bandwidth settings to default values.
- **Band -** Configure the working radio for the AP.
  - **2.4G -** 2.4G band radio will be activated.
  - **5G All -** 5G band radio will be activated. It is used to set the full band 5G radio on other AP series.
  - **5G Low -** 5.2G band radio will be activated. It is used to set the 5.2G radio on OAW AP-123x.
  - **5G High -** 5.8G band radio will be activated. It is used to set the 5.8G radio on OAW AP-123x.
  - **6G** - 6G band radio will be activated.
- **Channel Setting -** Configure the working channel of the radio. Allowed channels vary by country/ region.

    - **Auto** - Dynamically assigns the working channel by ACS (Auto Channel Selection).
    - Manually specify the channel (allowed channels vary by country/region).
- **Client Aware -** Enables/Disables Client Aware Feature. When enabled, Auto Channel Selection does not change channels for Stellar APs with connected clients, except for high-priority events such as RADAR detected. If "Client Aware" is Disabled, the Stellar AP may change to a more optimal channel, which may temporarily disrupt current client traffic.
- **Channel DRM -** Specify the channel scope for DRM. In some regions, specific unwanted channels can be scoped out automatic channel selection to avoid conflicts or law violation. Not supported on 2.4G Band.
- **CSA -** Enables/Disables Channel Switch Announcement. When enabled, the AP announces to clients that it is going to switch to a new channel. This allows clients that support CSA to move to the new channel and limit downtime.
- **CSA-Count -** The number of CSA announcements the AP sends before it switches to the new channel. (Default = 4)
- **Channel List -** Specify the available channel(s) that can be selected by DRM. Not supported on 2.4G Band.
- **Channel Width -** Configures the channel width. Channel width is used to control how broad the signal is for transferring data. By increasing the channel width, you can increase the speed and throughput of a wireless broadcast. However, larger channel width brings more unstable transmission in crowded areas with a lot of frequency noise and interference. The channel width support is different between 2.4, 5G, and 6G.
    - **2.4G -** Auto/20MHz
    - **5G -** Auto/20MHz/40MHz/80MHz/160MHz. Note that some high-frequency channels (e.g., 165) do not support 40MHz/80MHz/160MHz. If an AP is using these channels, a Channel Width of 40MHz/80MHz/160Mhz will not be available. For example, 160MHz is only supported on channel settings 36 through 128. Wi-Fi 6 Access Points AP132X, AP136X and new AP1351 all support 160Mhz channels.
    - **6G -** 20MHz/40MHz/80MHz/160MHz/320MHz



- **Power Setting -** Configures the transmit power of the wireless radio. Power range varies from different radios.
  - **2.4G -** Configure the power setting for 2.4G radio.
    - Auto - Dynamically assigned the 2.4G transmit power by APC (Auto Power Control)
    - Manually specify the power setting (3dBm - 40dBm)
  - **5G -** Configure the power setting for 5G radio.
    - Auto - Dynamically assigned the 5G transmit power by APC (Auto Power Control)
    - Manually specify the power setting (3dBm - 40dBm)
  - **6G -** Configure the power setting for 6G radio.
    - Auto - Dynamically assigns the 6G transmit power by APC (Auto Power Control)
    - Manually specify the power setting (3dBm - 40dBm)
- **Minimum Tx Power (dBm) -** Specify the minimum transmit power for auto power setting. This can prevent the AP from selecting a low transmit power resulting in poor quality transmission.
- **Maximum Tx Power (dBm) -** Specify the maximum transmit power for auto power setting.
- **External Antenna Gain (dBi) -** Specify the gain value for the external AP antenna. Only those AP Groups containing APs with external antennas (OAW-AP1222, OAW-AP1232) need to be configured with this attribute. It is recommended that you divide APs into several AP Groups when using different types of external antenna (e.g., Group A with an antenna gain value of 3-dBi, and Group B with an antenna gain value of 6-dBi).
- **Beacon Interval (ms) -** Specify the Beacon period for the AP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. (Range = 60 - 500, Default = 100)
- **Short Guard Interval -** Enables/Disables Short Guard Interval. In IEEE 802.11 OFDM-based communications, Guard Interval is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device. The standard symbol Guard Interval used in 802.11 OFDM is 800 nanoseconds in duration. To increase data rates, the 802.11n standard added optional support for a 400 nanoseconds guard interval (Short Guard Interval). This would

provide approximately an 11% increase in data rates. However, using the Short Guard Interval will result in higher packet error rates when the delay spread of the RF channel exceeds the Short Guard Interval, or if timing synchronization between the transmitter and receiver is not precise. By default, Short Guard Interval is disabled on the wireless radio.

- **MU-MIMO -** Enables/Disables Multi-User, Multiple-Input, Multiple-Output (MU-MIMO) feature. If enabled, the AP can communicate with multiple devices simultaneously. This decreases the time each device has to wait for a signal and speeds up the network.
- **High-Efficiency -** Enables/Disables 802.11ax high efficiency wireless functionality. If Disabled, an HE mode capable AP will downgrade to VHT (Very High Throughput) mode. Note that for 6G band, 802.11ax high efficiency wireless functionality is enabled by default and cannot be disabled.
- **Extremely High Throughput** - Enables/Disables IEEE 802.11be (Extremely High Throughput) for Wi-Fi 7. When enabled (the default), Wi-Fi 7 capable APs use high link utilization to maximize the transfer of data.
  Note: Before disabling Extremely High Throughput, make sure the radio is not selected in any WLAN configuration with MLO bands.

21 Oct 2025

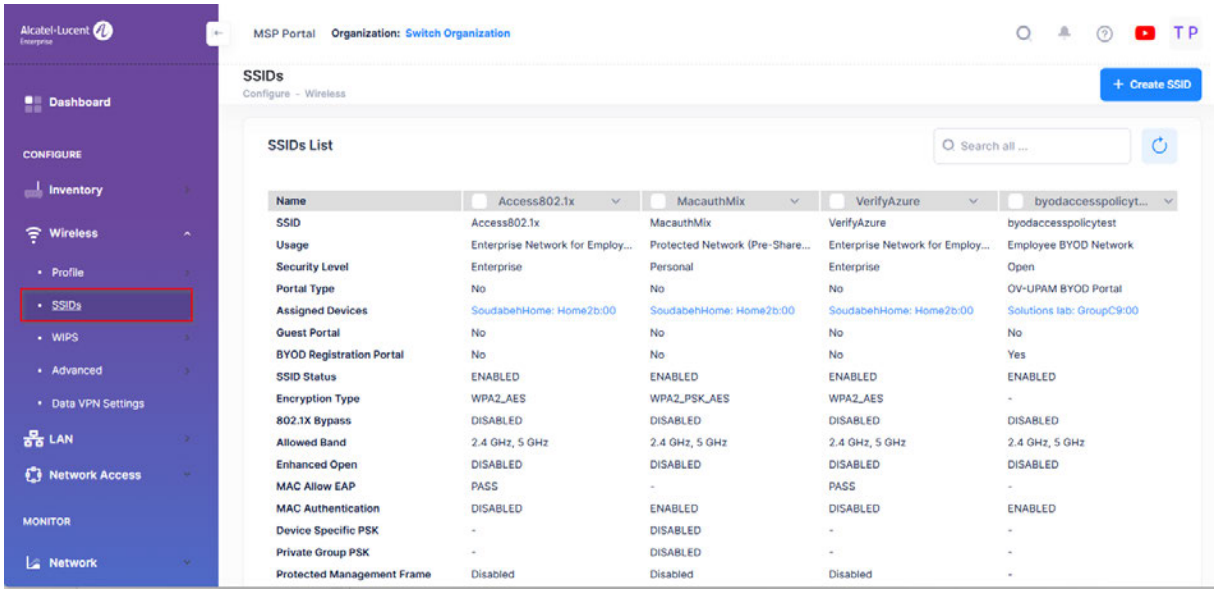
5.2 SSIDs

The SSID is the main domain object used by Stellar Access Point (AP) devices to broadcast Wi-Fi to clients and provide multiple levels of security for the client connection to the network. An SSID configuration is applied to an AP Group; all APs belonging to the assigned group will use the same SSID configuration.

> An SSID is an Organization-level entity, meaning that two SSIDs for the same Organization cannot have the same name. However, two different Organizations can each have an SSID with the same name.

The OmniVista Terra SSID application simplifies wireless network configuration with one-step provisioning, including SSID setup as well as authentication and policy configuration. When you create an SSID, relevant default configurations (Access Role Profile, Access Policy, Authentication Strategy, Guest Access Strategy, BYOD Access Strategy, AAA Server Profile, Tunnel Profile, and Global Configuration) are automatically created and linked to the SSID using a name derived from the SSID. As you go through the process of creating/editing an SSID, you can customize these default SSID configurations to fit your network requirements.

To manage the SSID configuration, navigate to the SSIDs screen by clicking on **Wireless > SSIDs** under the “Configure” section of the OmniVista Terra Menu (see page 45). The SSIDs List screen displays.



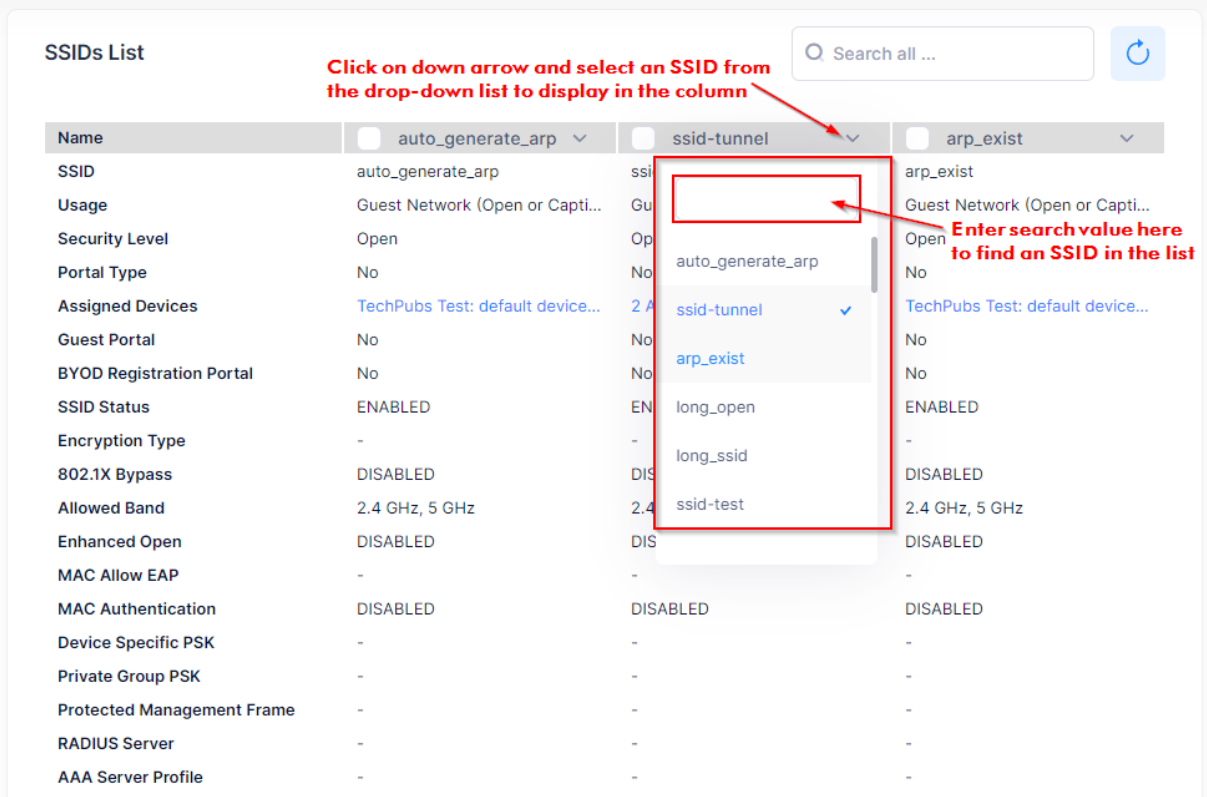
The SSIDs List screen displays information about all of the configured SSIDs. If a specific parameter has not been configured for an SSID, the field is blank. Scroll to view additional SSIDs. The SSIDs List screen is used to complete the following tasks:

- Customize the SSID List Display (see page 348) - You can customize the order in which SSIDs are displayed on the screen, prioritizing them so that specific SSIDs are shown in the first columns. This is particularly useful if the number of SSIDs requires scrolling to view additional SSIDs.
- Edit Related SSID Configurations (see page 349) - Quickly edit relevant related SSID configurations (for example, Access Role Profile, Access Policy, Authentication Strategy).

- Enable/Disable SSIDs (see page 349) - Enable or disable the broadcasting of the SSID(s).
- Create an SSID (see page 354) - Create a new SSID and apply the SSID to an Access Point (AP) group.
- Edit an SSID (see page 350) - Customize SSID settings to satisfy your network requirements.
- Delete an SSID (see page 351) - Delete an SSID configuration.
- Search an SSID Attribute Value (see page 352)- You can search any of the fields or attribute value from the SSIDs List by using the search box.

5.2.1 Customizing the SSIDs List Display

You can customize the order in which SSIDs are displayed on the screen, prioritizing them so that specific SSIDs are shown in the first columns. Click on the drop-down arrow at the top of a column to display a list of all configured SSIDs and select an SSID. The selected SSID will be displayed in that column.

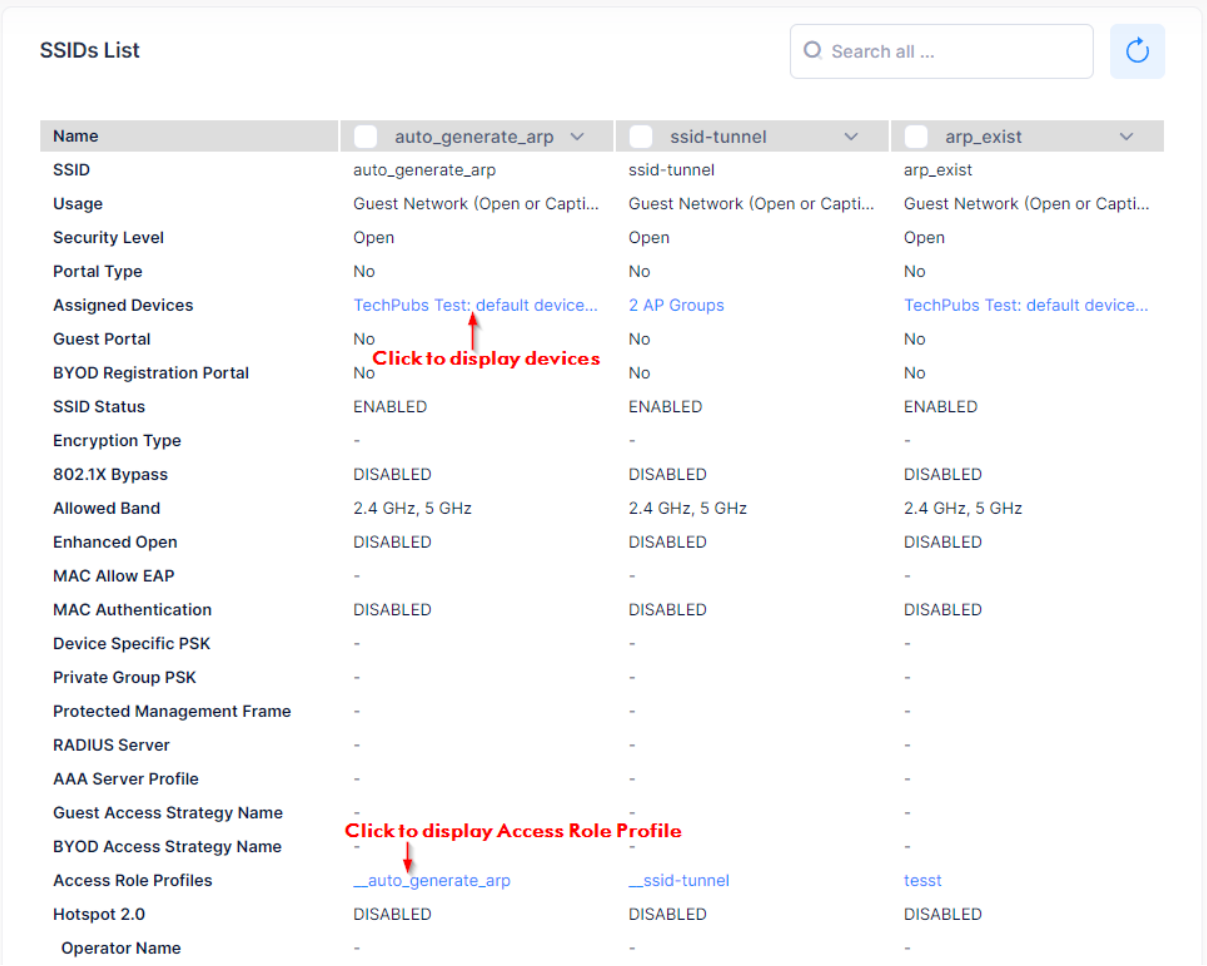


The SSID that was previously displayed will not be "moved" to another location. To re-display that SSID, go to another column and repeat the procedure to re-display that SSID in that column. However, If the selected SSID is already shown in another column, the two columns will swap positions.

If you have fewer than 30 SSIDs configured and create a new SSID, the new SSID will be displayed in the last column. However, if you have reached the maximum display of 30 SSIDs and create a new SSID, the SSID will not replace an existing SSID in the display. To display the SSID, you must click on the drop-down at the top of one of the columns and select the new SSID.

5.2.2 Editing Related SSID Configurations

You can quickly view or edit relevant related SSID configurations (for example, Access Role Profile, Access Policy, Authentication Strategy, Assigned Devices) from the SSIDs List screen. The names of these configurations are displayed as a hyperlink.

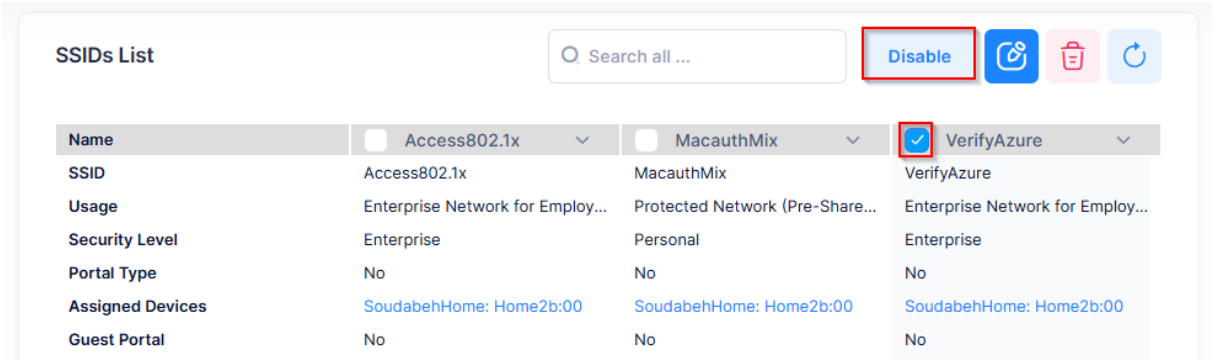


Click on the link to open a configuration window. The configuration will be pre-selected with the detailed configuration information displayed. Edit the configuration and click on the **Save** button to apply the update and return to the SSIDs List screen.

> Related configuration names that begin with "_ _" were generated during SSID configuration and are attached to the SSID. For example, when creating SSID "Guest6GHz", if you select to create an Access Role Profile for the SSID, the name automatically entered for the profile is "_ _Guest6GHz". See Creating an SSID (see page 354) online help for more information.

5.2.3 Enabling/Disabling an SSID

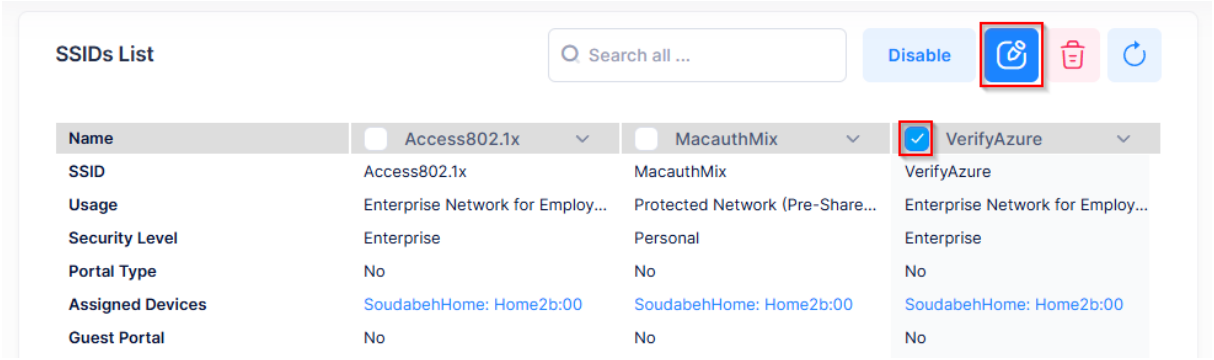
Click on the checkbox next to the SSID(s), then click on the **Enable** or **Disable** button to change the broadcasting status of the SSID(s).



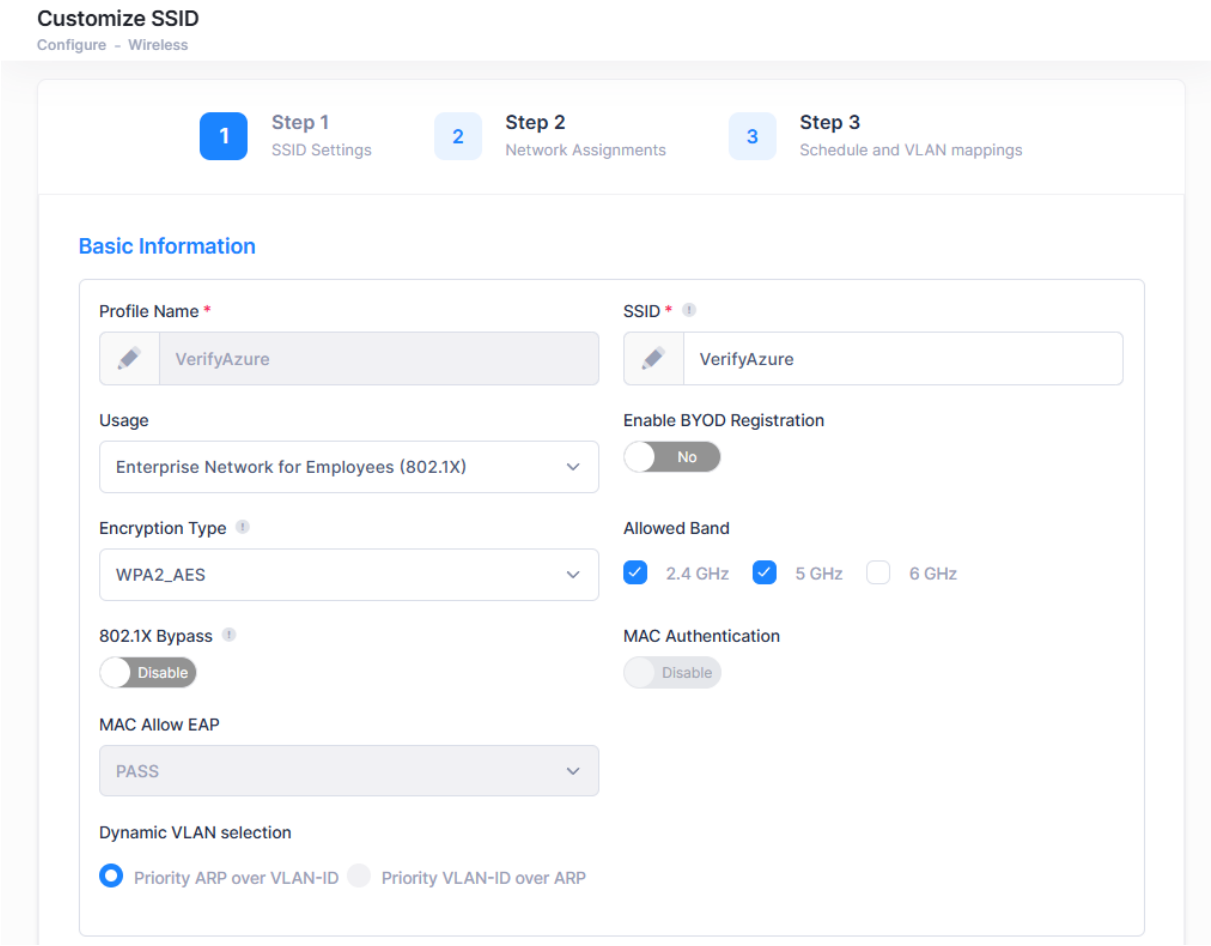
When you disable an SSID, the AP stops broadcasting the SSID; the configuration remains on the AP. When you enable an SSID, the AP begins broadcasting again.

5.2.4 Editing an SSID Configuration

Select an SSID by clicking on the checkbox in the upper-left corner of the SSID column, then click on the Edit icon.



The Customize SSID Screen opens.

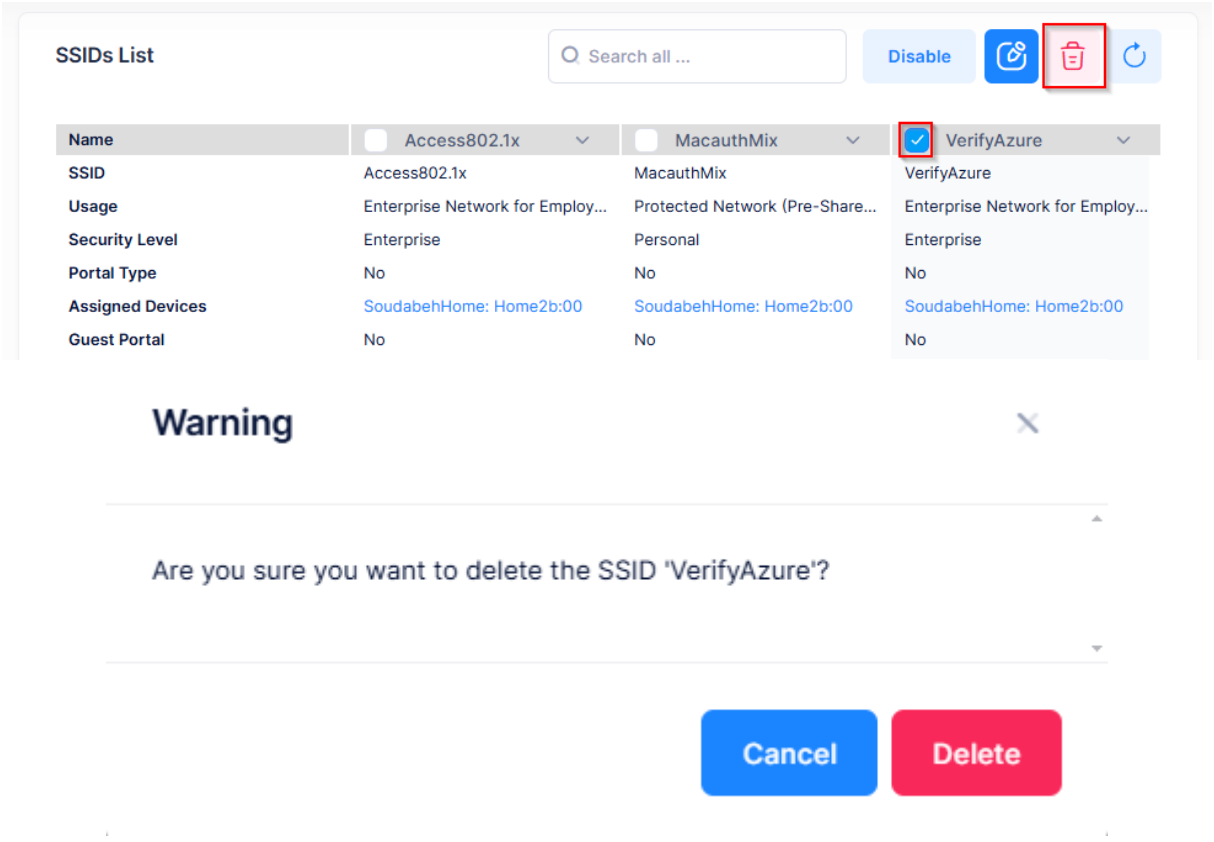


Edit the configuration as described here (see page 354) and click on the **Save** button. The new configuration will be saved and applied to the specified AP Groups.

> You can only edit one SSID at a time. You cannot edit the SSID Name.

5.2.5 Deleting an SSID

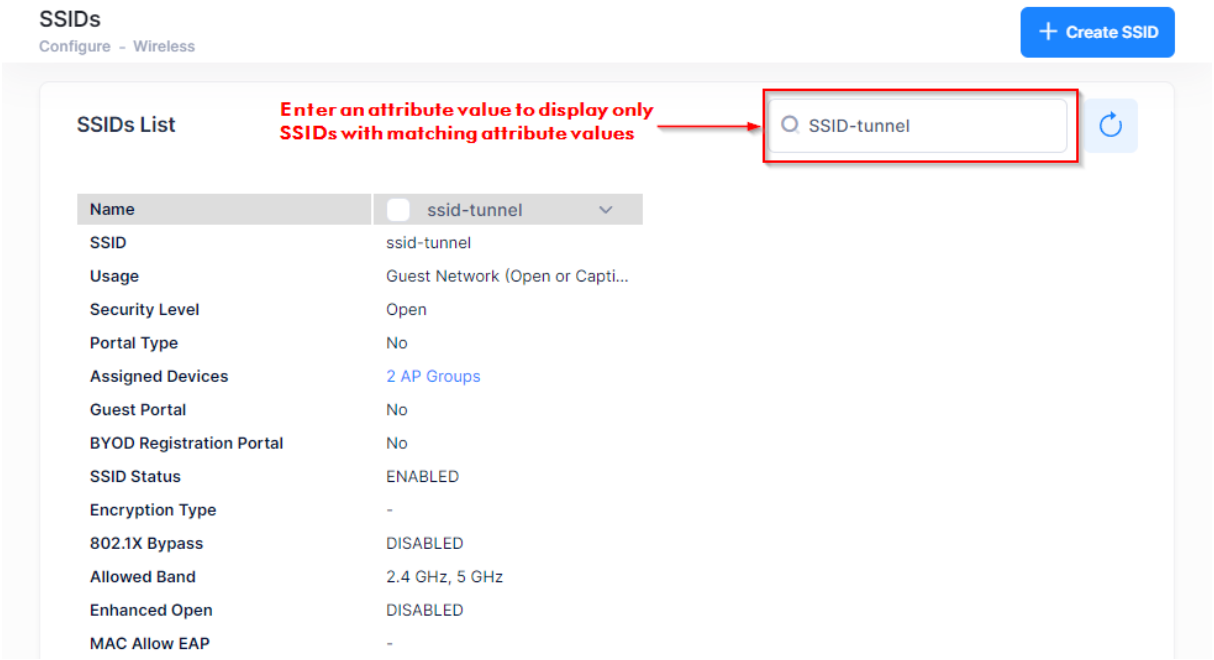
Select an SSID(s) by clicking on the checkbox in the upper-left corner of the SSID column, click on the Delete icon, then click **Delete** at the Confirmation Prompt.



When you delete an SSID you delete the relevant related configurations created for the SSID (for example, Access Role Profile, Access Policy, Authentication Strategy), unless those configurations are in use outside of this SSID.

5.2.6 Search an SSID Attribute Value

You can search for any of the possible field values or attribute values that exist in the SSIDs List by using the Search box option. The search results are refined based on the attribute value entered in the Search box. Only SSIDs that contain the matching search attribute are displayed in the search results.


SSIDs
Configure - Wireless
Create SSID
SSIDs List
Enter an attribute value to display only SSIDs with matching attribute values
SSID-tunnel
Name
ssid-tunnel
SSID
ssid-tunnel
Usage
Guest Network (Open or Capti...
Security Level
Open
Portal Type
No
Assigned Devices
2 AP Groups
Guest Portal
No
BYOD Registration Portal
No
SSID Status
ENABLED
Encryption Type
-
802.1X Bypass
DISABLED
Allowed Band
2.4 GHz, 5 GHz
Enhanced Open
DISABLED
MAC Allow EAP
-

21 Oct 2025

5.2.7 Creating an SSID Configuration

The Create SSID screen is used to define an SSID configuration and associate an SSID with an Access Point (AP) Group. To access this screen, click on **Create SSID** on the SSIDs (see page 347) screen.

The Create SSID screen provides the following step-by-step process for creating an SSID configuration:

1. SSID Settings

- Basic Information (see page 355) - Configures identifying information for the SSID (for example, profile name, SSID broadcast name, network usage, Captive Portal authentication, and allowed bands).
- Authentication Strategy (see page 363) - Selects an authentication server, authentication strategy, and access policy.
- Default VLAN/Network (see page 365) - Configures an Access Role Profile for the default network.
- Detailed SSID Settings (see page 365) - Configures detailed settings for SSID functionality (for example, hide SSID, advanced security, roaming controls, client controls, and data rates).

2. Network Assignments

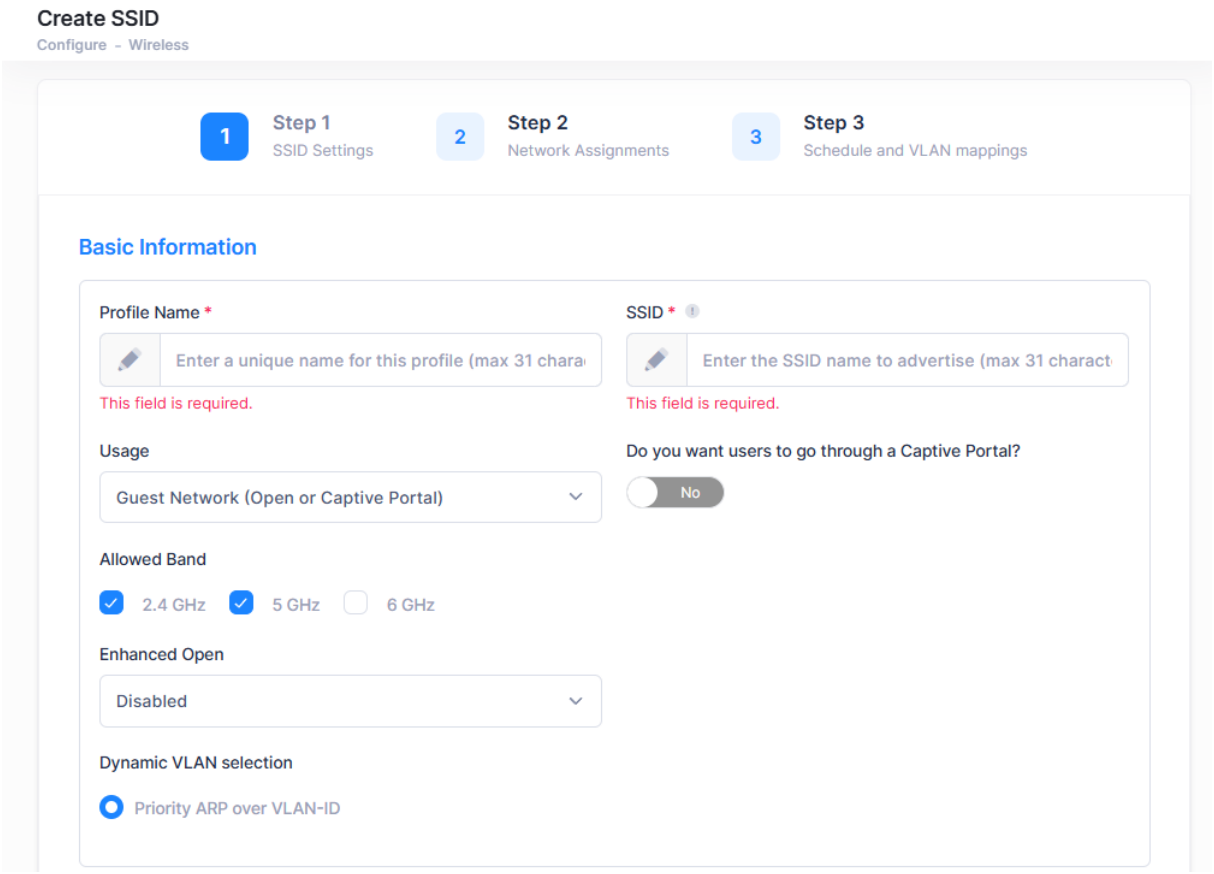
- Assign SSID(s) to AP Groups (see page 371) - Selects Access Point (AP) Groups from one or more Sites to which the SSID is applied.

3. Schedule and VLAN Mappings

- Schedule SSID Availability (see page 371) - Specify the days and/or time during which the SSID is active.
- VLAN/Tunnel Mapping (see page 371) - Map the SSID to a VLAN or a Guest Tunnel ID. Client traffic connecting to the Access Point on the SSID network is forwarded on the selected VLAN or Tunnel.

5.2.7.1 1. SSID Settings

5.2.7.1.1 Basic Information



Complete the fields as described below to provide the basic information for the SSID:

- **Profile Name** - A unique name to identify the management profile for the SSID.
- **SSID** - A name that uniquely identifies the wireless network (up to 31 characters). This is the wireless network name that is advertised to wireless clients.
- **Usage** - The SSID network usage. When you select a Usage from the list below, relevant related default configurations such as Access Policy, Authentication Strategy, Guest Access Strategy, and BYOD Access Strategy are automatically created and linked to the SSID using a name derived from the SSID. These configurations can then be customized for your network.
  - Guest Network (Open or Captive Portal) (see page 356) - Create a network for Guest Users. Suitable for setting up an Open Network with or without a Captive Portal.
  - Employee BYOD Network (see page 357) - Create a network for employees connecting with their own devices. Suitable for setting up an Open Network for Employee BYOD devices.
  - Enterprise Network for Employees (802.1X) (see page 357) - Create a network for employees connecting with known devices. Suitable for setting up an Enterprise Network for Employees accessing the network with Company Property or BYOD devices.

- Protected Network (Pre-Shared Key & an Optional Captive Portal) (see page 358) - Create a Protected Network for Guest Users. Suitable for setting up a Personal network that requires a PSK/Passphrase, with or without a Captive Portal.
- Protected Network for Employees (Pre-Shared Key & BYOD Registration Portal) (see page 361) - Create a Protected Network for employees connecting with their own devices. Suitable for setting up a Personal Network that requires a PSK/Passphrase for employee BYOD devices.
- **Guest Network (Open or Captive Portal) -** Create a network for Guest Users. Suitable for setting up an Open Network with or without a Captive Portal. This is typically used for Guests. When this Usage is selected, configure the following option:
  - **Do you want users to go through a Captive Portal? -** Enable/Disable Captive Portal Authentication for the SSID. When enabled, OmniVista Terra UPAM Captive Portal is used for authentication.
  - **Enhanced Open** - Enables/Disables the use of Wi-Fi Enhanced Open™ to secure an open SSID. Wi-Fi Enhanced Open™ is a security standard that is based on Opportunistic Wireless Encryption (OWE). When enabled, OWE is used to ensure that communication between each pair of endpoints is protected from other endpoints. Data sent between a client and an AP is provided individualized data protection. Wi-Fi Enhanced Open™ offers improved data privacy, while maintaining convenience and ease-of-use. This functionality is particularly useful for provisioning a secure open SSID in public spaces. You can also enable an Enhanced Open Transition Mode for the SSID. When this mode is enabled, the AP broadcasts two different types of BSSID: one legacy Open SSID on 2.4GHz/5.0GHz band and one Enhanced Open SSID on 2.4GHz/5.0GHz/6.0GHz band. This allows both Enhanced Open and Non-Enhanced Open clients to connect to the same open SSID without adversely impacting the end user experience. Select one of the following options to configure the Enhanced Open status for the SSID:
    - **Disabled** - Disable Enhanced Open for the SSID. If 2.4GHz and/or 5.0GHz is the allowed band (not 6.0GHz), Enhanced Open is disabled by default. Note that you cannot disable Enhanced Open if the 6.0GHz band is selected.
    - **Enabled** - Enable Enhanced Open for the SSID. If 6.0GHz is the allowed band, Enhanced Open is automatically enabled whether 2.4GHz or 5.0GHz is selected.
    - **Enabled - Transition Mode** - Enable Enhanced Open Transition Mode for the SSID. Note that the Enhanced Open Transition Mode is supported only on APs running AWOS 4.0.8 or above. Enabling this mode for APs running older AWOS versions may cause the SSID to revert to an open SSID after a reboot. Upgrading your network is highly recommended.
  - **Dynamic VLAN Selection** - Determines if an ARP or VLAN ID assignment is given priority.
    - **Priority ARP over VLAN-ID** - Enabled by default only if MAC authentication is not selected for the SSID usage. If an AP receives a RADIUS response with ARP and VLAN ID, it will select the ARP.
    - **Priority VLAN-ID over ARP** - If MAC authentication is selected for the SSID usage, then priority is given to selecting the VLAN ID over the ARP.

- **Employee BYOD Network -** Create a network for employees connecting with their own devices. Suitable for setting up an Open Network for Employee BYOD devices. Access to the network is granted after BYOD portal authentication.
  - **Enable BYOD Registration -** BYOD authentication for the SSID is enabled by default.
  - **Enhanced Open** - Enables/Disables the use of Wi-Fi Enhanced Open™ to secure an open SSID. Wi-Fi Enhanced Open™ is a security standard that is based on Opportunistic Wireless Encryption (OWE). When enabled, OWE is used to ensure that communication between each pair of endpoints is protected from other endpoints. Data sent between a client and an AP is provided individualized data protection. Wi-Fi Enhanced Open™ offers improved data privacy, while maintaining convenience and ease-of-use. This functionality is particularly useful for provisioning a secure open SSID in public spaces. You can also enable an Enhanced Open Transition Mode for the SSID. When this mode is enabled, the AP broadcasts two different types of BSSID: one legacy Open SSID on 2.4GHz/5.0GHz band and one Enhanced Open SSID on 2.4GHz/5.0GHz/6.0GHz band. This allows both Enhanced Open and Non-Enhanced Open clients to connect to the same open SSID without adversely impacting the end user experience. Select one of the following options to configure the Enhanced Open status for the SSID:
    - **Disabled** - Disable Enhanced Open for the SSID. If 2.4GHz and/or 5.0GHz is the allowed band (not 6.0GHz), Enhanced Open is disabled by default. Note that you cannot disable Enhanced Open if the 6.0GHz band is selected.
    - **Enabled** - Enable Enhanced Open for the SSID. If 6.0GHz is the allowed band, Enhanced Open is automatically enabled whether 2.4GHz or 5.0GHz is selected.
    - **Enabled - Transition Mode** - Enable Enhanced Open Transition Mode for the SSID. Note that the Enhanced Open Transition Mode is supported only on APs running AWOS 4.0.8 or above. Enabling this mode for APs running older AWOS versions may cause the SSID to revert to an open SSID after a reboot. Upgrading your network is highly recommended.
  - **Dynamic VLAN Selection** - Determines if an ARP or VLAN ID assignment is given priority.
    - **Priority ARP over VLAN-ID** - Enabled by default. If an AP receives a RADIUS response with ARP and VLAN ID, it will select the ARP.
    - **Priority VLAN-ID over ARP** - This option is not supported for Captive Portal or BYOD registration.
- **Enterprise Network for Employees (802.1X) -** Create a network for employees connecting with known devices. Suitable for setting up an Enterprise Network for Employees accessing the network with Company Property or BYOD devices. When this Usage is selected, configure the following options:
  - **Enable BYOD Registration -** Enable/Disable BYOD authentication for the SSID.
  - **Encryption Type** - Select the encryption type to use from the drop-down menu.
    - DYNAMIC_WEP - WEP with dynamic keys.
    - WPA_TKIP - WPA with TKIP encryption and dynamic keys using 802.1X.
    - WPA_AES - WPA with AES encryption and dynamic keys using 802.1X.

    - WPA2_TKIP - WPA2 with TKIP encryption and dynamic keys using 802.1X.
    - WPA2_AES - WPA2 with AES encryption and dynamic keys using 802.1X.
    - AUTO_WPA_WPA2 - Automatic WPA and WPA2 or mixed mode encryption with dynamic keys using 802.1X.
    - WPA3_AES256 - WPA3 with CNSA (Suite B) using 802.1X. Note that when WPA3_AES256 encryption is applied to an AP that does not support it, the encryption will automatically fall back to WPA2_AES.
    - WPA3_AES - WPA3 with AES encryption and dynamic keys using 802.1X.
  - **802.1X Bypass -** Enable/Disable 802.1X bypass administrative status. When 802.1X bypass is enabled, the user's 802.1X authentication method is performed conditionally based on the result of MAC Authentication. (Default = Disabled).
    - **MAC Authentication** - When 802.1X Bypass is enabled, MAC Authentication is automatically enabled and cannot be disabled.
    - **MAC Allow EAP** - When 802.1X Bypass is enabled, select Pass or Fail for MAC Allow Extensible Authentication Protocol (EAP).
  - **Dynamic VLAN Selection** - Determines if an ARP or VLAN ID assignment is given priority.
    - **Priority ARP over VLAN-ID** - If an AP receives a RADIUS response with ARP and VLAN ID, it will select the ARP.
    - **Priority VLAN-ID over ARP** - If an AP receives a RADIUS response with ARP and VLAN ID, it will select the VLAN. Note that this option is not supported if BYOD Registration is enabled for the SSID usage.
- **Protected Network (Pre-Shared Key & an Optional Captive Portal) -** Create a Protected Network for Guest Users. Suitable for setting up a Personal network that requires a PSK/Passphrase (see page 363), with or without a Captive Portal. This is typically used for Guests. When this Usage is selected, configure the following options:
  - **Do you want users to go through a Captive Portal? -** Enable/Disable Captive Portal Authentication for the SSID. When enabled, OmniVista Terra UPAM Captive Portal is used for authentication.
  - **Encryption Type** - Select the encryption type to use from the drop-down menu.
    - STATIC_WEP - Authentication with Static Wired Equivalent Privacy security algorithm.
    - WPA_PSK_TKIP - WPA with TKIP encryption using a preshared key.
    - WPA_PSK_AES - WPA with AES encryption using a preshared key.
    - WPA_PSK_AES_TKIP - WPA with TKIP and AES mixed encryption using a preshared key.
    - WPA2_PSK_TKIP - WPA2 with TKIP encryption using a preshared key.
    - WPA2_PSK_AES - WPA2 with AES encryption using a preshared key.
    - WPA3_SAE_AES - WPA3 with AES encryption using a preshared key, which ONLY allows WPA3 capable client accessing. When this encryption type is selected, the PSK, Device Specific PSK, and Private Group PSK parameters are not available.

  - WPA3_PSK_SAE_AES - WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing.
  - AUTO_WPA_WPA2 - Automatic WPA and WPA2 encryption or mixed mode using a preshared key.
- **Backward Compatibility** - Enables/disables using WPA3_PSK_SAE_AES encryption on 2.4GHz and 5.0GHz bands when encryption is automatically set to WPA3_SAE_AES for the 6.0GHz band. When the 6.0GHz band is selected for the SSID, the other bands inherit using WPA3_SAE_AES encryption, which some legacy devices cannot use to connect to the SSID. By default, Backward Compatibility is disabled. When enabled, the WPA3_PSK_SAE_AES Encryption Type is automatically used for the 2.4GHz and 5.0GHz bands and the 6.0GHz band continues to use WPA3_SAE_AES.
  Note: If the MLO Band setting includes 6.0GHz, then the Backward Compatibility option is automatically disabled.
- **Key Format -** PSK format. Select Passphrase (8-63 characters) or Pre-shared Key (64 characters).
- **PSK/Passphrase -** Enter a PSK Passphrase for authentication.
- **Confirm PSK/Passphrase -** Re-enter the PSK Passphrase.
- **Device Specific PSK** - Enables/Disables Device Specific PSK (see page 363). Device Specific PSK provides more security than traditional PSK. Select one of the following settings to enable Device Specific PSK.
  - **Prefer Device Specific PSK** - If the AAA Server sends the "AES-CBC-128" attribute along with the Radius Access Accept response, this value will be used. If the AAA server does NOT send the "AES-CBC-128" attribute, the key configured in the SSID will be used. Note that when this setting is selected or Device Specific PSK is disabled, the Private Group PSK feature is available to create private groups of client devices based on a Private Group PSK (PPSK) Entry.
  - **Force Device Specific PSK -** The value of "AES-CBC-128" attribute returned by AAA Server will be always used, whether it exists or not. The Private Group PSK feature is not available.
- **Private Group PSK** - Enables/Disables the grouping of Device Specific PSKs (see page 363). (This option is only available when Device Specific PSK is disabled or set to “Prefer Device Specific PSK”.) When Private Group PSK is enabled, complete the following fields to create a PPSK Entry:
  - **PPSK Entries** - At least one Private Group PSK (PPSK) Entry is required with the following parameters:
    - **Name** - Enter a unique name to identify the PPSK Entry. No two Entries can have the same Name.
    - **Passphrase** - Enter a unique PSK Passphrase for authentication. No two Entries can have the same Passphrase.
    - **Access Role Profile** - Select the name of an existing Access Role Profile or click on **Create Access Role Profile** to create a new profile to use (see the Access Role Profile (see page 514) online help). To edit the selected Access Role Profile, click on **Edit**.

- **Add more entries** - Click for each PPSK Entry that you want to add. Note that each SSID can have up to 16 PPSK Entries. The total number of entries across all SSIDs that exist on an AP cannot exceed 64 on any AP.

- **Dynamic Private Group PSK** - Enables/Disables the dynamic grouping of Device Specific PSKs. (This option is only available when Device Specific PSK is set to “Prefer Device Specific PSK” or “Force Device Specific PSK” and Encryption Type is set to “WPA2_PSK_AES.) When enabled:
  - The grouping of Device Specific PSKs is processed through UPAM.
  - The SSID Encryption Type is automatically set to “WPA2_PSK_AES” and Captive Portal is set to no. Both fields are disabled and cannot be changed.
  - Dynamic Private Group PSK (PGPSK) profiles containing PSK entries are configured in the UPAM database through the Dynamic PGPSK Configuration (see page 750) screen, instead of the SSID screen. Note that you must first create the SSID before you create any Dynamic Private Group PSK profiles.
  - When a client attempts to authenticate through the SSID, UPAM checks the Company Property (see page 716) list first to see if there’s a match for the device; if not, the list of entries in the Private Group PSK UPAM database are checked. When a device is authenticated through Dynamic Private Group PSK, the matched entry is added to the Dynamic PGPSK Configuration MAC table (see page 750).
  - Consider the following scenarios for using Dynamic Private Group PSK to connect to the SSID:
    - If the client MAC address was added in Company Property with Device Specific PSK disabled, then the client enters the Dynamic Group PSK passphrase to connect to the SSID.
    - If the client MAC address is not in Company Property, then the client enters the Dynamic Private Group PSK passphrase to connect to the SSID.
    - If the client MAC address was added in Company Property with Device Specific PSK enabled, then the client cannot connect to the SSID with the Dynamic Private Group PSK passphrase. Instead, the client can use the Device Specific PSK passphrase to connect to an SSID with ARP in MAC Authentication.
    - Client can only connect to the SSID with one Dynamic Private Group PSK passphrase. For example, if the client enters Dynamic Private Group PSK passphrase “guest-1” and successfully connects to the SSID (MAC address is added to Dynamic Private Group MAC list), but later attempts to connect to an SSID with a different passphrase (such as “guest-2”), the client cannot connect to the SSID. A different passphrase indicates a different role for network access. Each group should have a unique passphrase.
- **Dynamic VLAN Selection** - Determines if an ARP or VLAN ID assignment is given priority.

    - **Priority ARP over VLAN-ID** - Enabled by default. If an ARP receives a RADIUS response with ARP and VLAN ID, it will select the ARP.
    - **Priority VLAN-ID over ARP** - This option is not supported for Captive Portal or BYOD registration.
- **Protected Network for Employees (Pre-Shared Key & BYOD Registration Portal) -** Create Protected Network for employees connecting with their own devices. Suitable for setting up a Personal Network that requires a PSK/Passphrase (see page 363) for employee BYOD devices. Access to the network is granted after BYOD portal authentication. When this Usage is selected, configure the following options:
    - **Enable BYOD Registration -** BYOD authentication for the SSID is enabled by default.
    - **Encryption Type** - Select the encryption type to use from the drop-down menu.
        - STATIC_WEP - Authentication with Static Wired Equivalent Privacy security algorithm.
        - WPA_PSK_TKIP - WPA with TKIP encryption using a preshared key.
        - WPA_PSK_AES - WPA with AES encryption using a preshared key.
        - WPA_PSK_AES_TKIP - WPA with TKIP and AES mixed encryption using a preshared key.
        - WPA2_PSK_TKIP - WPA2 with TKIP encryption using a preshared key.
        - WPA2_PSK_AES - WPA2 with AES encryption using a preshared key.
        - WPA3_SAE_AES - WPA3 with AES encryption using a preshared key, which ONLY allow WPA3 capable client accessing. When this encryption type is selected, the PSK, Device Specific PSK, and Private Group PSK parameters are not available.
        - WPA3_PSK_SAE_AES - WPA3 and WPA2 mixed mode, which allow both WPA3 capable client as well as ONLY WPA2 capable client accessing.
        - AUTO_WPA_WPA2 - Automatic WPA and WPA2 encryption or mixed mode using a preshared key.
    - **Backward Compatibility** - Enables/disables using WPA3_PSK_SAE_AES encryption on 2.4GHz and 5.0GHz bands when encryption is automatically set to WPA3_SAE_AES for the 6.0GHz band. When the 6.0GHz band is selected for the SSID, the other bands inherit using WPA3_SAE_AES encryption, which some legacy devices cannot use to connect to the SSID. By default, Backward Compatibility is disabled. When enabled, the WPA3_PSK_SAE_AES Encryption Type is automatically used for the 2.4GHz and 5.0GHz bands and the 6.0GHz band continues to use WPA3_SAE_AES.
      Note: If the MLO Band setting includes 6.0GHz, then the Backward Compatibility option is automatically disabled.
    - **Key Format -** PSK format. Select Passphrase (8-63 characters) or Pre-shared Key (64 characters).
    - **PSK/Passphrase -** Enter a PSK Passphrase for authentication.
    - **Confirm PSK/Passphrase -** Re-enter the PSK Passphrase.
    - **Device Specific PSK** - Enables/Disables Device Specific PSK (see page 750). Device Specific PSK provides more security than traditional PSK. Select one of the following settings to enable Device Specific PSK.

- **Prefer Device Specific PSK -** If the AAA Server sends the "AES-CBC-128" attribute along with the Radius Access Accept response, this value will be used. If the AAA server does NOT send the "AES-CBC-128" attribute, the key configured in the SSID will be used. Note that when this setting is selected or Device Specific PSK is disabled, the Private Group PSK feature is available to create private groups of client devices based on a Private Group PSK (PPSK) Entry.
- **Force Device Specific PSK -** The value of "AES-CBC-128" attribute returned by AAA Server will be always used, whether it exists or not. The Private Group PSK feature is not available.

- **Private Group PSK** - Enables/Disables the grouping of Device Specific PSKs (see page 363). (Note that this option is only available when Device Specific PSK is disabled or set to “Prefer Device Specific PSK”.) When Private Group PSK is enabled, complete the following fields to create a PPSK Entry:
  - **PPSK Entries** - At least one Private Group PSK (PPSK) Entry is required with the following parameters:
    - **Name** - Enter a unique name to identify the PPSK Entry. No two Entries can have the same Name.
    - **Passphrase** - Enter a unique PSK Passphrase for authentication. No two Entries can have the same Passphrase.
    - **Access Role Profile** - Select the name of an existing Access Role Profile or click on **Create Access Role Profile** to create a new profile to use (see the Access Role Profile (see page 514) online help). To edit the selected Access Role Profile, click on **Edit**.
  - Click on **Add more entries** for each PPSK Entry that you want to create. Note that each SSID can have up to 16 PPSK Entries. The total number of entries across all SSIDs that exist on an AP cannot exceed 64 on any AP..
- **Dynamic VLAN Selection** - Determines if an ARP or VLAN ID assignment is given priority.
  - **Priority ARP over VLAN-ID** - Enabled by default. If an AP receives a RADIUS response with ARP and VLAN ID, it will select the ARP.
  - **Priority VLAN-ID over ARP** - This option is not supported for Captive Portal or BYOD registration.

- **Allowed Band** - Select one or more of the following band(s) that will be available on the network. Note that when 6 GHz is selected for the Allowed Band of a Protected Network or Protected Network for Employees, the only encryption type supported is WPA3_SAE_AES (which does not support PSK options).
  - **2.4 GHz**
  - **5 GHz**
  - **6 GHz**

5.2.7.1.1.1 Device Specific PSK (DSPSK)

When the Protected Network or the Protected Network for Employees option is selected for the SSID network usage and a device is configured for Device Specific PSK, when the AAA Server sends the RADIUS Access-Accept for MAC Authentication for the device, it will also send the specific pre-shared key for that device, differentiated by the device's MAC Address. This means that each device will have a different key.

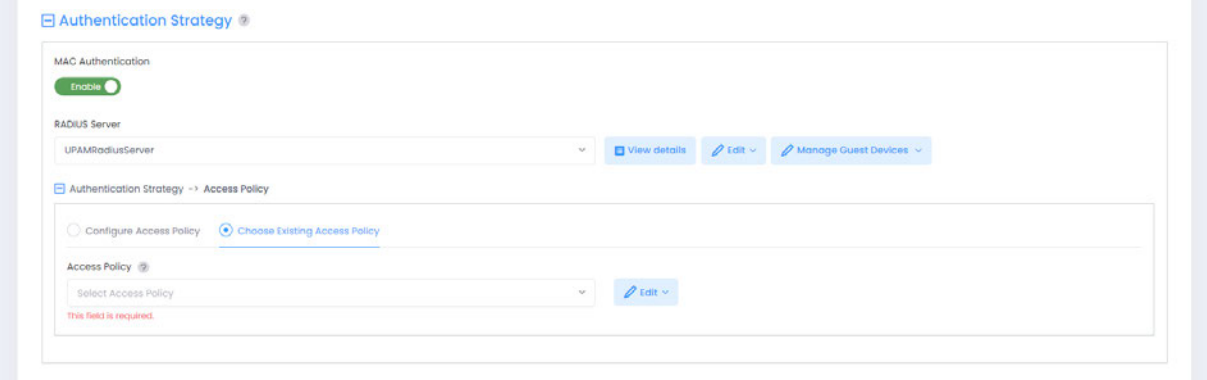
> Device Specific PSK will only work with a UPAM RADIUS Server and does not support AUTO_WPA_WPA2 encryption. Devices are configured for Device Specific PSK on the Company Property Screen. See the Company Property online help (see page 716) for more information. You can also configure a device for Device Specific PSK from the Authentication Records List. See the Authentication Records online help (see page 879) for more information.

5.2.7.1.1.2 Private Group PSK

When a PSK-enabled SSID is created, you can either create a static PSK or enforce Device Specific PSK. This provides a common Passphrase key, which is suitable for networks requiring network-wide common PSK. Enabling Private Group PSK (PPSK) allows you to create private groups of client devices based on a PPSK Entry. Each client device specifies a Passphrase when connecting to an SSID. If the passphrase matches any of the PPSK Entry, the client is placed in the specified Access Role Profile.

Configuring the Private Group PSK attribute is offered only when Device Specific PSK is Disabled or set to "Prefer Device Specific PSK". When the Device Specific PSK is set to "Force Device Specific PSK", OmniVista will not display the Private Group PSK attribute because the Passphrase specified in Company Property is used instead.

5.2.7.1.2 Authentication Strategy



Enable or disable MAC Authentication. When enabled, additional fields are displayed to select the RADIUS Server and the Access Policy to use for the Authentication Strategy. Complete the fields as described below:

- **RADIUS Server** - Select the RADIUS Server to use from the drop-down menu. Note that if you select a RadSec (TLS-Enabled Radius) Server, an AP can only support one RadSec Server and cannot support MAC authentication or External Captive Portal. If there are multiple RadSec

Servers set up, make sure that all SSIDs within an AP Group are configured to use the same RadSec server. The following options are available for the selected server:

- **View details** - Display configuration details about the selected RADIUS Server.
- **Edit** - Open the Edit RADIUS Server screen to modify server settings.
- **Manage Guest Devices** - Configure user access to company devices owned by the Organization (for example, printers, IP phones, laptops, tablets). This field may not be available based on the network usage selected for the SSID or the RADIUS Server selected.

Note that when you click on **Edit** or **Manage Guest Devices**, you are prompted to either discard current changes to open the related screen or open the related screen in a new browser tab.

- **Authentication Strategy → Access Policy** - Select one of the following options to specify an Access Policy for the SSID Authentication Strategy:
  - **Choose Existing Access Policy** (Default) - Select an existing Access Policy from the drop-down menu. The following options are available for the selected policy:
    - **View Details** - Display configuration details about the selected Access Policy.
    - **Edit** - Open the Edit Access Policy screen to modify the selected Access Policy configuration.
  - **Configure Access Policy** - Create a new Access Policy. When you select this option, the Access Policy name is automatically generated by adding "_ _" to the beginning of the SSID name (for example, if the SSID name is "MAC Auth", then the name assigned to the Access Policy is "_ _MAC Auth"). You can then customize the policy settings, as needed.
    - **Save this as a distinct Access Policy, for reuse** - Select this option if you want the automatically created Access Policy to be available for use after the associated SSID has been deleted.

The Access Policy that you create or select defines the Authentication Strategy that UPAM applies when a client connects to the SSID. However, the Access Policy displayed for the SSID configuration is not always the policy used for authentication when the client is connecting to the SSID. This can occur if there are multiple Access Policies with the same precedence and overlapping rules configured through the Access Policies screen (Configure > Network Access > UPAM-NAC > Access Policies).

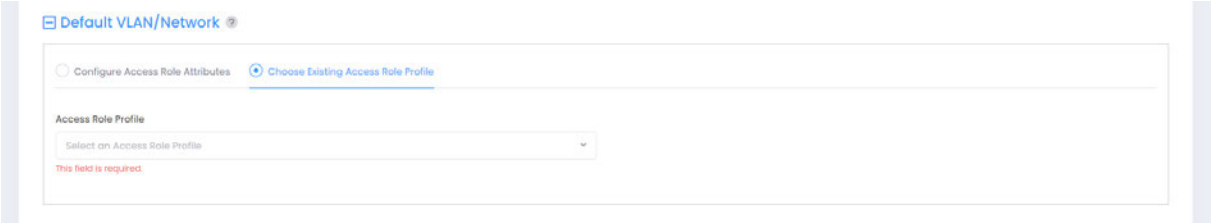
When a client connects to the SSID, UPAM selects the Access Policy with the highest precedence and evaluates whether its mapping rules align with the client's connection request. If a match is found, the associated authentication strategy is applied. If two Access Policies with the same precedence have identical mapping rules, UPAM defaults to the policy created first. This behavior may lead to unexpected results.

To prevent ambiguity, ensure that:

a) There are no Access Policies with overlapping rules, or

b) Access Policies with overlapping rules have different precedence. You can adjust the policy precedence configured for the Access Policies (Configure > Network Access > UPAM-NAC > Access Policies) to address these issues.

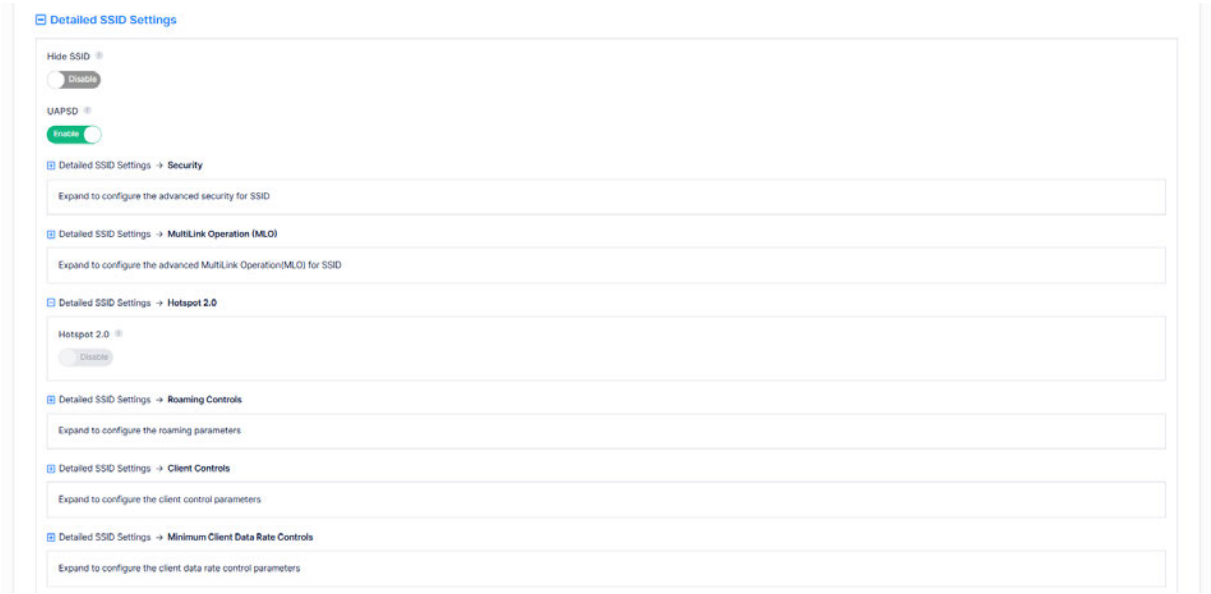
5.2.7.1.3 Default VLAN/Network



In this section, you can select one of the following options to apply an Access Role Profile to clients joining this SSID, if a role cannot be assigned by other role assignment methods.

- **Choose Existing Access Role Profile** (Default) - Select an existing Access Role Profile from the drop-down menu. The “VLAN” and “Use Tunnel” mappings are set according to the attributes defined in the selected Access Role Profile.
- **Configure Access Role Attributes** - When you select this option, the Access Role Profile name is automatically generated by adding “_ _” to the beginning of the SSID name (for example, if the SSID name is “MAC Auth”, then the name assigned to the Access Role Profile is “_ _MAC Auth”). You can then customize the default profile settings, as needed. See the Creating an Access Role Profile (see page 514) online help for information about configuring profile settings.
  - **Save this as a distinct Access Role Profile, for reuse** - Select this option if you want the automatically created Access Role Profile to be available for use after the associated SSID has been deleted.

5.2.7.1.4 Detailed SSID Settings



In this section, you can configure advanced SSID settings as described below:

- **Hide SSID -** Enables/Disables SSID in beacon frames. Note that hiding the SSID does very little to increase security. (Default = Disabled)
- **UAPSD -** Enables/Disables Unscheduled Automatic Power Save Delivery (UAPSD) on the SSID. UAPSD is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow that is delivered over the wireless media. Because UAPSD does not require the client to poll each individual packet that is buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. (Default = Enabled)
- **Detailed SSID Settings → Security**
  - **Classification Status -** Enables/Disables classification. If classification is enabled, traffic will be classified to a role based on the configured classification rules. Note that the precedence of role assignment methods is important. Classification Rules are only used if 802.1X/MAC authentication does not return a role, or the returned role is not matched with any configured roles in the device.
  - **MAC Pass Alt -** If MAC Authentication is enabled, select an Access Role Profile to assign to clients that pass MAC Authentication but did not receive a valid Access Role Profile.
  - **Client Isolation -** Enables/Disables Client Isolation. If enabled, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the router. (Default = Disabled)
  - **Protected Management Frame -** Configures whether connections are accepted from clients supporting Protected Management Frame for certain Security Levels/Encryption Types (Enterprise - WPA2_AES, WPA3_AES256, WPA3_AES; Protected- WPA2_PSK_AES, WPA3_SAE_AES, WPA3_PSK_SAE_AES). The Encryption Type option is provided based on the selected Usage for the SSID (see Basic Information (see page 355) above).
    - **Disabled -** Disables Protected Management Frame requirements.
    - **Optional -** Allows connections from clients supporting Protected Management Frame and clients that do not.
    - **Required -** Only allows connections from clients supporting Protected Management Frame.
- **Detailed SSID Settings → MultiLink Operation (MLO)**
  - **MLO** - Enables/Disables MLO. (Default = Disabled). Allows for the simultaneous sending and receiving of data between different frequency bands and channels.
    - **MLO Band** - When MLO is enabled, the bands selected are taken from the Allowed Band setting. For example, if Allowed Band is set to 2.4GHz and 5GHz, then the MLO band is set to 2.4GHz and 5GHz by default when MLO is enabled. When the Allowed Band is set to 2.4GHz, 5GHz, and 6GHz, you can change the MLO bands as needed. Note that when you change the MLO bands, it does not change the Allowed Bands.
- **Detailed SSID Settings → Hotspot 2.0**
  - **Hotspot 2.0 -** Enables/Disables Hotspot 2.0. Hotspot 2.0 is a new standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. Hotspot 2.0 was developed by the Wi-Fi Alliance and the Wireless Broadband Association to enable seamless hand-off of traffic without requiring additional user sign-on and authentication. Note that Hotspot 2.0 is only supported with Enterprise

WPA2_AES or Enterprise WPA3_AES256 Encryption. You must first select one of these Encryption types before you can enable Hotspot 2.0.

- **Operator Name -** The operator providing the Hotspot service (0 - 252 characters).
- **Venue Name -** The venue where the Hotspot is hosted (0 - 252 characters).
- **Venue Type -** The type of venue hosting the Hotspot.
- **Network Detail -** The type of Hotspot network.
- **Domain List -** The list of Hotspot Domains. You can have up to 16 Domain Names (1 - 255 characters each).
- **Roaming OIs** - The Roaming Organization Identifier. You can have up to 16 OIs. Each OI field is 3 characters in length if the organizationally unique identifier is an OUI, or 5 octets in length if the organizationally unique identifier is an OUI-36.

- **Detailed SSID Settings → Roaming Controls**
  - **L3 Roaming -** Enables/Disables Layer 3 roaming. Layer 3 roaming allows client to move between Access Points and connect to a new IP subnet and VLAN.
  - **FBD Update on Association -** Enables/Disables FDB Update on Association. If enabled, when a client roams to a new AP, the AP will send ARP packets to the uplink switch to notify the switch to change the downstream forwarding port for the wireless client's traffic.
  - **802.11k Status -** Enables/Disables 802.11k. The 802.11k protocol enables APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.
  - **802.11v Status -** Enables/Disables 802.11v. 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an Instant AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a client due to network load balancing or BSS termination. It also helps the client identify the best AP to transition to as they roam.
- **Detailed SSID Settings → Client Controls**
  - **Max Number of Clients Per Band -** The maximum number of clients allowed in each band. (Range = 1 - 256, Default = 64)
  - **802.11b Support -** Enables/Disables allowing 11b legacy clients connect to APs.
  - **802.11a/g Support** - Enables/Disables allowing 11a/g legacy clients connect to APs.
- **Detailed SSID Settings → Minimum Client Date Rate Controls**
  - **2.4GHz Minimum Client Data Rate Controller -** Enables/Disables 2.4G band access control based on client data rate.
  - **2.4GHz Minimum Client Data Rate -** 2.4G band client with lower data speed will not be given access.
  - **5GHz Minimum Client Data Rate Controller -** Enables/Disables 5G band access control based on client data rate.
  - **5GHz Minimum Client Data Rate -** 5G band client with lower data speed will not be given access.

  - **6GHz Minimum Client Data Rate Controller -** Enables/Disables 6G band access control based on client data rate.
  - **6GHz Minimum Client Data Rate -** 6G band client with lower data speed will not be given access,.
  - **Notes:**
    - Disabling lower bands has an impact on the coverage area.
    - Depending on the environment, we recommend 12 Mbps or 24 Mbps setting for minimum client data rates.
    - Higher Mbps value means less coverage; lower value means larger coverage.
- **Detailed SSID Settings → Minimum MGMT Rate Controls**
  - **2.4GHz Minimum MGMT Rate Controller -** Enables/Disables 2.4G band wireless management frame rate control.
  - **2.4GHz Minimum MGMT Rate -** 2.4G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
  - **5GHz Minimum MGMT Rate Controller -** Enables/Disables 5G band wireless management frame rate control.
  - **5GHz Minimum MGMT Rate -** 5G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
  - **6GHz Minimum MGMT Rate Controller -** Enables/Disables 6G band wireless management frame rate control.
  - **6GHz Minimum MGMT Rate -** 6G band wireless management frame transmit rate. Higher value means less coverage; lower value means larger coverage.
  - **Notes:**
    - Disabling lower bands has an impact on the coverage area.
    - Depending on the environment, using a 12 Mbps or 24 Mbps setting is recommended for minimum client data rates.
    - Higher Mbps value means less coverage; lower value means larger coverage.
- **Detailed SSID Settings → High-Throughput Control**
  - **A-MSDU -** Enables/Disables Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.
  - **A-MPDU -** Enables/Disables Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.
- **Detailed SSID Settings → Power Save Controls**
  - **DTIM Interval -** The Delivery Traffic Indication Message (DTIM) period in beacons. The DTIM interval determines how often the AP should deliver the buffered broadcast and multicast frames to associated clients in the "power save" mode. The default value is 1, which means the client checks for buffered data on the OAW-IAP at every beacon. You can configure a higher DTIM value for power saving (Range = 1 - 255).
- **Detailed SSID Settings → 802.11 Frame Controls**

    - **Advertise AP Name** - Enables/Disables the advertising of the AP name in the standard 802.11 beacon frame with a vendor-specific tag. The default value of Advertise AP name is false. When enabled, the AP name is displayed instead of the AP MAC address.
- **Detailed SSID Settings → Bandwidth Contract**
    - **Upstream Bandwidth -** The maximum bandwidth for traffic from the switch to the client
    - **Downstream Bandwidth -** The maximum bandwidth for traffic from the client to the switch.
    - **Upstream Burst -** The maximum bucket size used for traffic from the switch to the client. The bucket size determines how much the traffic can burst over the maximum bandwidth rate
    - **Downstream Burst -**The maximum bucket size used for traffic from the client to the switch. The bucket size determines how much the traffic can burst over the maximum bandwidth rate.
- **Detailed SSID Settings → Broadcast/Multicast Optimization**
    - **Broadcast Key Rotation -** Enables/Disables the broadcast key rotation function. If enabled, the broadcast key will be rotated after every interval time.
    - **Broadcast Key Rotation Time Interval -** The interval, in minutes, to rotate the broadcast key (Range = 1 - 1440, Default = 15).
    - **Broadcast Filter All -** Enables/Disables broadcast filtering. If enabled, all broadcast frames are dropped, except DHCP and Address Resolution Protocol (ARP) frames.
    - **Broadcast Filter ARP -** Enables/Disables broadcast filtering for ARP. If enabled, the AP will act as an "ARP Proxy". If the ARP-request packet requests a client's MAC address and the AP knows the client's MAC and IP address, the AP will respond to the ARP-request but not forward the ARP-request (broadcast) to all broadcast domains. This reduces ARP broadcast packet forwarding and significantly improves network performance. Note that APs do not act as ARP proxy for Gratuitous ARP packets. When the station gets an IP from DHCP or IP release/ renew, the station will send Gratuitous ARP packets. AP will not respond to such special ARP packets and broadcast them normally.
    - **Multicast Optimization -** Enable/Disables multicast traffic rate optimization.
    - **Multicast Based Channel Utilization -** Configures based channel utilization optimization percentage. (Range = 0 - 100, Default = 90)
    - **Number of Clients -** Configure the threshold for multicast optimization. This is the maximum number of high-throughput.
- **Detailed SSID Settings → 802.1p Mapping** - Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and 802.1p priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.
    - **Background -** WMM Background will be mapped to the 802.1p value.
        - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 1)
        - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 1, 2)

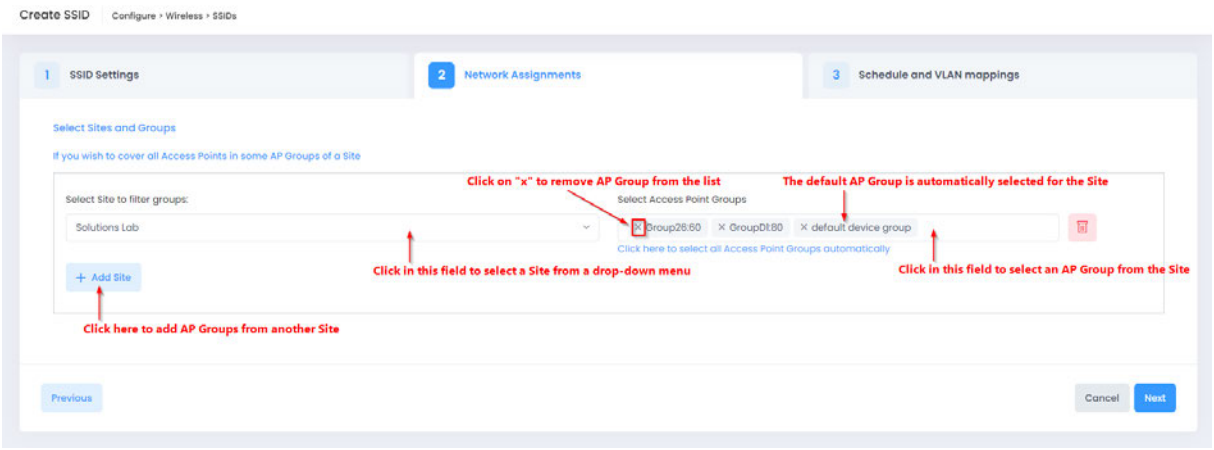
- **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 0, 3)
- **Video -** WMM Video will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 4)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 4, 5)
- **Voice -** WMM Voice will be mapped to the 802.1p value.
  - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 6)
  - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 6, 7)

- **Detailed SSID Settings → DSCP Mapping** - Used to configure the uplink and downlink mapping mechanism between Wi-Fi Multimedia (WMM) Access Categories and DSCP priority. Uplink traffic can only be mapped to a single value. Downlink traffic can be mapped to multiple values. Fields are populated with the default values. To modify a default uplink value, enter a new value in the field. To modify a default downlink value, enter a new value and click on the Add icon. To remove a value, click on the "x" next to the value.
  - **Trust Original DSCP -** If enabled, the original DSCP mapping for uplink traffic is trusted (Default = Disabled).
  - **Background -** WMM Background will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 10)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 2, 10)
  - **Best Effort -** WMM Best Effort will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 0)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 0, 18)
  - **Video -** WMM Video will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 40)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 24, 36, 40)
  - **Voice -** WMM Voice will be mapped to the 802.1p value.
    - **Uplink -** Maps uplink traffic (from AP to network). (Range = 0 - 7, Default = 46)
    - **Downlink -** Maps downlink traffic (from network to AP). (Range = (Range = 0 - 7, Default = 46, 48, 56)

After completing the necessary field values for the SSID Settings tab, click on **Next** to go to the Network Assignments tab (Step 2).

5.2.7.2 2. Network Assignments

An SSID configuration is applied to an AP Group; all APs belonging to the assigned group will use the same SSID configuration. The Network Assignments tab of the Create SSID screen is where you can apply SSIDs to AP Groups, as shown here:



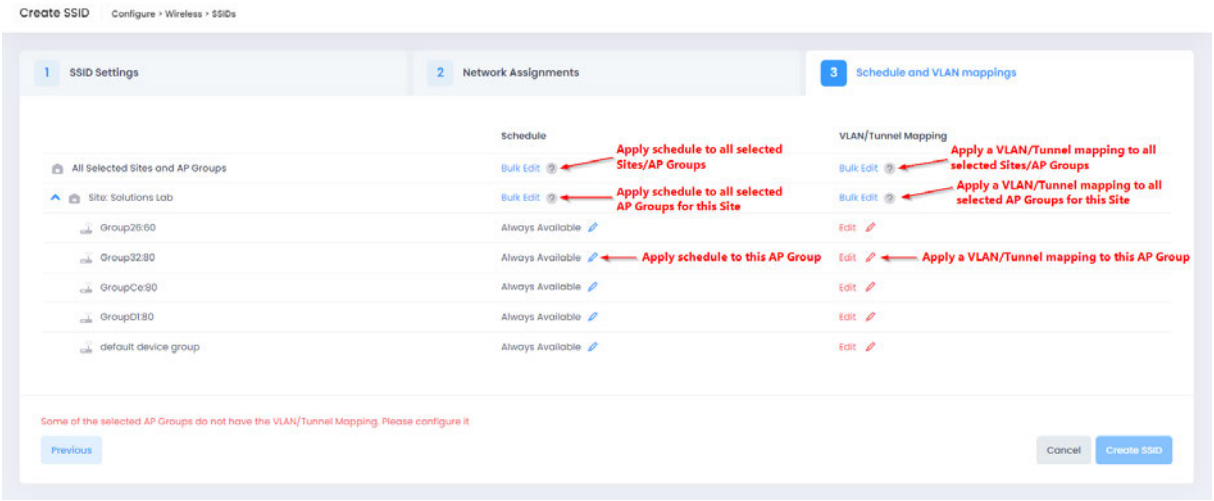
> The maximum number of SSIDs per band that an AP can support is based on the AP model and whether the Extended SSID Scale (see page 309) option is enabled for the AP Group to which the AP belongs.
>
> - Extended SSID Scale option is disabled (the default) - AP allows a maximum of 7 SSIDs per band. This means up to 7 SSIDs with Allowed Band = 2.4GHz and up to 7 SSIDs with Allowed Band = 5GHz. If you apply an SSID to an AP Group and it causes a breach of this maximum limit, the "Save" operation will fail on that AP Group.
> - Extended SSID Scale option is enabled - AP models that support more than 7 SSIDs per band will allow a maximum of 14 SSIDs per band. This means up to 14 SSIDs with Allowed Band = 2.4GHz and up to 14 SSIDs with Allowed Band = 5GHz. If you apply an SSID to an AP Group and it causes a breach of this maximum limit, the "Save" operation will fail on that AP Group.
>
> Note that the Extended SSID Scale status does not apply to 6GHz networks, which have a limit of 4 SSIDs per AP Group.

If you are editing the AP Group assignment for an SSID, all of the AP Groups to which the SSID was applied are displayed as pre-selected in the “Select Access Point Groups” field. You can then remove and/or add AP Groups, as needed.

When you are done selecting the AP Groups to apply to the SSID, click on **Next** to go to the Schedule and VLAN Mappings tab (Step 3).

5.2.7.3 3. Schedule and VLAN Mappings

The Schedule and VLAN Mappings tab is used to schedule the SSID availability (see page 372) for devices belonging to the selected AP Groups and to map a VLAN or Tunnel (see page 373) service to the SSID.

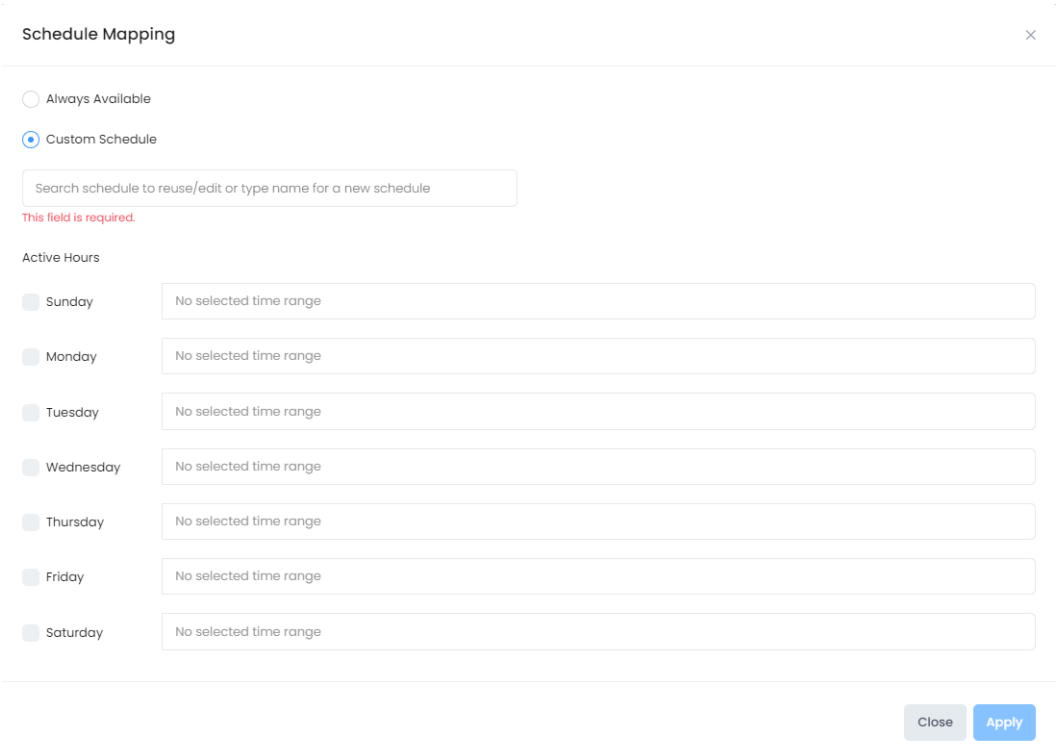


When you are done configuring the Schedule and VLAN/Tunnel mappings, click on **Create SSID**. The SSID profile is created.

5.2.7.3.1 Schedule

You can configure the SSID availability for all AP Groups across all Sites in the Organization, for all AP Groups associated with a specific Site, or for the selected AP Group.

When you click on the **Bulk Edit** option or the **Edit** option for an individual AP Group, the following Schedule Mapping screen opens:



- **Always Available** - The SSID network is available to clients 24/7.

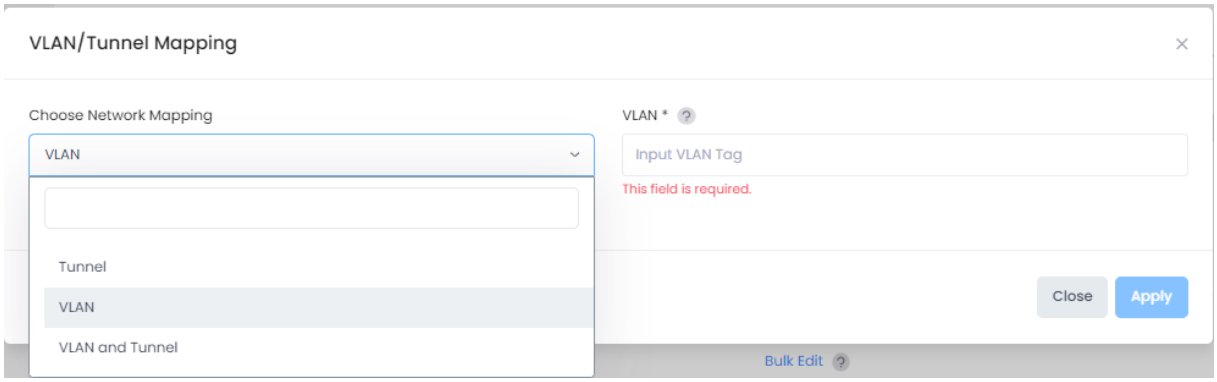
- **Custom Schedule** - Define specific days/times during which the SSID network is available to clients.
  - **Active Hours** - Select the days during which the SSID is active.
    - **Select Time** - When you select a specific day, you can also specify the time of day during which the SSID is active.

> You can configure up to 24 time ranges for an SSID schedule, but make sure that each time range does not overlap with any other time range.

5.2.7.3.2 VLAN/Tunnel Mapping

You can configure a VLAN/Tunnel mapping for all AP Groups across all Sites in the Organization, for all AP Groups associated with a specific Site, or for the selected AP Group.

When you click on the **Bulk Edit** option or the **Edit** option for an individual AP Group, the following VLAN/Tunnel Mapping screen opens:



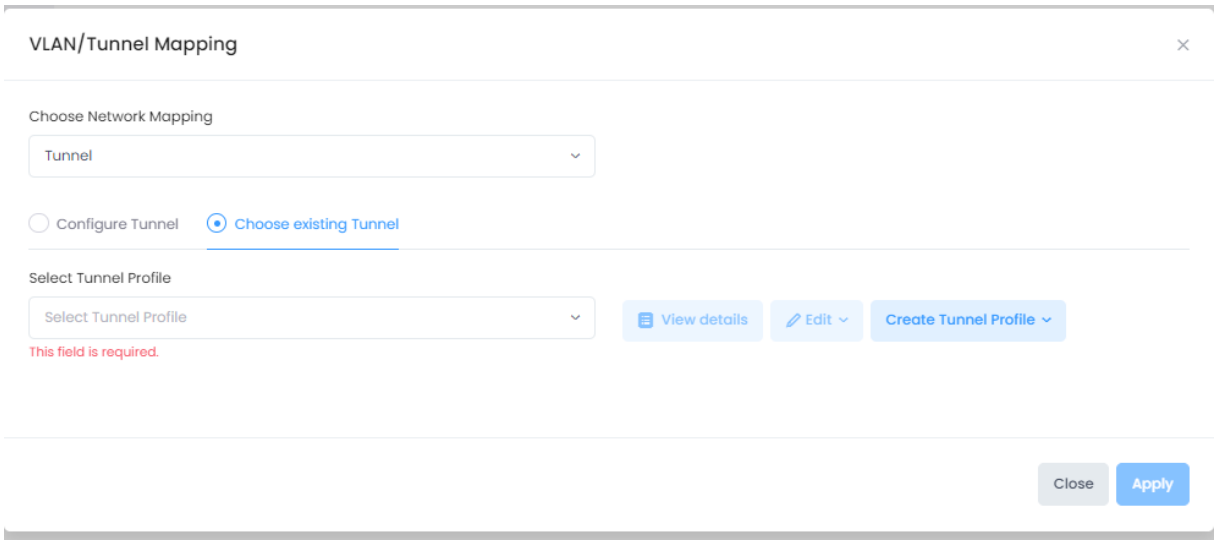
Select one of the following network mapping options from the drop-down menu:

- **VLAN**- Maps the profile to a specific VLAN ID tag on network devices. You can enter multiple VLAN ID tags in this field by specifying a range of VLAN IDs (10-20), individual VLAN IDs (25), or both (10-20, 25). Note that after each VLAN ID entry, you must press the tab key before making the next entry. For example, enter “10-20” press tab key, then enter “21” press tab key, then enter “22” press tab key, and so on. You can also click outside of this field after each entry, instead of pressing the tab key.
- **Tunnel -** Maps the profile to a Guest Tunnel.
- **VLAN and Tunnel -** Maps the profile to a VLAN and a Tunnel, allowing VLAN tagging inside the Guest Tunnel.

> **Notes:**
>
> - You cannot map the profile to VLAN 1, and the VLAN ID specified must not exceed 4090. Make sure that the VLAN ID does not overlap with other VLAN ID mappings.

- The ability to bind up to 256 VLANs to a WLAN/SSID on the AP13xx/AP14xx models is supported. However, not every AP model can accommodate 256 VLANs for all the configured SSIDs. The limitations are outlined below:
  - AP1301H can support 256 VLANs on a maximum of 2 SSIDs, with a total of 512.
  - AP1311/AP1301/AP1431/AP1411 can support 256 VLANs on a maximum of 4 WLANs/SSIDs, with a total of 1024.
  - AP1320/AP1331/AP1351/AP1451 can accommodate 256 VLANs on a maximum of 7 WLANs/SSIDs, with a total of 1792.

When you select the Tunnel mapping option, the following fields are displayed on the VLAN/Tunnel Mapping screen:



- **Configure Tunnel** - Select this option to define a Guest Tunnel service to assign to the SSID.. When you select this option, a Tunnel Profile is automatically created with the SSID name.
  - **Save this as a distinct Tunnel Profile, for reuse** - Select this option if you want the tunnel mapping to be available for use after the associated SSID configuration has been deleted. When you click on this option, you will be prompted to enter a Tunnel Profile name.
- **Choose Existing Tunnel** - Select an existing Guest Tunnel Profile from the drop-down menu or click on **Create Tunnel Profile** to open the Create Tunnel Profile screen and create a new Guest Tunnel Profile. You can also click on **View Details** to view information about the selected Tunnel Profile or click on **Edit** to open the Edit Tunnel Profile screen and make changes to the selected Tunnel Profile.

21 Oct 2025

5.3 Wireless Intrusion Protection System (WIPS)

An 802.11 network is open and borderless, making it vulnerable to attack (e.g., rogue APs, unauthorized clients, DoS attacks). The Wireless Intrusion Protection System (WIPS) application monitors the wireless radio spectrum for the presence of unsafe access points and clients, and can take countermeasures to mitigate the impact of foreign intrusions. WIPS provides an overview of wireless network threats/intrusions for Stellar APs, and enables users to set up policies to detect threats and take countermeasures.

You can view detailed information on intrusive APs and wireless attacks, and create policies to detect and react to the attacks. Detailed views and policies are configured using the following links under the WIPS application (**Configure > Wireless > WIPS**) of the OmniVista Terra Menu. (see page 45)

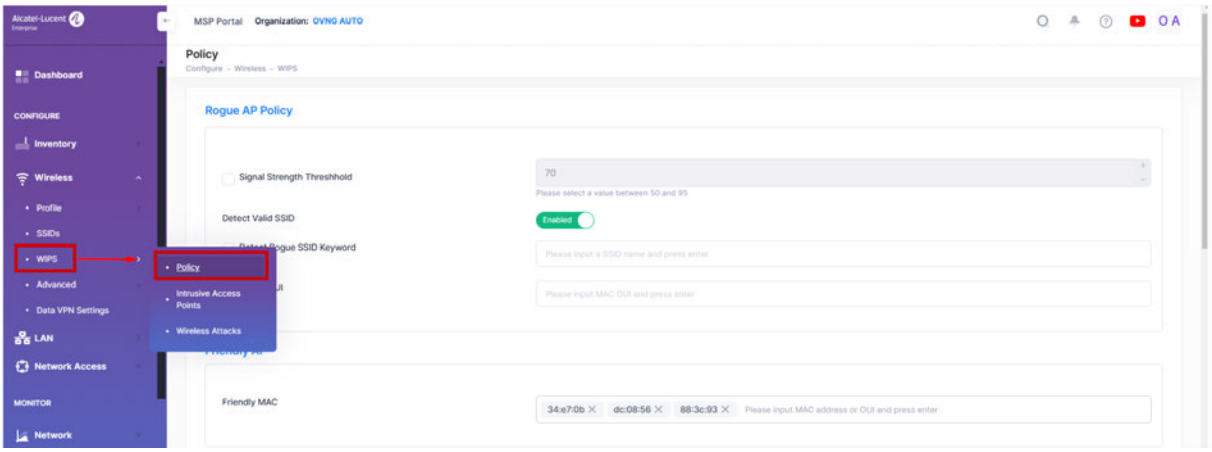
- Policy (see page 376)- Define rules for classifying rogue AP/wireless attacks and specify the measures that will be taken to react to the threats.
- Intrusive Access Points (see page 382) - Display detailed information about interfering APs and rogue APs, as well as clients connecting to the intrusive AP.
- Wireless Attacks (see page 385) - Display detailed wireless attack information.

21 Oct 2025

5.3.1 WIPS Policy

The WIPS Policy screen is used to configure policies for rogue AP and wireless attacks on the network. You can configure one overall policy for the Stellar wireless network. When an attack is detected based on the policy, the detected device is banned from the network and is displayed on the Client Blocklist (see page 858) for review.

To configure WIPS policies, navigate to the WIPS Policy screen by clicking on **Wireless > WIPS > Policy** under the “Configure” section of the OmniVista Terra Menu (see page 45). The WIPS Policy screen displays with the default settings for a Rogue AP Policy (see page 376) and Wireless Attack Detection Policy (see page 377).

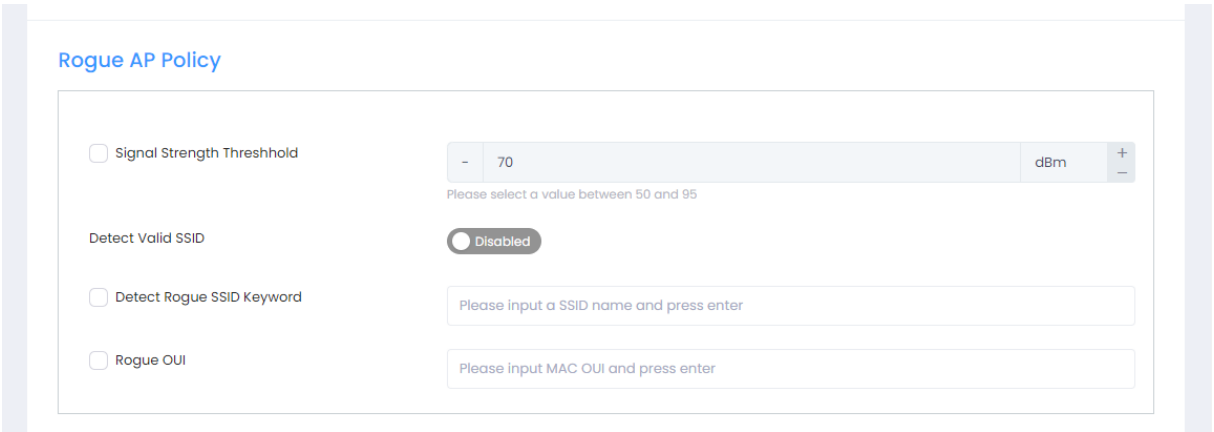


After creating a policy as described below, click on **Save** to activate the policy for the wireless network.

5.3.1.1 Creating Rogue AP Policies

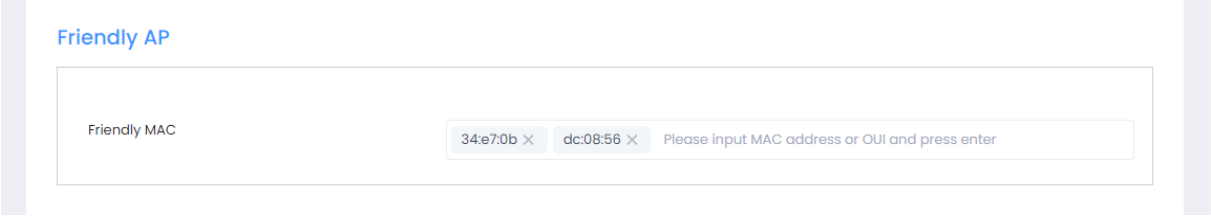
A rogue AP is an unauthorized AP connected to the wired side of the network, that is considered a security threat to the wireless network. An interfering AP is an AP seen in the wireless environment but not connected to the wired network, which is not considered a direct security threat. However, some interfering APs may have an impact on network quality and can interfere with valid client access to the network. Complete the fields below to configure rules to classify interfering APs as rogue APs.

5.3.1.1.1 Rogue AP Policy



- **Signal Strength Threshold -** If enabled, an interfering AP with greater RSSI than the setting value will be classified as rogue. By default, the RSSI matching rule is enabled and the threshold is set to -70 dbm. (Range is -50 to -90).
- **Detect Valid SSID -** If enabled, a foreign AP broadcasting the same SSID with valid Stellar network SSIDs will be classified as rogue. By default, the Detected Valid SSID rule is enabled.
- **Detect Rogue SSID Keyword -** If enabled, an interfering AP broadcasting and SSID that matches the characteristic specified by the user will be classified as rogue. The matching condition can be equal to or contain the configured keyword.
- **Rogue OUI -** If enabled, interfering APs matching this MAC OUI will be classified as rogue.

5.3.1.1.2 Friendly AP



- **Friendly MAC -** An AP classified as interfering or rogue can be trusted to be a "Friendly" AP by entering the MAC OUI of the AP - essentially creating a Vendor "Allowlist". These interfering APs will never be classified as rogue.

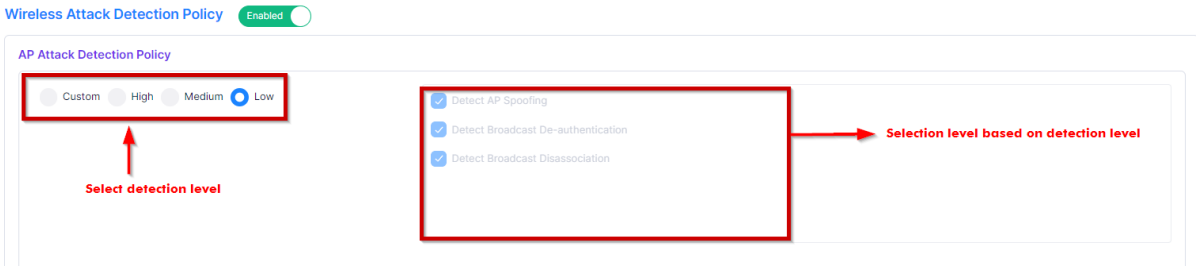
> The default MAC OUIs (34:e7:0b, dc:08:56, and 88:3C:93) are required for Stellar APs. Also note that you can have a maximum of 32 Friendly MAC OUIs/MAC addresses, including the two default Stellar AP MAC OUIs.

5.3.1.1.3 Containment Policy

- **Rogue AP Containment -** If enabled, the rogue AP containment function reduces the impact of the rogue AP on valid clients. By default, Rogue AP Containment is enabled.

5.3.1.2 Wireless Attack Detection Policy

A rogue AP is not the only threat to the wireless network, other wireless attacks can be detected and mitigated for both APs and Clients. To create Wireless Attack Detection Policies, you must enable **Wireless Detection**.



5.3.1.2.1 AP Attack Detection Policy

When configuring a policy, each detection policy can be set to one of the following levels. When a level is selected, all detection policies included in that level are displayed and selected.

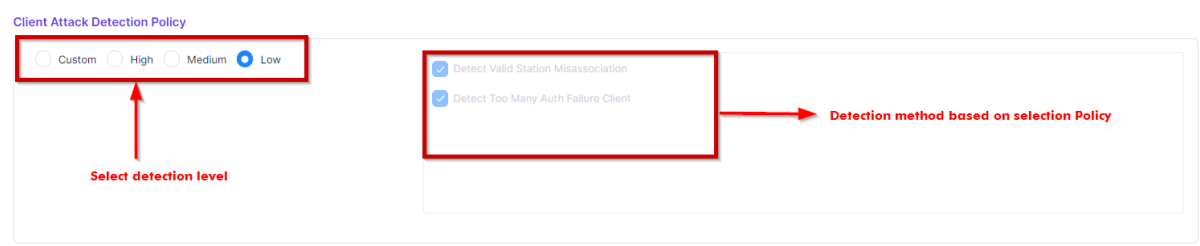
- **High -** Enables all applicable detection mechanisms, including all the options of low and medium level settings.
- **Medium -** Enables important detection mechanisms. This includes all the options of the low-level settings.
- **Low (Default) -** Enables only the most critical detection mechanisms.
- **Custom -** Enables only the selected detection mechanisms. When this level is selected all detection mechanisms are displayed. Select the ones you want to include in the policy.

An AP Attack Detection Policy detects multiple attacks originating from foreign APs. The following detection methods are available depending on the level selected.

- **Detect AP Spoofing -** An AP Spoofing attack involves an intruder sending forged frames that are made to look like they are from a valid AP.
- **Detect Broadcast De-authentication -** A de-authentication broadcast attempts to disconnect all clients in range. Rather than sending a spoofed de-authentication frame to a specific MAC address, this attack sends the frame to a broadcast address.
- **Detect Broadcast Disassociation -** By sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF), an intruder can disconnect all stations on a network for a widespread DoS.
- **Detect Adhoc Networks using VALID SSID -** If an unauthorized ad hoc network is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious ad hoc network, security breaches or attacks can occur.
- **Detect Long SSID -** Detects long SSIDs with more than 32 characters in the name.
- **Detect AP Impersonation -** In AP impersonation attacks, an AP assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for person-in-the-middle attacks, a rogue AP attempting to bypass detection, or a Honeypot attack.
- **Detect Adhoc Networks -** An ad hoc network is a collection of wireless clients that form a network among themselves without the use of an AP. If the ad hoc network does not use encryption, it may expose sensitive data to outside eavesdroppers. If a device is connected to a wired network and has bridging enabled, an ad-hoc network may also function like a rogue AP. Additionally, ad-hoc networks can expose client devices to viruses and other security vulnerabilities.

- **Detect Wireless Bridge -** Wireless bridges are normally used to connect multiple buildings together. However, an intruder could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges. In these networks, the presence of a bridge is a signal that a security problem exists.
- **Detect Null Probe Response -** A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.
- **Detect Invalid Address Combination -** In this attack, an intruder can cause an AP to transmit de-authentication and disassociation frames to its clients. Triggers that can cause this condition include the use of broadcast or multicast MAC address in the source address field.
- **Detect Reason Code Invalid of De-authentication -** De-authentication packets with invalid reason code will be classified as an attack.
- **Detect Reason Code Invalid of Disassociation -** Disassociation packets with invalid reason code will be classified as an attack.

5.3.1.2.2 Client Attack Detection Policy



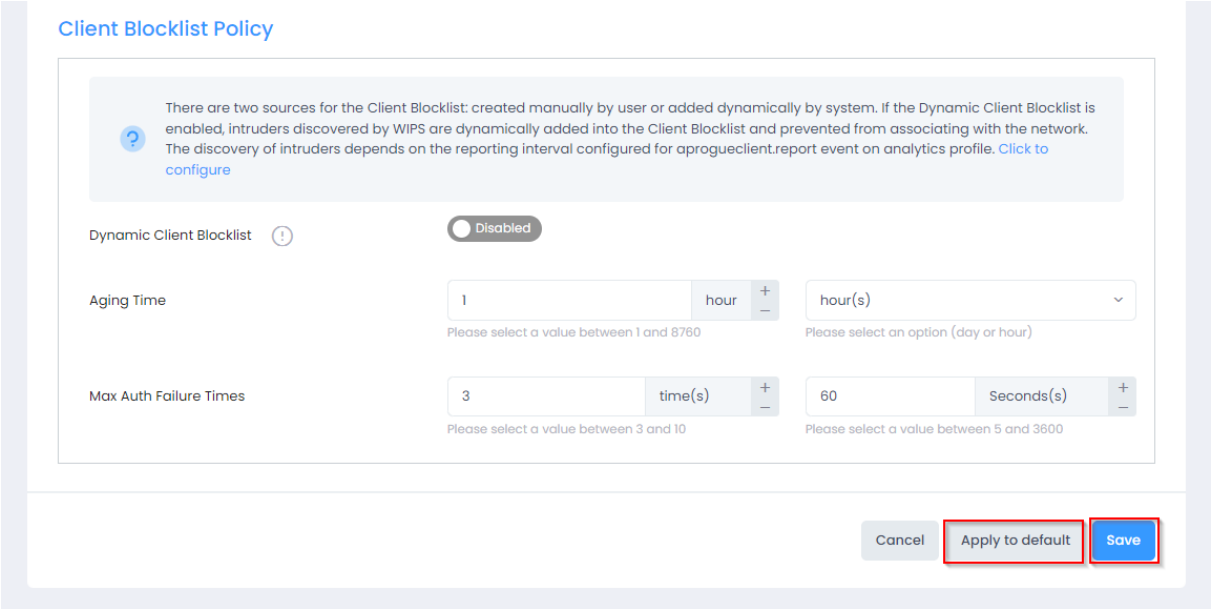
A Client Attack Detection Policy detects attacks originating from wireless clients. The following detection methods are available depending on the level selected.

- **Detect Valid Station Mis-association** - This feature does not detect attacks, but rather monitors valid wireless clients and their association within the network. Valid client mis-association is potentially dangerous to network security. The four types of mis-association monitored are:
  - **Valid Client Associated to a Rogue -** A valid client that is associated to a rogue AP
  - **Valid Client Associated to an Interfering AP -** A valid client that is associated to an interfering AP
  - **Valid Client Associated to a Honeypot AP -** A honeypot is an AP that is not valid but is using an SSID that has been designated as valid
  - **Valid Client in Ad Hoc Connection Mode -** A valid client that has joined an ad hoc network
- **Detect Omerta Attack -** Omerta is an 802.11 DoS tool that sends disassociation frames to all clients on a channel in response to data frames. The Omerta attack is characterized by disassociation frames with a reason code of 0x01. This reason code is “unspecified” and is not be used under normal circumstances.
- **Detect Unencrypted Valid Client -** A valid client that is passing traffic in unencrypted mode is a security risk. An intruder can sniff unencrypted traffic (also known as packet capture) with

software tools known as sniffers. These packets are then reassembled to produce the original message.

- **Detect 802.11 40MHZ Intolerance Setting -** When a client sets the HT capability “intolerant bit” to indicate that it is unable to participate in a 40MHz BSS, the AP must use lower data rates with all of its clients. Network administrators often want to know if there are devices that are advertising 40MHz intolerance, as this can impact the performance of the network.
- **Detect Active 802.11n Greenfield Mode -** When 802.11 devices use the HT operating mode, they can’t share the same channel as 802.11a/b/g clients. Not only can they not communicate with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.
- **Detect DHCP Client ID -** A client which sends a DHCP DISCOVER packet containing a Client-ID tag (Tag 61) which doesn't match the source MAC of the packet may be doing a DHCP denial-of-service to exhaust the DHCP pool.
- **Detect DHCP Conflict -** Clients which receive a DHCP address and continue to use a different IP address may indicate a mis-configured or spoofed client.
- **Detect DHCP Name Change -** The DHCP configuration protocol allows clients to optionally put the hostname in the DHCP Discover packet. This value should only change if the client has changed drastically (such as a dual-boot system). Changing values can often indicate a client spoofing/MAC cloning attack.
- **Detect Too Many Auth Failure Client -** Client which attempts to connect to Stellar AP but fails to pass the authentication for too many times, indicating an attack client.
- **Detect Malformed Frame-Assoc Request -** Some wireless drivers used in access points do not correctly parse the SSID information element tag contained in association request frames. A malicious association request with a null SSID can trigger a DoS or potential code execution condition on the targeted device.
- **Detect Long SSID At Client -** Detect long SSID in the wireless environment based on packets sent by clients.
- **Detect Reason Code Invalid of De-authentication -** Detect invalid De-authentication Reason Code.
- **Detect Reason Code Invalid of Disassociation -** Detect invalid Disassociation Reason Code.

5.3.1.2.3 Client Blocklist Policy



There are two sources for the Client Blocklist: created manually by the user or added dynamically by the system. If the **Dynamic Client Blocklist** option is enabled, intruders discovered by WIPS are dynamically added into the Client Blocklist and prevented from associating with the network.

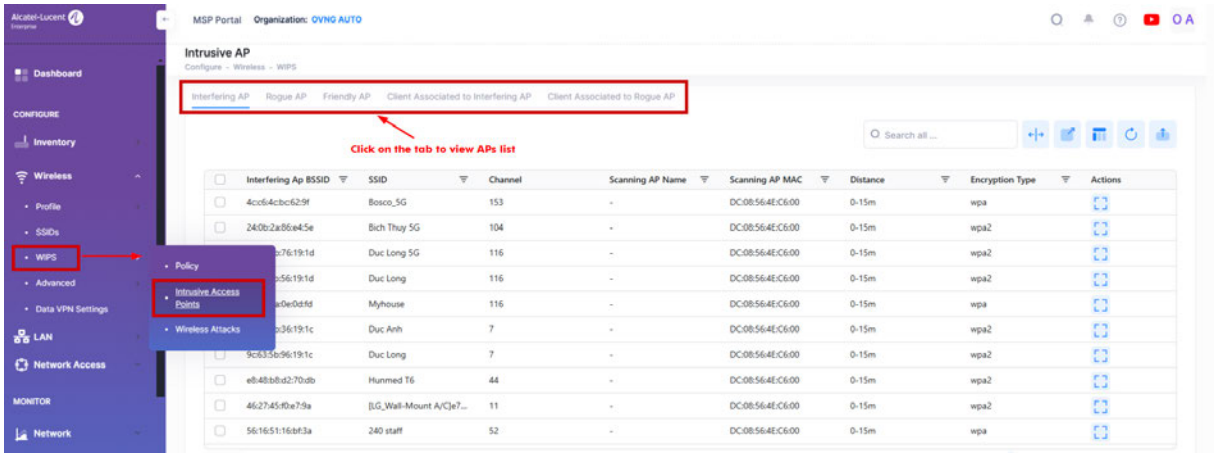
> The discovery of intruders depends on the reporting interval configured for the “aprogueclient.report” event in the OmniVista Terra Advanced Analytics (see page 775) profile.

The following detected items are added to the Client Blocklist by the system: List of Client Attack Detection, ad hoc clients, Clients associated to rogue AP.

- **Aging Time -** Aging time for the Client Blocklist. Once expired, a client will be removed from the Blocklist and allowed to be associated to the valid network until it is detected as a threat again. (Range = 1 hour to 365 days, Default = 1 Day).
- **Max Auth Failure Times -** Authentication failure times threshold. When a client fails to pass the authentication in the associated phase for too many times in a brief period, it will be classified as an attack and added into the Client Blocklist. (Range = 3 - 10 times per 5 - 3600 seconds, Default = 10 times per 60 seconds.

5.3.2 Intrusive Access Points

The WIPS Intrusive Access Points screen displays information about Intrusive APs on the network including Interfering APs (see page 382), Rogue APs (see page 383), Friendly APs (see page 383), Clients Associated to an Interfering AP (see page 383), and Clients Associated to a Rogue AP (see page 384). To access the WIPS Intrusive Access Points screen, click on **Wireless > WIPS > Intrusive Access Points** under the “Configure” section of the OmniVista Terra Menu (see page 45).



By default, the “Interfering AP” list is displayed. Click on one of the other list names to display the contents of other lists. For example, click on the “Friendly AP” tab to display the list of APs declared as “friendly”.

- A device on the "Interfering AP" list and “Rogue AP” can be added to the “Friendly AP” list by selecting the device(s) in the list, then selecting **Add to Friendly** from the “Actions” drop-down menu.
- Clients on the "Client Associated to an Interfering AP" list and the "Client Associated to a Rouge AP" list can be added to the Client Blocklist by selecting the Client(s) in the list, then selecting **Add To Client Blocklist** from the “Actions” drop-down menu.

The devices are not moved from one list to the other, but added to the other list, so that the WIPS application can maintain a history of device states.

5.3.2.1 Interfering APs

- **Interfering AP BSSID -** BSSID of the interfering AP.
- **SSID -** ESSID broadcast by the interfering AP.
- **Channel -** Working channel of radio frequency on the interfering AP.
- **Scanning AP Name -** Name of the valid AP that detected the interfering AP.
- **Scanning AP MAC -** MAC address of the valid AP that detected the interfering AP.
- **Distance -** Estimated distance between the interfering AP and the valid detecting AP.
- **Encryption Type -** Encryption method of ESSID broadcast by the interfering AP.
- **Attached Clients -** Clients associated to the interfering AP.

- **Signal Strength -** RSSI of the interfering AP.
- **Last Detected Time -** The latest time that the interfering AP was seen by the valid AP.

5.3.2.2 Rogue APs

- **Rogue AP BSSID -** BSSID of the rogue AP.
- **SSID -** ESSID broadcast by the rogue AP.
- **Channel -** Working channel of the radio frequency on the rogue AP.
- **Scanning AP Name -** Name of the valid AP that detected the rogue AP.
- **Scanning AP MAC -** MAC address of the valid AP that detected the rogue AP.
- **Distance -** Estimated distance between the rogue AP and the valid detecting AP.
- **Encryption Type -** Encryption method of ESSID broadcast by the rogue AP.
- **Attached Clients -** Clients associated to the rogue AP.
- **Signal Strength -** RSSI of the rogue AP.
- **Last Detected Time -** The latest time that the rogue AP was seen by the detecting AP.
- **Rogue Reason -** Indicates the reason for classifying the foreign AP as a rogue AP:
  - Signal Strength is Too Strong, Reducing Network Performance
  - Channel is Switching Too Often
  - Broadcasting Conflicted SSID, Misleading User Connection
  - Matching the Keyword of Suspected SSID
  - Matching the Suspected MAC OUI

5.3.2.3 Friendly APs

- **Friendly AP BSSID -** BSSID of the friendly AP.
- **SSID -** ESSID broadcasting by the friendly AP.
- **Channel -** Working channel of the radio frequency on the friendly AP.
- **Scanning AP Name -** Name of the valid AP that detected the friendly AP.
- **Scanning AP MAC -** MAC address of the valid AP that detected the friendly AP.
- **Distance -** Estimated distance between the friendly AP and the valid detecting AP.
- **Encryption Type -** Encryption method of ESSID broadcast by the friendly AP.
- **Attached Clients -** Clients associated to the friendly AP.
- **Signal Strength -** RSSI of the friendly AP.
- **Last Detected Time -** The latest time that the friendly AP was seen by the detecting AP.

5.3.2.4 Clients Associated to an Interfering AP

- **Interfering Client MAC -** MAC address of the interfering client.
- **In Blocklist -** Indicates whether the client was added into the Blocklist automatically and banned from accessing the network.

- **SSID -** ESSID to which the interfering client is associated.
- **Channel -** Working channel of the interfering client.
- **Interfering AP BSSID** - BSSID of the interfering AP to which the client is associated.
- **Distance -** Distance between the interfering client and the detecting AP.
- **Encryption Type -** Encryption method of the SSID to which the interfering client is associated.
- **Signal Strength -** RSSI of the interfering client.
- **Last Detected Time -** The latest time that the interfering client was seen by the detecting AP.

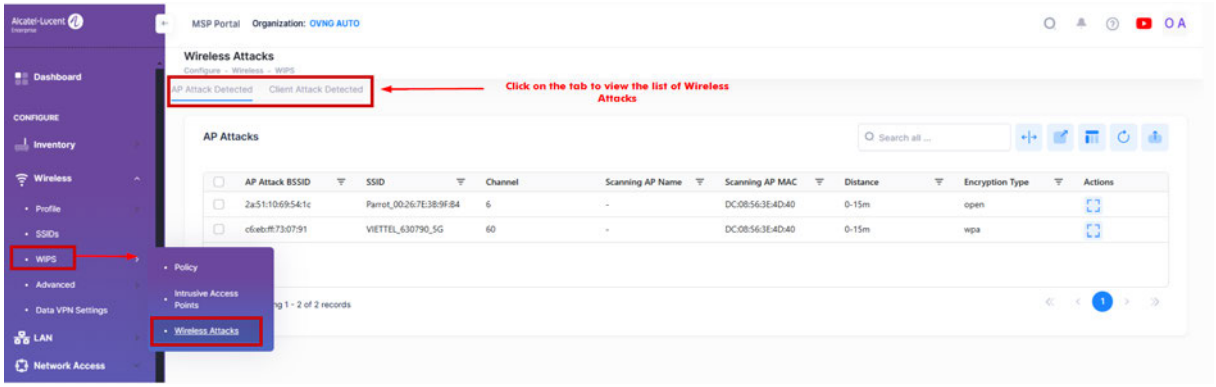
5.3.2.5 Clients Associated to a Rogue AP

- **Rogue Client MAC -** MAC address of the rogue client.
- **In Blocklist -** Indicates whether the client was added into the Blocklist automatically and banned from accessing the network.
- **SSID -** ESSID to which the rogue associated.
- **Channel -** Working channel of the rogue client.
- **Rogue AP BSSID** - BSSID of the rogue AP to which the client is associated.
- **Distance -** Distance between the rogue client and the detecting AP.
- **Encryption Type -** Encryption method of the SSID to which the rogue client is associated.
- **Signal Strength -** RSSI of the rogue client.
- **Last Detected Time -** The latest time that the rogue client was seen by the detecting AP.

21 Oct 2025

5.3.3 Wireless Attacks

The WIPS Wireless Attacks Screen displays information about wireless attacks on the network including AP attacks (see page 385) and Client attacks (see page 386). To access the WIPS Wireless Attacks screen, click on **Wireless > WIPS > Wireless Attacks** under the “Configure” section of the OmniVista Terra Menu (see page 45).



By default, the “AP Attack Detected” list is displayed. Click on **Client Attack Detected** to display that list.

- Devices in the “AP Attack Detected” list can be added to the “Friendly AP” list by selecting the device(s) in the list, then selecting **Add to Friendly** from the “Actions” drop-down menu.
- Devices in the “Client Attack Detected” list can be added to the Client Blocklist by selecting the device(s) in the list, then selecting **Add to Client Blocklist** from the “Actions” drop-down menu.

The devices are not moved from one list to the other, but added to the other list, so that the WIPS application can maintain a history of device states.

5.3.3.1 AP Attack Detected

- **Channel -** Working channel of the radio frequency of the attack AP.
- **Distance -** Estimated distance between the attack AP and the valid detecting AP.
- **Encryption Type -** Encryption method of the ESSID broadcast by the attack AP.
- **Signal Strength -** RSSI of the attack AP.
- **Last Detected Time -** The latest time that the attack AP was seen by the detecting AP.
- **Attack AP BSSID -** BSSID of the attack AP.
- **SSID -** ESSID broadcast by the attack AP.
- **Scanning AP Name -** Name of the valid AP that detected the attack AP.
- **Scanning AP MAC -** MAC address of valid AP that detected the attack AP.
- **Attached Clients -** Clients associated to the attack AP.
- **Attack Detection -** The Attack Detection Policy used (e.g., Detect Valid Station Misassociation).

5.3.3.2 Client Attack Detected

- **Channel** - Working channel of the attack client.
- **Distance -** Distance between the attack client and the detecting AP.
- **Encryption Type -** Encryption method of the SSID to which the attack client is associated.
- **Signal Strength -** RSSI of the attack client.
- **Last Detected Time -** The latest time that the attack client was seen by the detecting AP.
- **Attack Client MAC -** MAC address of the attack client.
- **In Blocklist -** Whether or not the client is in the Blocklist.
- **SSID -** ESSID to which the attack client is associated.
- **Attack AP MAC -** MAC address of the attack AP to which the client is associated.
- **Attack Detection -** The Attack Detection Policy used (e.g., Detect Valid Station Misassociation).

See WIPS Top N Attacks (see page 823) Online help for more information.

21 Oct 2025

5.4 Advanced

- **External Engines** (see page 388) - The External Engines application is used to declare server configurations for Aeroscout, Stellar Asset Tracking, Wifi RTLS, and Advanced Analytics. OmniVista Terra can integrate with an Aeroscout, OmniVista Terra WiFi RTLS, and OmniAccess Stellar Asset Tracking Server to provide Location Based Services (LBS); OmniVista Advanced Analytics to provide advanced analytics data to OmniVista Terra and above installations. BLE Location Service is a pre-configured service dedicated to OmniAccess Stellar Asset Tracking.
- **Certificates** (see page 394)- The Certificates application is used to configure/upload a Web Server/ External Portal Server Certificate File. This Certificate File is used to establish a secure connection between OmniVista Terra and APs when using the Web UI Device Management Tool as well as a secure connection to an External Portal Server. This application is also used to upload a Local LDAP Certificate File, which is used to establish a secure connection between an AP and a Local LDAP Server.
- **External Captive Portal** (see page 409) - The External Captive Portal Configuration file is used to provide secure communication between APs and an External Captive Portal Server. The management of external configuration files is done through Access Role Profiles. When the Captive Portal option for the Access Role Profile is set to “External”, you can specify the name of an External Captive Portal Configuration file to use. Traffic assigned to the profile will be redirected to the External Captive Portal Server identified in the configuration file.

21 Oct 2025

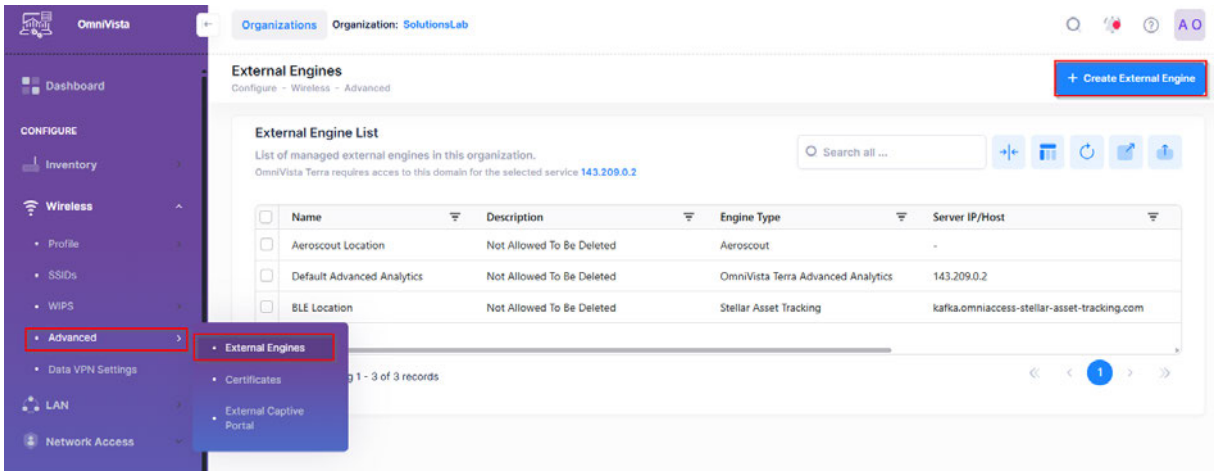
5.4.1 External Engines

The External Engines application is used to declare server configuration profiles for Aeroscout, Stellar Asset Tracking, Wifi RTLS, and Advanced Analytics engines. OmniVista Terra can integrate with an Aeroscout, OmniVista Terra WiFi RTLS, and OmniAccess Stellar Asset Tracking Server to provide Location Based Services (LBS); OmniVista Advanced Analytics to provide advanced analytics data to OmniVista Terra. BLE Location Service is a pre-configured service dedicated to OmniAccess Stellar Asset Tracking.

The Server Profile is configured for Access Points (APs) at the AP Group level using the AP Group Screen (see page 309). An Access Point retrieves the server configuration profile to use from the AP Group to which the AP belongs. Each AP Group is associated with a Provisioning Configuration (see page 313). APs that are members of the AP Group utilize the Provisioning Configuration to boot up and get a basic configuration. The associated Provisioning Configuration is where the name of the External Engine Server Profile to use is defined.

> An External Engine Server Profile is an Organization-level entity. The Server Profile is created in an Organization with a name that is unique across the entire Organization. You can not create two Server Profiles with the same name in the same Organization.

To manage the Server Profiles for External Engines, navigate to the External Engines screen by clicking on **Wireless > Advanced > External Engines** under the “Configure” section of the OmniVista Terra Menu (see page 45).



The External Engines screen displays a list of server configuration profiles and is used to create (see page 388), edit (see page 391), and delete (see page 393)profiles.

5.4.1.1 Creating a Server Profile

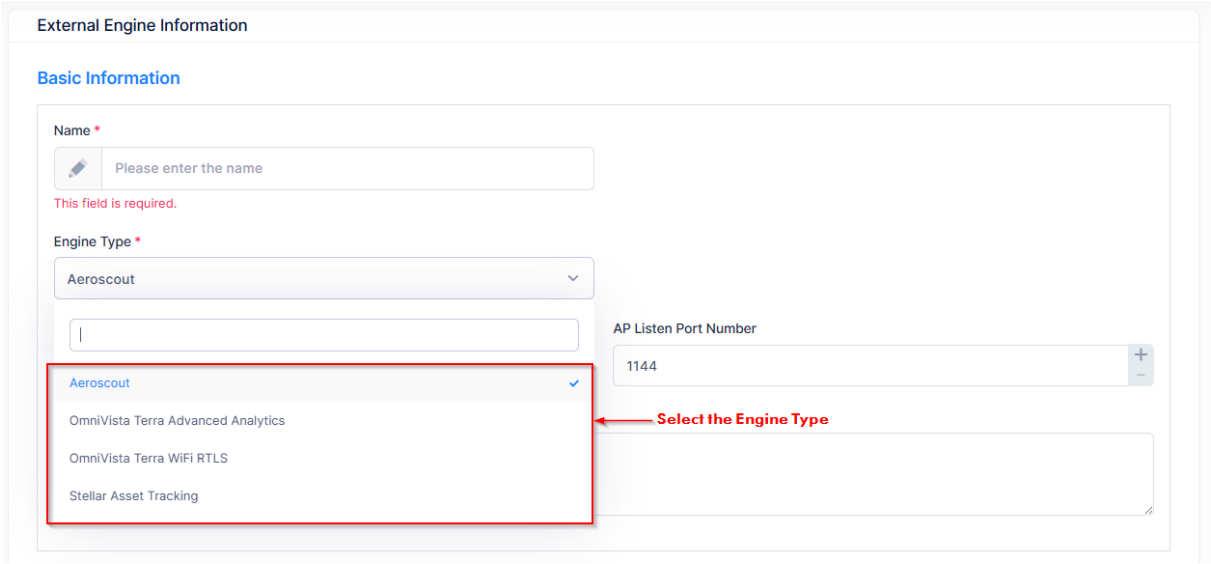
There are three default Server Profiles available:

- **Aeroscout Location** - Default Server Profile for the Aeroscout server.
- **Default Advanced Analytics** - Default Server Profile for OmniVista Terra Advanced Analytics server.

- **BLE Location** - Default Server Profile for Stellar Asset Tracking server.

You can use one of the default profiles or create a new one. Note that you can edit certain attribute values of the default profiles.

To create a new, customized Server Profile, click on **Create External Engine** on the External Engines screen to open the Create External Engine form. Assign the profile a name, then select the External Engine that you want to use for the profile from the Engine Type drop-down list.



Complete the fields as described below, then click on **Create External Engine** to create the server profile. The fields will vary depending on the Engine Type selected (for example, Aeroscout, Stellar Asset Tracking).

5.4.1.1.1 Basic Information

- **Name -** The name of the Server Profile.
- **Engine Type -** Select the application Location Engine from the drop-down:
  - **Aeroscout** (see page 389)**-** APs integrate with the Aeroscount location engine.
  - **OmniVista Terra Advanced Analytics** (see page 390) **-** APs integrate with Advanced Analytics for OmniVista Terra (Analytics Only Mode (see page 388) APs).
  - **OmniVista Terra WiFi RTLS** (see page 390) **-** APs integrate with OmniVista Terra to provide Wi-Fi RTLS Services.
  - **Stellar Asset Tracking** (see page 391) **-** APs integrate with Asset Tracking to provide BLE Location Based Services.
- **Description -** An optional description for the Server Profile.

5.4.1.1.2 Aeroscout

- **Server IP/Host -** The IP address or Host Name of the Aeroscout Engine.
- **AP Listen Port Number -** The AP Listen Port (Range = 0 - 65535, Default = 1144).
- **Wi-Fi Location**

- **Minimal Reporting Interval -** The interval (in seconds) for APs to report wireless scanning data to the Location Engine for location calculation (Default 30).
- **Un-Associated Clients -** If enabled (On), when a client report is started, unassociated client information will be sent to the Location Engine. If disabled (Off), only associated client information will be sent.

5.4.1.1.3 OmniVista Terra Advanced Analytics

- **Server IP/Host -** The IP address is set to 143.209.0.2 (Kafka VPN host) and is not configurable.
- **Server Port Number -** The server port number is set to 31123 (Kafka VPN port) and is not configurable.
- **QoE Events -** Select the QoE Events data that you want the AP to send to OmniVista Terra. By default, all events are selected.
- **Upload Interval -** Set the interval, in minutes, for uploading each type of QoE Event Data to OmniVista Terra. Range and default values are as follows:
  - **User Info -** Information about users accessing the wireless network (e.g., association, authentication, roaming, DHCP). (Range = 1 - 15, Default = 5)
  - **Short AP Info -** AP information (e.g., AP uptime, AP downtime). (Range = 1 - 15, Default = 3)
  - **AP Info -** Major AP information (e.g., AP CPU status, Memory status). (Range = 1 - 15, Default = 5)
  - **AP Radio Info -** AP wireless radio information (e.g., band, channel, power). (Range = 1 - 15, Default = 5)
  - **AP WLAN Info -** AP WLAN information (e.g., SSID info). (Range = 1 - 15, Default = 5)
  - **AP Channel Info -** AP Channel information (e.g., channel number, bandwidth). (Range = 15 - 60, Default = 5)
  - **AP Channel Change -** AP Channel change event update (Instant). Instant means that the AP will send the report every 30 seconds.
  - **AP Rogue Info -** AP rogue information (e.g., interfering APs, rogue APs). (Range = 15 - 60, Default = 60)
  - **AP Neighbor Info -** Detected AP neighbor information. (Range = 15 - 60, Default = 60)
  - **Rogue Client Info** - Rogue client information (Range = 15 - 60, Default = 60)
  - **Wired User Info -** Information about users accessing the Internet (e.g., website URL). (Range = 1 - 15, Default = 5)

5.4.1.1.4 OmniVista Terra WiFi RTLS

Note that creating an OmniVista Terra WiFi RTLS Location Engine profile is a pre-requisite for using the Location Applications (see page 943) (Wi-Fi Heatmap, Client Density). The Location Engine server profile must also be assigned to the Provisioning Configuration (see page 313) that is associated with the AP Group to which the AP is a member.

- **Server IP/Host -** The IP address is set to 143.209.0.2 (Kafka VPN host) and is not configurable.
- **Server Port Number -** The server port number is set to 31123 (Kafka VPN port) and is not configurable.
- **SSL/TLS** - When enabled (On), Secure Socket Layer and Transport Layer Security encryption is used to communicate with the Location Engine. (Default = On)
  - **Certificate** - If the SSL/TLS option is On, select an existing Certificate from the drop-down menu or click on **Create Stellar WiFi RTLS Certificate** to upload another certificate to use.
- **Upload Interval -** The interval (in seconds) for APs to report scanning data to the Location Engine for location calculation (Range = 15 - 255, Default = 30).
- **Un-Associated Clients -** If enabled (On), when a client report is started, unassociated client information will be sent to the Location Engine. If disabled (Off), only associated client information will be sent.

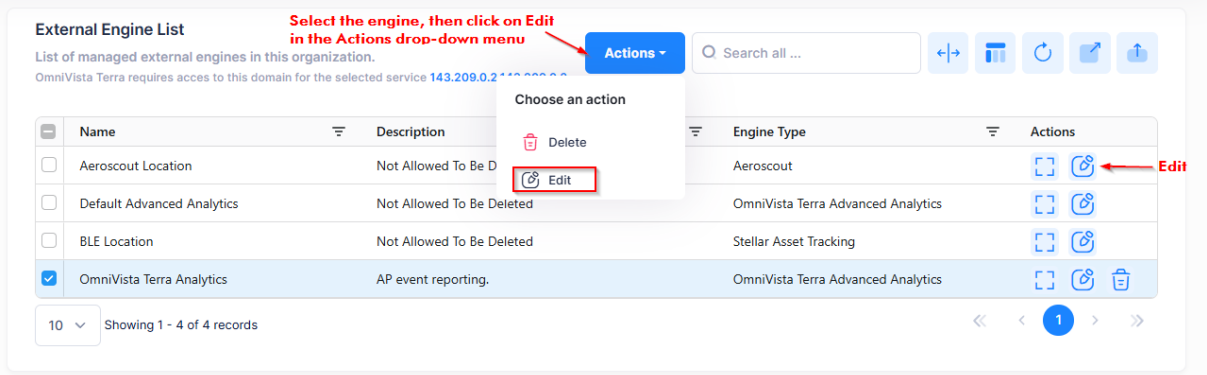
5.4.1.1.5 Stellar Asset Tracking

- **Server IP/Host -** The IP address or Host Name of the Location Engine (Default = 143.209.0.2, the IP address of the Kafka VPN host).
- **Server Port Number -** The server port number (Range = 0 - 65535, Default = 9093).
- **BLE Location**
  - **Upload Interval -** The interval (in seconds) for APs to report BLE scanning data to the Location Engine for location calculation (Range = 1 - 30, Default = 5). Note that the Upload Interval **must** be set to 2 seconds for Stellar Asset Tracking.
  - **Scanning Type Allowlist -** Select the BLE tag beacon format(s) that will be reported to the BLE Location Server (iBeacon, Eddystone-URL, Eddystone-UID, KonLoc, KonTLM, iBeaconPB, KonSP, Unknown RSSI, Unknown RSSI & Raw Data). Note that the following types are selected by default for Stellar Asset Tracking: iBeacon, iBeaconPB, KonLoc, and KonSP. You can select multiple types from the drop-down.
  - **RSSI Format -** Specify the BLE tag RSSI format reported to the Location Server.
    - **Average -** Report the average BLE tag RSSI calculated by all values scanned in an upload interval.
    - **List -** Report all the BLE tag RSSI values scanned in an upload interval.

5.4.1.2 Editing a Server Profile

You can select a Server Profile to edit by using one of the following methods:

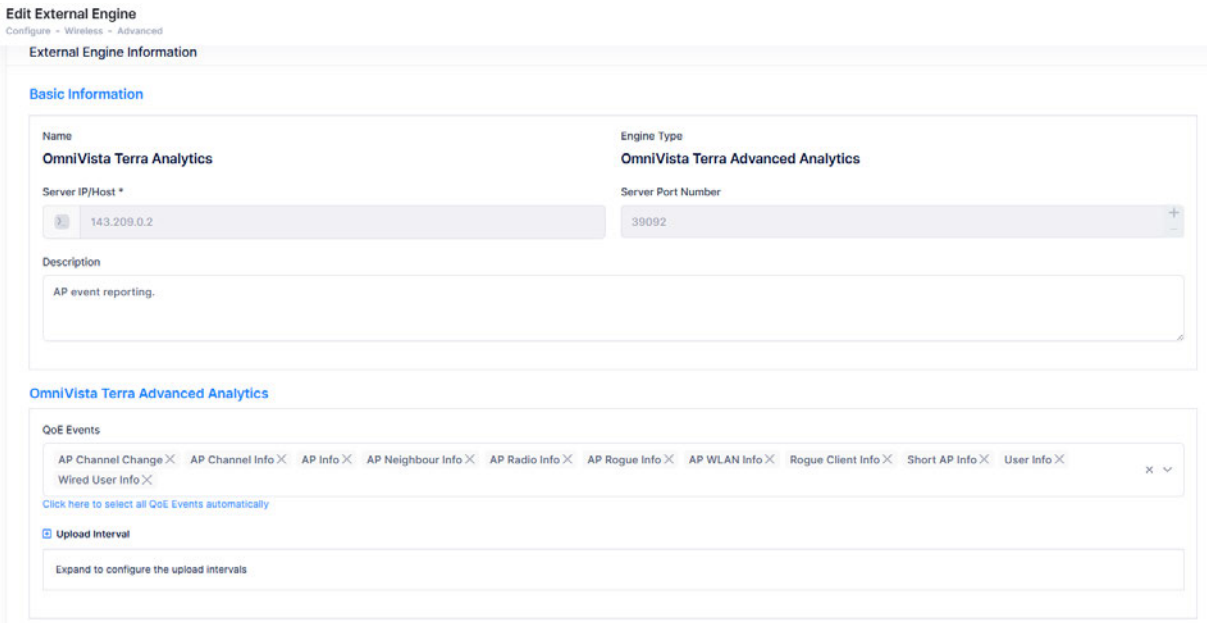
- Click on the pencil icon under the “Actions” column for the profile entry that you want to edit.
- Select the profile to edit, then click on **Edit** in the **Actions** drop-down menu.



You can also select one of the default profiles (Aeroscout Location, Default Advanced Analytics, BLE Location) to edit. The Edit External Engine screen appears.

Note that the following profile attributes are not configurable through the Edit External Engine screen:

- Basic Information for default profiles (Name, Engine Type, Server IP/Host, Server Port Number, and Description).
- Name and Engine Type for user-defined profiles configured with Aeroscout or Stellar Asset Tracking as the Engine Type.
- Name, Engine Type, Server IP/Host, and Server Port Number for user-defined profiles configured with OmniVista Terra Advanced Analytics or OmniVista Terra WiFi RTLS as the Engine Type.

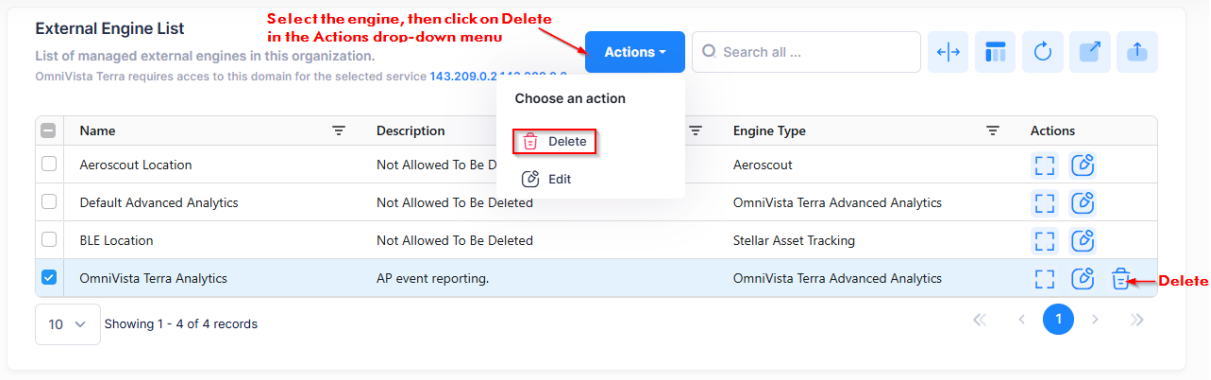


Edit the Server Profile fields as described here (see page 388), then click on **Save**. The updated profile configuration is applied to all AP Groups (see page 309) associated with the Provisioning Configuration (see page 313) to which the AP Group is linked.

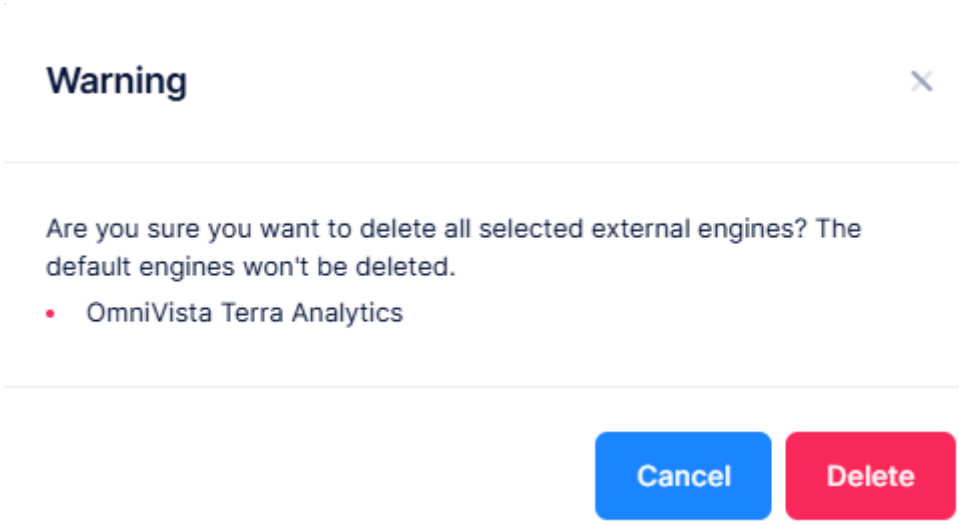
5.4.1.3 Deleting a Server Profile

You can select a Server Profile to delete by using one of the following methods:

- Click on the Delete icon under the “Actions” column for the profile entry that you want to delete.
- Select the profile to delete, then click on **Delete** in the **Actions** drop-down menu.



When the Confirmation Prompt appears, click on **Delete** to remove the profile.



You cannot delete the following profile types:

- A Server Profile that is associated with a Provisioning Configuration.
- Default Server Profiles (Aeroscout Location, Default Advanced Analytics, BLE Location).

21 Oct 2025

5.4.2 Certificates

The Certificates screen displays information and is used to create/upload the following certificates:

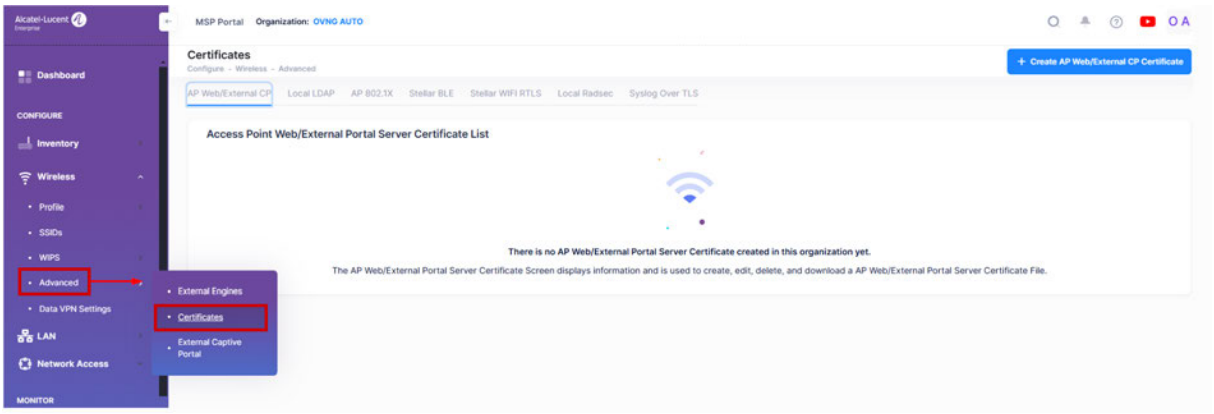
- **Web Server/External Portal Server Certificate** - Used to establish a secure connection between OmniVista Terra and APs when using the Web UI Device Management Tool as well as a secure connection to an External Portal Server.
- **Local LDAP Certificate** - Used to establish a secure connection between an AP and a Local LDAP Server.
- **802.1X Client Certificate** - Used to establish a secure connection between an AP and an OmniSwitch.
- **Stellar BLE Certificate** - Used to establish a secure connection between an AP and a BLE destination server for Asset Tracking.
- **Stellar WiFi RTLS Certificate** - Used to establish a secure connection between an AP and an external server to provide real-time location data.
- **Local RadSec** - Used to establish a secure connection between an AP and a local, third-party RADIUS Server that uses RadSec (RADIUS-over-TLS).
- **Syslog Over TLS** - Used to establish a secure connection between an AP and a remote Syslog Server

Once the certificates are created/uploaded, they are applied to Access Points at the AP Group level using the AP Group screen (see page 309). An Access Point retrieves the certificates to use from the AP Group to which the AP belongs. Each AP Group is associated with a Provisioning Configuration (see page 313). APs that are members of the AP Group utilize the Provisioning Configuration to boot up and get a basic configuration. The associated Provisioning Configuration is where the certificates to use are specified.

> A Certificate file is an Organization-level entity. The Certificate is created in an Organization with a name that is unique across the entire Organization. You can not create two Certificates with the same name in the same Organization.

To manage the Certificates configuration, navigate to the Certificates screen by clicking on **Wireless > Advanced > Certificates** under the “Configure” section of the OmniVista Terra Menu (see page 45).

The Certificates screen is where you can view existing certificate information (see page 401), create/upload (see page 395), edit, (see page 400)and delete (see page 401)certificates. The screen provides a separate tab for each of the six types of certificates. Click on the desired tab to view existing certificates and/or create new ones.



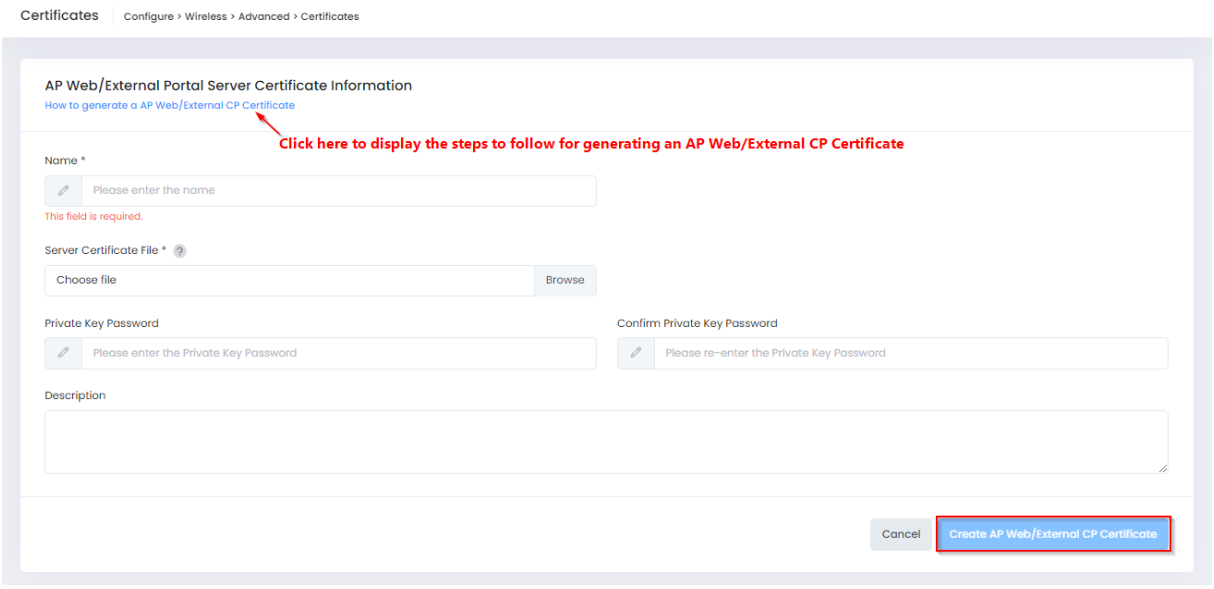
5.4.2.1 Creating a Certificate

Click on one of the tabs shown to select which certificate you want to create and/or upload.

- AP Web/External Portal Server (see page 395)
- Local LDAP
- AP 802.1X (see page 397)
- Stellar BLE (see page 397)
- Stellar WiFi RTLS (see page 398)
- Local RadSec (see page 399)
- Syslog Over TLS (see page 400)

5.4.2.1.1 Creating an Access Point Web/External Portal Server Certificate

Select the Access Point Web/External Portal Server tab on the Certificates screen, then click on **Create AP Web/External Portal Server Certificate** to open the following screen to define the certificate information:



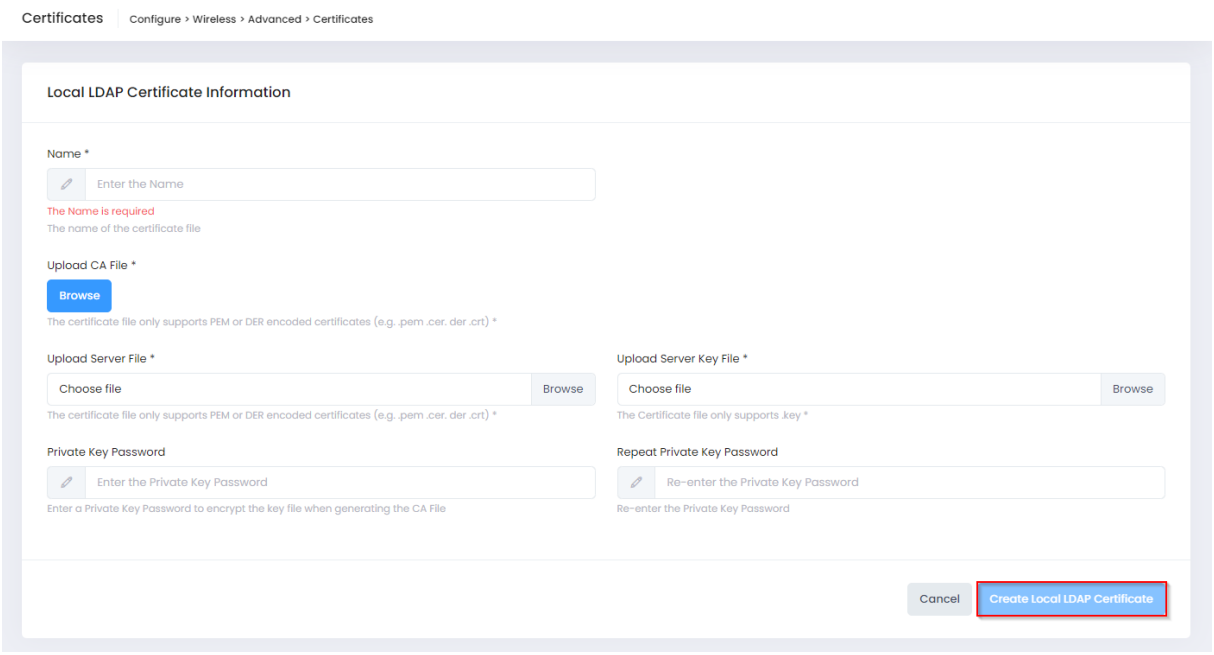
Complete the fields as described below, then click on Create AP Web/External Portal Server Certificate when you are finished creating/uploading the certificate.

- **Name -** The name of the certificate file.
- **Server Certificate File** - Click on **Browse** to locate the PEM file to upload. Make sure that the certificate file is in UNIX format.
- **Private Key Password -** The Private Key Password to use when generating the key file.
- **Confirm Private Key Password** - Re-enter the password.
- **Description -** Enter a description for the certificate file.

Important Note: APs only support certificates based on FQDN, not IP Address. When generating the CSR file, you must match the "CN" field to the URL "mywifi.al-enterprise.com".

5.4.2.1.2 Uploading a Local LDAP Certificate

Select the Local LDAP tab on the Certificates screen, then click on **Create Local LDAP Certificate** to open the following screen to define the certificate information:



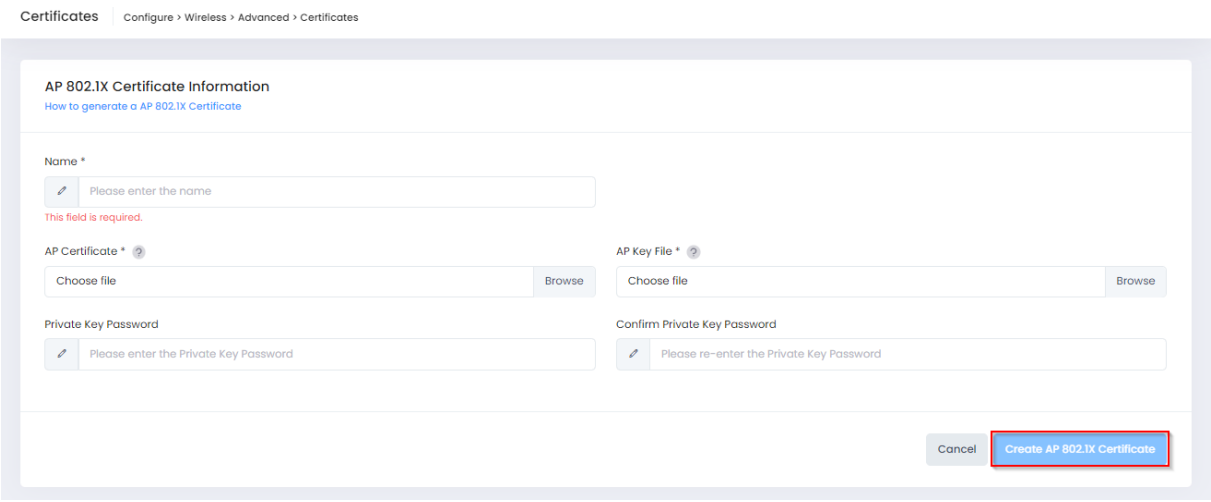
Complete the fields as described below, then click on **Create Local LDAP Certificate** when you are finished uploading the certificate.

- **Name -** Enter a Name for the Certificate.
- **Upload CA File -** Click on **Browse** to locate and import the LDAP Server's CA Certificate (PEM or DER encoded certificates only).
- **Upload Server File -** Click on **Browse** to locate and import the AP Certificate File (PEM or DER encoded certificates only).

- **Upload Server Key File -** Click on **Browse** to locate and import the AP Certificate Private Key File.
- **Private Key Password -** Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Repeat Private Key Password** - Re-enter the Private Key password.

5.4.2.1.3 Uploading an 802.1X Client Certificate

Select the AP 802.1X tab on the Certificates screen, the click on **Create AP 802.1X Certificate** to open the following screen to define the certificate information:



Complete the fields as described below, then click on **Create AP 802.1X Certificate** when you are finished uploading the certificate.

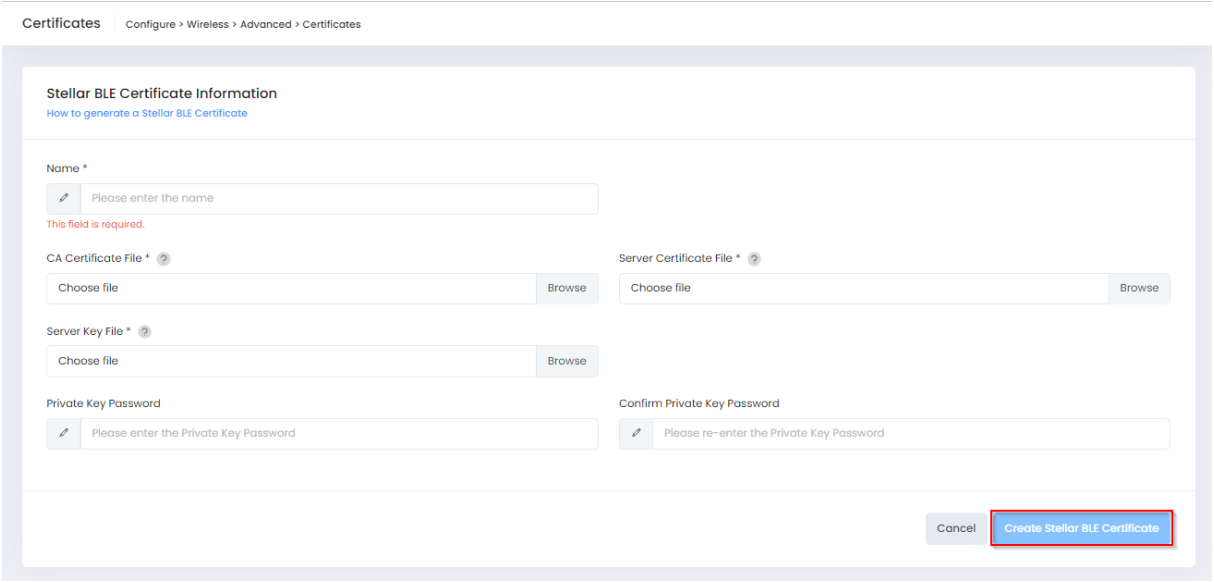
- **Name** - Enter a Name for the Certificate.
- **AP Certificate** - Click on **Browse** to locate and import the 802.1X Client CA Certificate (PEM or DER encoded certificates only).
- **AP Key File** - Click on **Browse** to locate and import the AP Certificate Private Key File (.key certificates only).
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Confirm Private Key Password** - Enter the Private Key Password again.

5.4.2.1.4 Uploading a Stellar BLE Certificate

The Stellar BLE data reporting channel to any Asset Tracking application uses Kafka. However, the built-in common device certificate on the AP allows communication only with Stellar AP Asset Tracking solutions. You can now upload a custom device certificate to the AP that will support sending BLE data to third-party Asset Tracking applications.

Refer to Stellar BLE Data Format (see page 403) for information about the data format used to send BLE messages to third-party Asset Tracking applications.

To upload a device certificate, select the Stellar BLE tab on the Certificates screen, then click on **Create Stellar BLE Certificate** to open the following screen to define the certificate information:



Complete the fields as described below, then click on **Create Stellar BLE Certificate** when you are finished uploading the certificate.

- **Name** - Enter a Name for the Certificate.
- **CA Certificate File** - Click on Browse to locate and import the Stellar BLE CA Certificate (PEM or DER encoded certificates only).
- **Server Certificate File** - Click on **Browse** to locate and import the AP Certificate File (PEM or DER encoded certificates only).
- **Server Key File** - Click on Browse to locate and import the AP Certificate Private Key File (.key certificates only).
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Confirm Private Key Password** - Enter the Private Key Password again.

5.4.2.1.5 Uploading a Stellar WiFi RTLS Certificate

The Stellar WiFi RTLS data reporting channel uses Kafka. However, the built-in common device certificate on the AP allows communication only with the OmniVista Terra 10 Stellar WiFi engine. You can now upload a custom device certificate to the AP that will support sending WiFi RTLS data to third-party RTLS applications.

Refer to Stellar WiFi RTLS Data Format (see page 405) for information about the data format used to send RTLS messages to third-party RTLS applications.

To upload a device certificate, select the Stellar WIFI RTLS tab on the Certificates screen, then click on **Create Stellar WIFI RTLS Certificate** to open the following screen to define the certificate information:

Complete the fields as described below, then click on **Create Stellar WIFI RTLS Certificate** when you are finished uploading the certificate.

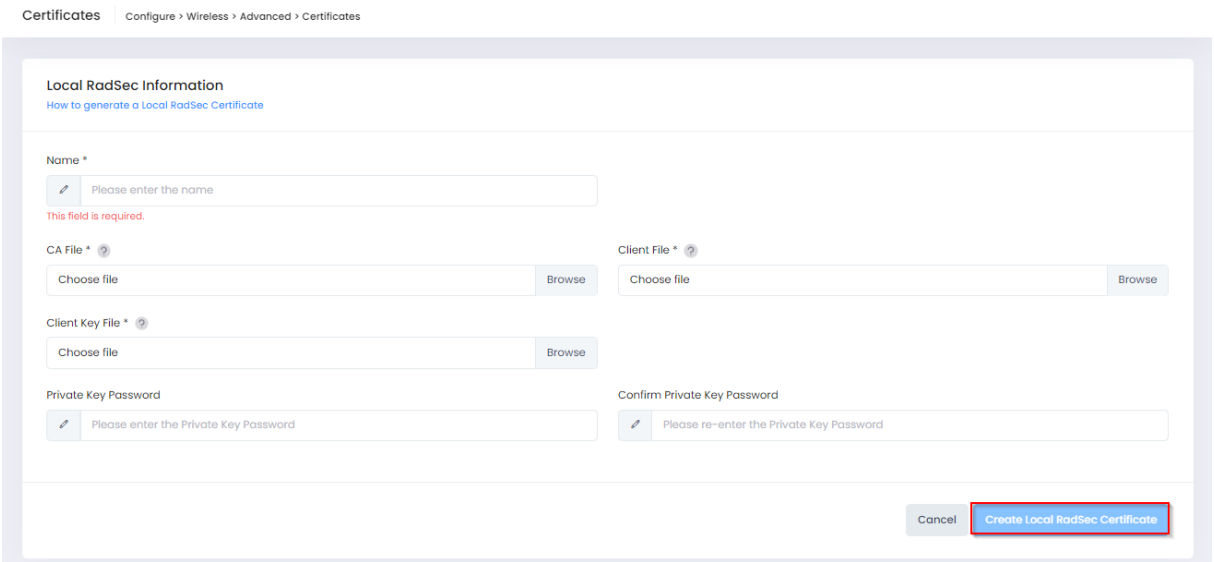
- **Name** - Enter a Name for the Certificate.
- **CA Certificate File** - Click on Browse to locate and import the Stellar WIFI RTLS CA Certificate (PEM or DER encoded certificates only).
- **Server Certificate File** - Click on **Browse** to locate and import the AP Certificate File (PEM or DER encoded certificates only).
- **Server Key File** - Click on Browse to locate and import the AP Certificate Private Key File (.key certificates only).
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Confirm Private Key Password** - Enter the Private Key Password again.

5.4.2.1.6 Uploading a Local RadSec Certificate

An AP can communicate as a RadSec client with a local RADIUS Server that uses RadSec (RADIUS-over-TLS). To establish a secure connection between an AP RadSec client and the local RADIUS Server:

- Upload a RadSec Certificate to the AP (refer to Local RadSec Certificate (see page 407) for more information).
- Enable TLS on the local RADIUS Server.

To upload a RadSec Certificate, select the Local RadSec tab on the Certificates screen, then click on **Create Local RadSec Certificate** to open the following screen to define the certificate information:



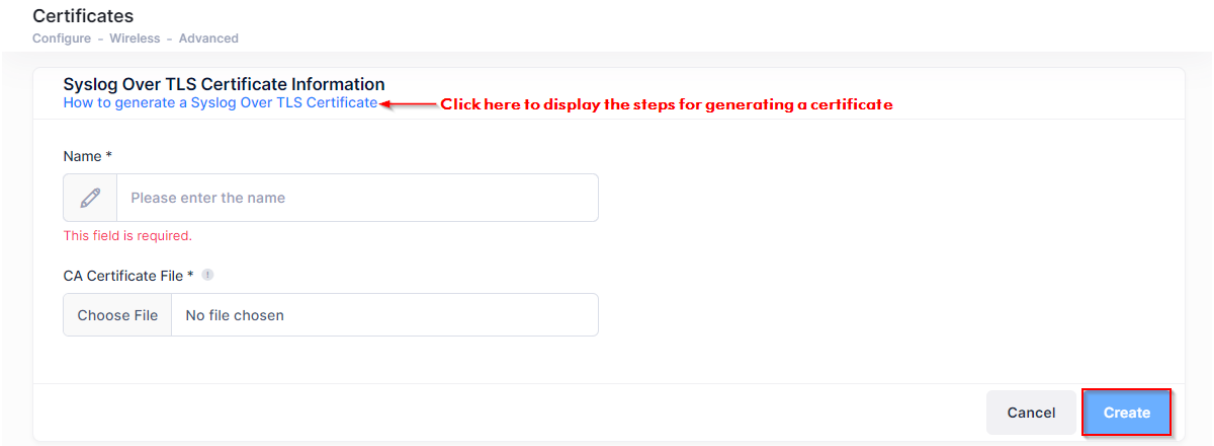
Complete the fields as described below, then click on **Create** when you are finished creating/uploading the certificate.

- **Name** - Enter a Name for the Certificate.

- **CA File** - Click on **Browse** to locate and import the RadSec Server CA Certificate (PEM or DER encoded certificates only). The CA Certificate file is used to verify RadSec and is added to the trust store for the AP.
- **Client File** - Click on **Browse** to locate and import the AP Certificate File (PEM or DER encoded certificates only).
- **Client Key File** - Click on the **Browse** and locate the AP Certificate Private Key File (.key certificates only).
- **Private Key Password** - Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Confirm Private Key Password** - Enter the Private Key Password again.

5.4.2.1.7 Uploading a Syslog Over TLS Certificate

The Syslog Over TLS Certificate is used when configuring remote logging of AP events over TLS for an AP Group (see page 309). To upload a Syslog Over TLS Certificate, select the Syslog Over TLS tab on the Certificates screen, then click on **Create Syslog Over TLS Certificate** to open the following screen to define the certificate information.



Complete the fields as described below, then click on **Create**.

- **Name** - Enter a Name for the Certificate.
- **CA Certificate File** - Click on **Choose File** and locate the Syslog Over TLS CA Certificate.

5.4.2.2 Editing a Certificate

The only attribute you can edit is the description of a Web Server/External Portal Server Certificate (Local LDAP certificates cannot be edited). Click on **Access Point Web/External Portal Server** tab and select the certificate in the Certificate List, then click on the Edit icon under the “Actions” column. When you are done editing the description, click on **Save**.

5.4.2.3 Deleting a Certificate

To delete a certificate, select the certificate in the Certificate List and click on the delete icon under the “Actions” column. When the confirmation prompt appears, click on **Delete** to delete the selected certificate.

> You cannot delete an AP Web/External Portal Server Certificate if it is associated with a Provisioning Configuration.

5.4.2.4 Certificate List

Web Server/External Portal Server File

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **Description -** User-configured description for the certificate file.

Local LDAP File

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **CA File Name -** The name of the CA file.
- **Server File Name -** The name of the certificate file.
- **Key File Name -** The name of the key file.

AP 802.1X File

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -**Validity ending time of the certificate file.
- **AP Certificate File Name -** The name of the CA file.
- **Key File Name -** The name of the key file.

5.4.2.4.1 Stellar BLE

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **Client CA File Name -** The name of the CA file.
- **Client Certificate File Name -** The name of the client certificate file.
- **Client Certificate Key File Name -** The name of the client key file.

- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

5.4.2.4.2 Stellar WiFi RTLS

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **Client CA File Name -** The name of the CA file.
- **Client Certificate File Name -** The name of the client certificate file.
- **Client Certificate Key File Name -** The name of the client key file.
- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.

5.4.2.4.3 Local RadSec

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **CA File Name -** The name of the CA file.
- **Client Certificate File Name -** The name of the client certificate file.
- **Client Certificate Key File Name -** The name of the client key file.
- **Issued By-** The entity that issued the certificate.
- **Issued To -** The entity to which the certificate was issued.
- **Assigned Groups and Devices** - The AP Groups and associated Sites to which the certificate is applied.

5.4.2.4.4 Syslog Over TLS

- **Name -** The name of the certificate file.
- **Validity Start Time -** Validity starting time of the certificate file.
- **Validity Stop Time -** Validity ending time of the certificate file.
- **CA Certificate File Name -** The name of the CA file.
- **Issued To -** The entity to which the certificate was issued.
- **Issued By-** The entity that issued the certificate.
- **Assigned Groups and Devices** - The AP Groups and associated Sites to which the certificate is applied.

5.4.2.5 Stellar BLE Data Format

Consider the following information and data format that is used to send BLE messages to third-party Asset Tracking applications:

- The payload data format of the Bluetooth gateway report is an array of JSON, which contains one or more Bluetooth device information scanned in a reporting cycle.
- The reported information includes information about the scanned Bluetooth device and the Bluetooth gateway. Consider the following data format used to report the scanned information.

Field		Description	Format	Type
data	timestamp	When the device was scanned	**ISO 8601 time format** *2019-04-28T23:54:32-0800*	String
	advType	Broadcast frameworks	*iBeacon / Edyuid / Edyurl / KonLoc / KonTLM / iBeaconPB /KonSP/S1 /UnKnow*	String
	deviceMac	Mac of the scanned device	*dc08560034ef*	String
	txPower	The strength of the signal measured at 1 meter from the device	*If not ibeacon frame, default value 0*	Int
	rssi	Detected device RSSI value	*Average: {"50":268}* *Complete: {"-44":20,"-45":25,"-47":26}*	Object
	rawData	Complete Broadcast message *(If AdvType is **KonTLM** or **iBeaconPB** or **KonSP**, report the field, otherwise not)*	*0201061AFF4C00021 5FACEC0DEFEEDCAFE FACEC0DEFEEDCAFE0 0140012C5*	String
dataType		Type of device being scanned	*ble / wifi / ble_wifi*	String
bleMac		Bluetooth mac for gateway device	*dc08561325df*	String
wlanMac		Wlan mac for gateway device	*dc08561325c0*	String
apModel		Model of AP device	*OAW-AP1201*	String
timestamp		When gateway report data	**Unix time format** *1556524473*	Long Int

Notes:

1. To get smoothing BLE data, if the RssiFormat is “average” and the number of scans in a reporting cycle is greater than three, the highest and lowest values are removed and the average value is taken.
2. To include the channel of the BLE channel of collected RSSI:
    a. BLE has only three fixed broadcast channels, and in a broadcast event, a broadcast packet is transmitted on each channel. As a result, it is not possible for the scanning device to specify that the scanning should take place on a specific channel.

b. In a scanning event, the device will scan three channels in turn, and the scanned response data does not contain the channel.

c. If it is the scanning channel of the WiFi, that is supported.

The reporting JSON data format is similar to the following:

For normal scene, that is to say the “filter_mode” is set to “NoFilter” and “RssiFormat” is set to “average”, The AdvType does not contain KonTLM & iBeaconPB.


```
{
    "data":[
        {
            "timestamp":"2019-04-28T23:54:32-0800",
            "advType":"iBeacon",
            "deviceMac":"dc08562afd7f",
            "txPower":-69,
            "rssi":{"-50":268}
        },
        {
            "timestamp":"2019-04-28T23:54:35-0800",
            "advType":"iBeacon",
            "deviceMac":"dc08562ad85f",
            "txPower":-69,
            "rssi":{"-52":236}
        }
    ],
    "dataType":"ble",
    "bleMac":"dc08561325df",
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```


21 Oct 2025

5.4.2.6 Stellar WiFi RTLS Data Format

Consider the following information and data format that is used to send WiFi RTLS data to third-party RTLS applications:

- The payload data format of the gateway report is an array of JSON, which contains one or more WiFi device information scanned in a reporting cycle.
- The reported information includes information about the scanned WiFi device and the gateway. Consider the following data format used to report the scanned information.

Field		Description	Format	Type
data	timestamp	When the device was scanned	**ISO 8601 time format** *2019-04-28T23:54:32-0800*	String
	channel	The channel on which the ap operates	*11*	int
	scannedChannel	The channel to which the device is scanned	*6*	int
	deviceMac	Mac of the scanned device	*dc08560034ef*	Int
	isAssociated	Is associated or not	*True / False*	int
	rssi	Detected device RSSI value	*-69*	int
wlanMac		Wlan mac for gateway device	*dc08561325c0*	String
apModel		Model of AP device	*OAW-AP1201*	String
timestamp		When gateway report data	**Unix time format** *1556524473*	Long Int

The reporting JSON data format is similar to the following:

For normal scene, “RssiFormat” is set to “average”, the report data format as follows:

```
{
    "data":[
        {
            "timestamp":"2029-10-28T23:54:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad8c0",
            "isAssociated ":0,
            "rssi": {“-33”: 6}
        },
        {
            "timestamp":"2029-10-28T23:56:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad840",
            "isAssociated ":0,
            "rssi": {“-32”: 4}
```

```
        }
    ],
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```


For normal scene, “RssiFormat” is set to “complete”, the report data format as follows:


```
{
    "data":[
        {
            "timestamp":"2029-10-28T23:54:32-0800",
            "channel":1,
            "sannedScannel":11,
            "deviceMac":"dc08562ad8c0",
            "isAssociated ":0,
            "rssi": {“-33”: 6, “-36”:4}
        }
    ],
    "wlanMac":"dc08561325c0",
    "apModel":"OAW-AP1201",
    "timestamp":1556524473
}
```


21 Oct 2025

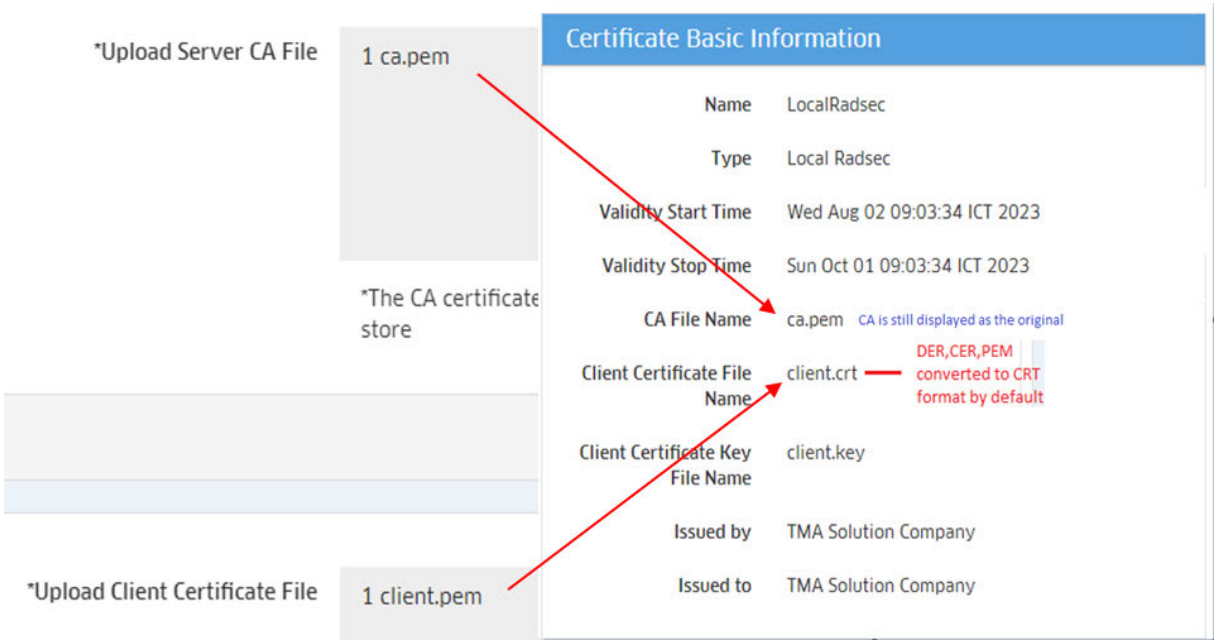
5.4.2.7 Local RadSec Certificate

Local RadSec Certificate in OmniVista is supported to provide a TLS-enabled connection between RadSec Client (Stellar AP) and RadSec Server (TLS-enabled RADIUS server). Creating a certificate consists of four ingredients: CA, Client Certificate, Client Key and Password for the Key. From OmniVista, an Admin user can push these certificates to the AP by selecting the Local RadSec option in the AP Group.

To create a Local RadSec Certificate in OmniVista, you must upload and import three ingredient files:

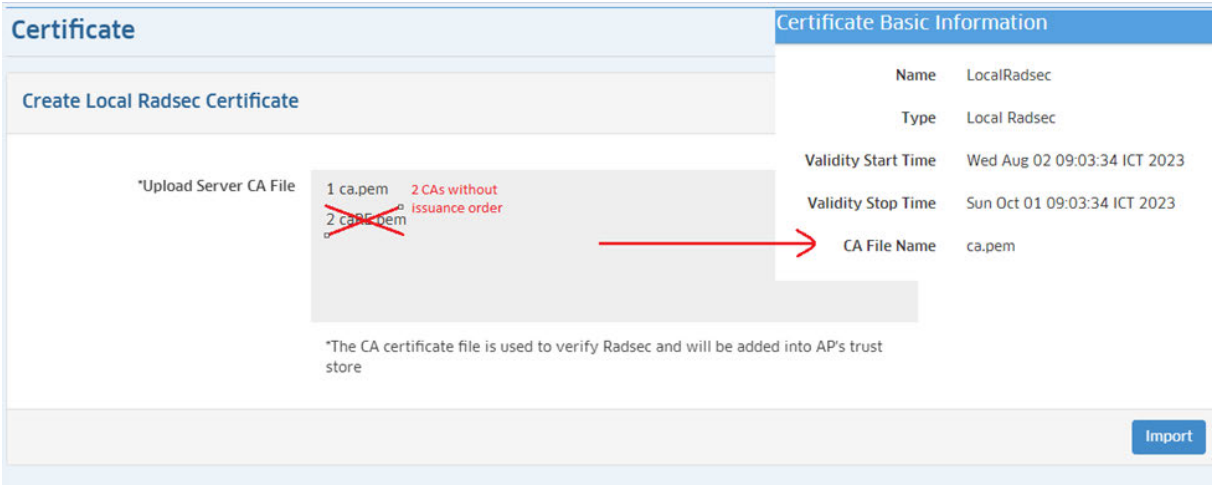
- **CA Certificate file:** Supports only PEM or DER encoded certificates (e.g. .pem .cer. der .crt) and multiple CAs with issuance order.
- **Client Certificate file:** Supports only PEM or DER encoded certificates. However, OV will translate all acceptable formats to **.crt** format due to AP's requirement.
- **Client Key file:** Supports only **.key** file.

And, Password for Client Key.



Notes:

1. Do not import multiple CAs without an issuance order. If you import multiple CAs without an issuance order, OmniVista only parses and applies the first one to the AP.



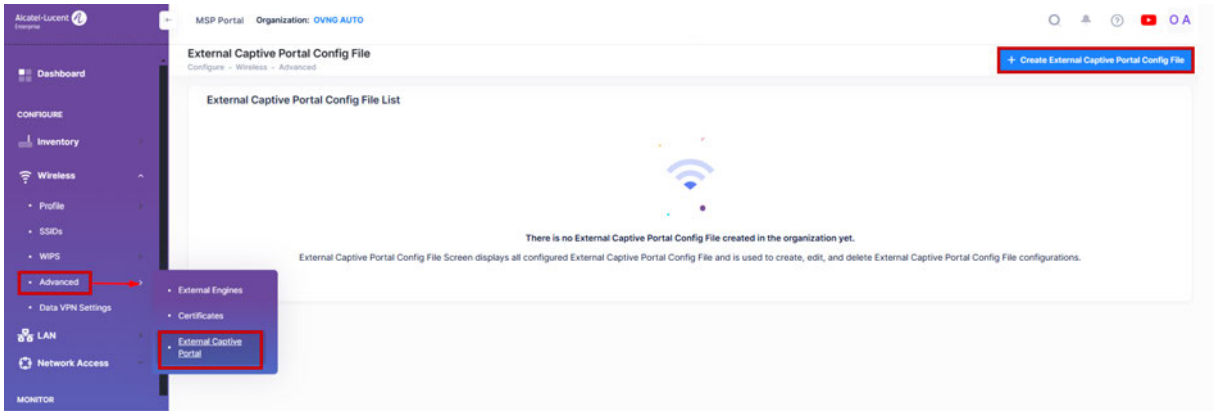
2. Make Client Certificate and Client Key in two files separately. Client Certificate file should not include Client Key because when OmniVista converts certificate to CRT format, only the certificate part is converted, and the private key part is ignored.
3. CA Certificate file will be converted to CRT format and applied to AP, but content of the Certificate part is not changed.

21 Oct 2025

5.4.3 External Captive Portal

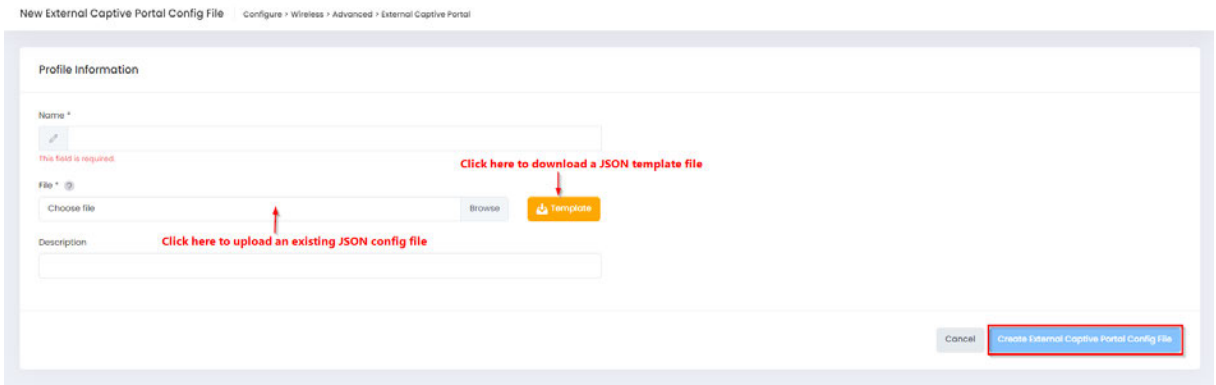
The External Captive Portal Configuration file is used to provide secure communication between APs and an External Captive Portal Server. The management of external configuration files is done through Access Role Profiles. To bind the External Captive Portal to an SSID, change the Captive Portal option of the Access Role Profile to “External”, then assign the Access Role Profile to the SSID. Traffic assigned to the profile is redirected to the External Captive Portal server identified in the configuration file.

The External Captive Portal screen displays information (see page 413) about External Captive Portal Configuration files and is used to create (see page 409), edit (see page 410), download (see page 412), and delete (see page 412)an external configuration file. To access this screen, click on **Wireless > Advanced > External Captive Portal** under the “Configure” section of the OmniVista Terra Menu (see page 45).



5.4.3.1 Creating an External Captive Portal Configuration File

To create an External Captive Portal Configuration file, click on **Create External Captive Portal Config File** to open the New External Captive Portal Config File screen.



Complete the fields as described below, then click on **Create External Captive Portal Config** File.

- **Name** - Enter a unique name to identify the external configuration file.
- **File** - Click on this field to locate and upload an existing JSON file. Note that only JSON files are supported.

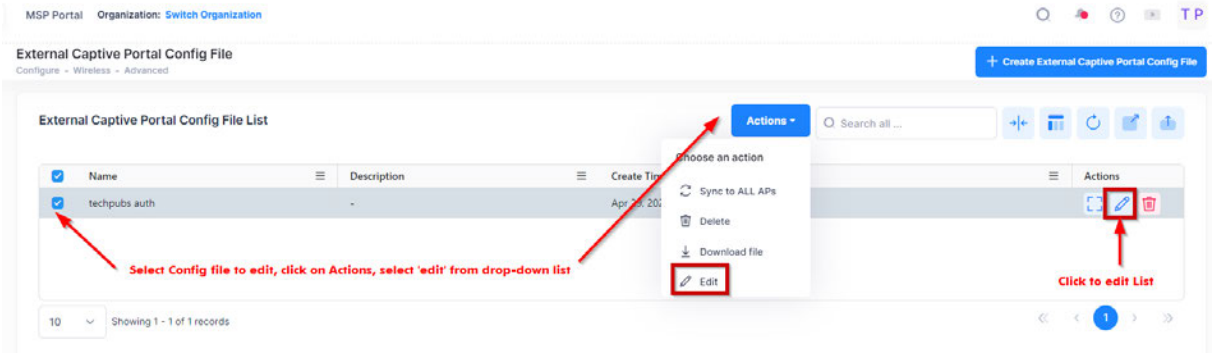
- **Template** - You can click on **Template** to download a JSON template file that you can use to create an External Captive Portal Configuration file. Once you have completed and saved the external configuration file, click on **Browse** to locate and upload the file you created.
- **Description** - Enter an optional description for the External Captive Portal Configuration file.

> When you are done creating and/or uploading an External Captive Portal Configuration file, you must push the configuration file(s) to all of the APs in the network. Click here (see page 411)for more information.

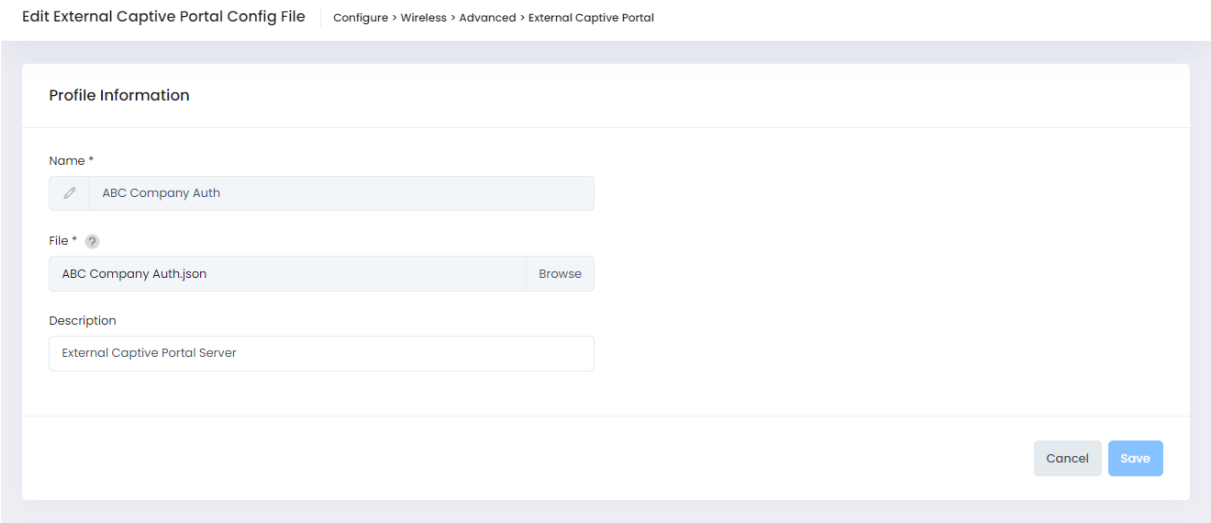
5.4.3.2 Editing an External Captive Portal Configuration File

You can edit the values for an existing External Captive Portal Configuration file by accessing the Edit External Captive Portal Config File screen. Use one of the following methods to access this screen:

- Select the configuration file to edit by clicking o the checkbox next to the entry, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the configuration file that you want to edit.



The following Edit External Captive Portal Config File screen displays. Edit the fields as described above (see page 409), then click on **Save**.

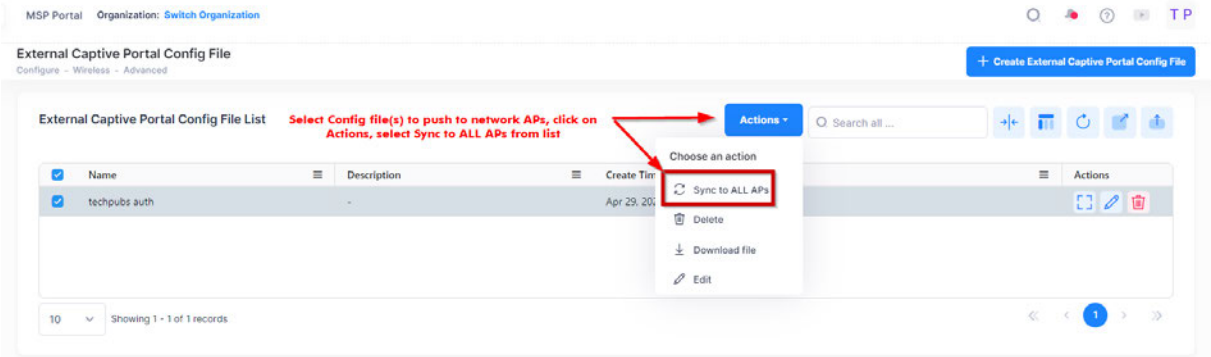


When you are done editing an External Captive Portal Configuration file, you must push the configuration file(s) to all of the APs in the network. Click here (see page 409)for more information.

5.4.3.3 Deploying the External Captive Portal Configuration File

When you are done creating or editing an External Captive Portal Configuration file, you can push the configuration files to all the APs in your network. Use one of the following methods to select the configuration files to push to the APs:

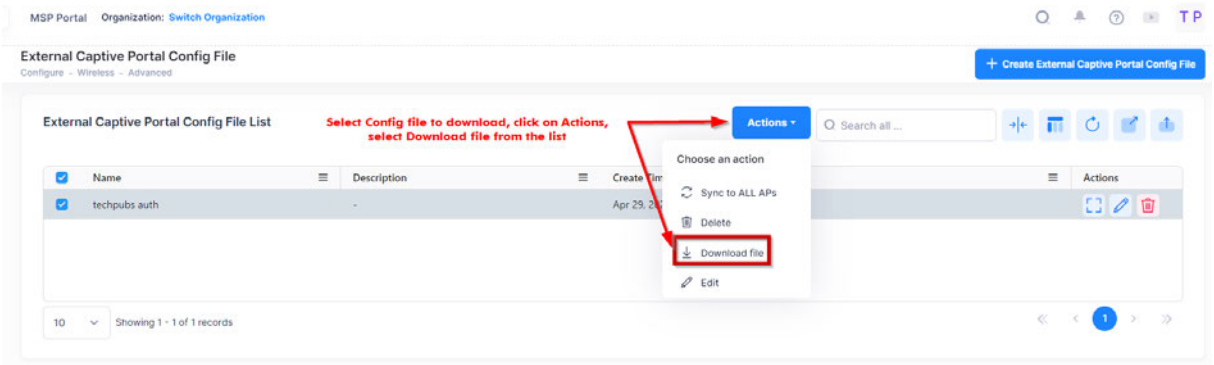
- Click on **Actions** and select **Sync to ALL APs** to push all of the configuration files to all of the APs.
- Select the configuration file(s) to push to all of the APs by clicking on the checkbox next to the table entry, click on **Actions**, then select **Sync to ALL APs**.



The External Captive Portal Configuration file that an AP should use is designated in the Access Role Profile (see page 514) to which AP client traffic is assigned.

5.4.3.4 Downloading the External Captive Portal Configuration File

You can download one or more External Captive Portal Configuration files to your machine. Select the configuration file(s) to download by clicking on the checkbox next to the table entry.

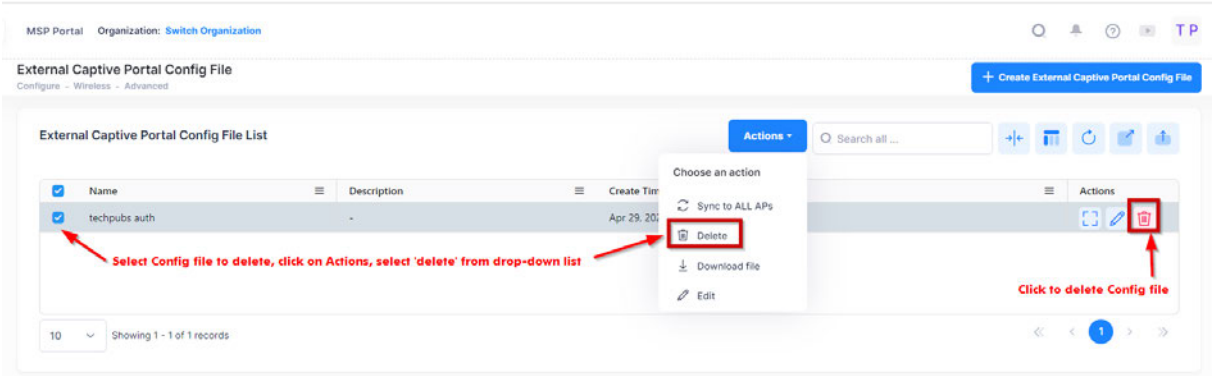


The JSON configuration file will be downloaded to your designated download folder.

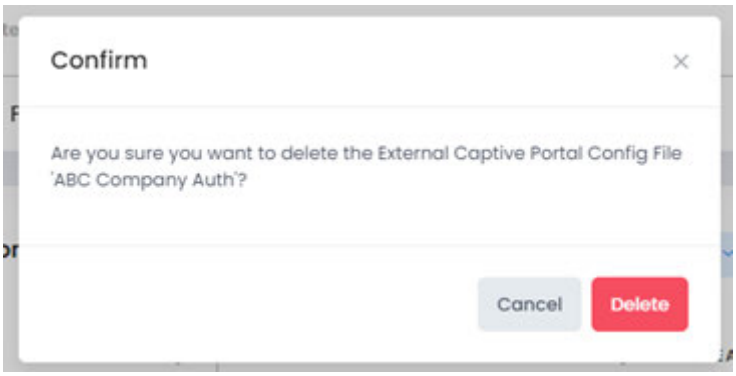
5.4.3.5 Deleting an External Captive Portal Configuration File

To delete an External Captive Portal Configuration file, use one of the following methods to select the configuration file(s) that you want to delete:

- Select the configuration file(s) to delete by clicking on the checkbox next to the table entry, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the configuration file that you want to delete.

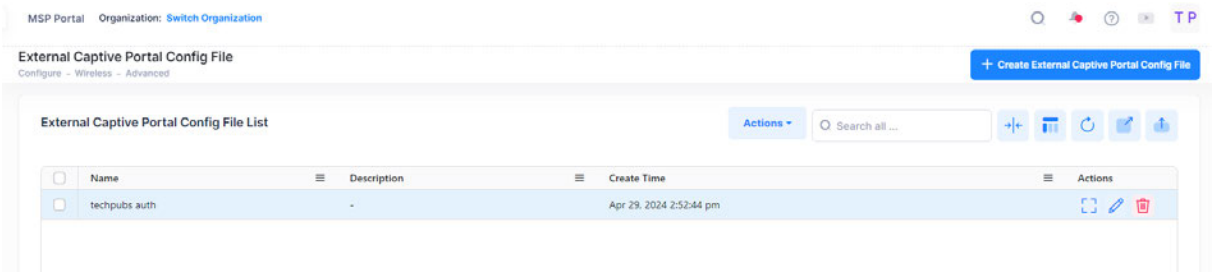


When the following confirmation prompt appears, click **Delete** to delete the selected configuration file.



5.4.3.6 External Captive Portal Configuration File List

- **Name -** The name of the configuration file.
- **Description -** User-configured description for the configuration file
- **Create Time -** The date and time when the configuration file was uploaded to OmniVista Terra.



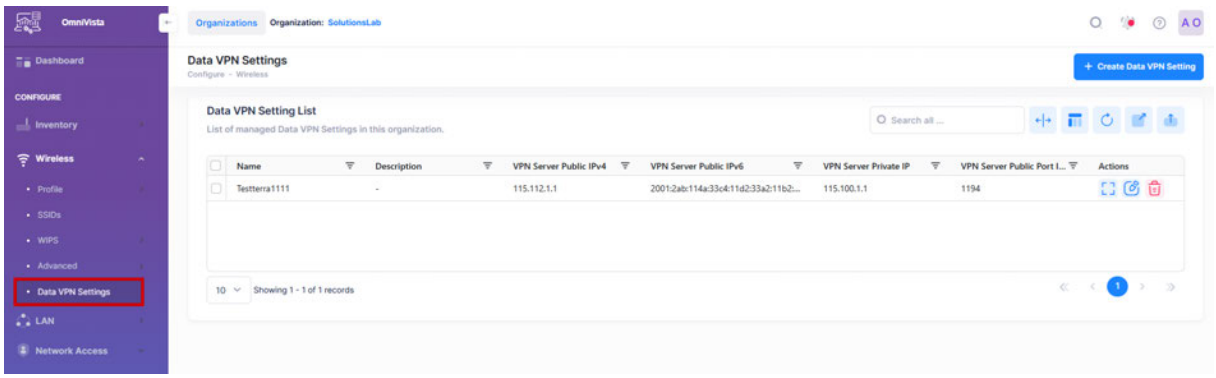
21 Oct 2025

5.5 Data VPN Settings

The Data VPN Settings screen is used to define settings for a Data VPN Settings Profile that Stellar Access Points will use to access remote functionality. An Access Point retrieves the Data VPN Server Profile to use from the AP Group (see page 309) to which the Access Point belongs. Each AP Group is associated with a Provisioning Configuration (see page 313). Access Points that are members of the AP Group utilize the Provisioning Configuration to boot up and get a basic configuration. The associated Provisioning Configuration is where the name of the Data VPN Server Profile to use is defined. A Data VPN Settings Profile is also specified when configuring a Data VPN Tunnel Profile.

Use the Data VPN Settings screen to display information (see page 417) about configured Data VPN Server Profiles. This screen is also used to create (see page 414), edit (see page 417), delete (see page 417), and export (see page 417)Data VPN Server Profile Settings.

To access the Data VPN Settings screen, click on **Wireless > Data VPN Settings** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Data VPN Settings screen displays.



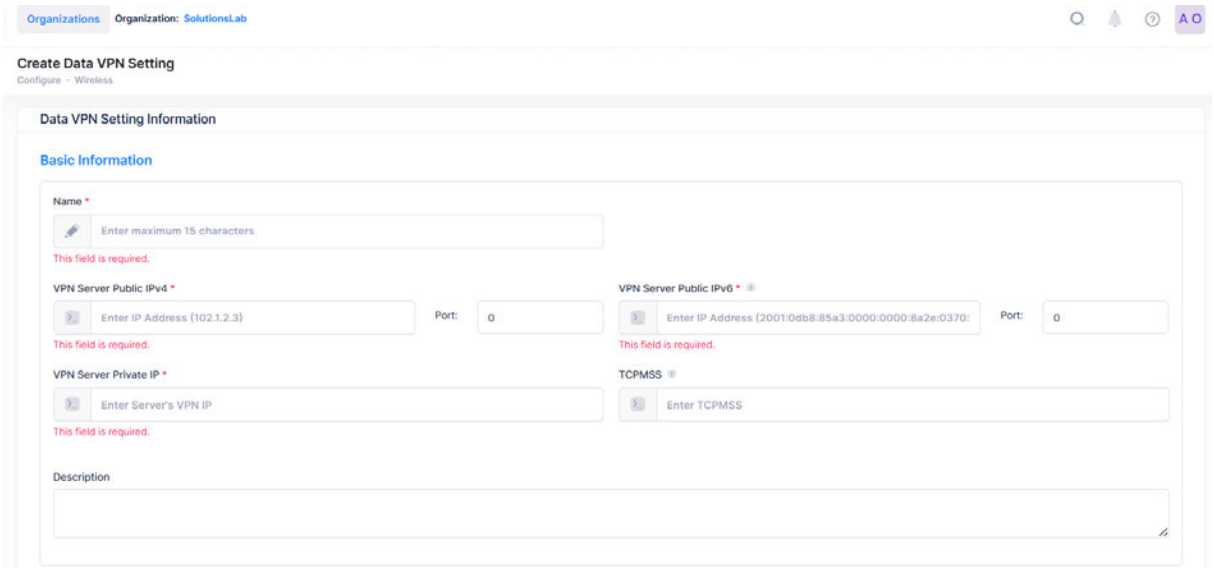
5.5.1 Creating a Data VPN Server Profile

The Create Data VPN Setting screen is used to define settings for a Data VPN Server Profile. To access this screen, click on **Create Data VPN Setting**.

Complete the following sections of the Create Data VPN Setting screen to define the settings for a Data VPN Server Profile:

- **Basic Information** (see page 415) - Configures identifying information for the Data VPN Server Profile (for example, profile name, the public and VPN IP address for the VPN Server, and optional description).
- **VPN Clients IP Address Pool** (see page 415) - Creates an IP pool that is used to assign IP addresses to clients connecting to the VPN tunnel.
- **Encryption Keys** (see page 416) - Configure or automatically generate a public and private key to provide secure communication between the Data VPN Server and client.

5.5.1.1 Basic Information

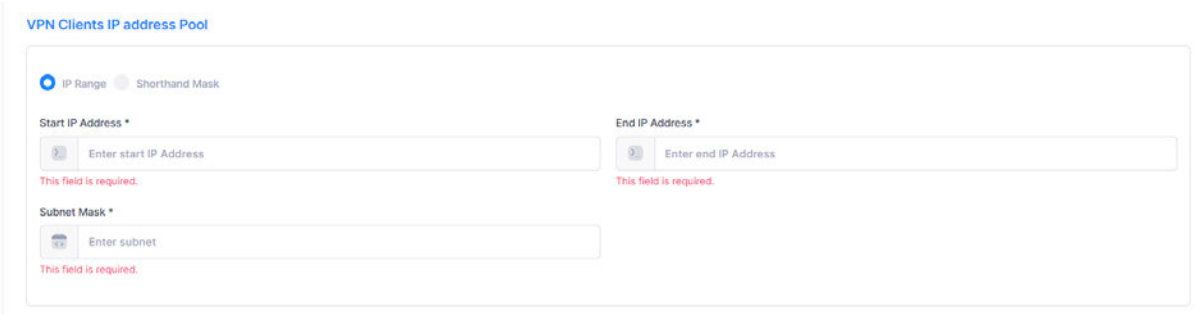


Complete the fields as described below to define the basic information settings for the Data VPN Server Profile:

- **Name** - A unique, user-defined name to assign to the Data VPN Server Profile. (1 - 64 characters) Note that the name setting only allows lowercase, uppercase, numeral, special characters(_ -), and cannot start with "-" or contain a space between words (for example, entering "Data_Center_VPN" is allowed, but "Data Center VPN" is not).
- **VPN Server Public IPv4 -** The public IPv4 address of the Data VPN Server.
- **VPN Server Public IPv6 -** The public IPv6 address of the Data VPN Server.
- **VPN Server Public Port -** The network port of the Data VPN Server. (Range = 1 - 65535)
- **VPN Server Private IP -** The VPN IP address of the Data VPN Server. The IP address must be within the specified IP Range (see page 415).
- **TCPMSS** - The TCP Maximum Segment Size (TCP MSS) attribute can be used to control the maximum size of packets going out through a connection. Specifically, it will cause the AP and VPN Server to choose a smaller TCP window and frame size to avoid fragmentation as much as possible. This is especially useful for Dual-stack Lite(DS-Lite) ISP connections
- **Description** - Optional description for the Data VPN Server Profile. (1 - 255 characters)

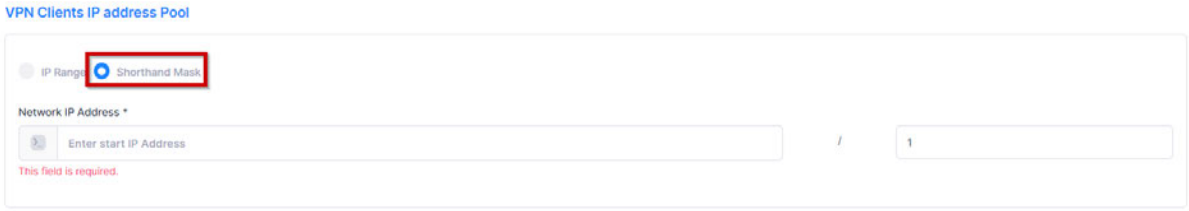
5.5.1.2 VPN Clients IP Address Pool

Select the **IP Range** or **Shorthand Mask** radio button and complete the fields as described below to create the IP pool from which IP addresses will be assigned to clients connecting to the VPN tunnel.



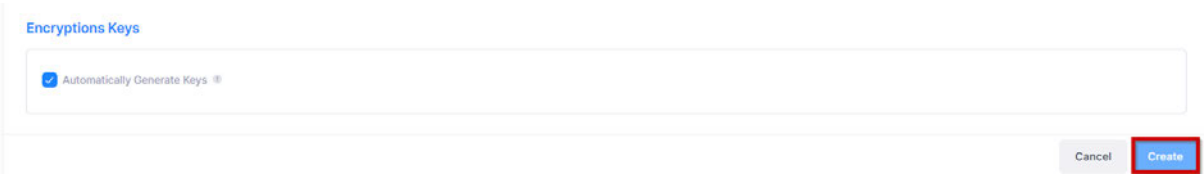
- **IP Range**
  - Enter the Starting and Ending IP Address in the range and Subnet Mask (for example., Starting IP Address = 192.168.1.1, Ending IP Address = 192.168.1.254 with subnet mask = 255.255.255.0).

Note: The pool for VPN Clients must contain the VPN Server Private IP.



- **Shorthand Mask**
  - Enter the IP pool shorthand mask format (for example, 192.168.1.0/24).

5.5.1.3 Encryption Keys



The Public and Private key for the server is automatically generated by default. To configure the encryption keys, uncheck the box next to the “Automatically Generate” option.

- **Server's Public Key -** The Data VPN Server’s public key used for secure communication between the Data VPN Server and client.
- **Server's Private Key -** The Data VPN Server’s private key used for secure communication between Data VPN Server and client.

When you are done completing the Basic Information, VPN Clients IP Address Pool, and Encryption Keys sections, click on **Create** at the bottom-right of the screen.

5.5.2 Editing a Data VPN Setting

Select the Data VPN Server Profile that you want to edit from the Data VPN Settings List, then click on **Edit** from the “Actions” drop-down menu. The Edit Data VPN Setting screen opens. Edit the fields as described in Creating a Data VPN Server Profile (see page 414), then click on Save to retain your changes.

5.5.3 Deleting a Data VPN Setting

Select the Data VPN Server Profile that you want to delete from the Data VPN Settings List, then click on **Delete** from the “Actions” drop-down menu. Click **Delete** on the Confirmation Prompt to confirm that you want to delete the profile.

5.5.4 Exporting a Data VPN Setting

Select a Data VPN Server Profile in the Data VPN Settings List and click on **Export** at the top of the list. The settings will be downloaded in a .conf file to your Download Directory. You can then import the settings into a Remote Data VPN Server.

5.5.5 Data VPN Settings List

The Data VPN Settings List displays the following information for each Data VPN Server Profile:

- **Name -** User-configured name for the Data VPN Server. It must be unique. (1 - 64 characters)
- **Description -** A description of the Data VPN Server. (1 - 255 characters)
- **VPN Server Public IPv4 -** The public IPv4 address of the Data VPN Server.
- **VPN Server Public IPv6 -** The public IPv6 address of the Data VPN Server.
- **VPN Server Private IP** - The VPN IP address of the Data VPN Server.
- **VPN Server Public Port -** The network port of the Data VPN Server.
- **TCPMSS** - The TCP MSS value, if used.
- **VPN Clients IP Address Pool** - Whether IP Range or Shorthand Mask is used to specify the IP address pool from which IP addresses are assigned to clients connecting to the VPN tunnel.
- **Network IP Address** - Displays the network IP address if the Shorthand Mask option is used to specify the Client VPN IP Address Pool,
- **Length IP Address** - Displays the length of the IP address if the Shorthand Mask option is used to specify the Client VPN IP Address Pool.
- **Start IP Address** - Displays the starting IP address if the IP Range option is used to specify the Client VPN IP Address Pool.
- **End IP Address** - Displays the ending IP address if the IP Range option is used to specify the Client VPN IP Address Pool.
- **Subnet Mask** - Displays the value of the subnet mask if the IP Range option is used to specify the Client VPN IP Address Pool.

6 Configure and Manage LANs

VLANs are used to segment network traffic so that VLAN configuration and port assignment is handled through software. This eliminates the need to physically change a network device connection or location when adding or removing devices from the VLAN broadcast domain.

The initial configuration for all switches consists of a default VLAN 1 and all device ports are initially assigned to this VLAN. If additional VLANs are not configured on the switch, then the entire switch is treated as one large broadcast domain. All ports will receive all traffic from all other ports.

In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. The user specifies a VLAN ID to create, modify or remove a VLAN and to assign switch ports to a VLAN. When a packet is received on a port, the VLAN ID for that port is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID.

The operational status of a VLAN remains inactive until at least one active switch port is assigned to the VLAN. This means that VLAN properties, such as Spanning Tree and/or router interfaces, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.

CLI-based provisioning provides a simplified method for deploying and configuring switches. User-configured templates are utilized to automatically push a configuration to switches during the onboarding process or to push a different configuration to a provisioned switch.

To access the LAN group of applications, click on the **LAN** option under the “Configure” section of the OmniVista Terra Menu (see page 45). When you click on the **LAN** option, the following list of applications is provided to assist with configuring VLAN network management:

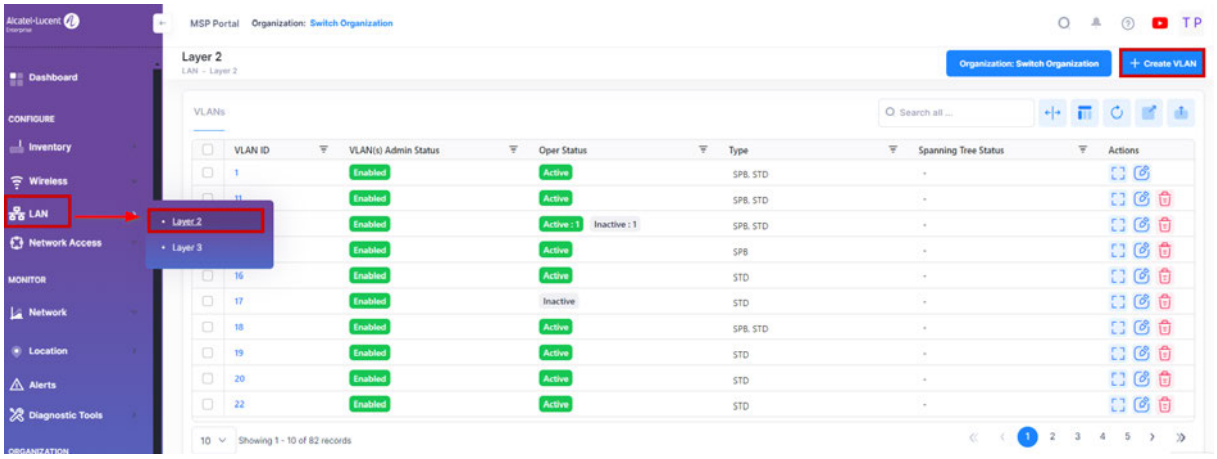
- Layer 2 (see page 419)
- Layer 3 (see page 443)
- CLI Based Provisioning (see page 451)

21 Oct 2025

6.1 Configure and Manage Layer 2 VLANs

The OmniVista Layer 2 VLAN screen displays (see page 426) information about all VLANs configured on managed devices; and is used to create (see page 419), edit (see page 423), and delete (see page 424) VLANS on LAN Devices. It is also used to perform certain actions on a VLAN (e.g., enable VLANs (see page 424), disable VLANs (see page 425), view Spanning Tree parameters (see page 431), and configure an IP Router Interface (see page 438)).

To manage the VLAN configuration, navigate to the VLANs screen by clicking on **LAN > Layer 2** under the “Configure” section of the OmniVista Terra Menu (see page 45). The VLAN List screen displays.



6.1.1 Creating a VLAN

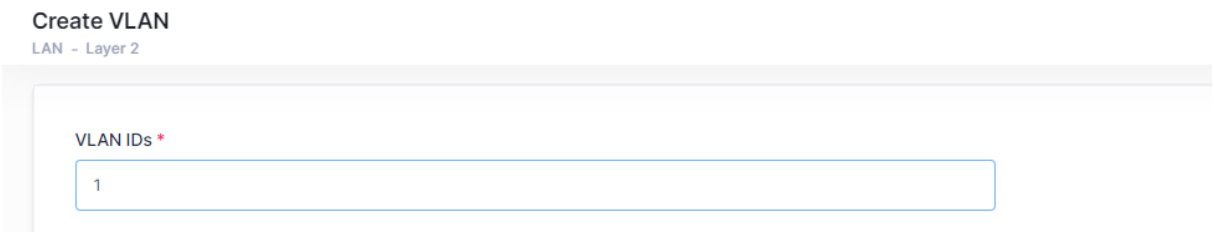
To access this screen, click on **Create VLAN** at thehe top-right side of the VLANs Table.

The Create VLAN screen provides the following step-by-step process for creating a VLAN:

- **VLAN IDs** (see page 419) - Each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned at the creation time of VLAN and is not a modifiable parameter. (Range = 2 - 4094).
- **VLAN Configuration Template** (see page 420) - The VLAN Configuration Screen is used to select the default VLAN IDs, assigning the default ports and modify VLAN administrative status.
- **Switch Selection** (see page 421) - Select the Switch or LAN devices from the available list to create a VLAN.

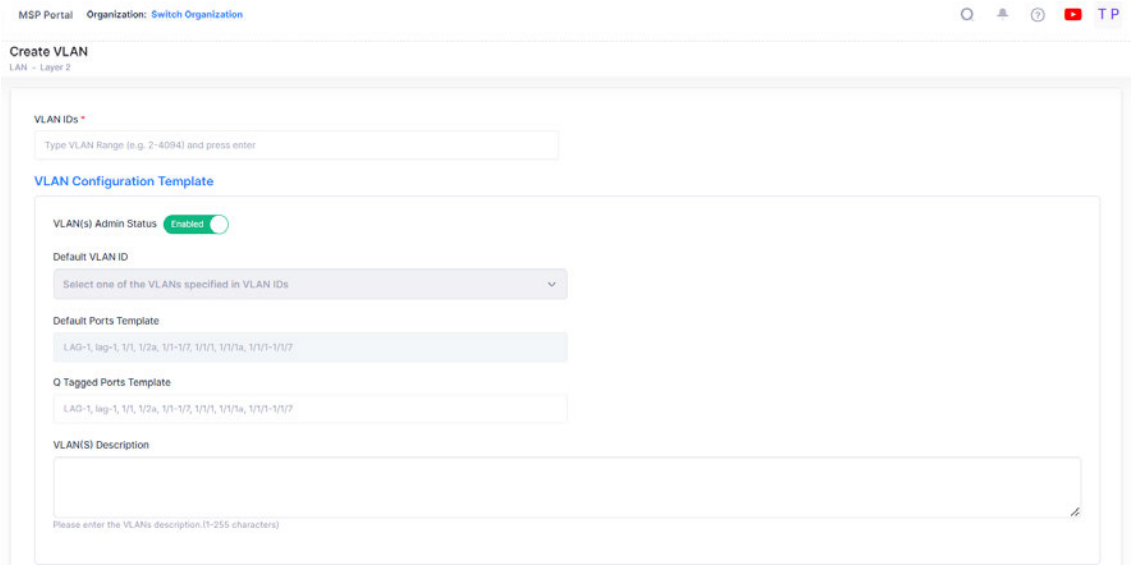
6.1.1.1 VLAN IDs

Enter the VLAN ID number (Range = 2 - 4094). To create a single VLAN, enter a single VLAN ID (e.g. 5) or enter a range of VLANs (e.g., 500-505). Note that you cannot enter a VLAN ID for a VLAN that has already been created.



6.1.1.2 VLAN Configuration Template

The VLAN Configuration Template contents are applied to all selected devices, subject to availability of ports on devices. Complete the fields as described below to provide the configuration information for the VLAN:



- **VLAN(s) Admin Status -** This is the global administrative status of the VLAN (Enabled/ Disabled). The configured value will be applied to all the selected switches. You can also configure the Admin status for individual switch from “Selected devices” table by clicking on the column value.
- **Default VLAN ID -** Enter the VLAN ID of one of the VLANs. This will be the default VLAN for the configured ports.
- **Default Ports Template -** It is used to configure default (untagged) ports for all selected devices. The configuration will be added to selected devices if the port is available on device. For example, if you enter port 1/5 as a default port when creating VLAN 100, port 1/5 will be added as a default port for all devices having port 1/5. If a selected device does not have port 1/5, the default port will not be created on the device. Ports or Link Aggregates must be entered in the format shown (e.g., LAG-1, lag-1, 1/1, 1/2a, 1/1-1/7, 1/1/1, 1/1/1a, 1/1/1-1/1/7).
- **Q Tagged Ports Template -** It is used to configure Q-Tagged ports for all selected devices. The configuration will be added to selected devices if the port is available on device. For example , if you enter port 1/3 as a Q-Tagged Port when creating VLAN 100, port 1/3 will be added as a Q-Tagged port for all devices having port 1/3. If a selected device does not have port 1/3, the Q-

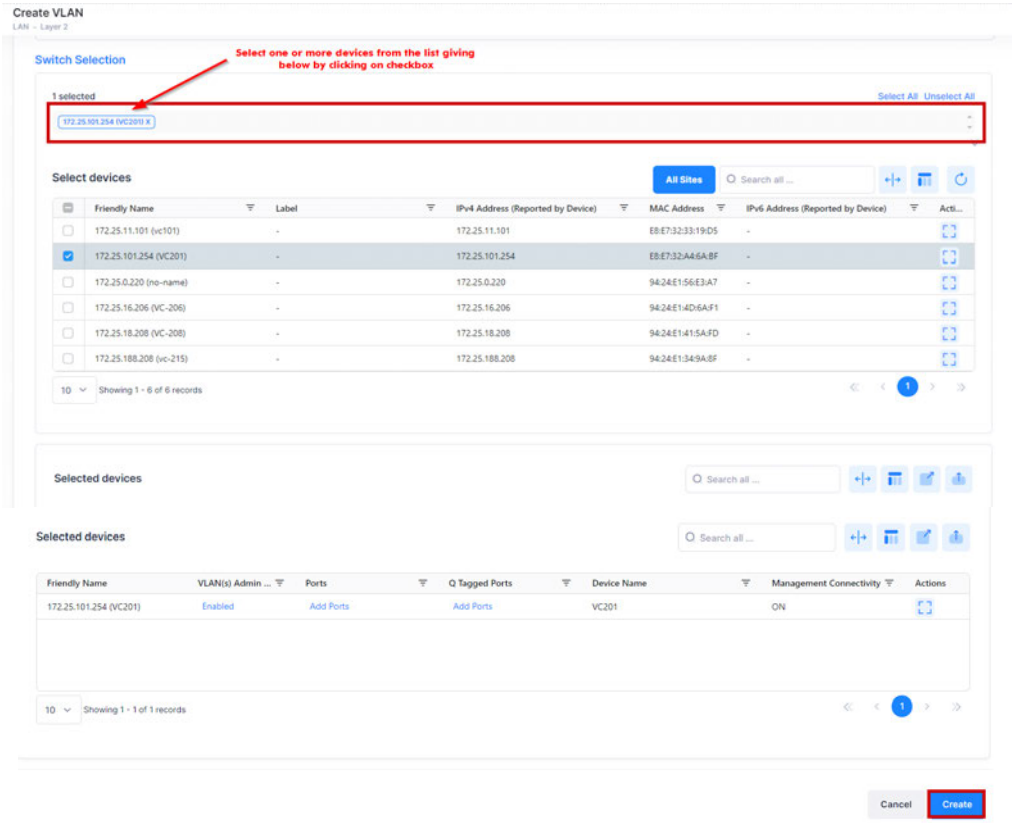
Tagged port will not be created on the device. Ports or Link Aggregates must be entered in the format shown (e.g., LAG-1, lag-1, 1/1, 1/2a, 1/1-1/7, 1/1/1, 1/1/1a, 1/1/1-1/1/7).

- **VLAN(s) Description -** Enter an optional description for the VLAN(s). If you do not enter a description, the VLAN ID is used.

6.1.1.3 Switch Selection

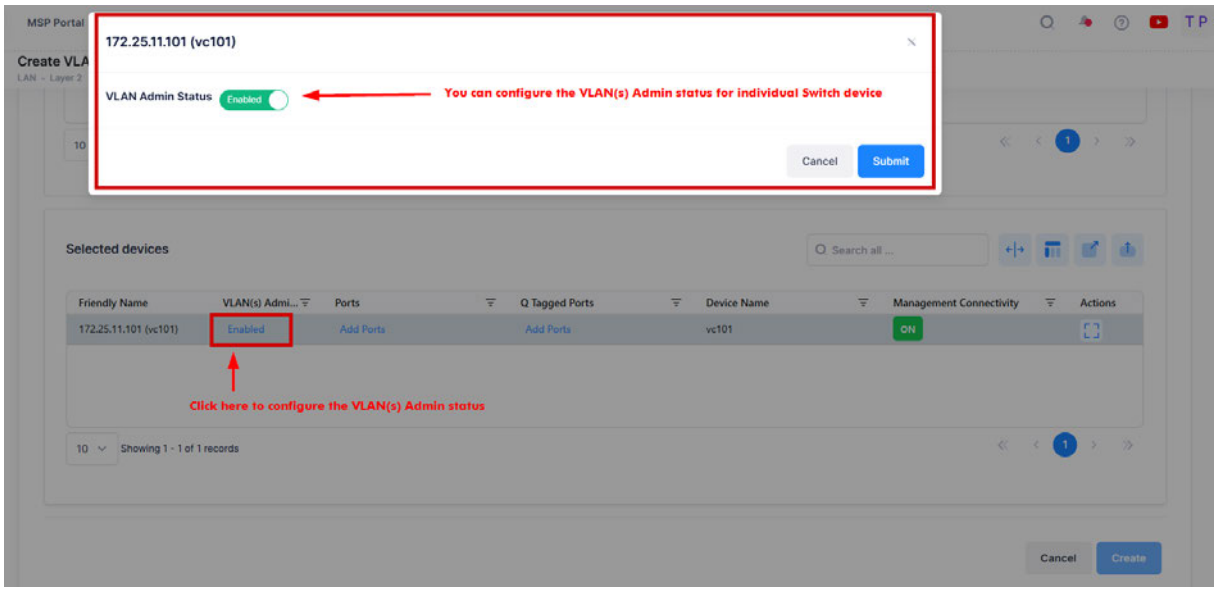
Select the devices from the available list to be included in the VLAN. The “Select devices” table will display only those switches which are having management connectivity “ON” state.

The selected devices will be displayed at the bottom of the section.



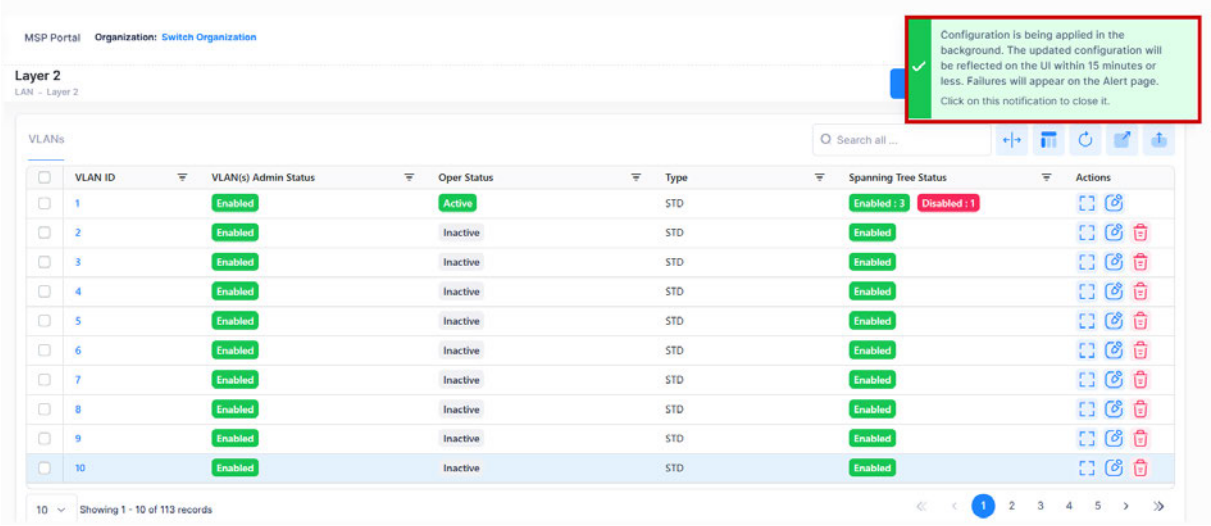
You can configure VLAN(s) Admin Status, Ports and Q Tagged Ports column for individual devices from the “Selected devices” table.

For example, you can configure the VLAN(s) Admin status for the individual device as shown below:



When you are done with the Switch Selection, click on **Create** to complete the process of Creating a VLAN.

Note: If you request for **create/update/delete of VLANs** from OminVista Terra, then the configuration operation is done in the background. You can view the updated configuration results after certain time interval and the following alert message appears on the screen as shown below- **"Configuration is being applied in the background. The updated configuration will be reflected on the UI within 15 minutes (periodic polling) or less (immediate polling). Failure will appear on the Alerts page."**

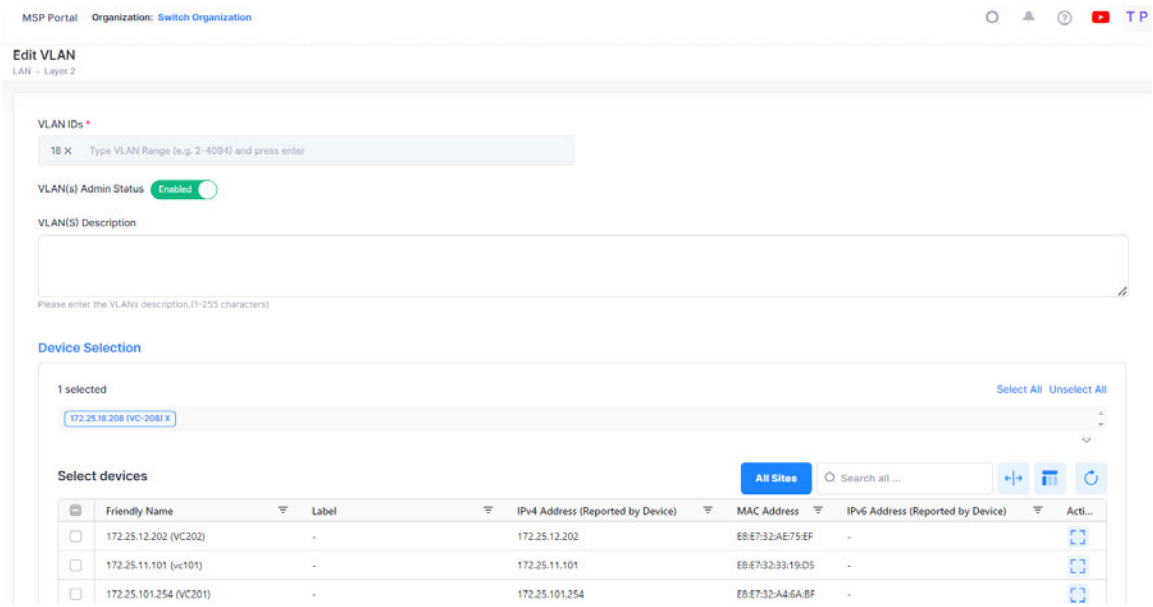


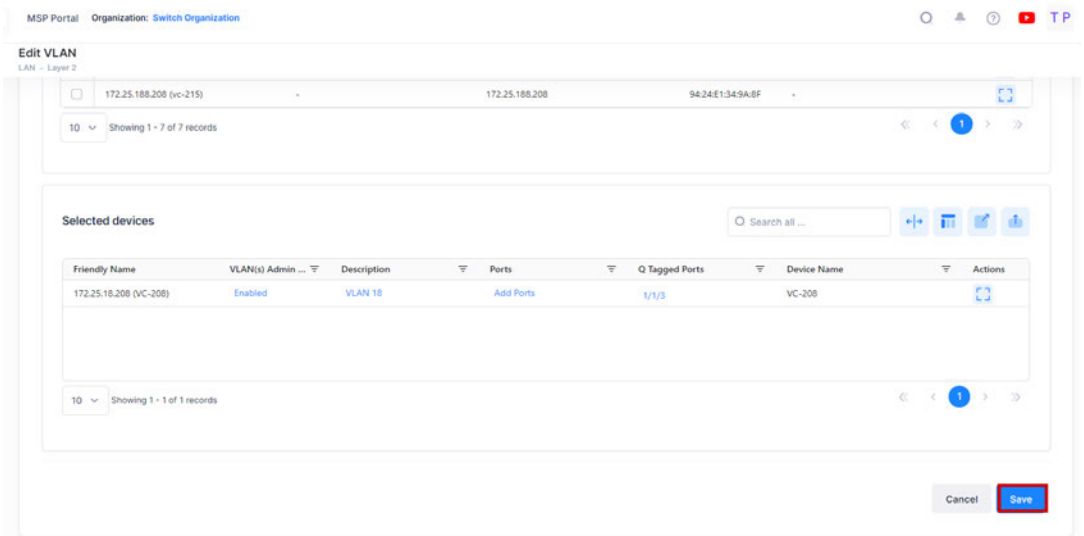
6.1.2 Editing a VLAN

Select a VLAN ID in the VLANs List and click on the Edit icon under the “Actions” column. The Edit VLAN Information screen opens on which you can edit the VLAN Admin status and selected devices for VLAN configuration, as described above (see page 420).

Consider the following while editing a VLAN:

1. VLAN(s) Admin Status and VLAN(s) Description are the Global attribute value, therefore, the configured value will be applied to all the selected switches. You can configure this value for individual switch from “Selected devices” table by clicking on the column value.
2. If the selected device Management connectivity status is “OFF” and the VLAN already exists for that device, then it will be read only in device selection. You will not be able to modify any configuration for that device.



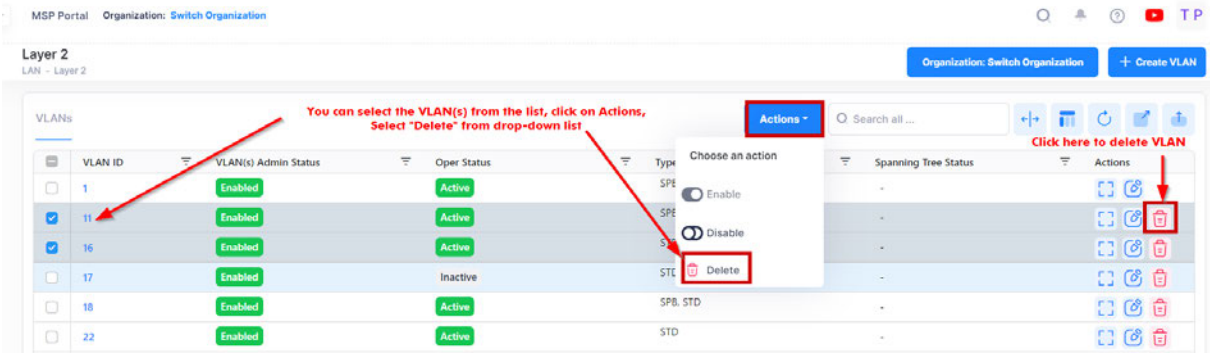


Click on **Save** to save the changes.

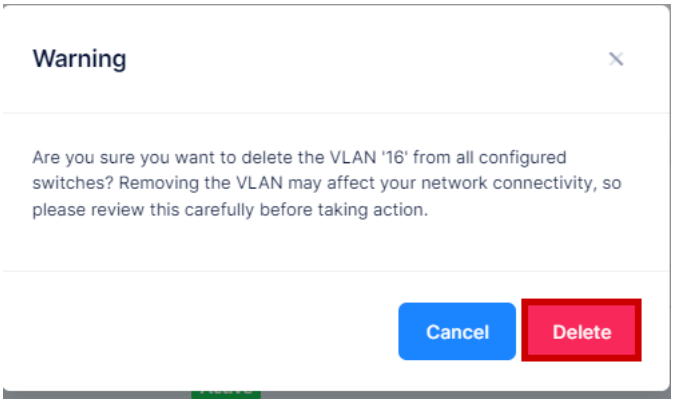
6.1.3 Deleting a VLAN

To delete a VLAN, select a VLAN(s) in the VLANs Table by clicking on the checkbox next to the VLANs and use one of the following methods to select the VLAN you want to delete:

- Select the VLAN to delete by clicking on the checkbox next to the VLANs, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the VLAN(s) that you want to delete.



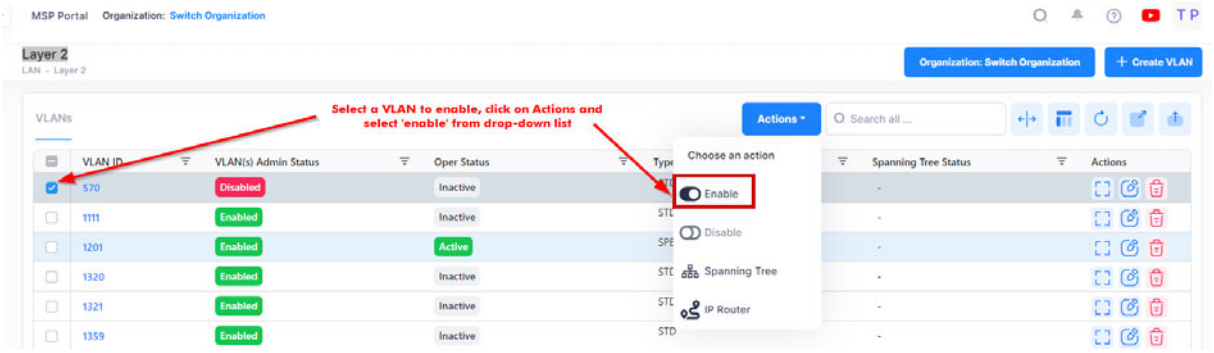
When you select the VLAN(s) you want to delete, the following confirmation prompt appears:



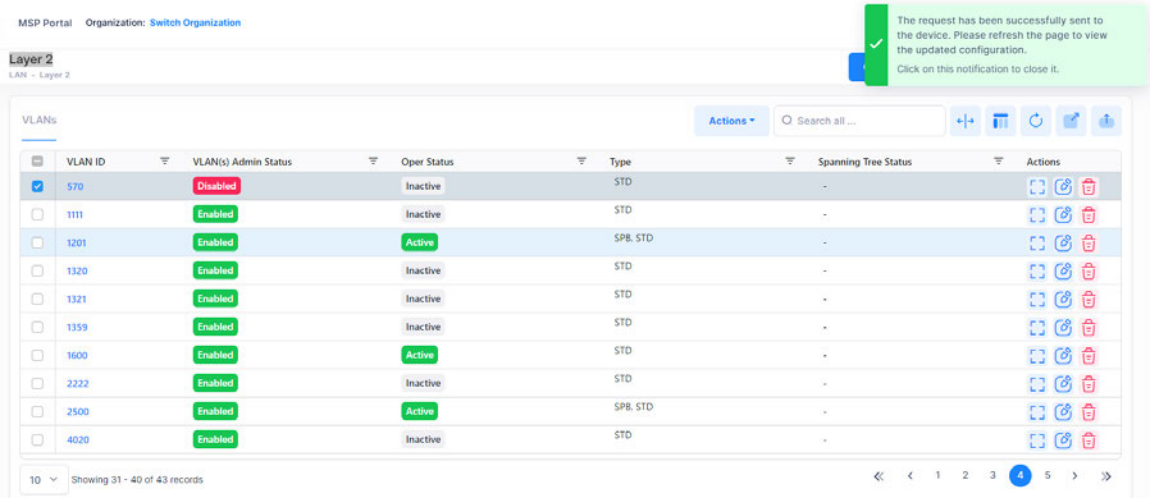
Click on **Delete** to confirm that you want to delete the selected VLAN(s). The VLAN will be removed from all the devices to which it was assigned.

6.1.4 Enabling a VLAN

To enable a VLAN(s), select one or more VLANs in the table, click on the **Actions** and select **Enable** button.

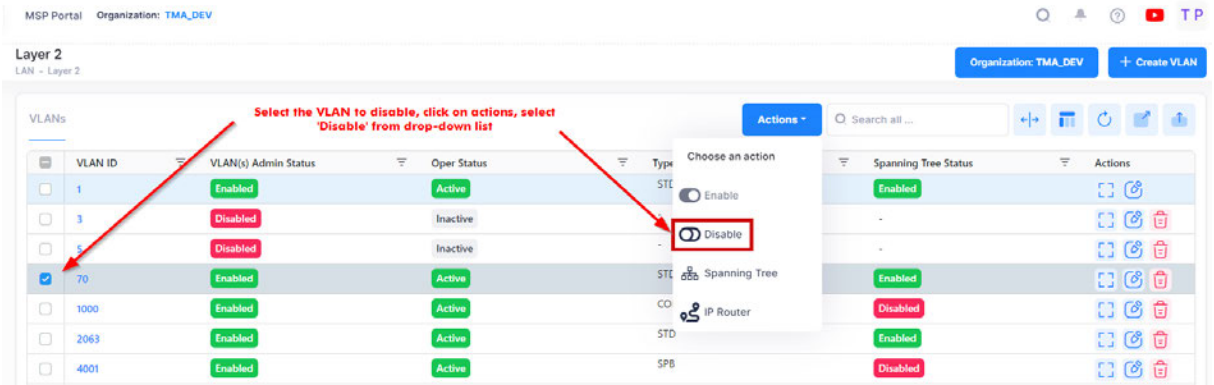


You will get the below notification message displayed on the screen after raising request to enable a VLAN(s).

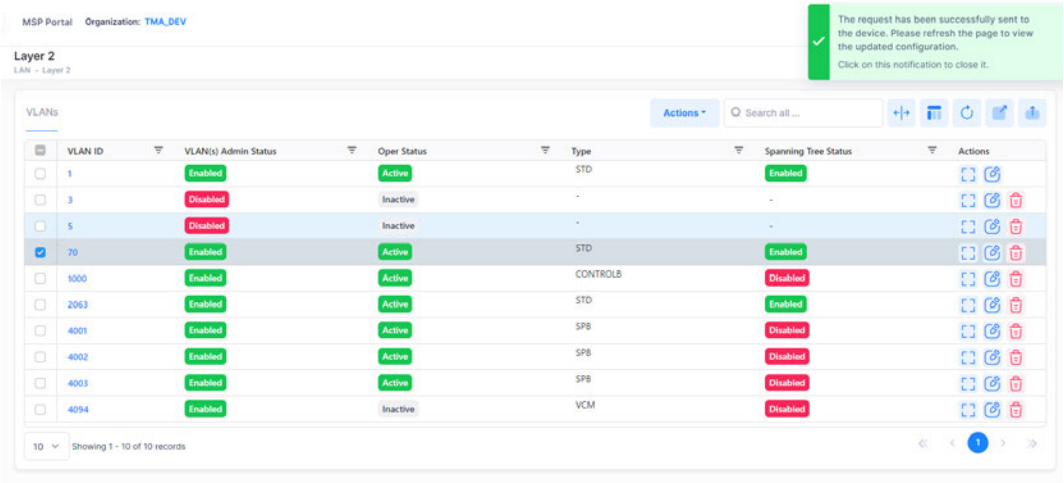


6.1.5 Disabling a VLAN

To disable a VLAN(s), select one or more VLANs in the table, click on the **Actions** and select **Disable** button.

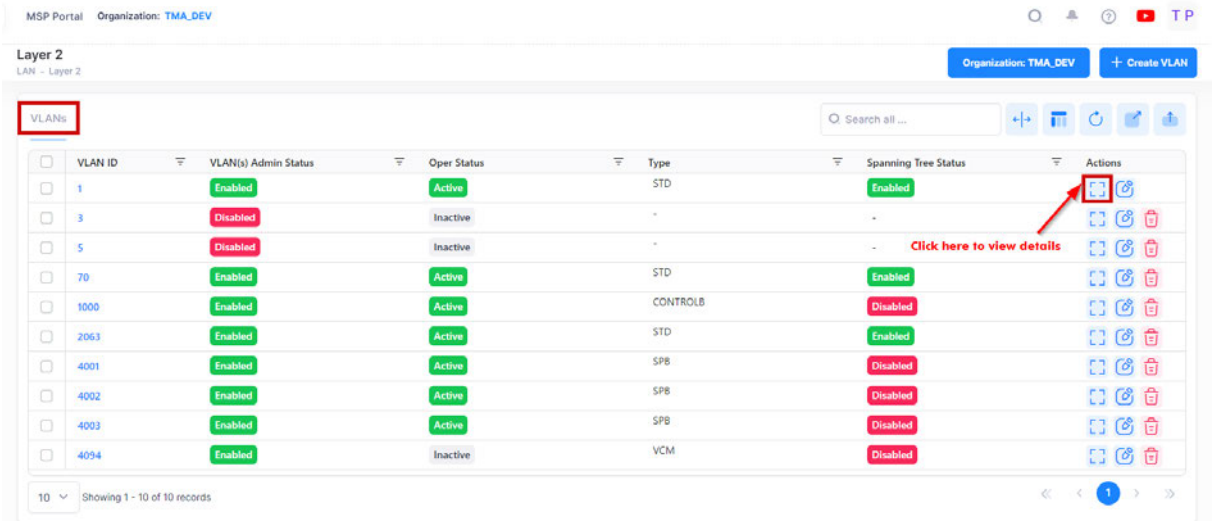


You will get the below notification message displayed on the screen after raising request to disable a VLAN(s).



6.1.6 Display VLAN Details

The VLAN Table displays VLANs configured on the network. The VLANs Table displays basic (see page 426) information about each VLAN. To view detailed (see page 427) information about a VLAN, select the VLAN, click on the **View Details** button of the VLAN Table.



6.1.6.1 Basic Information

The VLAN Table displays basic information about each VLAN.

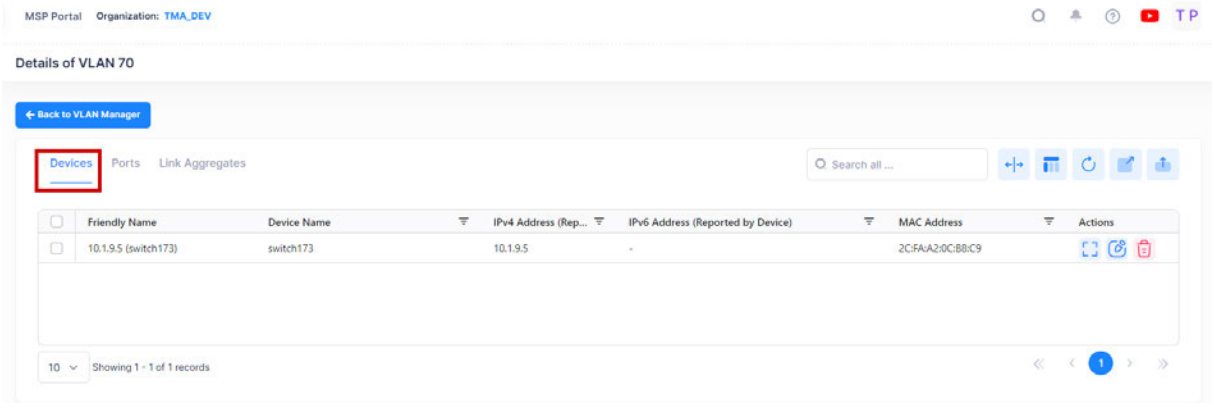
- **VLAN ID -** In compliance with the IEEE 802.1Q standard, each VLAN is identified by a unique number, referred to as the VLAN ID. This number is assigned at the time of creation of the VLAN and is not a modifiable parameter. When a network device packet is received on a port, the port's VLAN ID is inserted into the packet. The packet is then bridged to other ports that are assigned to the same VLAN ID. In essence, the VLAN broadcast domain is defined by a collection of ports and packets assigned to its VLAN ID. (Range = 1 - 4094)
- **Admin Status -** The administrative status of the VLAN (Enabled/Disabled). It display the number of devices for VLAN which are Enabled and Disabled. By default, the administrative status is

enabled when a VLAN is created. When a VLAN is administratively disabled, static port and dynamic mobile port assignments are retained but traffic on these ports is not forwarded. However, VLAN rules remain active and continue to classify mobile port traffic for VLAN membership.

- **Oper Status -** The VLAN operational status (Active/Inactive). It displays the number of devices for VLAN which are active and inactive. This parameter is not modifiable; switch software determines if the VLAN is operationally active or inactive and sets the appropriate field value. A VLAN's operational status remains inactive until at least one active switch port is assigned to the VLAN and the VLAN's administrative status is enabled. This means that VLAN properties, such as Spanning Tree or router ports, also remain inactive. Ports are considered active if they are connected to an active network device. Non-active port assignments are allowed, but do not change the VLAN's operational state.
- **VLAN Type -** The type of VLAN is determined at the time the VLAN is created (e.g., Standard, BVLAN, Control BVLAN).
- **Spanning Tree Status -** The Spanning Tree Status (Enabled/Disabled) for the VLAN. When a VLAN is created, an 802.1D standard Spanning Tree Algorithm and Protocol (STP) instance is enabled for the VLAN by default. STP evaluates VLAN port connections to determine if there are redundant data paths between the same VLAN on other switches. If a redundant path does exist, STP determines which path to block in order to provide a loop-free network topology. In this manner, STP ensures that there is always only one active data path between any two switches (VLANs). When a change occurs, such as a path is disconnected or a path cost change, the Spanning Tree Algorithm activates the blocked path to restore the network connection.

6.1.6.2 Detailed Information

The Detail Screen provides detailed information about devices in the selected VLAN. Click on the **Additional Information** button or **VLAN ID** to display Devices (see page 427), Ports (see page 428), or Link Aggregates (see page 430) information. The following screen will appears.



6.1.7 Devices

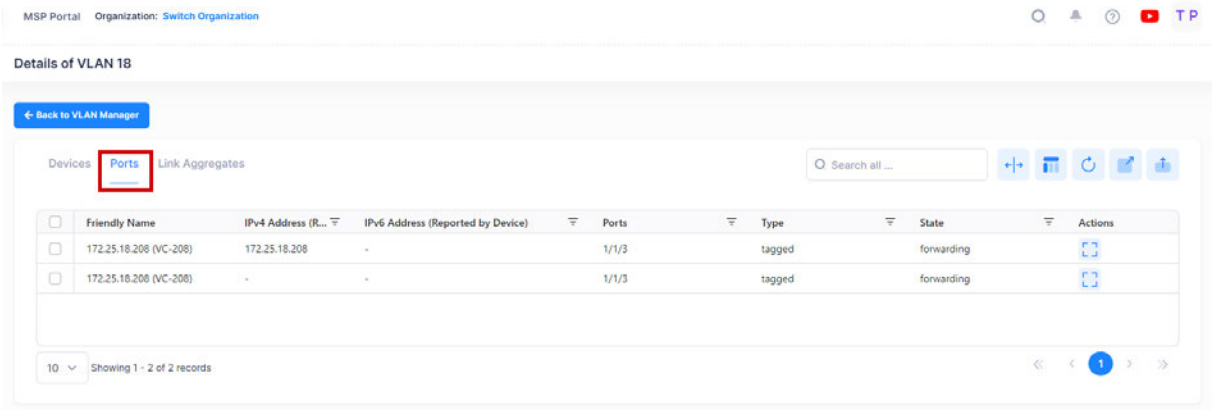
For Devices, the following field values are provided:

- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Device Name -** The user-configured name for the device.
- **IPv4 Address(reported by device) -** The IPv4 address of the device.
- **IPv6 Address(reported by device) -** The IPv6 address of the device(if defined).
- **MAC Address** - The MAC address of the device.
- **Device Version -** The version number of the device software.
- **Location -** The physical location of the device (user-defined, up to 255 characters). If you did not specify a location the field displays "Unknown".
- **Management Connectivity** - The following management connectivity values indicate the various stages of device connectivity with OmniVista.
  - **Blank** - The device is in an initial state (not yet onboarded).
  - **On** - When a device is successfully provisioned or OmniVista receives heartbeat from the device, management connectivity transitions to “On”.
  - **Unknown** - If OmniVista does not receive any heartbeat, the management connectivity status transitions from “On” to “Unknown”.
  - **Off** - After a certain amount of time with no heartbeat, the management connectivity status transitions from “Unknown” to “Off”.
- **Device Type -** The device model (e.g., AOS).
- **VLAN ID -** The VLAN ID number (e.g., VLAN 10).
- **VLAN Description -** A text string up to 32 characters. This parameter defaults to the VLAN ID number (e.g., VLAN 10) if a description is not specified at the time the VLAN is created.
- **VLAN Admin Status -** The administrative status of the VLAN (Enabled/Disabled).
- **VLAN Type -** The type of VLAN is determined at the time the VLAN is created (e.g., Standard, BVLAN, Control BVLAN).
- **Spanning Tree Status -** The Spanning Tree Status for the VLAN (Enabled/Disabled).
- **Oper Status -** The VLAN operational status (Active/Inactive).
- **Router Protocol -** The protocol for the VLAN virtual router port. If no router port is configured for the VLAN, then "Unknown" appears in this field. A VLAN is available for routing when a virtual router port is defined for that VLAN and at least one active port has joined the VLAN. If a VLAN does not have a router port, its ports are in essence firewalled from other VLANs.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.

6.1.8 Port View

You can click on the **Ports** tab to view the Port related detail information for specific VLAN as shown below.



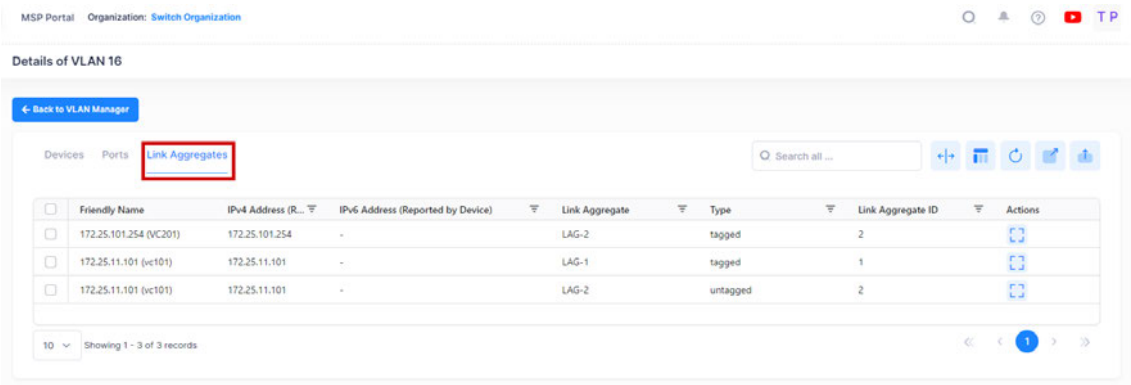
For Ports, the following field values are provided:

- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **IPv4 Address(reported by device) -** The IPv4 address of the device.
- **IPv6 Address(reported by device) -** The IPv6 address of the device(if defined).
- **Port -** The VLAN slot/port number.
- **Port Type -** The Port Type parameter indicates how the port assignment to the current VLAN was made.
  - **Default -** The port is a fixed port that was statically assigned to the VLAN, which is now the configured default VLAN for the port.
  - **Q Tagged -** The port is a fixed port that was statically assigned to the VLAN using the 802.1Q tagging feature. The VLAN is a static secondary VLAN assignment for the 802.1Q tagged port.
  - **Mobile -** The port is a mobile port that was dynamically assigned to the VLAN when traffic received on the port match traffic rules defined for the VLAN. The VLAN is a dynamic secondary VLAN assignment for the mobile port.
- **Port State -** The status of the VLAN port assignment.
  - **Forwarding -** Port is active and forwarding traffic on this VLAN.
  - **Inactive -** Port is not active (administratively disabled, down, or nothing is connected to the port).
  - **Blocking -** Port is active, but not forwarding any traffic on this VLAN.
  - **Filtering -** Mobile port traffic is filtered for the VLAN; only traffic received on the port that matches VLAN rules is forwarded. Occurs when a mobile port's VLAN is administratively disabled or the port's default VLAN status is disabled. Does not apply to fixed ports.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.

6.1.8.1 Link Aggregate View

You can click on the **Link Aggregates** tab to view the related detail information for specific VLAN as shown below.

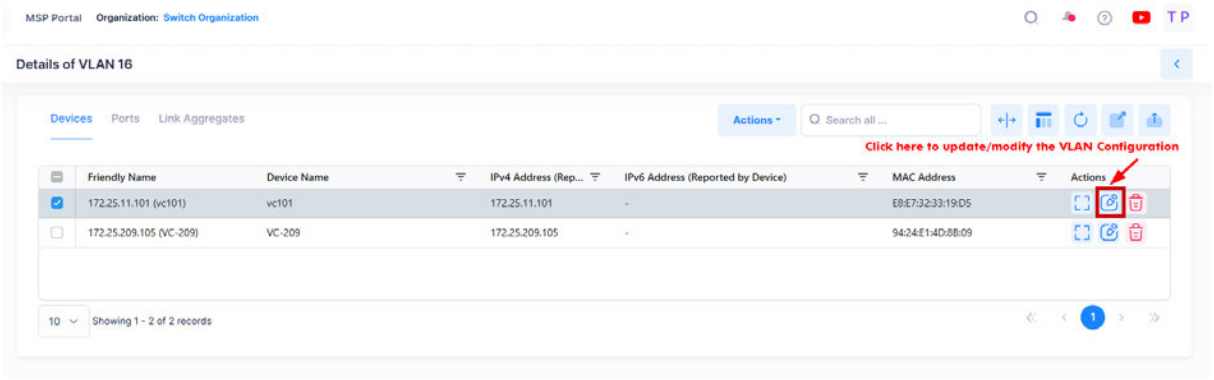


For Link Aggregates, the following field values are provided:

- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **IPv4 Address(reported by device) -** The IPv4 address of the device.
- **IPv6 Address(reported by device) -** The IPv6 address of the device(if defined).
- **Link Aggregate ID-** The ID of the link aggregate group of ports. This number was assigned when the aggregate was created.
- **Link Aggregate -** An optional textual description (up to 32 characters) for the link aggregate.
- **Type -** The Port Type parameter indicates how the port assignment to the current VLAN was made.
  - **Default -** The port is a fixed port that was statically assigned to the VLAN, which is now the configured default VLAN for the port.
  - **Q Tagged -** The port is a fixed port that was statically assigned to the VLAN using the 802.1Q tagging feature. The VLAN is a static secondary VLAN assignment for the 802.1Q tagged port.
  - **Mobile -** The port is a mobile port that was dynamically assigned to the VLAN when traffic received on the port match traffic rules defined for the VLAN. The VLAN is a dynamic secondary VLAN assignment for the mobile port.

6.1.8.2 Edit the VLAN Configuration from VLAN Details View

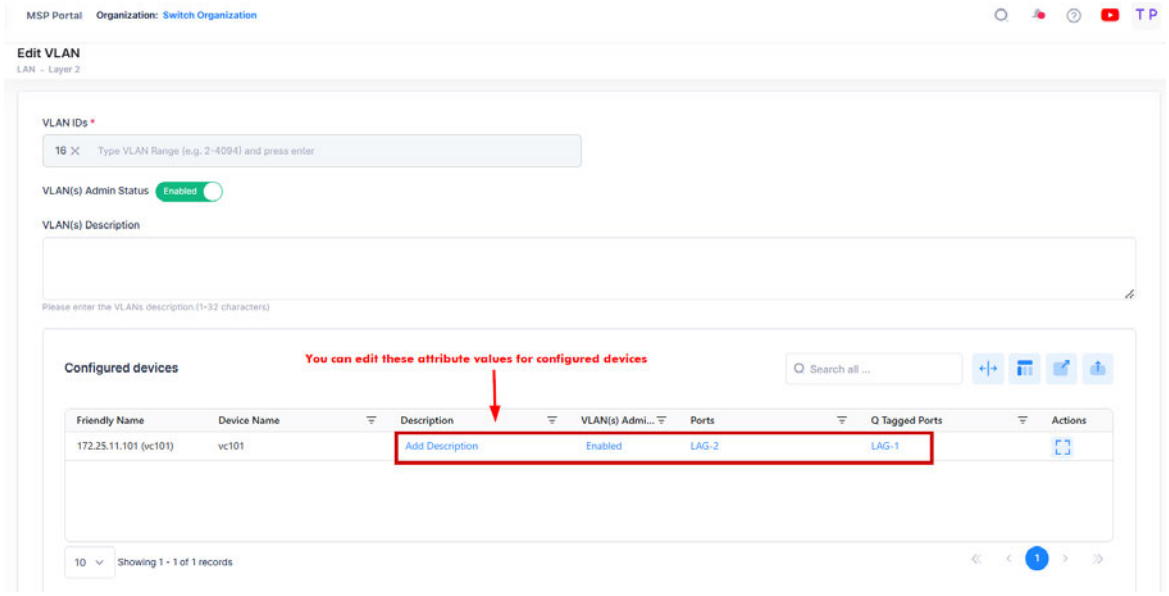
Select the device in the Devices List and click on the Edit icon under the “Actions” column to modify or update the VLAN configuration on Switch devices from the VLAN Details screen.



The Edit VLAN Information screen opens on which you can edit the VLAN(s) Admin status, VLAN(s) Description, Ports and Q tagged Ports for VLAN configuration on configured devices as shown below.

Consider the following while editing the VLAN configuration on selected devices:

1. You cannot modify the VLAN ID(s) of the devices.
2. You cannot add new devices to existing VLAN(s). Use Global VLAN Edit option from **VLANs Main Summary screen** to add new device to existing VLAN(s).
3. You can modify or update the ports and Q tagged ports value.
4. VLAN(s) Admin Status and VLAN(s) Description are the Global attribute value, therefore, the configured value will be applied to all the selected switches. You can configure this value for individual switch from “Selected devices” table by clicking on the column value.

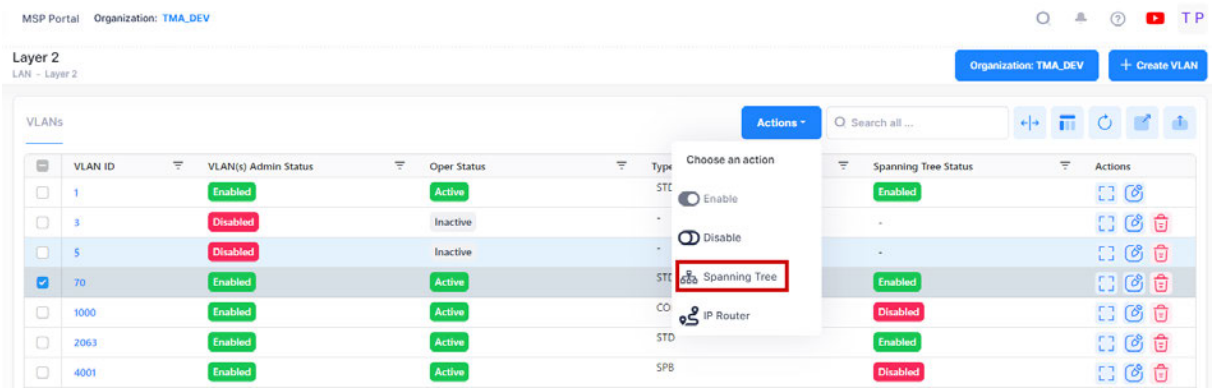


Click on **Save** button to save the changes.

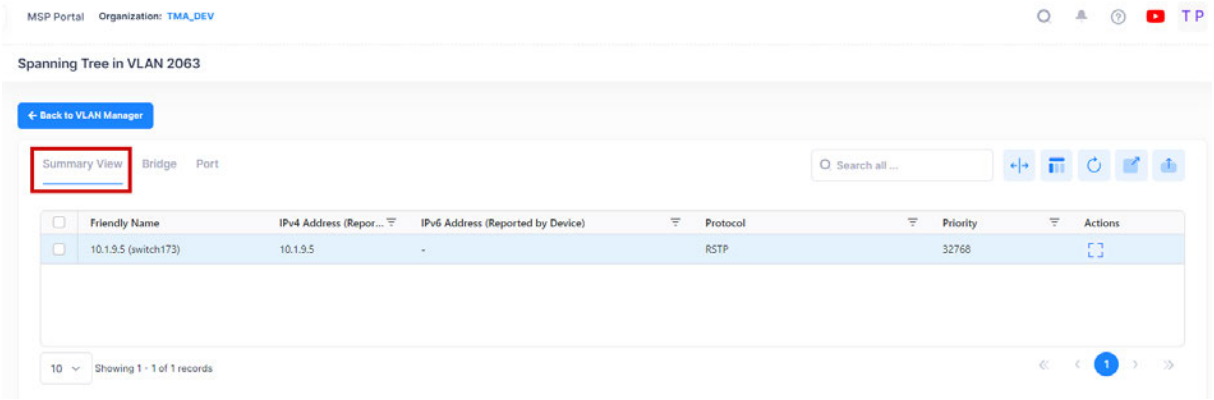
6.1.9 Viewing Spanning Tree

The Spanning Tree Screen is used to view Spanning Tree configuration information for devices in a VLAN, and to modify Spanning Tree Bridge or Port Parameters. To view/edit Spanning Tree information for a VLAN, select the VLAN in the VLANs Table, then select **Spanning Tree** from the **Actions** drop-down menu at the top of the screen.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



By default, a Summary (see page 432) view is displayed. Click on the **Bridge** or **Port** tab at the top of the screen to view bridge (see page 434) or port (see page 435) information as shown below.



6.1.9.1 Summary View

The Summary View displays a summary of the Spanning Tree information for devices in the selected VLAN. The following field values are displayed:

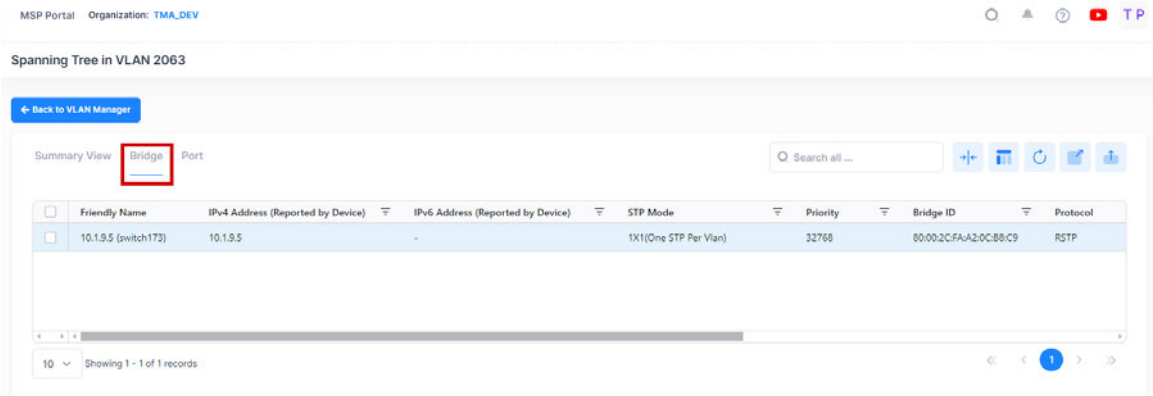
- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **IPv4 Address(reported by device) -** The IPv4 address of the device.
- **IPv6 Address(reported by device) -** The IPv6 address of the device(if defined).
- **Protocol -** The VLAN spanning tree algorithm protocol. The algorithm determines the state and role of a port within the spanning tree topology:
  - **STP (802.1D) -** Standard Spanning Tree Algorithm and Protocol (Default).
  - **RSTP (802.1W) -** Rapid Spanning Tree Algorithm and Protocol. RSTP is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure.
  - **MSTP (802.1S) -** Multiple Spanning Tree Protocol. MSTP is an enhancement to 802.1Q Common Spanning Tree Instance (CST). When the switch is running in Flat Mode, a single

Spanning Tree instance is applied across all VLAN port connections. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTI) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, Flat Mode can now support the forwarding of VLAN traffic over separate data paths. Note that MSTP in VLAN spanning tree view is only displayed for Instance 0 under VLAN 1. None of the other instances will be displayed.

- **Priority -** The bridge priority value (0 - 65535) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. (Default = 32768)
- **Maximum Age -** The amount of time, in seconds, that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. (Range = (6- 40, Default = 20)
- **Path Cost -** The cost of the path to the root for this Spanning Tree instance.
- **Mode -** The Spanning Tree operating mode for the switch:
  - **Flat Mode (Single Spanning Tree) -** The Spanning Tree Algorithm is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 both connect to the same switch, then Spanning Tree Algorithm will block one of these ports.
  - **1x1 (One Spanning Tree per VLAN) -** A single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge in that it will have its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max age and forward delay. Note: By default, the Spanning Tree operating mode is set to One Spanning Tree Per VLAN (available only on AOS switch platforms).
- **Bridge ID -** The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the bridge MAC address.
- **Root ID-** The bridge identifier of the root of the spanning tree as determined by the Spanning Tree Algorithm and Protocol.
- **Time Since Last Topology Change -** The amount of time, in hundredths of a second, since the last topology change was detected by this Spanning Tree instance.
- **Total Topology Change -** The number of topology changes detected by this spanning tree instance since the management entity was last reset or initialized.
- **Root Port -** The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.
- **Next Best Root Cost -** The cost of the next best root port for this Spanning Tree instance.
- **Next Best Root Port -** The port that offers the next best (second lowest) cost path to the root bridge for this Spanning Tree instance.
- **Network Maximum Age -** The Maximum Age time value for the root bridge.
- **Network Hello Time -** The Hello Time value for the root bridge.
- **Network Hold Time -** The amount of time, in hundredths of a second, in which this spanning tree instance can transmit no more than two Configuration Bridge Protocol Data Units (BPDU).
- **Network Forward Delay -** The forward delay time value for the root bridge.

6.1.9.2 Bridge View

The Bridge View List displays a Spanning Tree bridge information for devices in the selected VLAN. To access the Bridge View click on the **Bridge** tab in the VLAN Manager Spanning Tree screen as shown below.



The following field values are displayed:

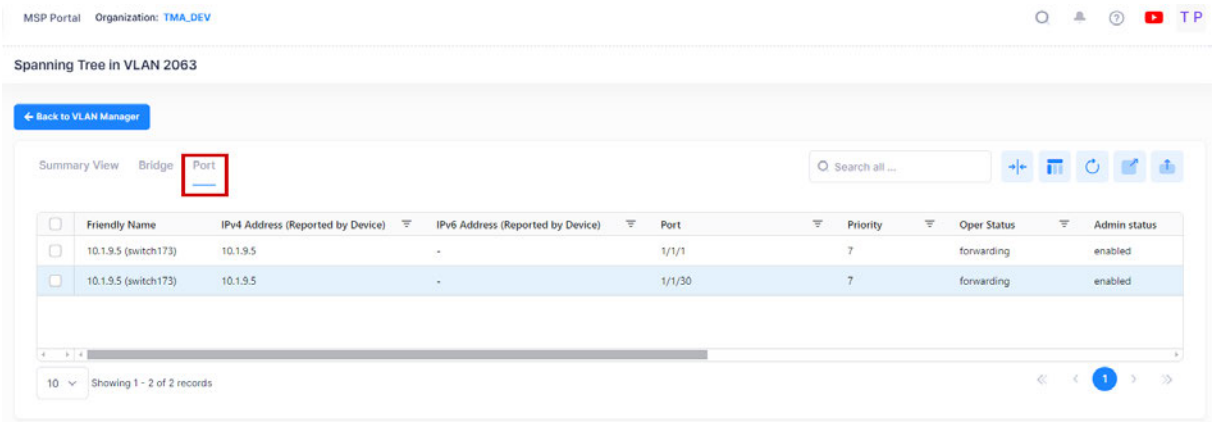
- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **IPv4 Address(reported by device) -** The IPv4 address of the device.
- **IPv6 Address(reported by device) -** The IPv6 address of the device(if defined).
- **Protocol -** The VLAN spanning tree algorithm protocol. The algorithm determines the state and role of a port within the spanning tree topology:
  - **STP (802.1D) -** Standard Spanning Tree Algorithm and Protocol (Default).
  - **RSTP (802.1W) -** Rapid Spanning Tree Algorithm and Protocol. RSTP is based on the 802.1D standard algorithm and is designed to provide quick recovery in the event of a link, port or device failure.
  - **MSTP (802.1S) -** Multiple Spanning Tree Protocol. MSTP is an enhancement to 802.1Q Common Spanning Tree Instance (CST). When the switch is running in Flat Mode, a single Spanning Tree instance is applied across all VLAN port connections. MSTP allows the configuration of Multiple Spanning Tree Instances (MSTI) in addition to the CST instance. Each MSTI is mapped to a set of VLANs. As a result, Flat Mode can now support the forwarding of VLAN traffic over separate data paths. Note that MSTP in VLAN spanning tree view is only displayed for Instance 0 under VLAN 1. None of the other instances will be displayed.
- **Priority -** The bridge priority value (0 - 65535) for the VLAN. The lower the number, the higher the priority value. The bridge priority value is used by the spanning tree algorithm to determine which VLAN should serve as the root of the spanning tree. (Default = 32768)
- **STP Mode -** The Spanning Tree operating mode for the switch:
  - **Flat Mode (Single Spanning Tree) -** The Spanning Tree Algorithm is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 both connect to the same switch, then Spanning Tree Algorithm will block one of these ports.

- **1x1 (One Spanning Tree per VLAN) -** A single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge in that it will have its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max age and forward delay. Note: By default, the Spanning Tree operating mode is set to One Spanning Tree Per VLAN (available only on AOS switch platforms).

- **Bridge ID -** The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the bridge MAC address.
- **Network Maximum Age -** The amount of time, in seconds, that spanning tree information learned from BPDUs received on VLAN ports is retained. When this information has aged beyond the maximum age value, the information is discarded. (Range = (6- 40, Default = 20)
- **Network Hello Time -**The Hello Time value for the root bridge.
- **Network Forward Delay -**The forward delay time value for the root bridge.

6.1.9.3 Port View

The Port View List displays a Spanning Tree port information for devices in the selected VLAN. To access the Port View click on the **Port** tab in the VLAN Manager Spanning Tree screen as shown below.



The following field values are displayed:

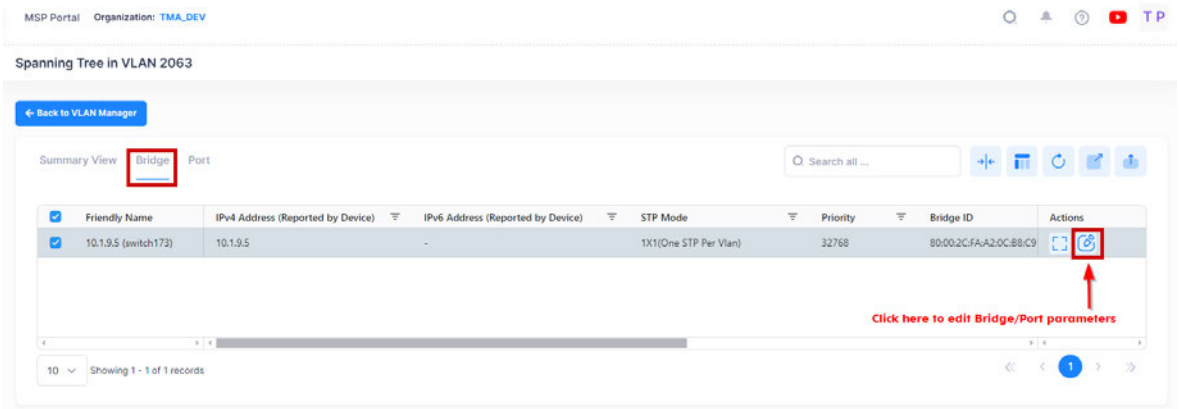
- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **IPv4 Address(reported by device) -** The IPv4 address of the device.
- **IPv6 Address(reported by device) -** The IPv6 address of the device(if defined).
- **Port -** The slot/port number.
- **Priority -**The port priority value for the VLAN. The lower the number, the higher the priority value. The port priority is used to determine which port offers the best path to the root when multiple paths have the same path cost. If the priority values are the same for all ports in the path, then the port with the lowest physical switch port number is selected. (Range = (0 - 15, Default = 7)
- **Oper Status -** The operational state of the port as determined by the spanning tree algorithm:

  - **Disabled -** Physical port is down or administratively disabled.
  - **Blocking or Discarding -** Port does not transmit or receive data to prevent a network loop.
  - **Listening -** Port is preparing to transmit data.
  - **Learning -** Port is learning MAC addresses seen on the port.
  - **Forwarding -** Port is transmitting and receiving data.
- **Admin Status -** The Spanning Tree status for the port (Enabled/Disabled). If disabled, the port state is set to forwarding for the VLAN Spanning Tree instance. This status value, however, is ignored if Spanning Tree is disabled for the associated VLAN. By default, Spanning Tree is enabled on all switch ports.
- **Path Cost -** The path cost value for the port. This value specifies the contribution of a port to the path cost towards the root bridge that includes the port. If the path cost is set to 0, then a default value based on link speed is used. (Range = (0 - 65535).
- **Manual Mode -** The mode used for managing the port's state:
  - **Blocking or Forwarding (Manually Set) -** If the port state is manually set to Blocking or Forwarding, the port remains in that state until it is changed and does not participate in the spanning tree algorithm.
  - **No (Dynamic) -** Dynamic mode defers configuration of the port state to the spanning tree algorithm. By default, this parameter is set to No (Dynamic).
- **Admin Connection -** The port's administratively set connection type. This parameter is used by the 802.1w Rapid Spanning Tree Protocol (RSTP) to determine if a port is eligible for rapid transition to the forwarding state.
  - **No Point to Point -** Port connects to multiple switches.
  - **Point to Point -** Port connects directly to another switch.
  - **Auto Point to Point -** Connection type is automatically defined to No Point to Point or Point to Point based on the port's operational status. (Default)
  - **Edge Port -** Port is at the edge of a bridged LAN, does not receive BPDU, and has only one MAC address learned. Edge ports, however, will operationally revert to a No Point to Point connection type if a BPDU is received on the port.
- **Port Role -** The role of the port for this Spanning Tree instance (e.g., Root, Designated, Alternate, Backup).
- **Oper Connection -** The operational connection type for the port:
  - **No Point to Point -** Port connects to multiple switches.
  - **Point to Point -** Port connects directly to another switch.
  - **Auto Point to Point -** Connection type is automatically defined to No Point to Point or Point to Point based on the port's operational status. (Default)
  - **Edge Port -** Port is at the edge of a bridged LAN, does not receive BPDU, and has only one MAC address learned. Edge ports, however, will operationally revert to a No Point to Point connection type if a BPDU is received on the port.
  - **Non-Significant -** Port is inactive.

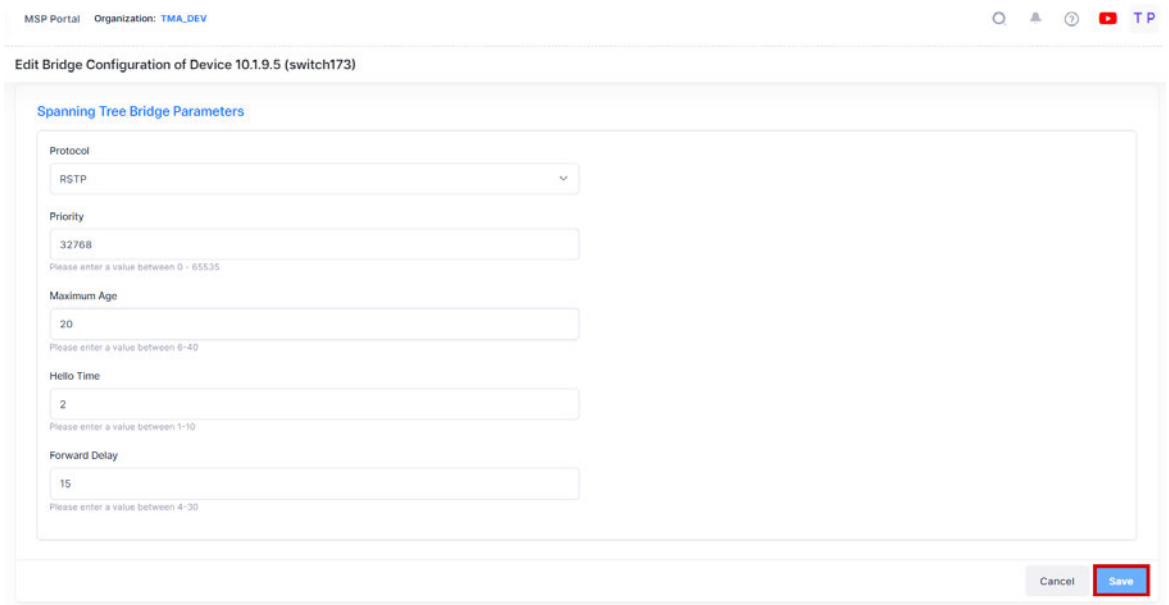
6.1.10 Editing an STP Configuration

You can edit Spanning Tree Bridge or Port parameters on switches in a VLAN. Select the VLAN in the VLANs Table, then select Spanning Tree from the **Actions** drop-down menu at the top of the screen to bring up the Spanning Tree Summary View Table for the VLAN.

Click on the **Bridge** or **Port** tab at the top of the table to bring up the Bridge or Port Table. Select a switch/port in a table then click on the Edit icon.



The following screen will appears:



Edit the Bridge (see page 434) or Port (see page 435) parameters as described above and click on the **Save** button. Repeat to edit additional Bridge or Port parameters.

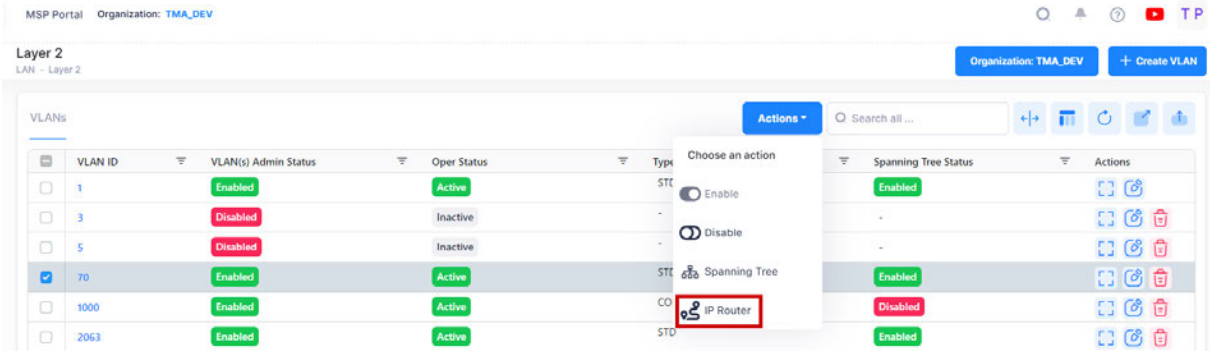
Note: Spanning Tree software is active on all switches by default. As a result, a loop-free network topology is automatically calculated based on default Spanning Tree switch, VLAN (bridge), and port parameter values. It is only necessary to configure Spanning Tree bridge parameters to change how the topology is calculated and maintained.

6.1.11 IP Router

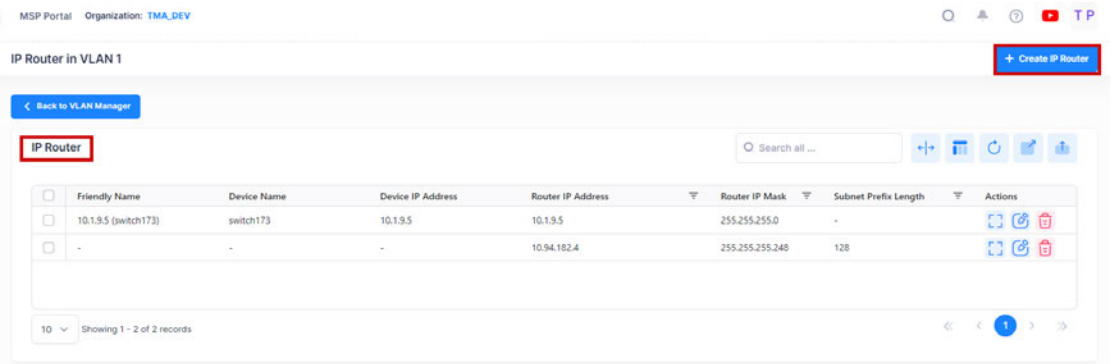
Network device traffic is bridged (switched) at the Layer 2 level between ports that are assigned to the same VLAN. However, if a device needs to communicate with another device that belongs to a different VLAN, you must configure an IP router interface on a device in the VLAN to enable Layer 3 routing to transmit traffic between VLANs.

A VLAN is available for routing when at least one IP router interface is defined for that VLAN and at least one active port is associated with the VLAN. If a VLAN does not have a router interface, the ports associated with that VLAN are in essence firewalled from other VLANs.

The IP Router Screen in the VLANs application is used to view and configure IP Routers on a VLAN. To configure an IP router for a VLAN, select the VLAN in the VLANs Table, then select **IP Router** from the **Actions** drop-down menu at the top of the screen.



The IP Router Screen will appear:



The VLAN Manager IP Router Screen displays (see page 438) all configured IP router interfaces for the selected VLAN. It is also used to create (see page 439), edit (see page 440), and delete (see page 441) IP router interfaces on devices in the VLAN.

6.1.11.1 Viewing IP Router Interfaces

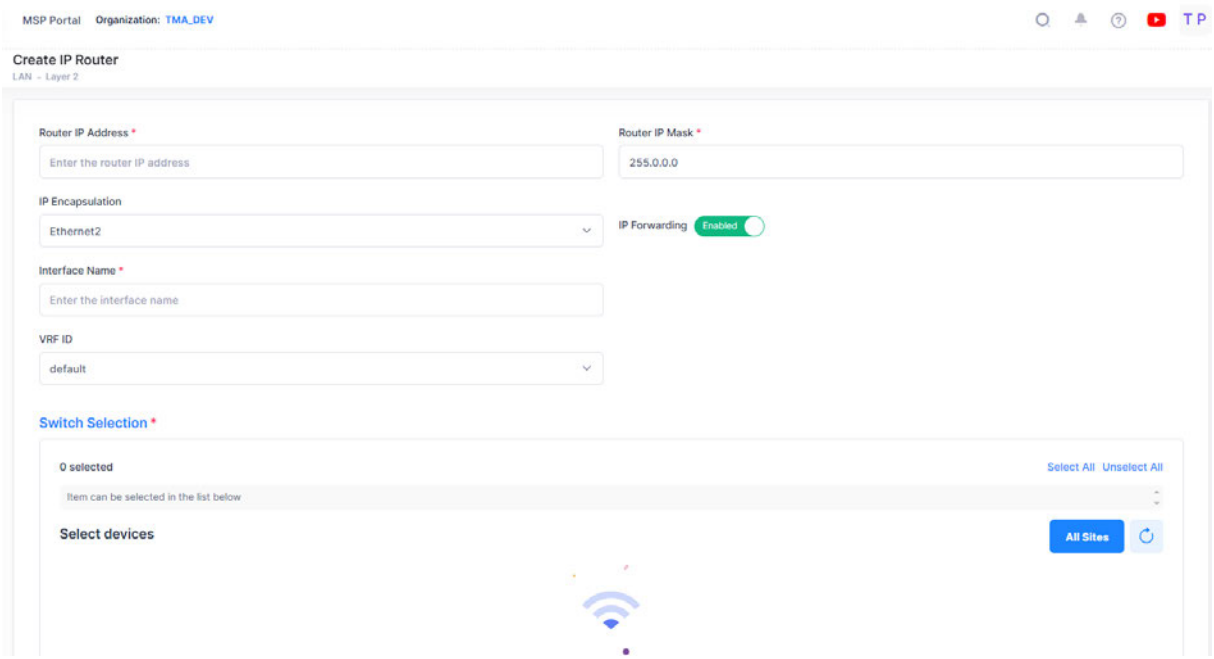
The Router Screen displays all configured IP router interfaces for the selected VLAN. The fields are defined below.

- **Device Name -** The user-configured name for the device on which the interface is configured.

- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Device IP Address -** The IP address of the device.
- **Router IP Address -** The IP address of the IP router interface.
- **Router IP Mask -** The IP router subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **Subnet Prefix Length** - The number that specifies the range of devices on a network and is written as a slash (/) followed by an integer between 1 and 128.
- **IP Encapsulation -** The IP router interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **IP Forwarding -** The router interface forwarding status (Enabled/Disabled). A forwarding router interface sends IP frames to other subnets. A "no forwarding" router interface acts as a host only. It receives IP frames from other router interfaces. (Default = Enabled).
- **Interface Name -** The user-defined interface name (up to 20 characters).
- **VRF ID -** The VRF ID. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured, or if the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance.

6.1.11.2 Creating an IP Routing Interface

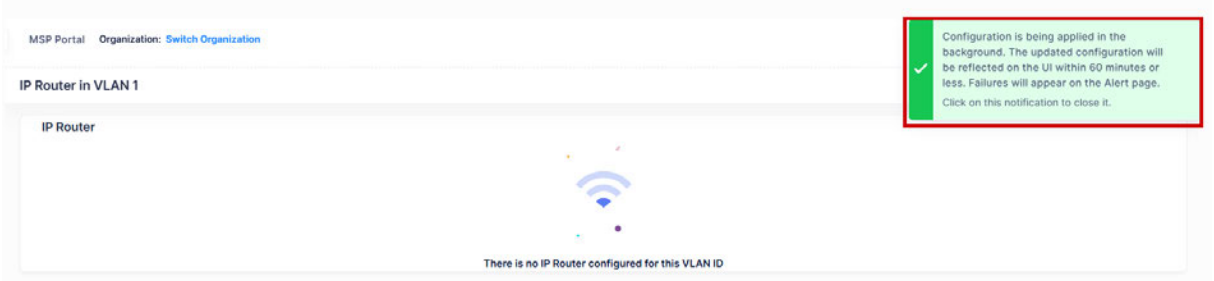
Click on the **Create IP Router** tab to create an IP router interface on a device in a VLAN. The following create screen appears:



Complete the fields as described below, then click on the **Create** button.

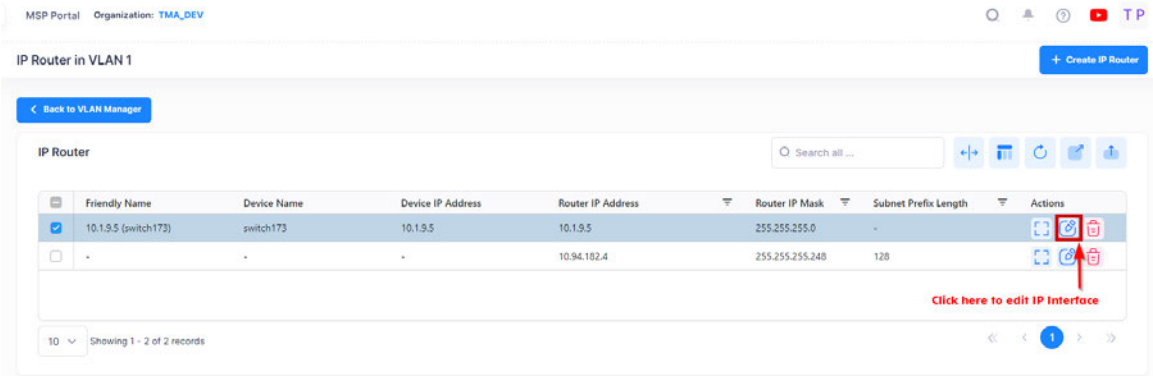
- **Router IP Address -** The IP address of the IP router interface. Router interface IP addresses must be unique. You cannot have two router interfaces with the same IP address.
- **Router IP Mask -** The IP router subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **IP Encapsulation -** The IP router interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the router interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **IP Forwarding -** The router interface forwarding status (Enabled/Disabled). A forwarding router interface sends IP frames to other subnets. A "no forwarding" router interface acts as a host only. It receives IP frames from other router interfaces. (Default = Enabled).
- **Interface Name -** The user-defined interface name (up to 32 characters).
- **VRF ID -** The VRF ID. If configured, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface. If the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance.
- **Switch Selection** - Select a Switch device from the available list of devices that are members of the VLAN by clicking on the checkbox next to the **Select devices** list. Select the device(s) on which you want to create an IP router interface and click on **Create** button.

Note: When you request for **create/update/delete** of an IP Router Interface from OminVista Terra, the configuration operation is done in the background. You can view the updated configuration results after certain time interval and the following alert message appears on the screen as shown below.



6.1.11.3 Editing an IP Router Interface

To edit an IP router interface on a device, select the interface in the IP Router Table and click on the Edit icon.

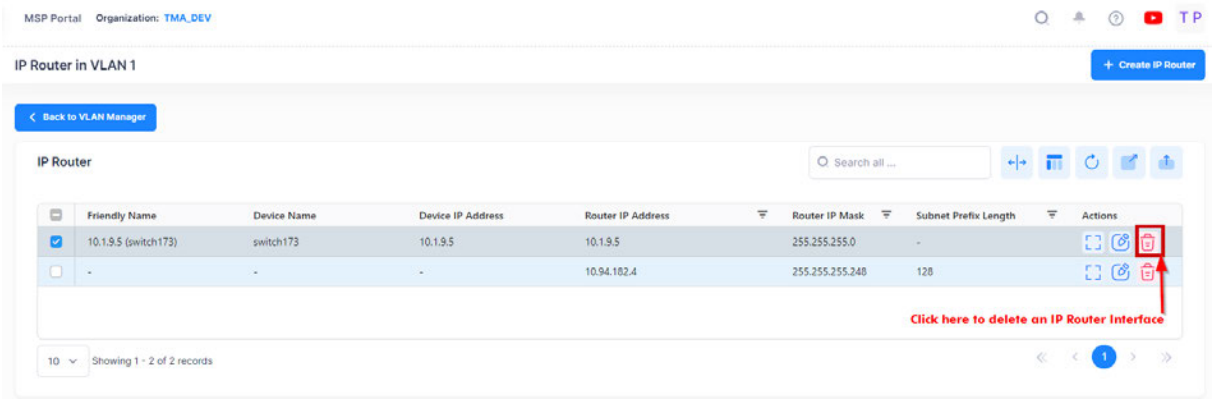


Edit any fields as described above (see page 440) and click on **Save**.

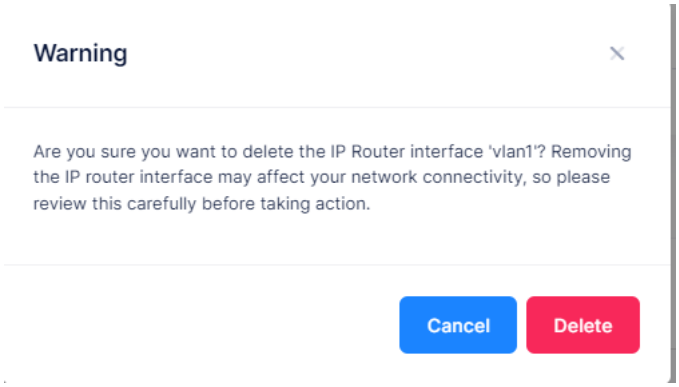
> You cannot edit the Interface Name or VRF fields.

6.1.11.4 Deleting an IP Router Interface

To delete an IP router interface, select the interface in the IP Router Table, then click on the Delete icon as shown below.



When you select the IP Router Interface you want to delete, the following confirmation prompt appears:



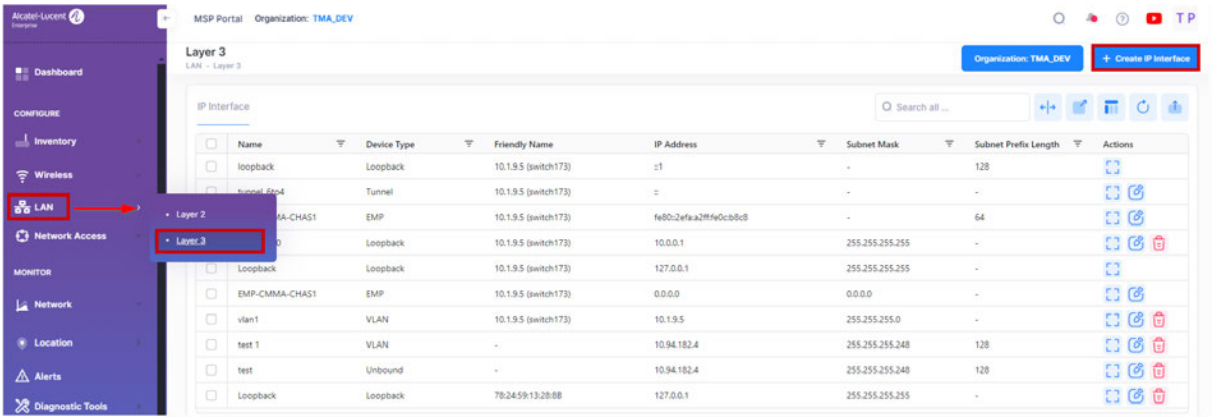
Click on **Delete** to confirm that you want to delete the selected IP Router Interface. The IP Router Interface will be removed from all the devices to which it was assigned.

21 Oct 2025

6.2 Configure and Manage Layer 3 VLANs

The VLAN Manager IP Interface Screen is used to view (see page 448) configured IP interfaces on a device; and to create (see page 443), edit (see page 446), and delete (see page 447) IP interfaces on devices.

To manage the VLAN configuration, navigate to the IP Interface screen by clicking on **LAN > Layer 3** under the “Configure” section of the OmniVista Terra Menu (see page 45). The IP Interface screen displays.



6.2.1 Creating an IP Interface

The Create IP Interface screen is used to create an IP Interface on a device. To access this screen, click on **Create IP Interface** button.

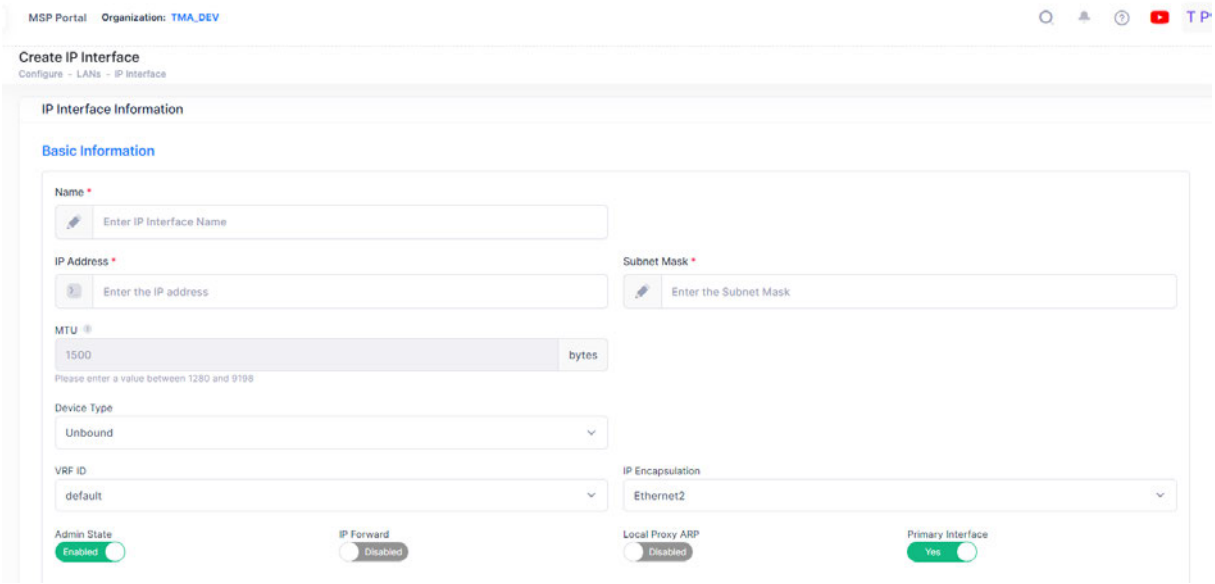
The Create IP Interface screen provides the following step-by-step process for creating an IP interface:

- **Basic information** (see page 443) - Configures the interface name, IP address, subnet mask and device type.
- **Switch Selection** (see page 445) - Select the Switch or LAN devices from the available list to create an IP Interface .

Complete the following sections of the Create IP Interface screen, then click on **Create** Button.

6.2.1.1 Basic Information

Complete the fields as described below for configuring basic information to create an IP Interface.



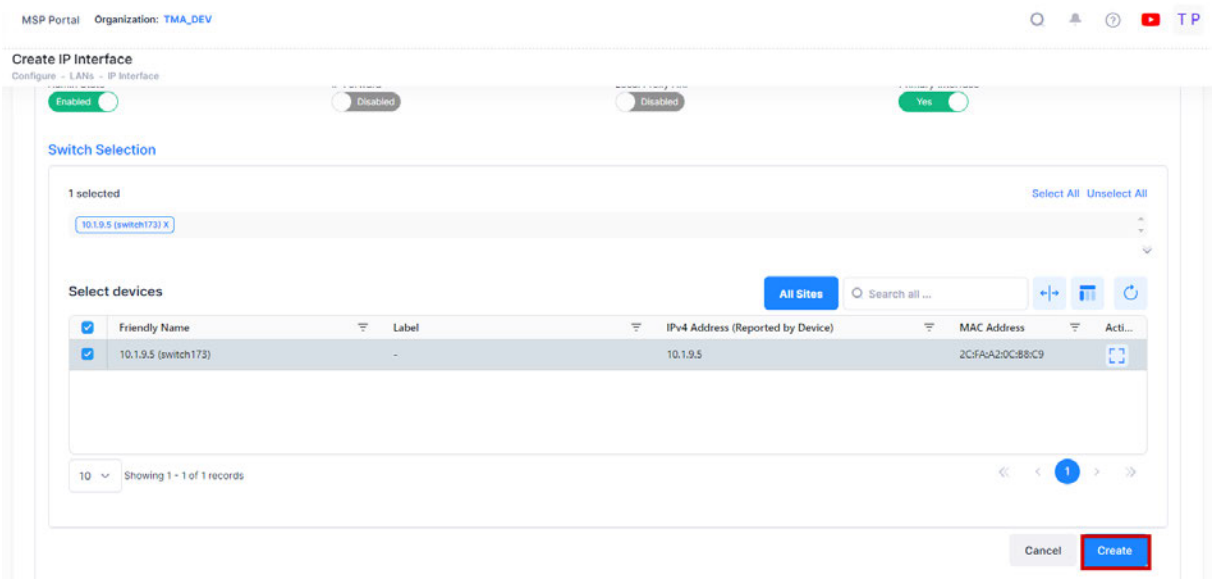
- **Name -** The user-configured interface name.
- **IP Address -** The IP address of the IP interface.
- **Subnet Mask -** The IP interface subnet mask value. The default value for this field is based on which network class range the IP address falls within; Class A, B, or C. (255.0.0.0, 255.255.0.0, or 255.255.255.0).
- **MTU -** The Maximum Transmission Unit size set for the interface.
- **Device Type -** The type of device bound to the interface:
  - **Unbound -** No device is bound to the interface.
  - **VLAN -** Associates a VLAN with the interface. You must enter the VLAN ID in the VLAN ID field.
  - **EMP -** The Ethernet Management Port is bound to the interface.
  - **Loopback -** A loopback interface configured for testing.
  - **GRE Tunnel -** A GRE Tunnel is configured for the interface. You must enter the Tunnel Source and Destination.
  - **IPIP Tunnel -** An IPIP Tunnel is configured for the interface. You must enter the Tunnel Source and Destination.
  - **VPN Tunnel** -A VPN tunnel is configured for the interface. Please note that the device type "VPN Tunnel" option is only available if the VPN tunnel is created prior to the creation of the IP interface.
- **VRF ID -** The VRF ID. If the device supports the Multiple VRF feature, select a VRF from the drop-down menu to assign the interface to a configured VRF instance (by default all interfaces are assigned to the Default VRF). You can assign a new interface to a VRF; however, you cannot edit the VRF ID of an existing interface. If the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance. VRF instances are created on the switch through the CLI or WebView application.
- **IP Encapsulation -** The IP interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the interface uses when generating frames that are

forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)

- **Admin State -** The administrative state of the interface (Enable/Disabled). (Default = Enabled)
- **IP Forward -** The interface forwarding status (Enabled/Disabled). A forwarding interface sends IP frames to other subnets. A "no forwarding" interface acts as a host only. It receives IP frames from other interfaces. (Default = Enabled).
- **Local Proxy ARP -** Local Proxy ARP status (Enabled/Disabled). The Local Proxy ARP feature is an extension of the Proxy ARP feature, but is enabled on an IP interface and applies to the VLAN bound to that interface. When Local Proxy ARP is enabled, all ARP requests received on VLAN member ports are answered with the MAC address of the IP interface that has Local Proxy ARP enabled. In essence, all VLAN traffic is now routed within the VLAN instead of bridged. (Default = Disabled)
- **Primary Interface -** If set to "Yes", designates the IP interface as the primary interface for the VLAN. If set to "No", the first interface bound to the VLAN becomes the primary by default. (Default = “Yes”)

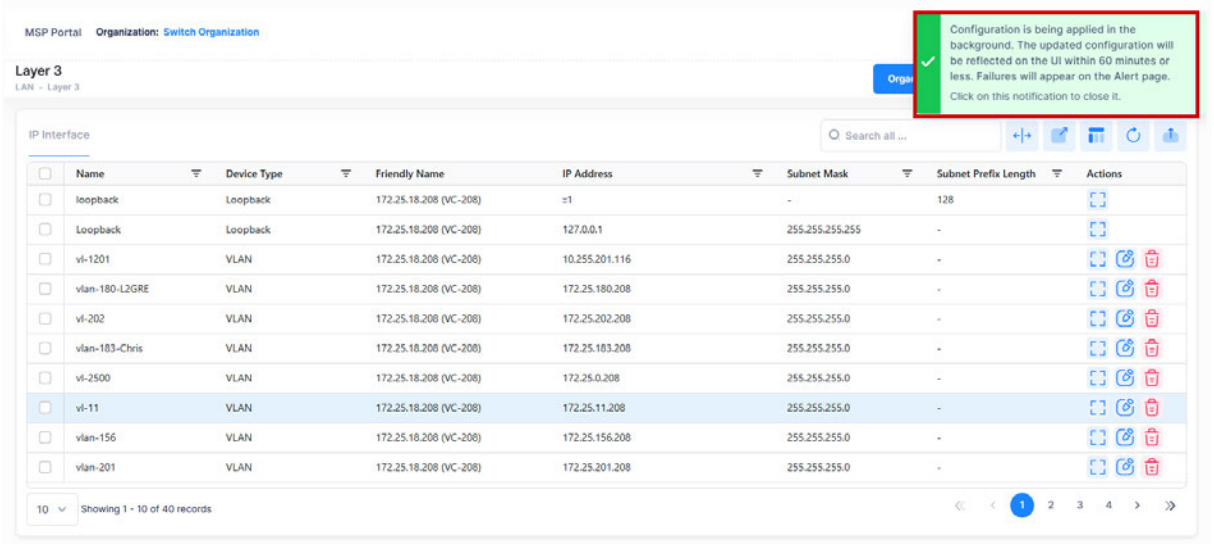
6.2.1.2 Switch Selection

Select the devices from the available list on which you want to configure the interface. You can select the multiple devices also.



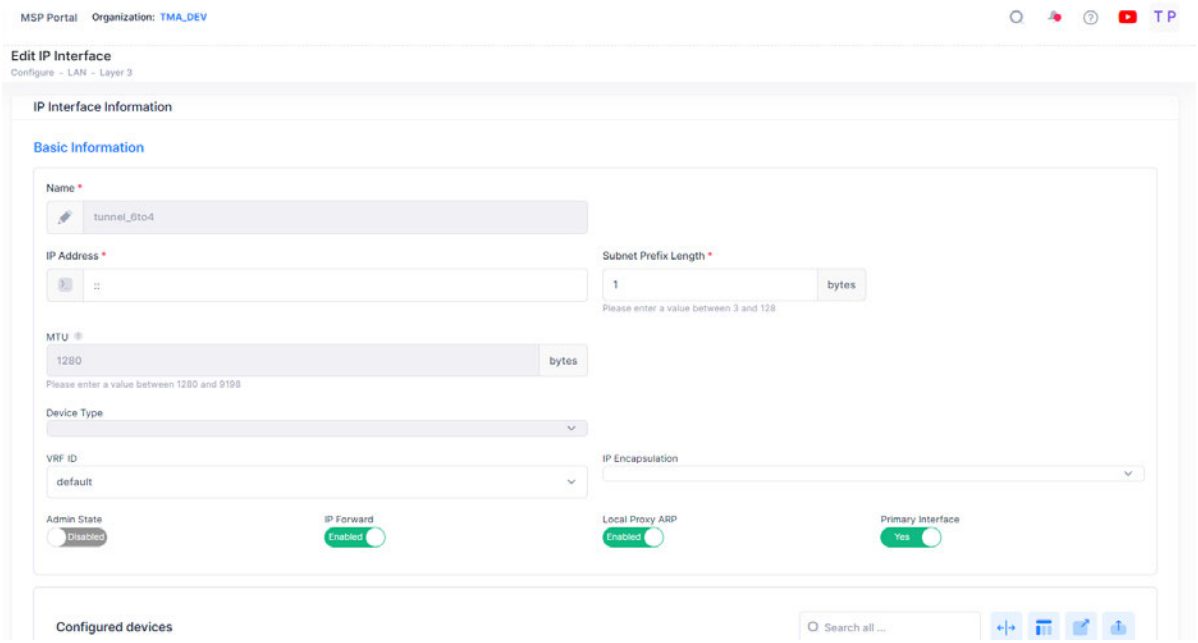
When you are done with the Switch Selection, click on **Create** button to complete the process of Creating an IP Interface.

Note: When you requests for **create/update/delete** of an IP Interface from OminVista Terra, the configuration operation is done in the background. You can view the updated configuration results after certain time interval and the following alert message appears on the screen as shown below.



6.2.2 Editing an IP Interface

Select an IP Interface from the IP Interface List and click on the Edit icon under the “Actions” column. The Edit IP Interface Information screen opens on which you can edit the basic information and add new devices or remove existing devices from the configured devices list for an IP Interface, as described above (see page 444).



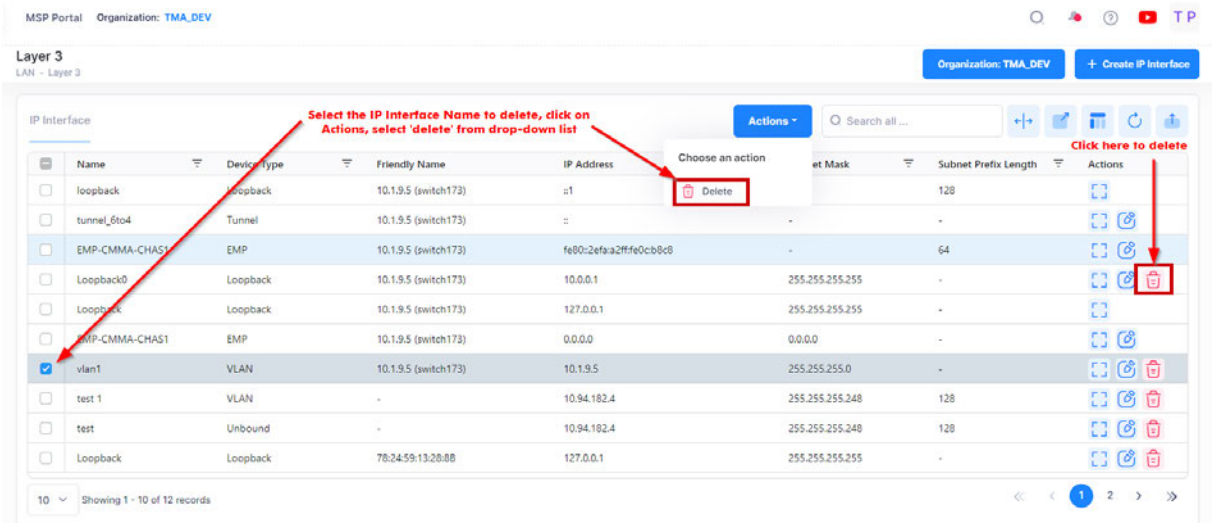
Click on **Save** button to save the changes.

Note: You cannot edit the Interface Name, Device type, and VRF fields. IP Interfaces with device type 'Loopback' and name as 'Loopback' (case sensitive for IPv4 interface and case insensitive for IPv6 interface) cannot be edited.

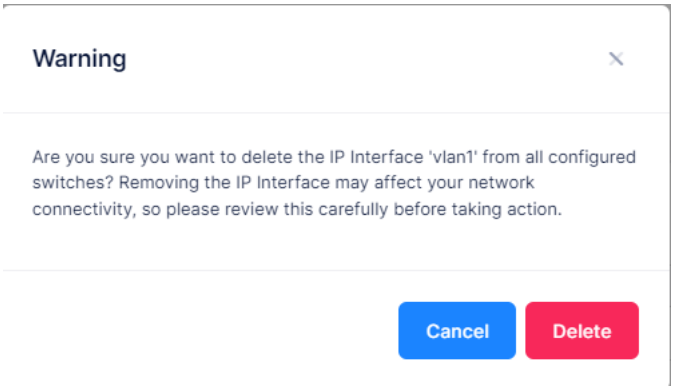
6.2.3 Deleting an IP Interface

To delete an IP Interface, use one of the following methods to select the interface you want to delete:

- Select the IP Interface name to delete by clicking on the checkbox next to the list, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the list that you want to delete.



When you select the IP Interface you want to delete, the following confirmation prompt appears:



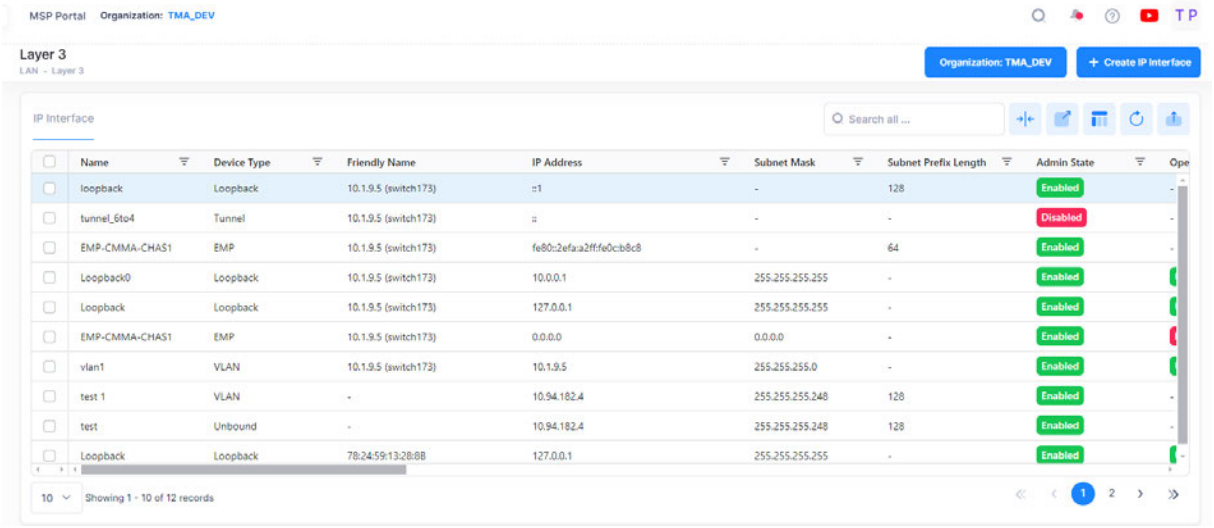
Click on **Delete** to confirm that you want to delete the IP Interface.

Consider the following use cases while deleting an IP Interface:

1. IP Interfaces with device type 'EMP' cannot be deleted.
2. IP Interface with device type 'Tunnel' and name 'tunnel_6to4' cannot be deleted.
3. IP Interfaces with device type 'Loopback' and name 'Loopback' (case sensitive for IPv4 interface and case insensitive for IPv6 interface) cannot be deleted.

6.2.4 View IP Interfaces

The Interface List displays basic and detailed information for all IP interfaces configured for the devices. Click on an entry in the list to view additional information about an interface.



The following field values will be displayed:

- **Name -** The user-configured interface name.
- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **IP Address -** The IP address of the IP interface.
- **Subnet Mask -** The IP interface subnet mask value.
- **Subnet Prefix Length** - The number that specifies the range of devices on a network and is written as a slash (/) followed by an integer between 1 and 128.
- **Admin State -** The administrative state of the interface (Enable/Disabled).
- **Oper State -** The operational state of the interface.
- **Device Type -** The type of device bound to the interface:
  - **Unbound -** No device is bound to the interface.
  - **VLAN -** Associates a VLAN with the interface. You must enter the VLAN ID in the VLAN ID field.
  - **EMP -** The Ethernet Management Port is bound to the interface.
  - **Loopback -** A loopback interface configured for testing.
  - **GRE Tunnel -** A GRE Tunnel is configured for the interface. You must enter the Tunnel Source and Destination. The GRE Tunnel devices are supported only on OS10K Switches.
- **IP Forward -** The interface forwarding status (Enabled/Disabled). A forwarding interface sends IP frames to other subnets. A "no forwarding" interface acts as a host only. It receives IP frames from other interfaces. (Default = Enabled).
- **MTU -** The Maximum Transmission Unit size set for the interface.
- **VLAN ID -** Interface is associated with a VLAN ID..

- **IP Forward -** The interface forwarding status (Enabled/Disabled). A forwarding interface sends IP frames to other subnets. A "no forwarding" interface acts as a host only. It receives IP frames from other interfaces. (Default = Enabled).
- **IP Encapsulation -** The IP interface frame encapsulation value (Ethernet 2 or SNAP). The frame encapsulation determines the framing type the interface uses when generating frames that are forwarded out VLAN ports. Select an encapsulation that matches the encapsulation of the majority of IP VLAN traffic. (Default = Ethernet 2)
- **VRF ID -** The VRF ID. If multiple VRFs are configured on the device, the VRF ID is displayed. If none are configured, or if the feature is not available on the device, the column will display "Default", indicating that the switch is operating as a single routing instance.
- **Local Proxy ARP -** Local Proxy ARP status (Enabled/Disabled). (Default = Disabled)
- **Primary Interface -** If set to "True", designates the IP interface as the primary interface for the VLAN. If set to "False", the first interface bound to the VLAN becomes the primary by default. (Default = False)
- **Oper Reason -** An explanation of the operational state. If the interface is up the field will indicate "Interface Up". If the interface is down, an explanation is displayed:
  - **Unbound -** No device is bound to the interface.
  - **Device Down -** Device bound to the interface is down.
  - **Admin Down -** The admin state of the interface is down.
  - **No Such Device -** Device does not exist.
  - **No Router MAC -** No MAC address available for the interface.
  - **Tunnel Source Invalid -** The source IP address of the tunnel is invalid.
  - **Tunnel Destination Unreachable -** The destination IP address of the tunnel is not reachable.
- **Router MAC -** The switch MAC address assigned to the interface. Each interface assigned to the same VLAN shares the same switch MAC address.
- **Broadcast Address -** The default broadcast address value. The default value for this field is based on the default network class range of the IP address assigned to the router interface. For example, a class A IP address, such as 10.0.0.2, has a default broadcast address of 10.255.255.255. A class C address, such as 198.181.10.2, has a default broadcast address of 198.181.10.255.
- **Actual Primary -** Indicates if the interface is the configured and/or actual primary interface for the device (True/False).
- **Tunnel ID** - The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
- **Tunnel Source IP Address Type** - The source IP address is specified in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
- **Tunnel Source IP Address** - A tunnel source IP address is the interface that is used as the source address for an encapsulated GRE or IPIP packet.
- **Tunnel Destination IP Address Type** - The destination IP address is specified in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

- **Tunnel Destination IP Address** - A tunnel destination IP address is the interface that is used as the destination address for an encapsulated GRE or IPIP packet.

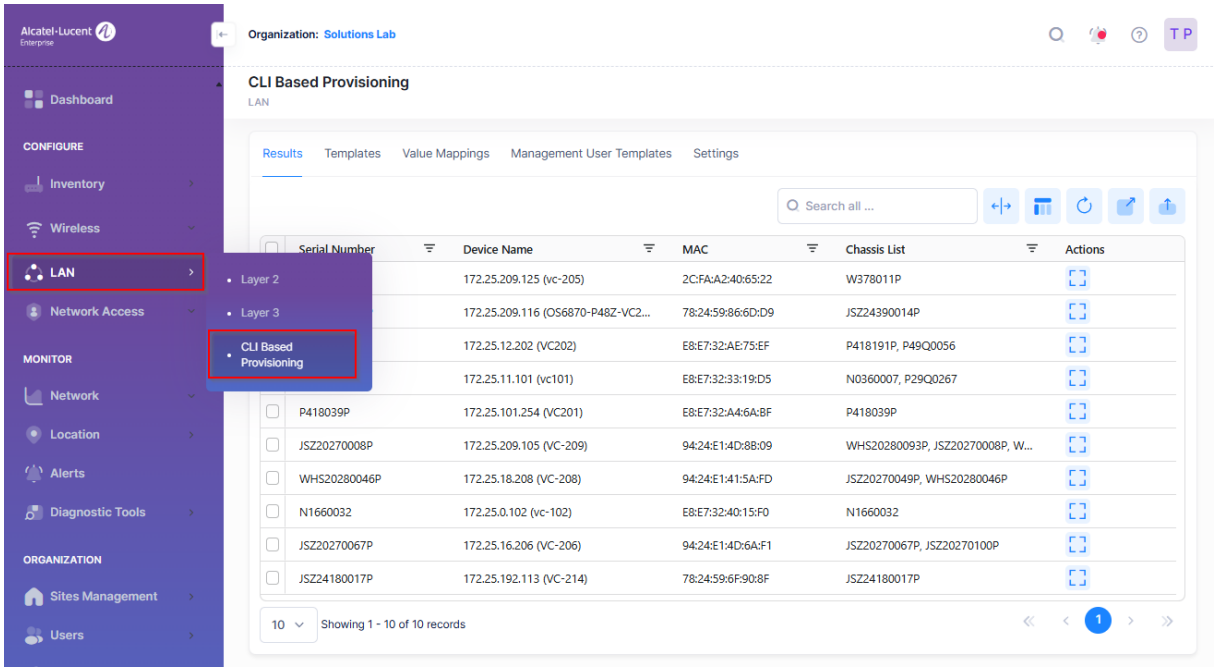
21 Oct 2025

6.3 CLI Based Provisioning

CLI-based provisioning provides a simplified method for deploying Switches. User-configured templates are utilized to automatically push Management User and Switch Configurations to Switches. Using CLI-based provisioning, you create Management User and Switch Provisioning Templates for specific switches. The templates are assigned to a Switch when the Switch is added to the Device Catalog (see page 195). When a switch contacts the OmniVista Terra Activation Server, the Management User and Switch Provisioning Templates are automatically pushed to the switch. Once the configuration is complete, the switch is onboarded and is manageable by OmniVista Terra.

> There are switch configuration steps that must be completed to enable provisioning on a switch. See Onboarding Devices for OmniVista Terra Management (see page 13) for more information about provisioning switches, including switch setup, configuration workflow, and troubleshooting.

To access CLI-based provisioning, click on **LAN > CLI Based Provisioning** under the “Configure” section of the OmniVista Terra Menu (see page 45).



The following CLI-based provisioning screens are used to provision Switches:

- **Results** (see page 453)- Displays information about all switches that have gone through the provisioning process (e.g., templates pushed to the switch, provisioning success/failure). The screen is also used to "Force Provision" a configuration to a provisioned switch. When you "Force Provision", the configuration is pushed to the switch the next time the switch contacts the OmniVista Terra Server.
- **Templates** (see page 459)- Displays a list of Configuration Templates that you can use to push a configuration to the Switch. The Configuration Template contains CLI commands that are

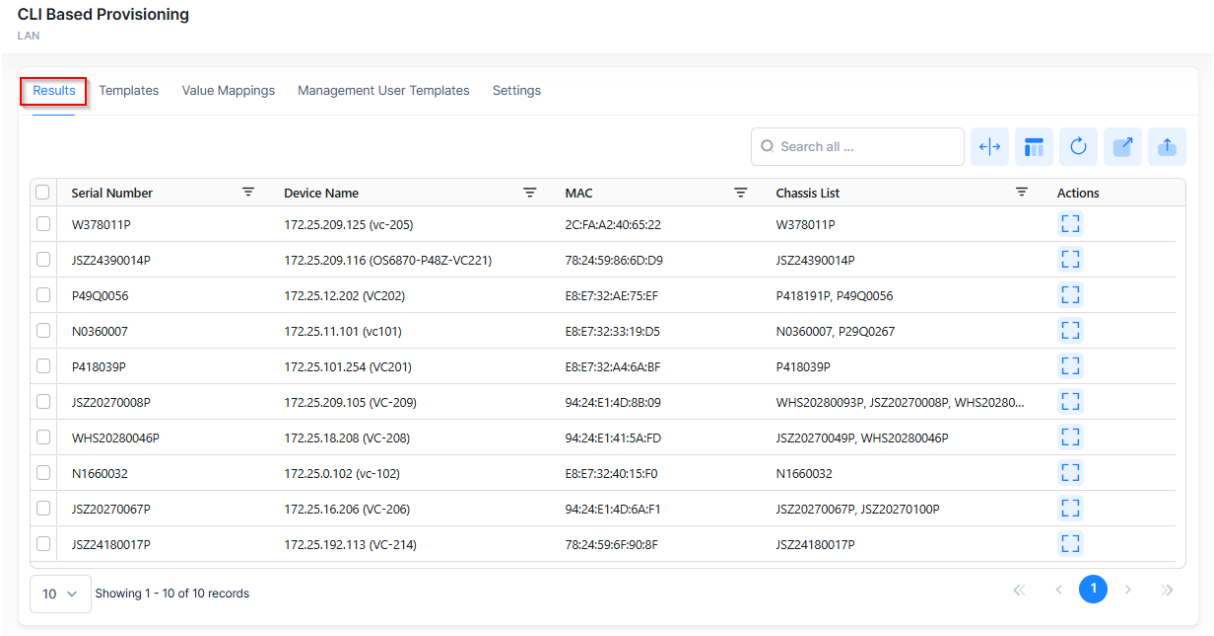
applied during the onboarding process before the Switch becomes managed. This screen is also used to create, edit, and delete Configuration Templates.

- **Value Mappings** (see page 467) - Displays a list of Value Mappings that are used to define variables in Configuration Templates. If you create a Configuration Template that uses variables, then you must create value mappings for those variables. This screen is also used to create, edit, and delete value mappings
- **Management User Templates** (see page 472) - Displays a list of Management User Templates. OmniVista Terra uses SSH to log into the switch using the credentials specified in the Management User Template and configures/provisions the switch. This screen is also used to create, edit, and delete Management User Templates.
- **Settings** (see page 478)- Configures the onboarding process for a switch that has no Initial Configuration.

21 Oct 2025

6.3.1 Results

The CLI Based Provisioning Results screen displays information (see page 454) about all switches that have attempted provisioning through CLI Based Provisioning. The screen is also used to Force Provision a configuration (see page 453) to a device.

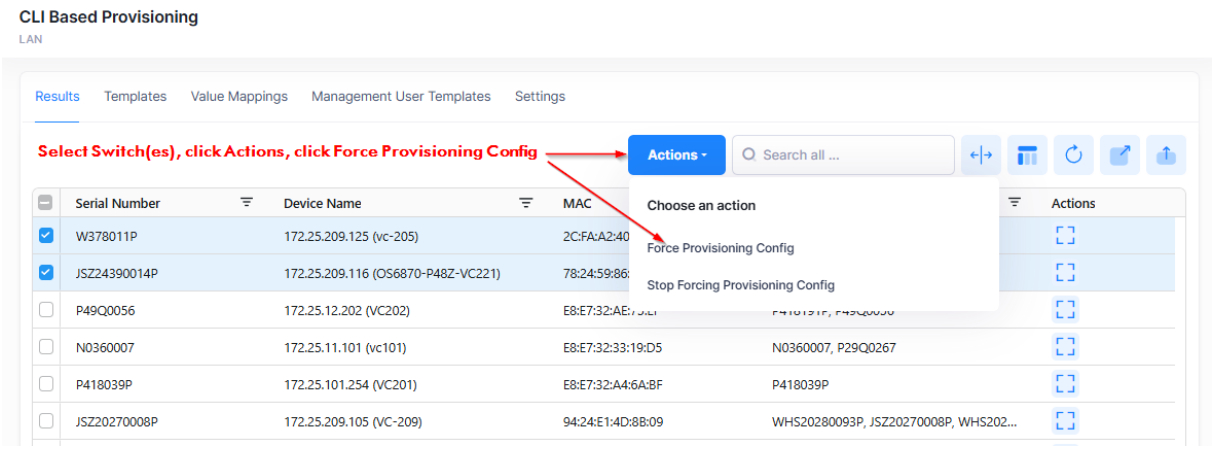


There are switch configuration steps that must be completed to enable provisioning on a switch. See Onboarding Devices for OmniVista Terra Management (see page 13) for more information about provisioning switches, including switch setup, configuration workflow, and troubleshooting.

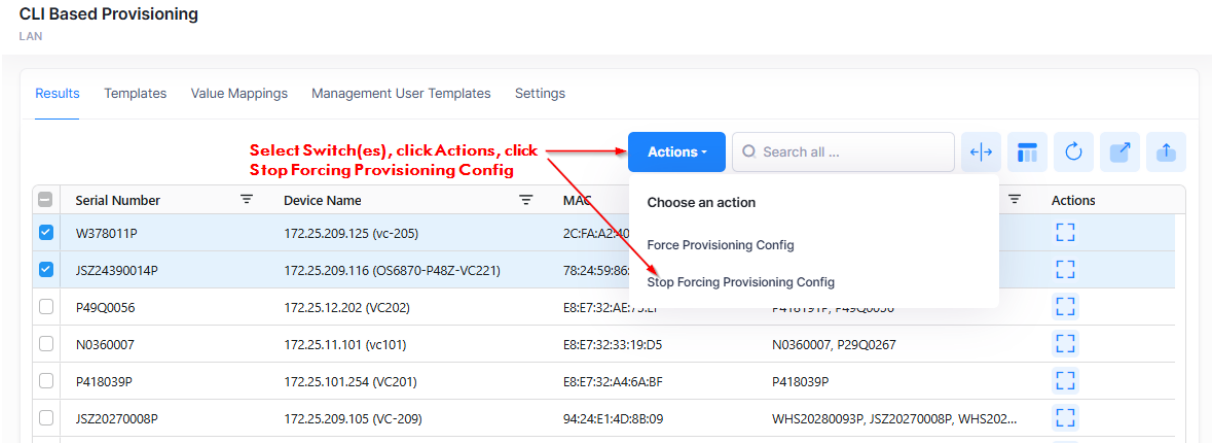
6.3.1.1 Force Provisioning

A switch may fail provisioning because of a problem with the configuration contained in a Provisioning Template, or you may want to push a different configuration to a provisioned switch. Once a switch is provisioned through CLI-based provisioning, the switch contacts the OmniVista Terra Server ("Calls Home") at regular intervals. Force Provisioning is used to push a provisioning configuration to a switch the next time the switch contacts the OmniVista Terra Server. After creating or modifying CLI-based provisioning templates associated with the Switch, manually push the new configuration to the switch(es) as described below.

Select switch(es) in the Results screen list, click on **Actions**, select **Force Provisioning Config**, then click **OK** at the Confirmation Prompt. The configuration will be pushed to the selected switch(es) the next time the switch contacts the OmniVista Terra.



If you decide that you do not want to execute the Force Provisioning Config command, click on **Actions**, select **Stop Forcing Provisioning Config**, then click **OK** at the Confirmation Prompt to stop this process before the next "Call Home".

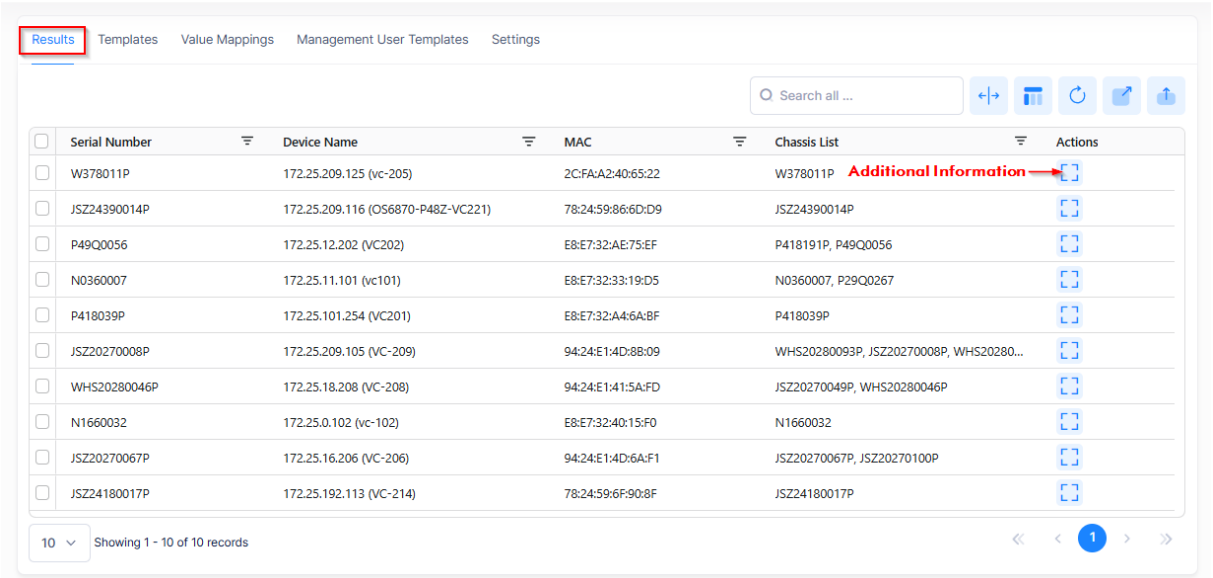


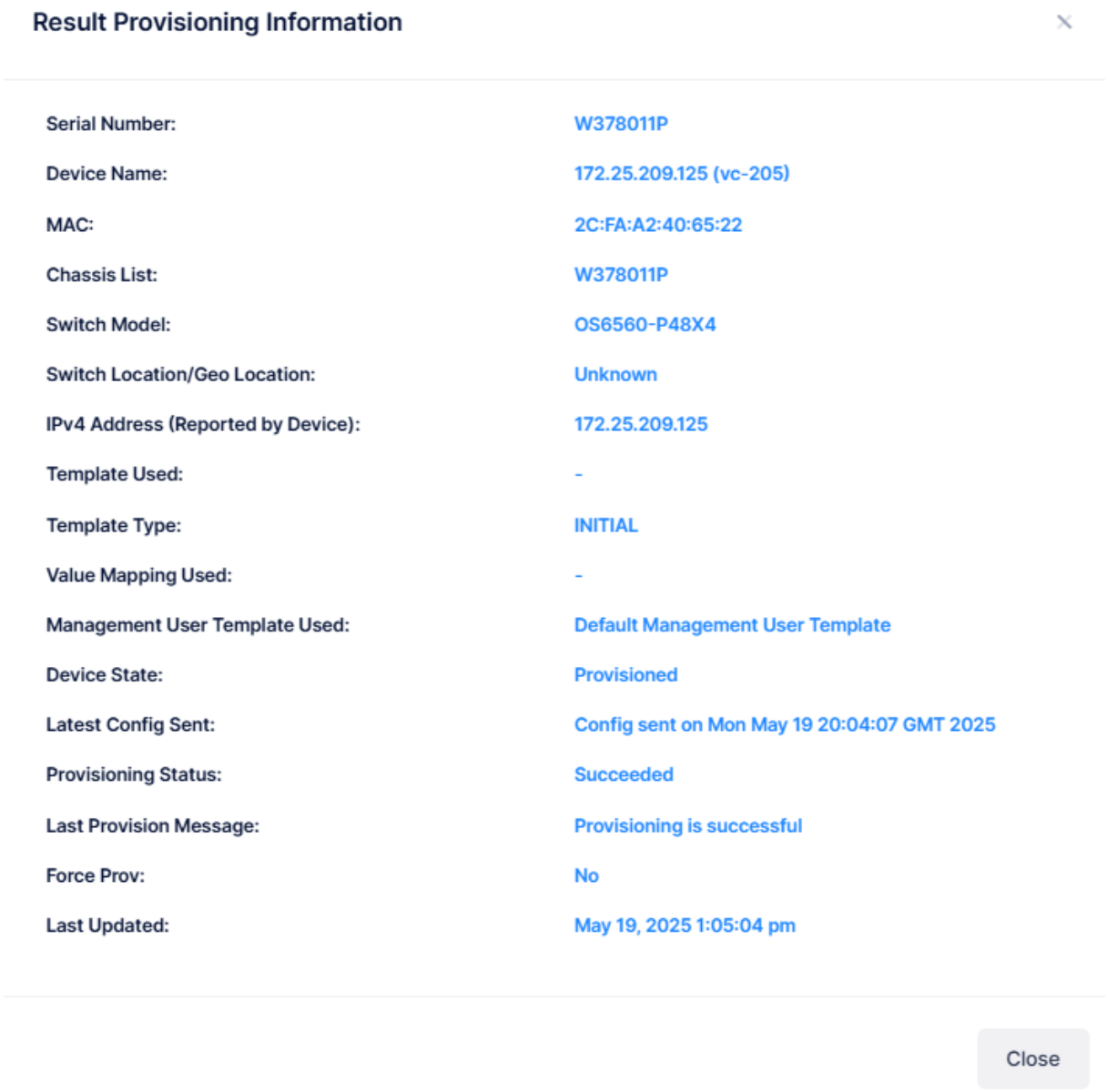
6.3.1.2 Display Provisioning Results Information

Click the icon in the “Actions” column next to a Results entry to display the Results Provisioning Information screen. The information displayed on this screen is defined below.

CLI Based Provisioning

LAN





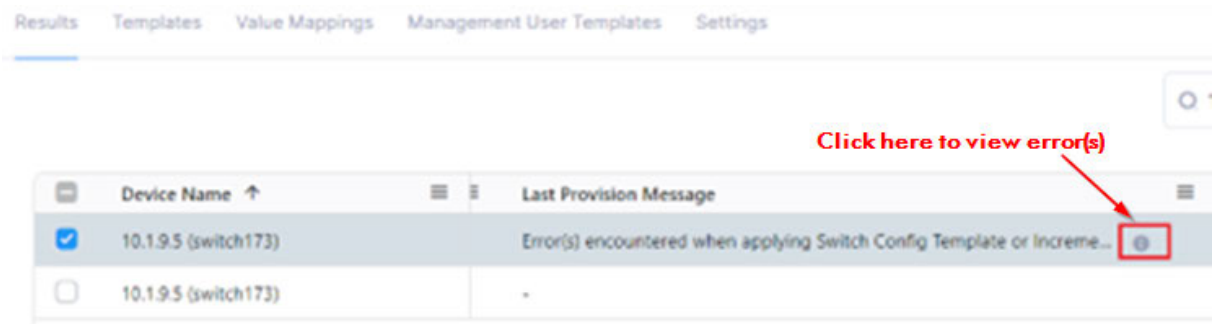
- **Serial Number -** The switch serial number.
- **Device Name -** The switch name set in the Preferences application.
- **MAC -** The switch MAC Address.
- **Chassis List -** Displays a list of serial number for a stack or VC of 2 or more switches, or one serial number for standalone or a VC of 1.
- **Switch Model -** The switch model (e.g., OS6350-P10).
- **Switch Location/Geo Location -** The switch location, if set.
- **IPv4 Address (Reported by Device) -** The switch IPv4 address reported by the switch.
- **Template Used -** The name of the Switch Provisioning Template applied to the switch, if applicable. Click on the template name to view additional information about the template.

- **Template Type** - **Initial** (template applies CLI commands for initial configuration) or **Incremental** (template applies CLI commands when assigned to a switch).
- **Value Mapping Used -** The Value Mapping parameters used if the Switch Provisioning Template is a Dynamic Template (contains variables). Click on the name of the Value Mapping to view the mapping information.
- **Mgmt Users Template Used -** The Management Users Template applied to the switch. Click on the template name to view additional information about the template.
- **Device State** - Indicates if the devices is in the process of Provisioning or is already Provisioned.
  - **Waiting for contact** - Device has been added, but the Provisioning step has not been performed
  - **Provisioning** - Device is provisioning.
  - **Provisioned** - Device onboarded and the template was successfully applied.
  - **Provisioned partially** - There are some invalid commands in the provisioning template and allow device onboarding with this template.
  - **Provisioning Failed** - Provisioning failed for the device.
- **Latest Config Sent -** The most recent time the latest configuration was sent to the switch. Click on this field entry to view the switch configuration file name and contents that was sent to the switch.
- **Provisioning Status -** The result of the latest provisioning attempt for the device (Succeeded/ Failed).
  - **Succeeded** - Provisioning was successful.
  - **Succeeded, but with errors** - Provisioning successful but there is the error. Check the Last Provision Message (see page 457) to view the error.
  - **Failed -** Provisioning failed.
  - **Being Executed** - In the process of applying Incremental Template to devices.
- **Last Provision Message -** Information regarding the last provisioning status.
- **Force Prov -** Indicates whether or no the device was configured through "Force Provisioning" (Forced/No).
- **Last Updated -** The date/time when the provisioning information was last updated.

> After OmniVista issues the "Configuration Apply" command for the Provisioning Template, OmniVista retrieves the status of the operation by checking the output of the "show configuration status" message. If for some reason, OmniVista is unable to receive this message (due to connectivity loss or the switch closing connection due to an SSH session timeout, for example), OmniVista will assume that the Provisioning Template was successfully applied, and report the provisioning process as "Successful" on the Results Screen.

6.3.1.2.1 Checking the Last Provision Message to Troubleshoot Provisioning Error

When the Device Status indicates “Succeeded, but with errors”, you can click on the Last Provision Message for the device to view error details. For example:

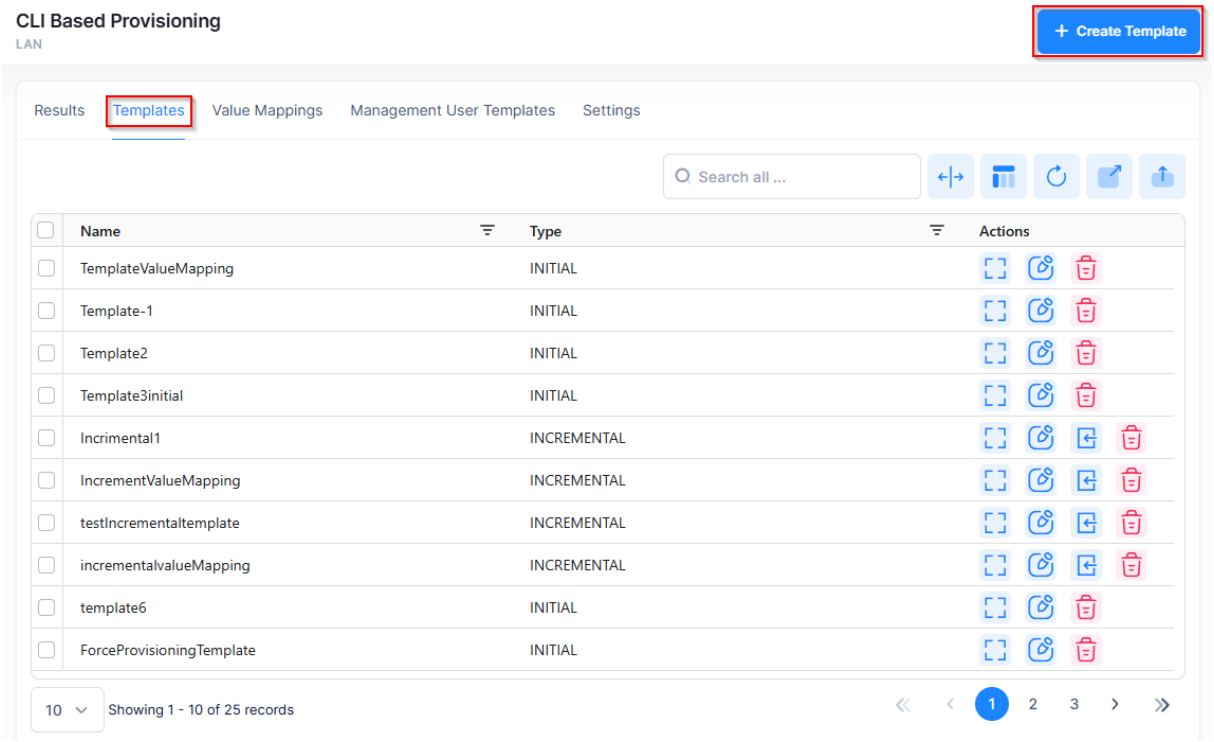


A screen similar to the following displays the error(s) encountered during device provisioning:

21 Oct 2025

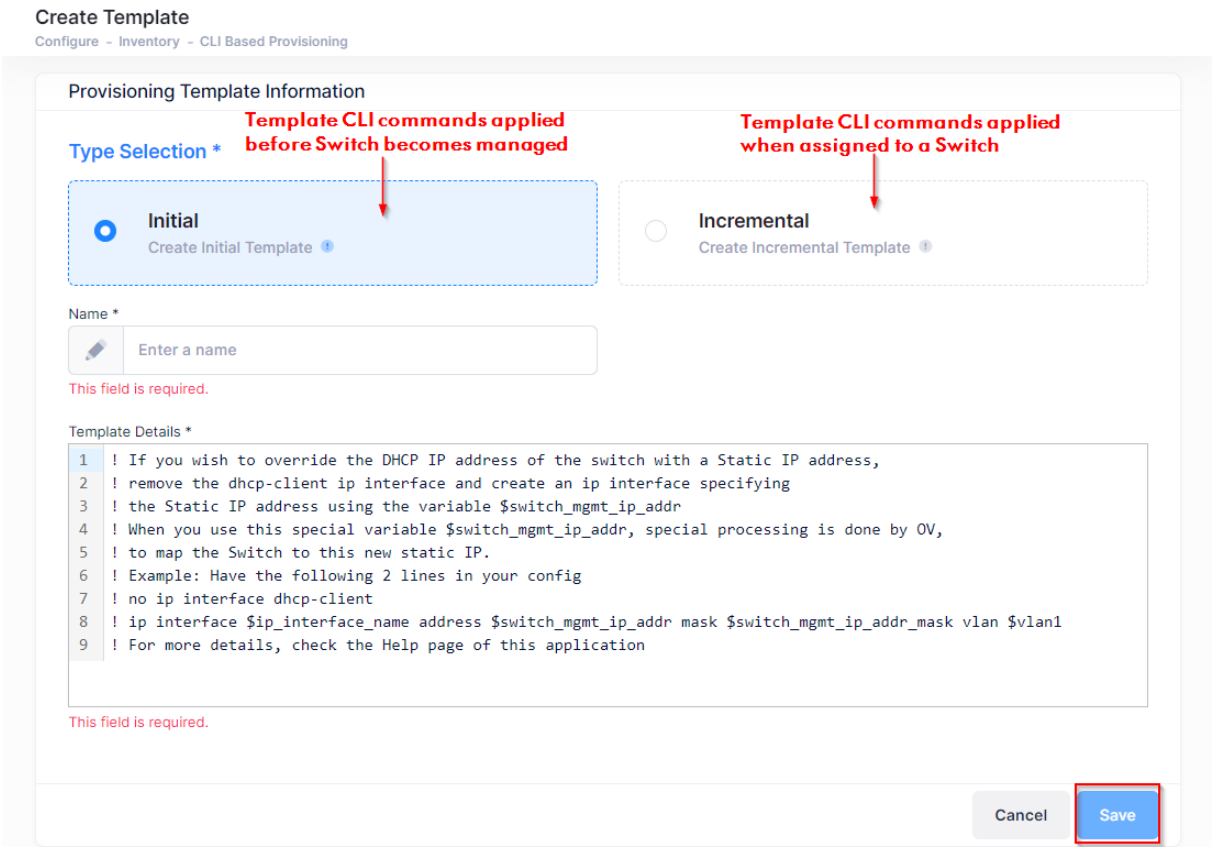
6.3.2 Templates

The CLI Based Provisioning (see page 451) Templates screen displays information (see page 465) about Provisioning Templates that you can use to push a configuration to the Switch. The Provisioning Template contains CLI commands that are applied during the onboarding process before the Switch becomes managed. This screen is also used to create (see page 459), edit (see page 463), and delete (see page 464)Provisioning Templates.



6.3.2.1 Creating a Provisioning Template

To create a Provisioning Template, click on **Create Template** to bring up the Create Template screen. Complete the fields as described below, then click on **Save**.



- **Type Selection** - Select the type of Provisioning Template that you want to create (Initial or Incremental):
  - **Initial** - An Initial template is assigned to a Switch when the Switch is added to the Device Catalog (see page 195) or when editing device settings for an existing Switch. The CLI commands in the template are applied during the onboarding process before the Switch becomes managed.
  - **Incremental** - An Incremental template is assigned to one or more managed Switches. The CLI commands in the template are applied when the template is assigned (see page 462).
- **Name** - Enter a name to assign to the Provisioning Template.
- **Template Details**

- Instructions for configuring a Static IP address for a specific switch (using a Serial Number Rule or MAC Address Rule) are displayed when you bring up the Provisioning Template. Follow the instructions if you want to configure a Static IP Address in the template. The instructions are commented out. You can delete them or just configure the template below them.
- You cannot configure a Static IP address that is assigned to a device in the Device Catalog List. You must first delete that device from the Device Catalog List before using that IP address. If a device serial number (or a device with same IP address) already exists in the Device Catalog List, it must first be deleted from the Device Catalog List before it can be onboarded again.

The Provisioning Template is created using CLI syntax. A Provisioning Template is a set of commands that are read by the switch on reloading. A template can be static or dynamic. A Static Template (see sample below) is a template without variables. It is useful for deployments where all switches can work with exactly the same configurations. The IP address is typically given by a DHCP server in such a deployment.

```
vlan 5 port default 1/1-48
ip interface vlan-5 address 192.168.5.3/24 vlan 5
ip multicast static-neighbor vlan5 port 1/49
ip multicast static-neighbor vlan5 port 1/50
ip multicast static-neighbor vlan5 port 1/51
ip multicast static-neighbor vlan5 port 1/52
lanpower start 1
system name Switch2
aaa authentication default local

```

Certain commands that are handled by the Provisioning Manager in AOS cannot be included in a Provisioning Template (e.g., user admin password, write memory, configuration apply). If these commands are included in a Provisioning Template, provisioning will fail. If provisioning fails for any reason, go to the Results (see page 453) screen and check the "Last Provision Message" column for more information. If the Provisioning Template is the problem, make any necessary updates to the Provisioning Template, and save it. The next time the switch contacts OmniVista Terra, provisioning should be successful.

A Dynamic Template (see sample below) is a template with variables. It allows you to reuse the same Provisioning Template even though different switches might need different values for some configurations. For example, different branches of an enterprise might use a different subnet range or VLAN.

```
vlan 1 disable
vlan $VLAN members ports $PORTS tagged
no ip interface dhcp-client
ip interface $INTERFACE_NAME address $STATIC_IP/24 vlan $VLAN
```

Special characters cannot be used when creating mapping variables (e.g., @ # +). OmniVista Terra will ignore special characters. For example, "$test" is a correct mapping variable format. "$test@#+" will also be read as "$test" by OmniVista Terra. Also note that mapping variables cannot have spaces. If required, multi-word variables must be separated by an underscore (e.g., $test_1, not $test 1 or $test-1).

If you are using a Dynamic Template, a Value Mapping is required to define the variables used in the Dynamic Template. At the time you select a Dynamic Template for a Switch, you are prompted to select an existing Value Mapping or create a new mapping. Use the Value Mappings screen (see page 467) to view existing and/or create new variable mappings.

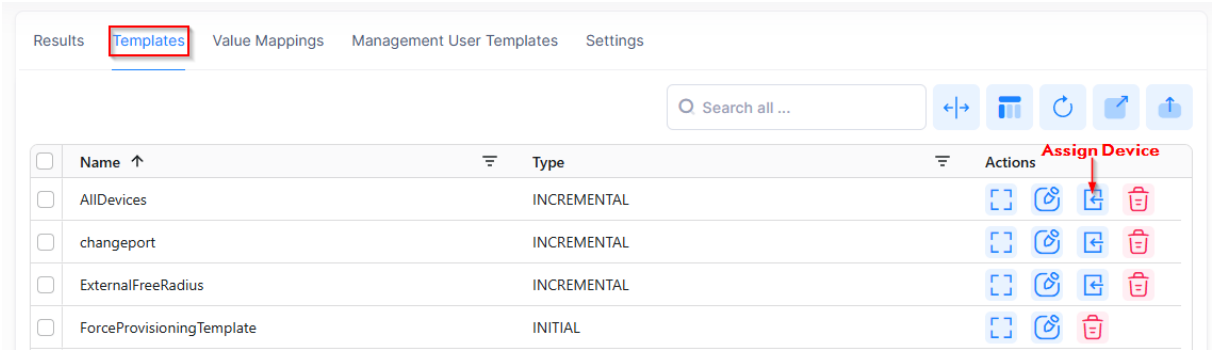
6.3.2.1.1 Assigning an Incremental Template

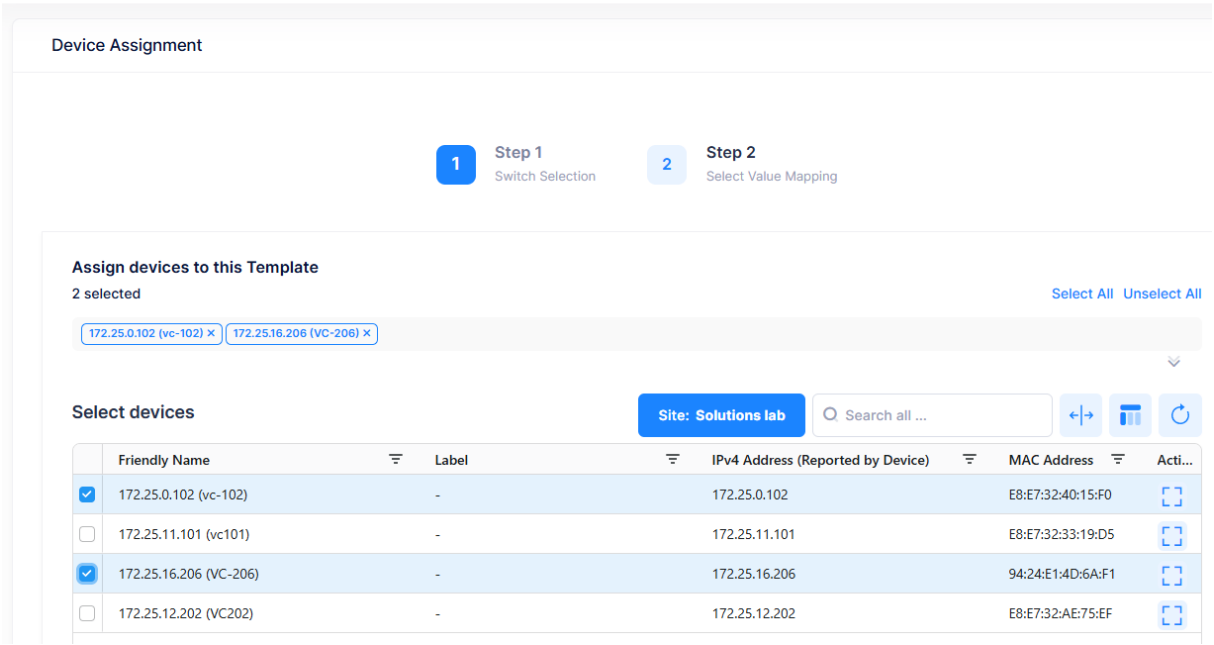
There are two options for assigning an Incremental template to a switch:

- Assign the device when you create the template.
- Assign the device to an existing template.

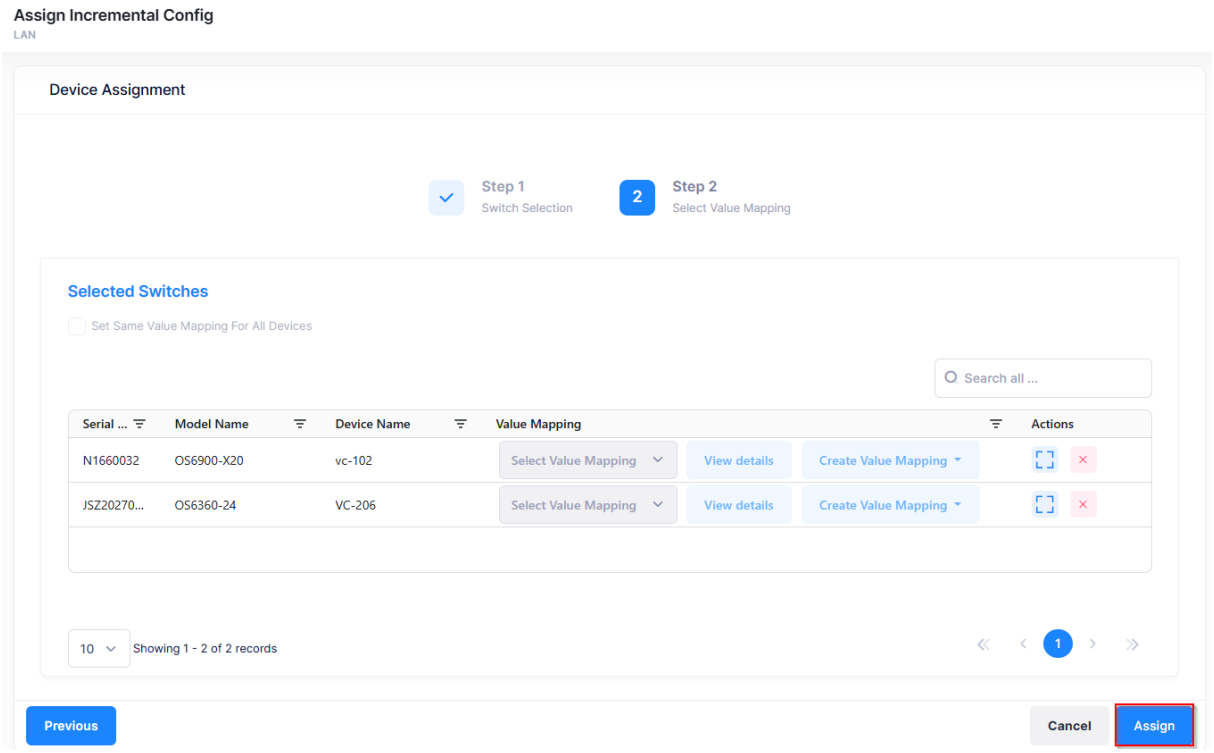
When an Incremental Template is created, if you click on **Save**, the template is saved without a device assignment. You can later assign the template to a device as follows:

Select the template that you want to assign and click on the Assign Device icon under the “Actions” column. The Assign Incremental Config screen opens.





Step 1 - Select the switch device(s) that you want to assign to the template, then click on **Next** at the bottom-right corner of the screen.



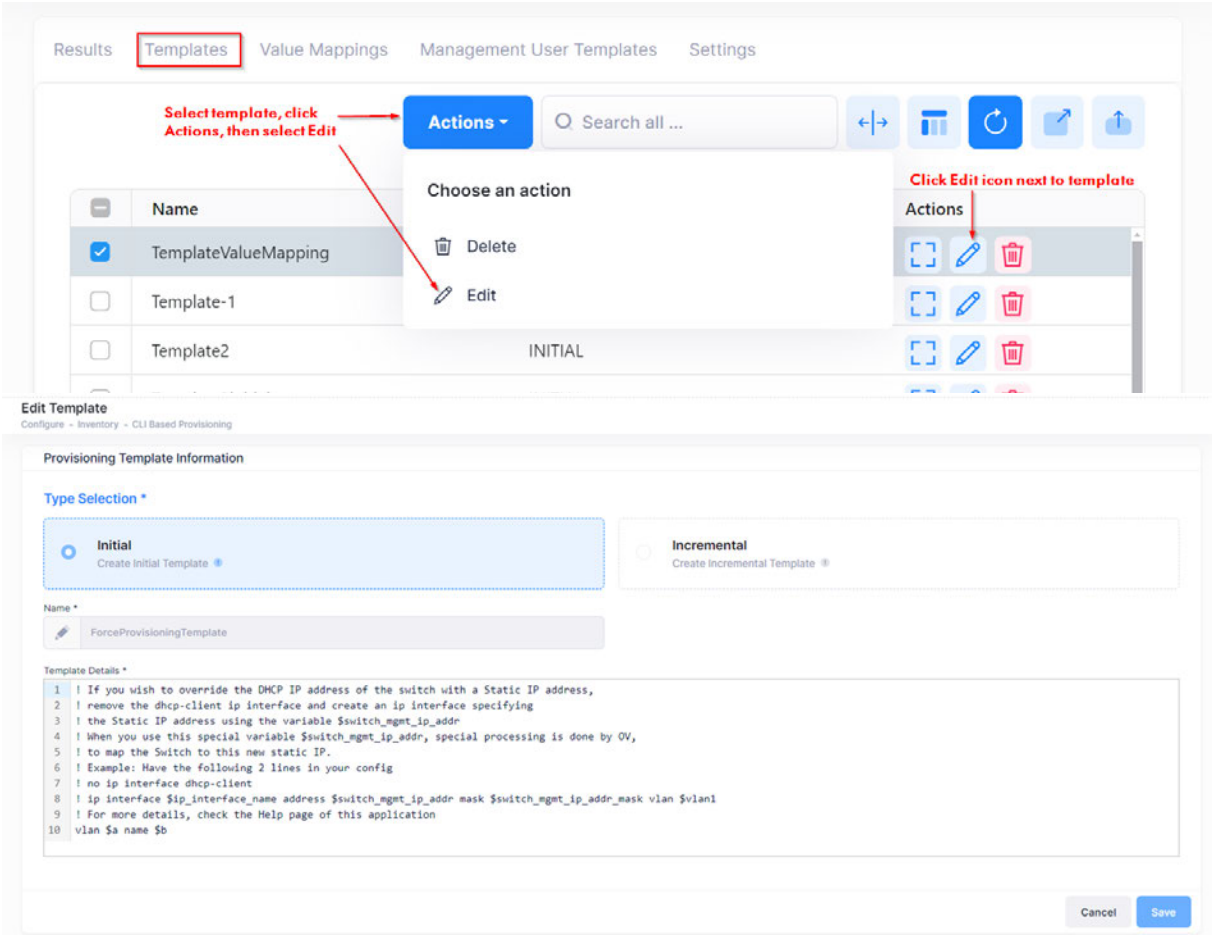
Step 2 - Select the Value Mappings, if any, for the selected switches, then click on **Assign**.

6.3.2.2 Editing a Provisioning Template

You can edit the Provisioning Template to modify the CLI commands. For example, if the Results (see page 453)screen indicates provisioning failed due to a problem with the Provisioning Template, you can edit the template file to correct the problem.

To modify Provisioning Template commands, select an existing template and click on the Edit icon under the “Actions” column or select Edit from the **Actions** drop-down menu to bring up the Edit Template screen. Edit the CLI commands as needed, then click on **Save**.

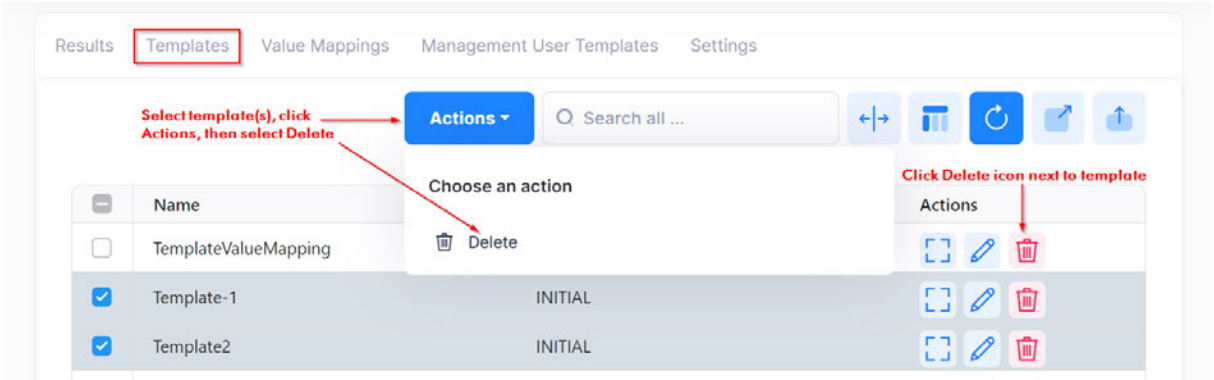
> You cannot change the type of template or the template name. For example, if the template was created as an “Initial” template, you cannot change the template type to “Incremental”. You can change the CLI commands in “Template Details”.



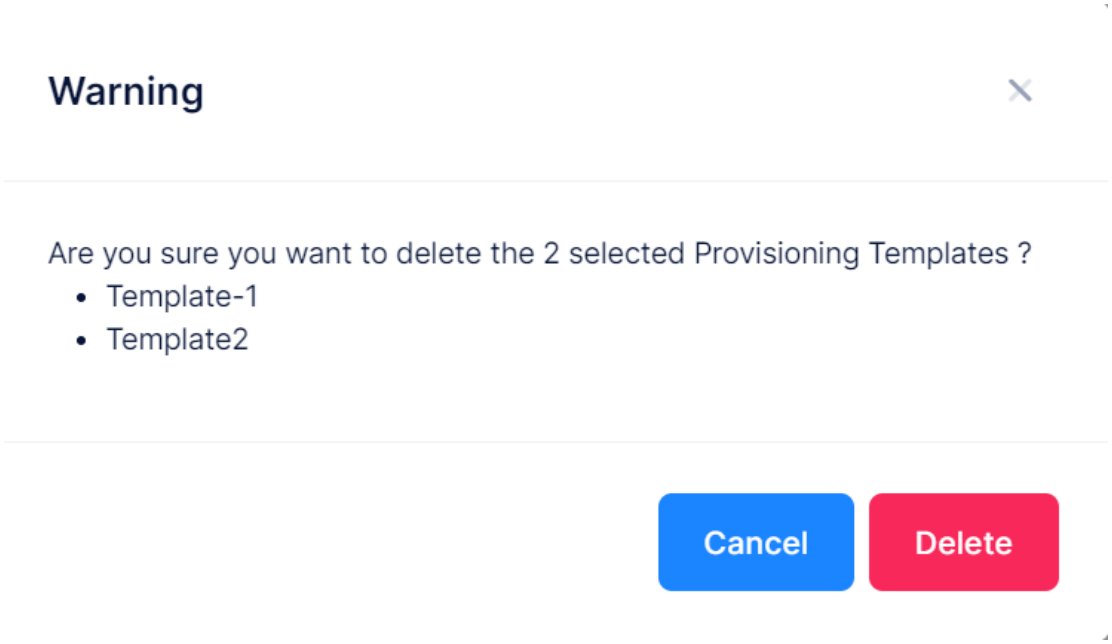
6.3.2.3 Deleting a Provisioning Template

You can delete one or more Provisioning Templates from the templates list using one of the following methods:

- To delete one or more Provisioning Templates, select the template(s) that you want to delete, then click on **Actions** and select **Delete** from the drop-down menu.
- To delete a single Provisioning Template, click on the Delete icon under the “Actions” column next to the template that you want to delete.



When you select one or more templates to delete, you are prompted with a Warning message to confirm your delete request.

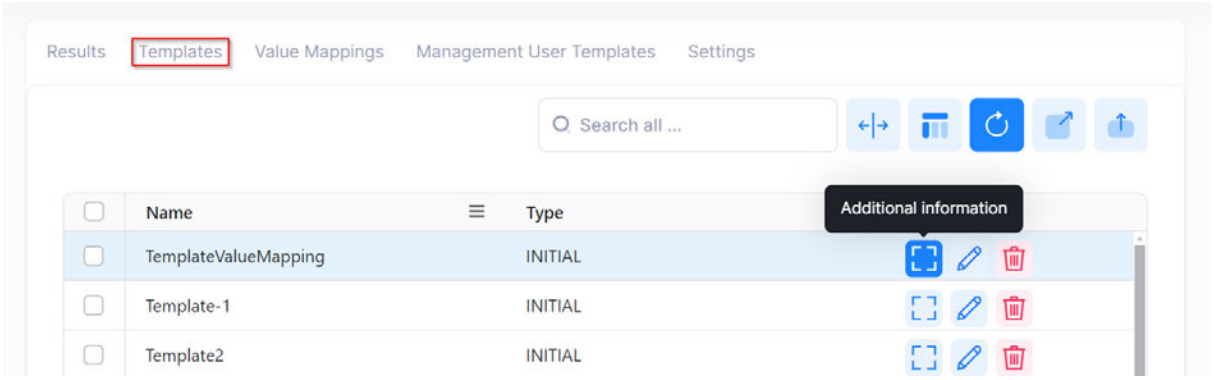


Click on **Delete** to confirm that you want to delete the Provisioning Templates listed in the Warning message.

> You can not delete a template that is assigned to a device. For example, if you attempt to delete template “TP-NAR” that was already applied to the initial Provisioning Template and assigned to devices, you will receive an error message.

6.3.2.4 Display Provisioning Template Information

Click the Additional Information icon next to a Provisioning Template entry to display the Provisioning Template Information screen. The information displayed on this screen is defined below.



Name - The name assigned to the template.

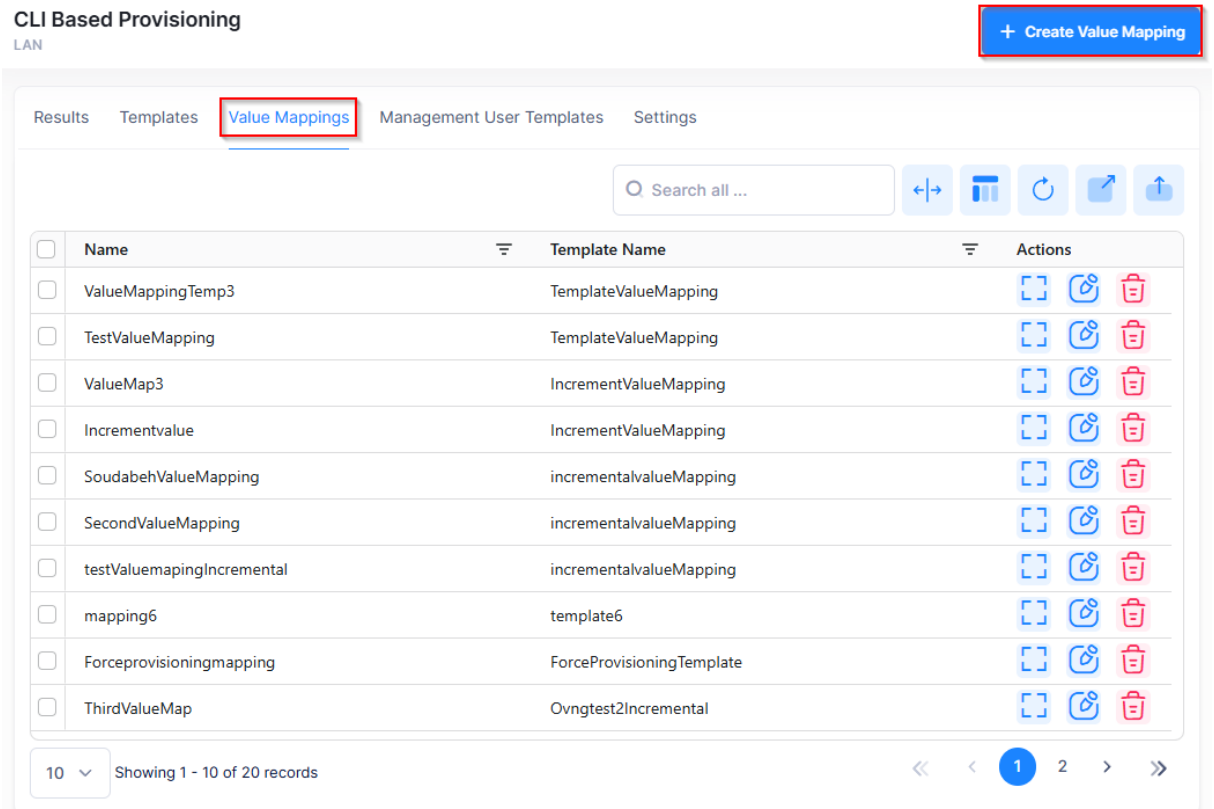
Type - The type of template (Initial or Incremental)

Template Details - The CLI commands that are pushed to the switch and appended to the switch configuration.

21 Oct 2025

6.3.3 Value Mappings

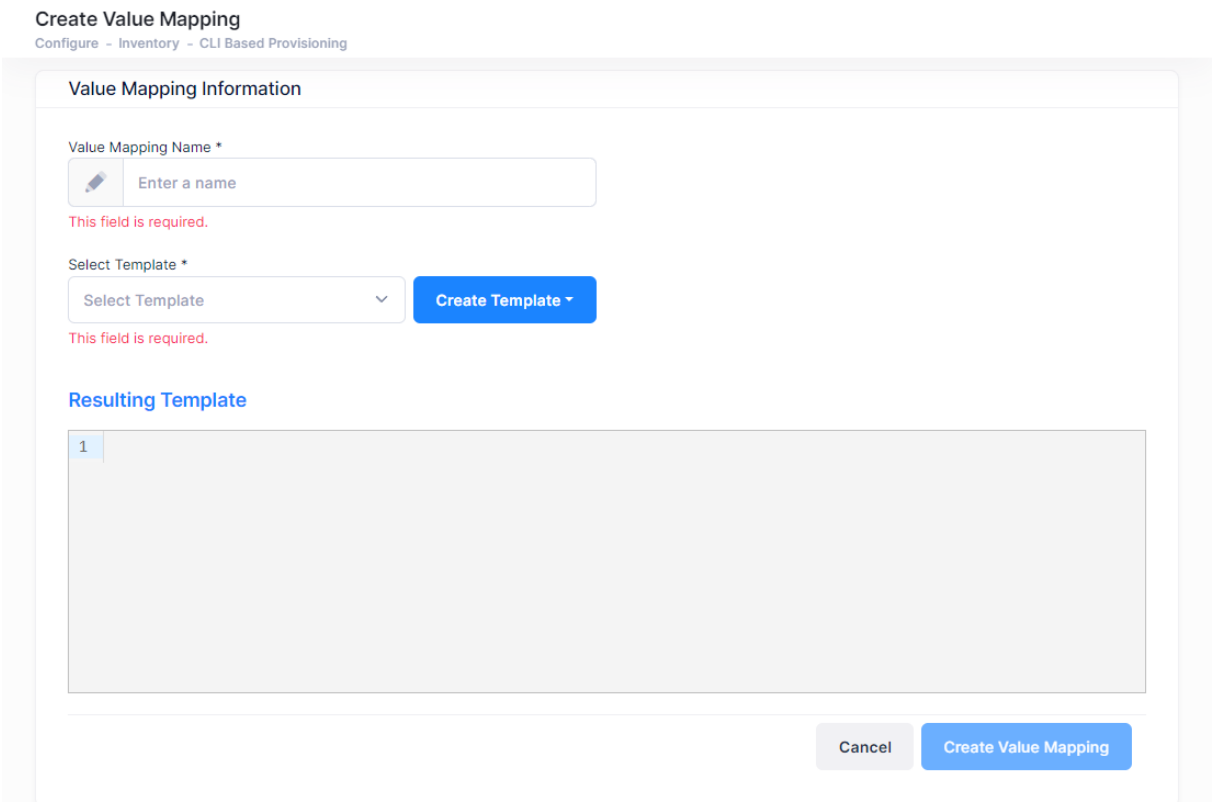
A Dynamic Provisioning Template (see page 459) contains variables that are mapped to values defined in the Value Mapping assigned to the template. The Value Mappings screen displays information (see page 470) about existing Value Mappings between mapping templates and Dynamic Provisioning Templates. The screen is also used to create (see page 467), edit (see page 469), or delete (see page 470)Value Mappings.



If the Provisioning Template (see page 459) you selected when adding or editing a device contains variables, you are required to enter the name of a Value Mapping Template. You can select an existing mapping template or create a new mapping template.

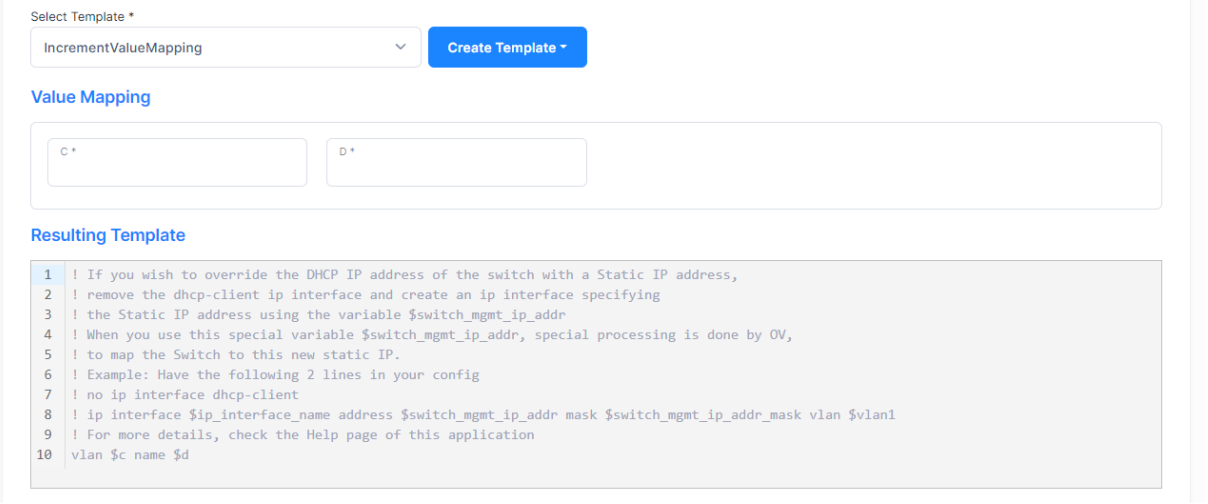
6.3.3.1 Creating a Value Mapping

To create a value mapping for a Dynamic Provisioning Template, click **Create Value Mapping** on the Value Mappings screen to bring up the Create Value Mapping screen.



On the Create Value Mapping screen,

- Enter a name to assign to the mapping template. This is the name that will appear if you select a Dynamic Provisioning Template when adding a switch or editing switch settings.
- Select an existing Dynamic Provisioning Template from the drop-down list or click on **Create Template** to open the Create Template screen and create a new template. (see page 459) Only Provisioning Templates that contain variables will appear in the drop-down list.
- When you select a Dynamic Provisioning Template, the variables for the Dynamic Provisioning Template are displayed under “Value Mapping” and the contents of the Dynamic Provisioning Template are shown under “Resulting Template”.

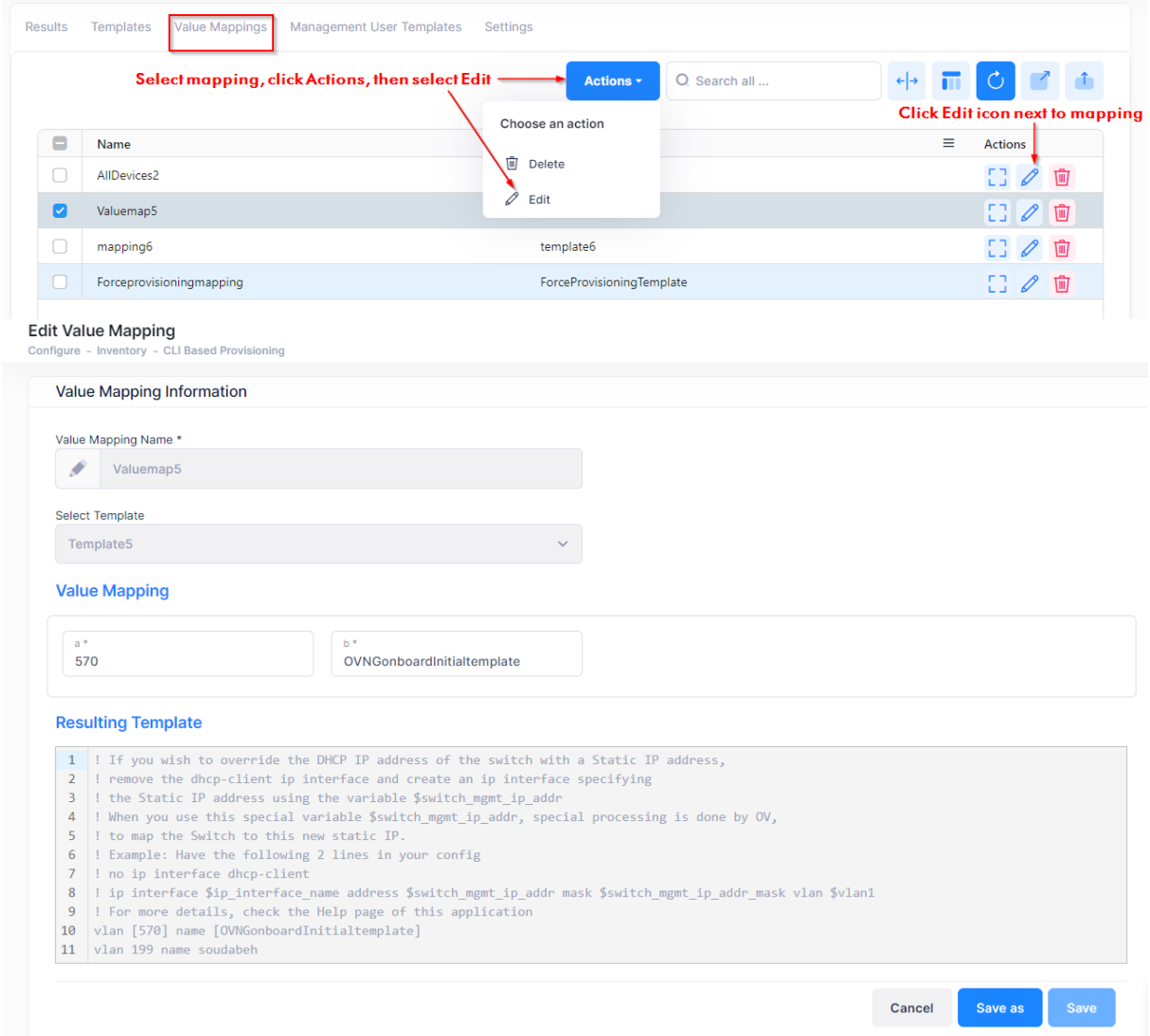


- Enter values for each of the variables and click on **Create Value Mapping**. Note that when you enter a value for a variable, it is automatically filled in where that variable appears in the template contents.

6.3.3.2 Editing a Value Mapping

You can edit a Value Mapping to modify the variable definitions for the associated Dynamic Provisioning Template. To change the variable definitions, select an existing Value Mapping and click on the Edit icon under the “Actions” column or select Edit from the **Actions** drop-down menu to bring up the Edit Value Mapping screen. Edit the variable definitions as needed, then click on **Save**.

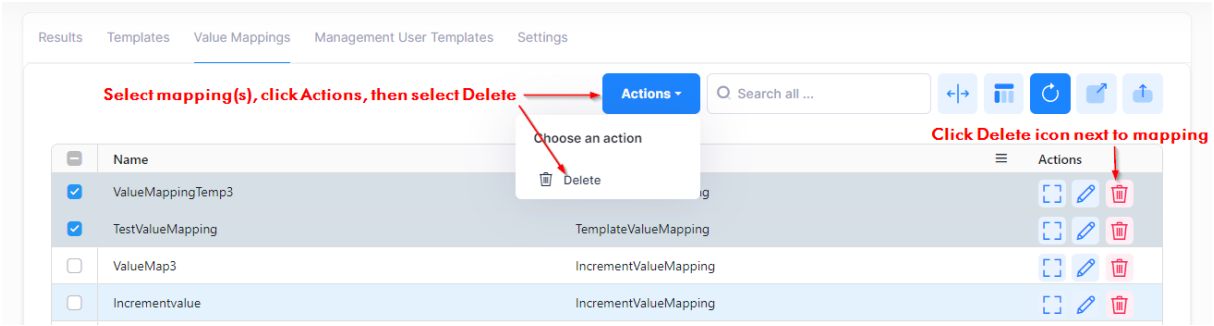
Note that you can click on **Save As** before you make any changes to save the Value Mapping under a different name. This allows you to create a new mapping based on an existing mapping but with different variable definitions.



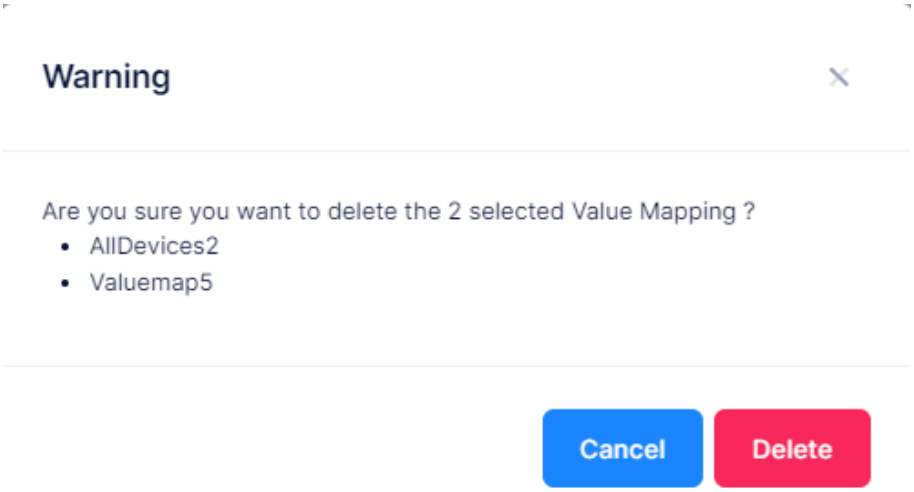
6.3.3.3 Deleting a Value Mapping

You can delete one or more Value Mappings from the list using one of the following methods:

- To delete one or more Value Mappings, select the mapping(s) that you want to delete, then click on **Actions** and select **Delete** from the drop-down menu.
- To delete a single Value Mapping, click on the Delete icon under the “Actions” column next to the template that you want to delete.



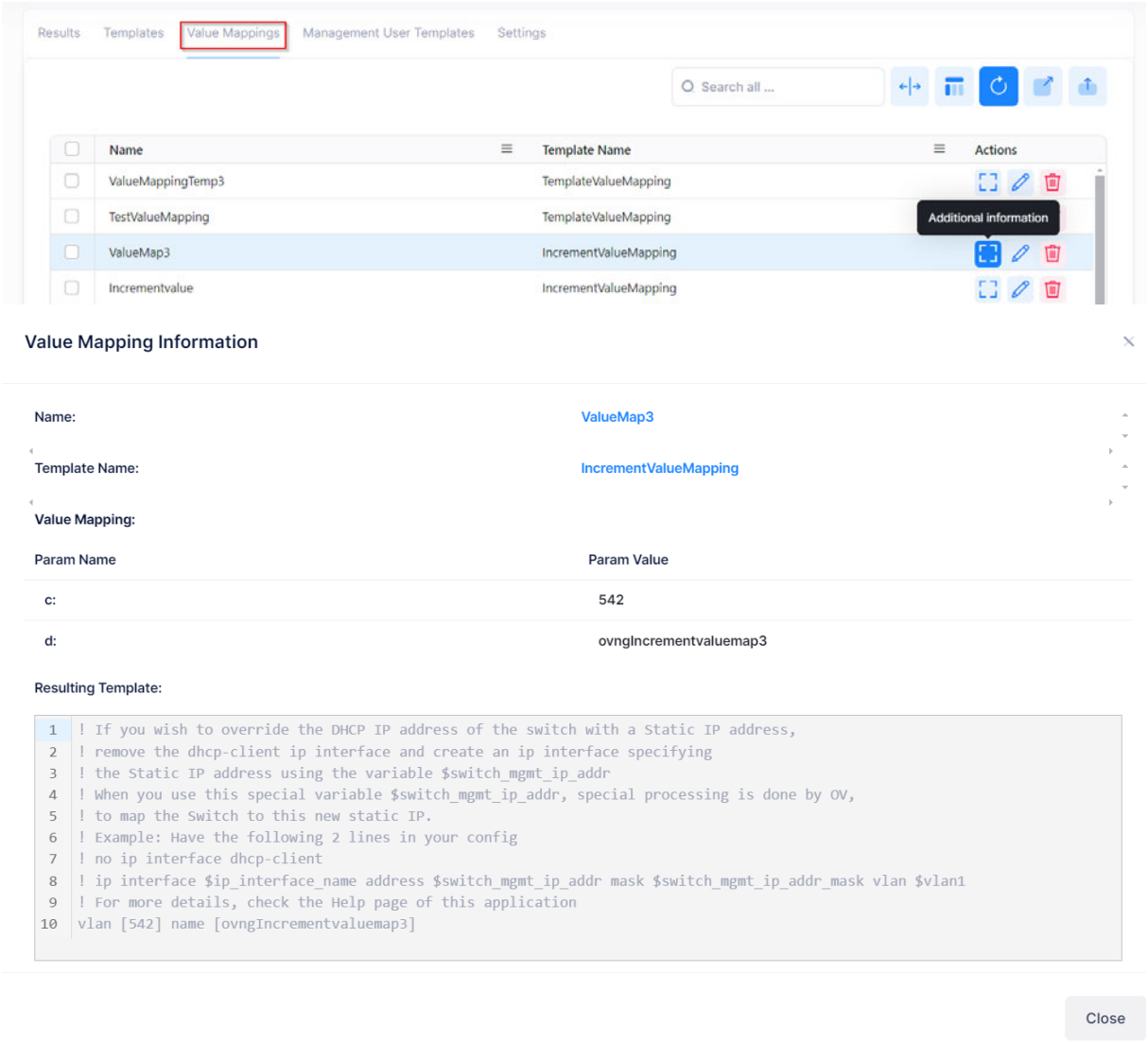
When you select one or more Value Mappings to delete, you are prompted with a Warning message to confirm your delete request.



Click on **Delete** to confirm that you want to delete the Value Mappings listed in the Warning message.

6.3.3.4 Display Value Mapping Information

Click the icon in the “Actions” column next to a Value Mapping entry to display the Value Mapping Information screen. The information displayed on this screen is defined below.



Name - The name assigned to identify the Value Mapping.

Template Name - The name of the Provisioning Template assigned to the Value Mapping.

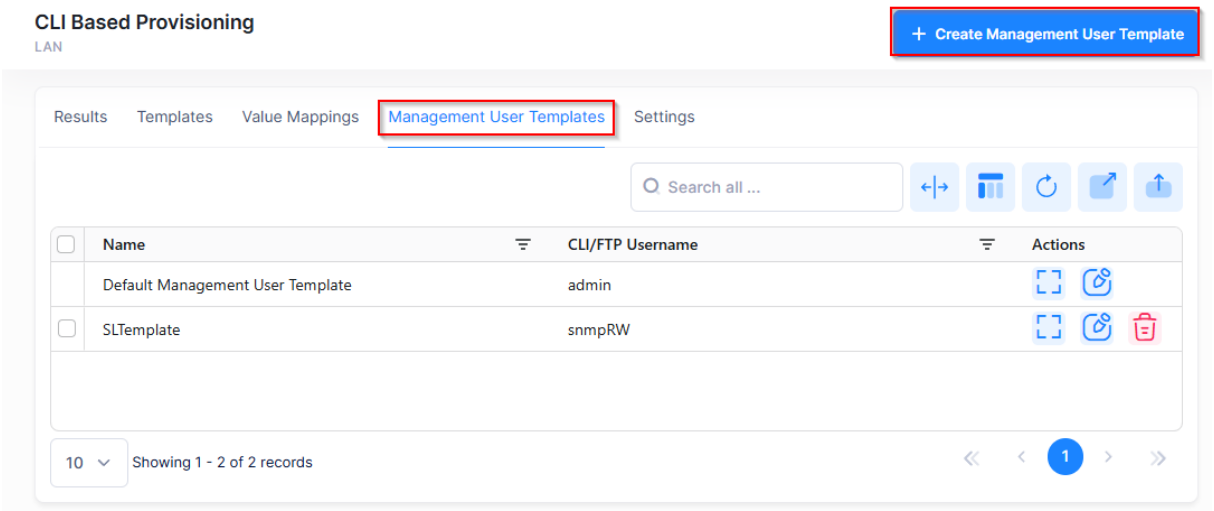
Value Mapping - The values defined for the variables contained in the assigned Provisioning Template.

Resulting Template - The Provisioning Template CLI commands with the variables defined.

21 Oct 2025

6.3.4 Management User Templates

The CLI Based Provisioning (see page 451) Management User Templates screen displays information (see page 476) about Management User Templates. OmniVista Terra uses SSH to log into the switch using the credentials specified in the Management User Template and configures/provisions the switch. This screen is also used to create (see page 472), edit (see page 475), and delete (see page 475)Management User Templates.



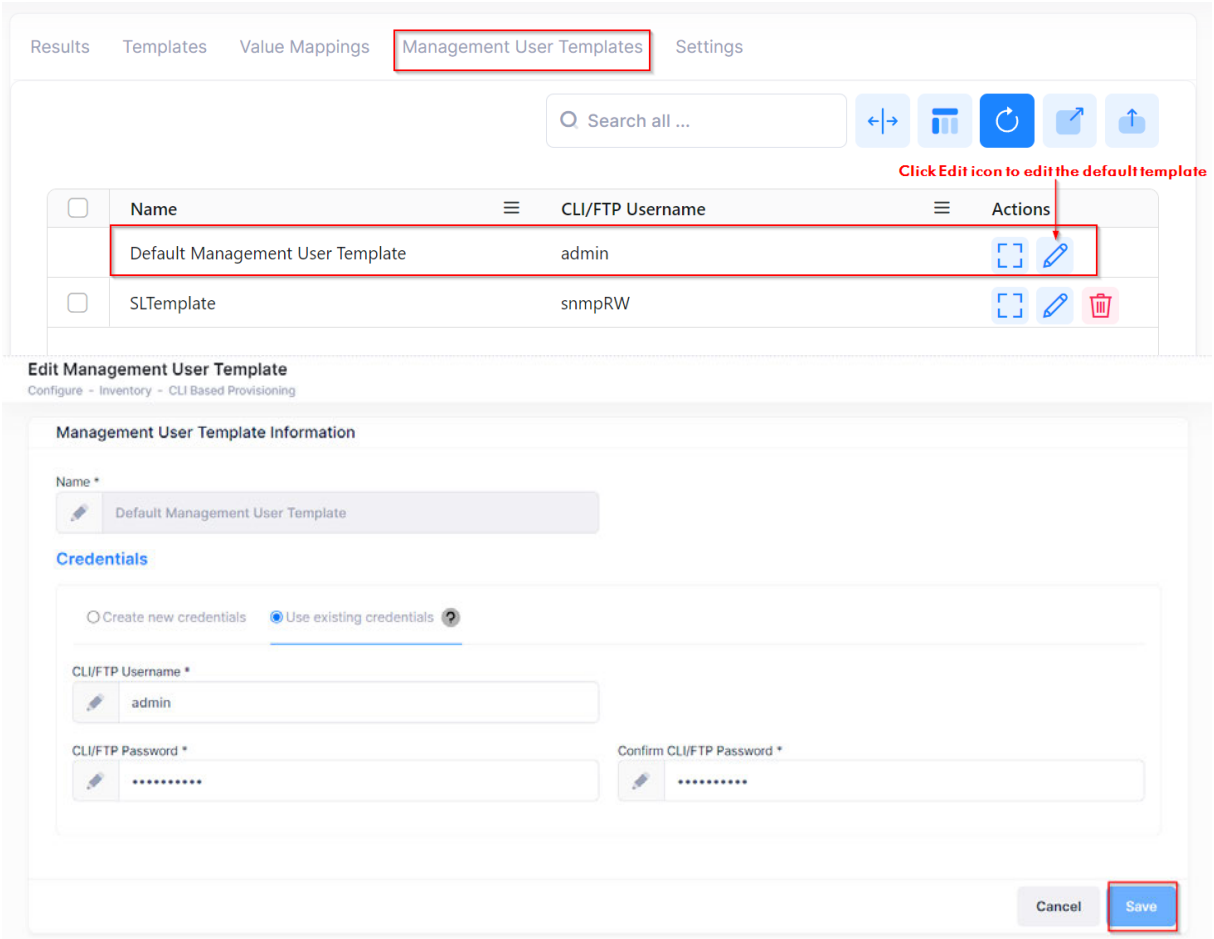
6.3.4.1 Configuring Management User Templates

By default, the Default Management User Template is pushed to the Switch unless you select a different template. You can edit the pre-configured default template (see page 472) or create and save custom Management User Templates (see page 474).

6.3.4.1.1 Configuring the Default Management User Template

The Default Management User Template uses the “admin/switch” login credentials to connect with the Switch. To edit the Default User Template to change the login credentials, click on the Edit icon to bring up the Edit Management User Template screen. Edit the fields as described below, then click **Save**.

> You cannot delete the Default Management User Template or change the template name. However, you can edit the credentials that OmniVista Terra will use to connect with a Switch.

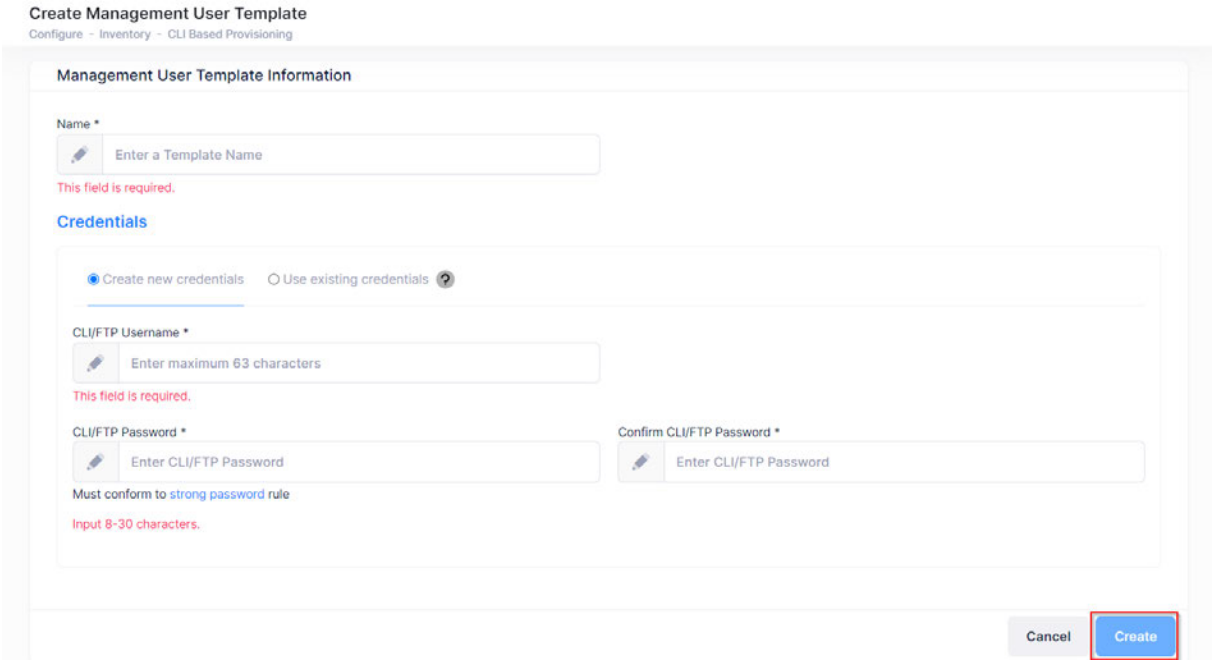


- **Create new credentials** - Configure the CLI/FTP Username/Password for CLI/FTP access to the Switch.
  - **CLI/FTP User Name -** The user name that OmniVista Terra will use to establish CLI/FTP sessions with the switch. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the device when configuration files are saved and restored (see note below).
  - **CLI/FTP Password -** The password that OmniVista Terra will use to establish CLI/FTP sessions with the switch. The user name specified will be used to auto-login to devices when CLI sessions are established. It will also be used to perform FTP with the switch when configuration files are saved and restored.
  - **Confirm CLI/FTP Password -** Confirm the CLI/FTP Password.
- **Use existing credentials** - Use the existing CLI/FTP Username/Password currently configured on the switch for CLI/FTP access. Enter the CLI/FTP Username/Password. OmniVista will expect that these credentials exist on the switch. If they do not, the switch will fail during provisioning with an error message displayed on the Results screen.

If the switch username/password differs from the one defined in the Default Management Users Template, OmniVista cannot connect to the switch and provisioning will fail. An entry for the switch appears on the Results Screen with a Provisioning Status of "Failed". If this happens, configure the "Use existing credentials" option on the Management Users Template, and "Force Provision" the switch. See the Results (see page 453) screen online help for more information on "Force Provisioning".

6.3.4.1.2 Creating a Custom Management User Template

To create a custom Management User Template to use instead of the Default Management User Template, click on **Create Management User Template** to bring up the Create Management User Template screen.



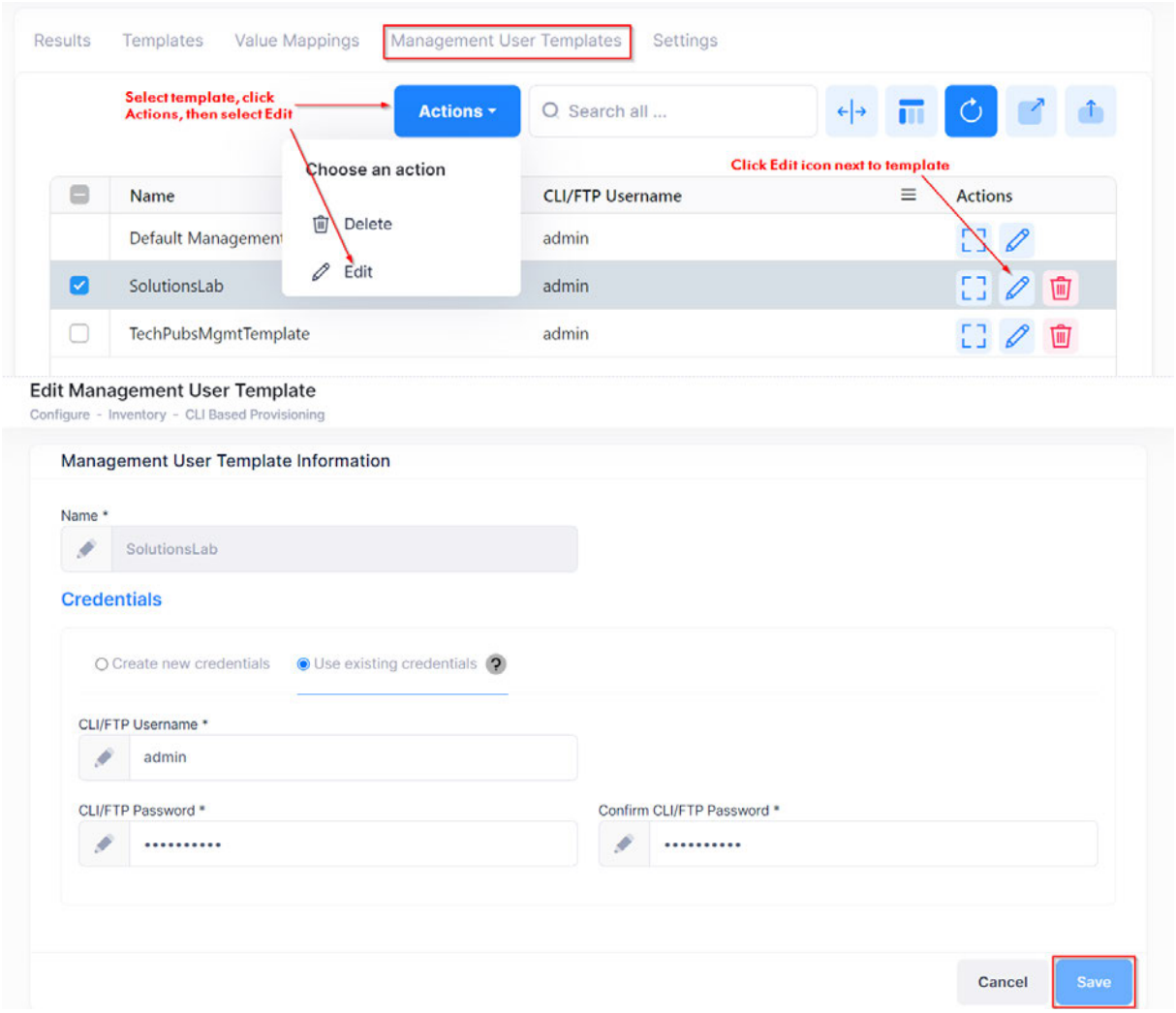
Complete the fields as described above (see page 472), then click **Create**. The new custom template is now available to select for CLI Based Provisioning.

If the switch username/password differs from the one defined in the custom Management Users Template, OmniVista cannot connect to the switch and provisioning will fail. An entry for the switch appears on the Results Screen with a Provisioning Status of "Failed". If this happens, configure the "Use existing credentials" option on the Management Users Template, and "Force Provision" the switch. See the Results (see page 453) screen online help for more information on "Force Provisioning".

6.3.4.2 Editing a Custom Management User Template

You can edit a custom Management User Template to modify login credentials. For example, if the username/password specified in the template do not match the login credentials on the switch, you will want to change the username/password defined in the custom Management Users Template.

To change the login credentials, select an existing custom template and click on the Edit icon under the “Actions” column or select Edit from the **Actions** drop-down menu to bring up the Edit Management User Template screen. Edit the login credentials as needed, then click on **Save**.

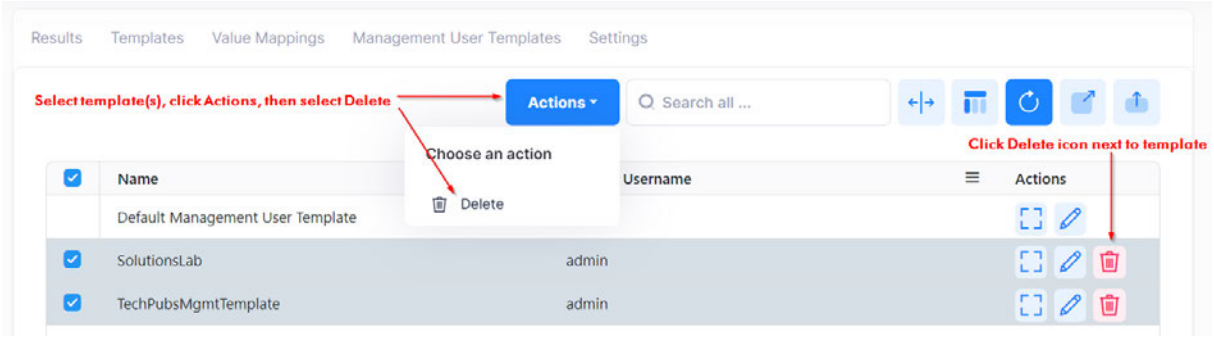


6.3.4.3 Deleting a Custom Management User Template

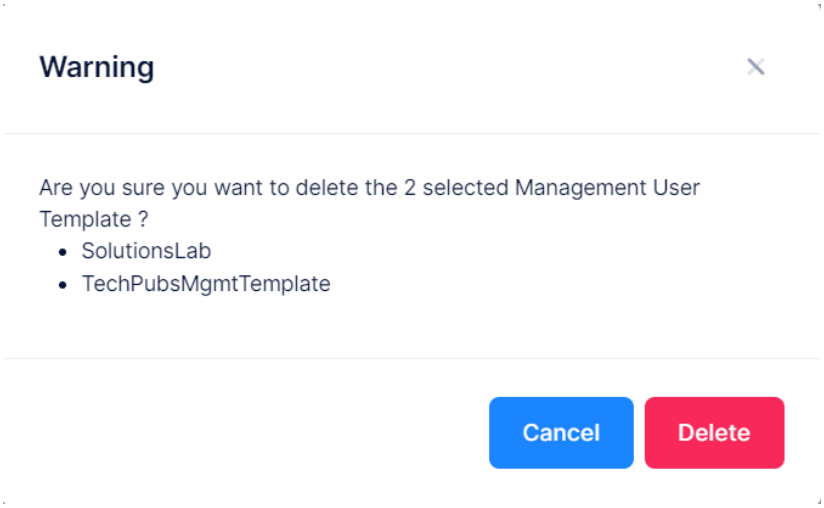
You can delete one or more custom Management User Templates from the templates list using one of the following methods:

- To delete one or more custom Management User Templates, select the template(s) that you want to delete, then click on **Actions** and select **Delete** from the drop-down menu.
- To delete a single custom Management User Template, click on the Delete icon under the “Actions” column next to the template that you want to delete.

Note that you cannot delete the Default Management User Template; only custom templates can be deleted.



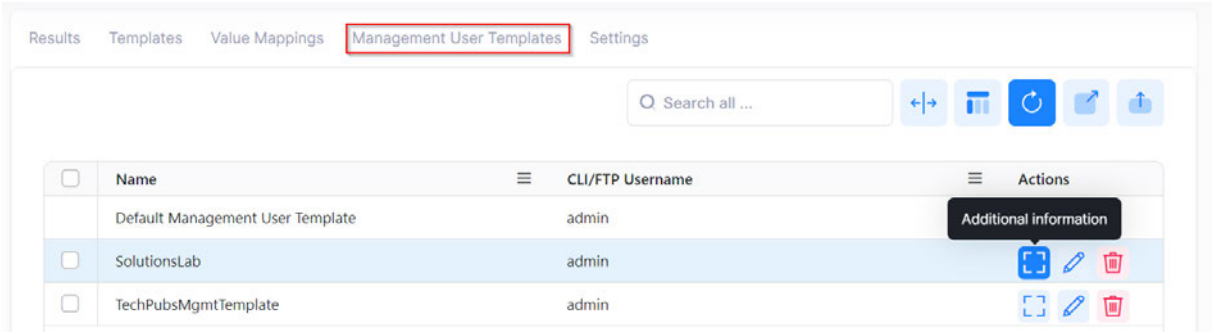
When you select one or more custom Management User Templates to delete, you are prompted with a Warning message to confirm your delete request.

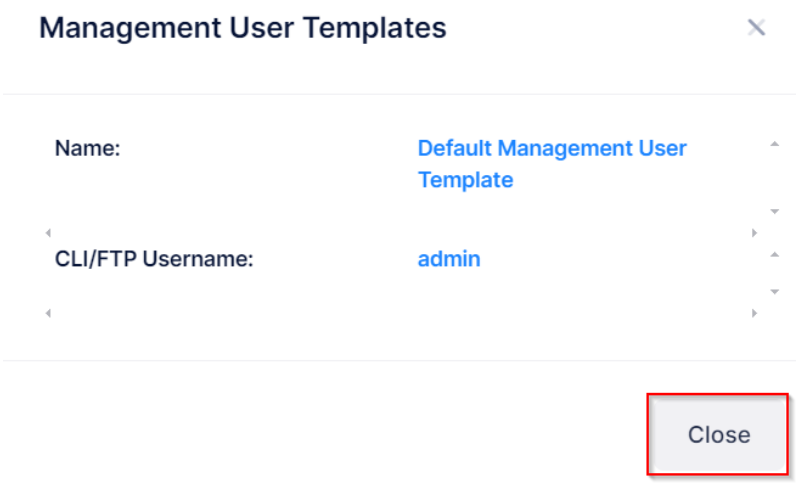


Click on **Delete** to confirm that you want to delete the custom Management User Templates listed in the Warning message.

6.3.4.4 Display Management User Template Information

Click the icon in the “Actions” column next to a Management User Template entry to display the Management User Templates information screen. The information displayed on this screen is displayed below.


Results
Templates
Value Mappings
Management User Templates
Settings
Search all ...
Name
CLI/FTP Username
Actions
Default Management User Template
admin
Additional information
SolutionsLab
admin
TechPubsMgmtTemplate
admin

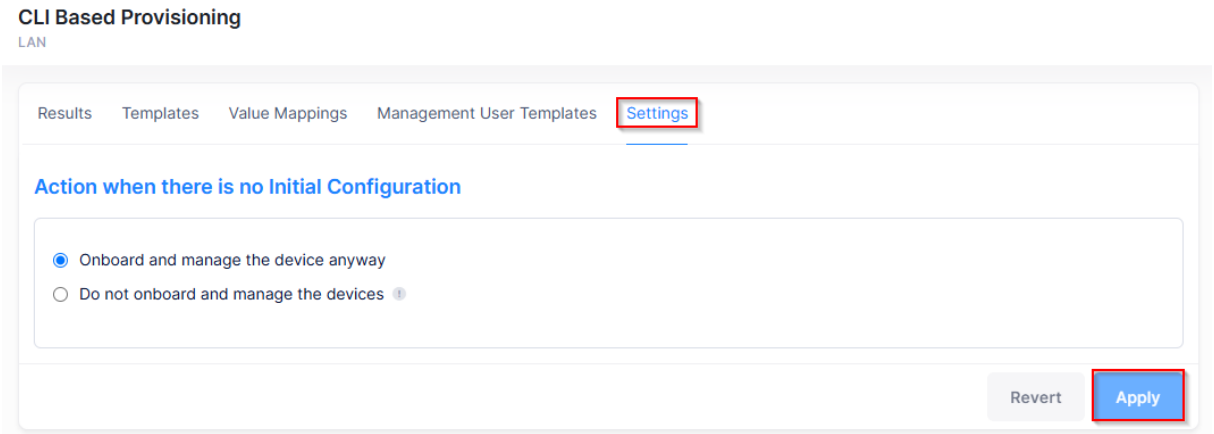

Management User Templates
Name:
Default Management User Template
CLI/FTP Username:
admin
Close

21 Oct 2025

6.3.5 Settings

The CLI Based Provisioning (see page 451) Settings screen allows you to configure the onboarding process for a switch that has no Initial Configuration (no Provisioning Template, no Value Mapping).

> There are switch configuration steps that **must** be completed to enable provisioning on a switch. See Onboarding Devices for OmniVista Terra Management (see page 13) for more information, such as switch setup, configuration workflow, and troubleshooting.



- **Onboard and manage the device anyway** - Select this option if you want to onboard a Switch that was added to the Device Catalog (see page 169)with no Initial Configuration. The Switch will onboard and provision successfully with no Initial Configuration.
- **Do not onboard and manage the device** - Select this option if you do not want to onboard a Switch that has no Initial Configuration. Provisioning will fail, but the Switch will continue to attempt onboarding until an Initial Configuration is defined for the Switch.

Select one of the settings, then click **Apply**. The changes take effect immediately.

21 Oct 2025

7 Configure Network Access Control

The OmniVista Terra Network Access group of applications are accessed by clicking on the **Network Access** option under the “Configure” section of the OmniVista Terra Menu (see page 45).

When you click on the **Network Access** option, the following list of applications is provided to assist with configuring access controls for the wireless network:

- Unified Access (see page 481) - The Unified Access application provides unified wireless device configuration of security functions for Access Points (APs) on OmniAccess Wireless devices. In addition to device authentication and classification, you can create Access Role Profiles (similar to User Network Profiles) to configure network access controls for one or more user devices. Unified Access contains applications that work together with the Authentication Servers application to seamlessly authenticate and configure QoS for both device types.
- **Authentication Servers**
  - RADIUS Servers (see page 589) - Displays all RADIUS Servers known to OmniVista Terra. It also enables you to add, modify, and delete RADIUS Servers from the RADIUS Servers Management List. A RADIUS Server that supports Vendor Specific Attributes (VSAs) is required. VSAs carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server.
  - LDAP Servers (see page 597) - Displays all LDAP Authentication Servers known to OmniVista Terra. It also enables you to add, modify, and delete LDAP Servers from the list of LDAP Servers known to OmniVista Terra. Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The protocol was developed as a way to use directory services over TCP/IP and to simplify the Directory Access Protocol (DAP) defined as part of the Open Systems Interconnection (OSI) effort.
- **Groups** - Enables you to create the following groups, which can be used in various policy conditions
  - MAC Groups (see page 605) - Displays all configured MAC Groups. The screen is used to create, edit, and delete MAC Groups, which can be used in creating various policy conditions, such as source MAC group condition and destination MAC group condition.
  - IP Groups (see page 608) - Displays all configured IP Groups. The screen is used to create, edit, and delete IP Groups, which can be used in creating various policy conditions.
  - Service Groups (see page 610) - Displays all configured Service Groups. The screen is used to create, edit, and delete Service Groups, which can be used in creating various policy conditions.
  - Service Policies (see page 612) - Displays all configured Service Policies, which are assigned to a Service Group. This screen is used to create, edit, and delete Service Policies.
  - Service Ports (see page 616) - Displays all configured Service Ports, which are assigned to Service Policies. By default, the TCP radio button is selected and TCP Services are displayed. Click on the UDP radio button to display UDP Services. The screen is used to create, edit, and delete Service Ports.
- UPAM-NAC (see page 619) - The Unified Policy Authentication Manager (UPAM) is a unified access management platform for Stellar AP Series devices. UPAM supports both Captive Portal server

and RADIUS server; and can be used to implement MAC authentication and Captive Portal authentication. User Profiles can be supported in the OmniVista database or on external servers.

- User Accounts (see page 707) - The Accounts application is used to create login accounts for specific types of users (Employees, Guests) in the local UPAM database. In addition, a Company Property List provides the ability to define devices owned by a company (for example, printers, IP phones, laptops, tablets) and specify which user accounts can access the devices for daily use.
- Application Visibility (see page 766) - The Application Visibility Signature Profiles screen displays all configured Signature Profiles. Signature Profiles are created from a Signature File, which contains Application Signature information for individual applications/protocols as well as application groups (pre-configured groups of related applications/protocols).

21 Oct 2025

7.1 Unified Access

The Unified Access application provides unified device configuration of security functions for Access Points (APs) and AOS Switches (OmniSwitch). In addition to device authentication and classification, you can create Access Role Profiles (similar to User Network Profiles) to configure network access controls for one or more user devices.

Unified Access consists of the following applications that work together with the Authentication Servers application to seamlessly authenticate and configure QoS for devices. These applications are accessible by clicking on **Network Access > Unified Access** under the “Configure” section of the OmniVista Terra Menu (see page 45).

- **Access Auth Profile** (see page 483) - Displays all configured Access Authentication Profiles and is used to create, edit, and delete Access Authentication Profiles. An Access Authentication Profile defines the parameters for the authentication process applied to client traffic received on device ports.
- **AAA Server Profile** (see page 497) - Displays information about the configured authentication, authorization, and accounting (AAA) Server Profiles and is used to create, edit, and delete AAA Server Profiles. This type of profile defines specific AAA parameters that can be used in an Access Authentication Profile or Captive Portal Profile. When an AAA Server Profile is assigned to device traffic through an Access Authentication Profile, the parameter values defined in the profile will override any existing global AAA configuration.
- **Access Role Profiles** (see page 514) - Displays all configured Access Role Profiles and is used to create, clone, edit, and delete Access Role Profiles. An Access Role Profile contains the various UNP properties (e.g., QoS Policy List attached to the UNP, Captive Portal Authentication) for users assigned to the profile. An Access Role Profile is considered as a user role with which every client in the network is associated.
- **Unified Policies** (see page 533) - Displays configured Unified Policies and is used to create, edit, delete, and view Unified Policies. Unified Policies are QoS Policies that can be applied to devices.
- **Unified Policies List** (see page 551) - Displays all configured Unified Policy Lists, including the Unified Policies included in each list, and is used to create, edit, and delete Unified Policy Lists. A Unified Policy List is a set of Unified Policies that are grouped together and assigned to devices as a group.
- **IoT Categorization** (see page 558) - Displays information about device categories, and is used to create, edit, and delete custom categories. OmniVista Terra monitors network packets to determine the types of client devices connected to an IoT-enabled Access Point or switch and interfaces with Device Fingerprinting Service to categorize them. When a device is initially categorized, it will be assigned to one of the available, top-level categories (e.g., Phone, Tablet, or Wearable). As OmniVista monitors packets and learns more about a device, the category assigned to the device will become more specific. As OmniVista learns more about the device, the device may be categorized as an "Apple Mobile Device", and then an "Apple iPhone". As OmniVista learns these new categories, they are added to the IoT Categorizations List.
  - A default set of hierarchical categories is provided. These default categories cannot be deleted, but can be edited to assign an Access Role Profile to the category.

    - In addition to the default set of hierarchical categories, you can create custom categories that you can edit and delete. There are two types of custom categories: hierarchy and MAC-based.
        - A custom hierarchy category specifies the hierarchy categorization a device must match to be associated with the custom category.
        - A custom MAC-based category specifies the MAC address a device must have to be associated with the custom category.
    - Category-based device authentication is configurable by assigning an Access Role Profile to a category (default or custom) with the option of Automatic Enforcement.
- **Tunnel Profiles** (see page 569) (AP Only) - Displays all configured Tunnel Profiles and is used to create, edit, and delete Guest Tunnel Profiles. When you create a Tunnel Profile, you configure the parameters that can be mapped to an Access Role Profile to authenticate a Guest Client, and map the client to a Guest UNP profile that is mapped to an L2 GRE service.
- **Location Policies** (see page 576) (AP Only) - Displays information about configured Location Policies and is used to create, edit, and delete a Location Policy. A Location Policy defines a specific location where a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.
- **Access Classification** (see page 579) (AP Only) - Displays information about configured Access Classification Rules that are assigned to Access Role Profiles and is used to create, edit, and delete classification rules. Assigning Access Classification Rules to an Access Role Profile provides an additional method for classifying a device into the Access Role Profile. If authentication is not available or does not return a profile name, for whatever reason, Access Classification rules are applied to determine the Access Role Profile assignment.
- **Period Policies** (see page 585) (AP Only) - Displays information about configured Period Policies and is used to create, edit, and delete a Period Policy. A Period Policy specifies the days and times during which a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

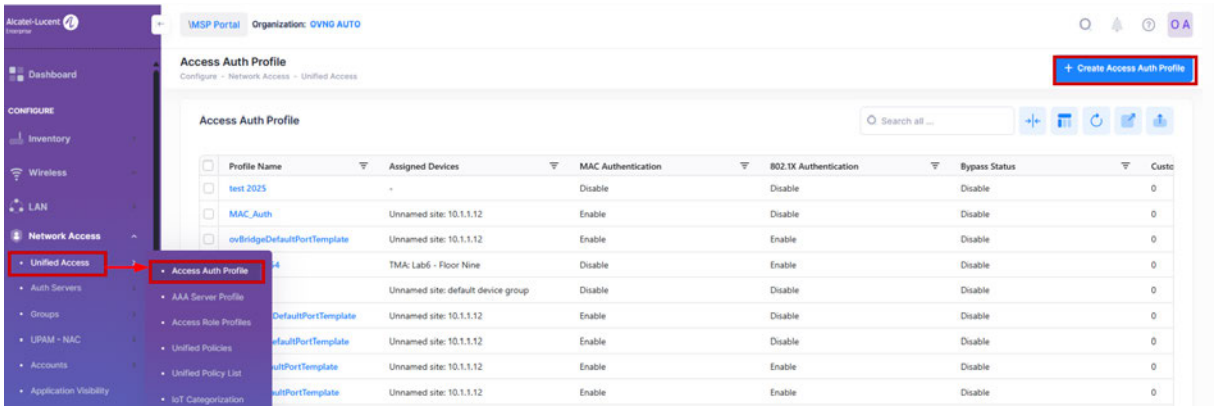
To implement a global redirect configuration for Captive Portal authentication on an OmniSwitch, you have to manually configure the redirect settings through the switch CLI. This step is required until OmniVista Terra supports Global Configuration in a future release. To configure a redirect for Captive Portal authentication, refer to the online help for Onboarding Devices for OmniVista Terra Management (see page 13).

21 Oct 2025

7.1.1 Access Authentication Profile

The Access Authentication Profile defines the authentication process for client traffic received on both wired devices (Switch devices) and wireless devices (Steller AP downlink Port). Profile parameters are used to configure 802.1X and MAC authentication, Access Classification, the AAA Server Profile to use for authentication, the Access Role Profile to assign, etc.

Use the Access Auth Profile screen to display information (see page 493) about all of the configured Access Authentication Profiles. This screen also allows you to create (see page 483), edit (see page 490), and delete (see page 491)profiles. To access the Access Auth Profile screen, click on **Network Access > Unified Access > Access Auth Profile** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.1.1.1 Creating an Access Authentication Profile

The Create Access Auth Profile screen is used to select profile settings, devices, and the downlink ports to which the profile is applied. To access this screen, click on **Create Access Auth Profile**.

Consider the following use cases when configuring Access Authentication Profile:

- When a Switch device polls for Access Auth profile information and the database does not have an existing Access Auth Profile, OmniVista will automatically create an Access Auth Profile with the correct configuration and Assignment Port that polls from the Switch device.
- When a Switch device polls for Access Auth profile information and the database already has an existing Access Auth Profile, OmniVista will only update the Network Assignment Port of the Access Auth Profile belonging to that specific Switch device, not the device configuration.
- When a Switch device polls and there is no Access Auth profile information, but the database has an existing Access Auth Profile, OmniVista will delete the Network Assignment - Port belonging to that specific Switch device.
- You can apply the AAA Server Profile on the Access Auth Profile page to Switch and verify that the AAA server profile has been successfully applied.
- You can change the new AAA Server profile on the Access Auth Profile screen for Switch, and verify that the AAA server profile should be applied to Switch.
- You can create an Access Auth profile without an AAA server profile and verify no AAA server profiles are pushed to Switch.

- You can unlink the AAA server profile on the Access Auth Profile page. However, the AAA server profile wouldn't be deleted from Switch, only if that AAA server profile is still being used somewhere in Switch. The AAA server profile template would still be retained on the User Interface screen.

The Create Access Auth Profile screen provides the following step-by-step process for creating an Access Authentication Profile:

1. **Access Auth Profile Settings** (see page 484)

- **Basic Information** - Configures the profile name and the status of MAC and 802.1X authentication.
- **No Auth/Failure/Alternate** - This section is used to configure the actions taken if a device assigned to a profile fails authentication.
- **Advanced Settings** - Configures the advanced 802.1X authentication settings for the Profile.

2. **Device Selection** (see page 488)

Select the specific set of devices or Group of devices from the available device list. The Access Authentication Profile is applied to those APs or Switch devices.

3. **Port Assignments** (see page 489)

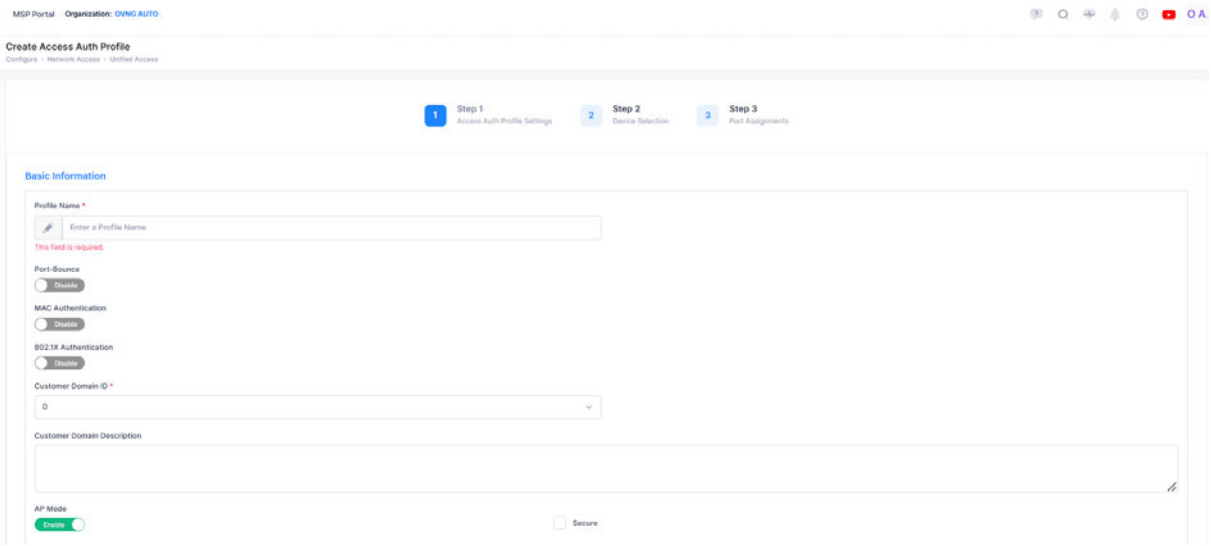
- **Ports** - An Access Auth Profile can be assigned to the Switch devices or Steller APs. Select the Switch Port(s) or AP downlink port(s) to which OmniVista will apply the Access Authentication Profile.

7.1.1.1.1 1. Access Auth Profile Settings

Complete the fields for the Basic Information (see page 484) and No Auth/Failure/Alternate (see page 486) sections on the Access Auth Profile Settings tab as described below, then click **Next** to go to the next tab (Step 2).

Basic Information

This section is used to configure basic settings for the profile.

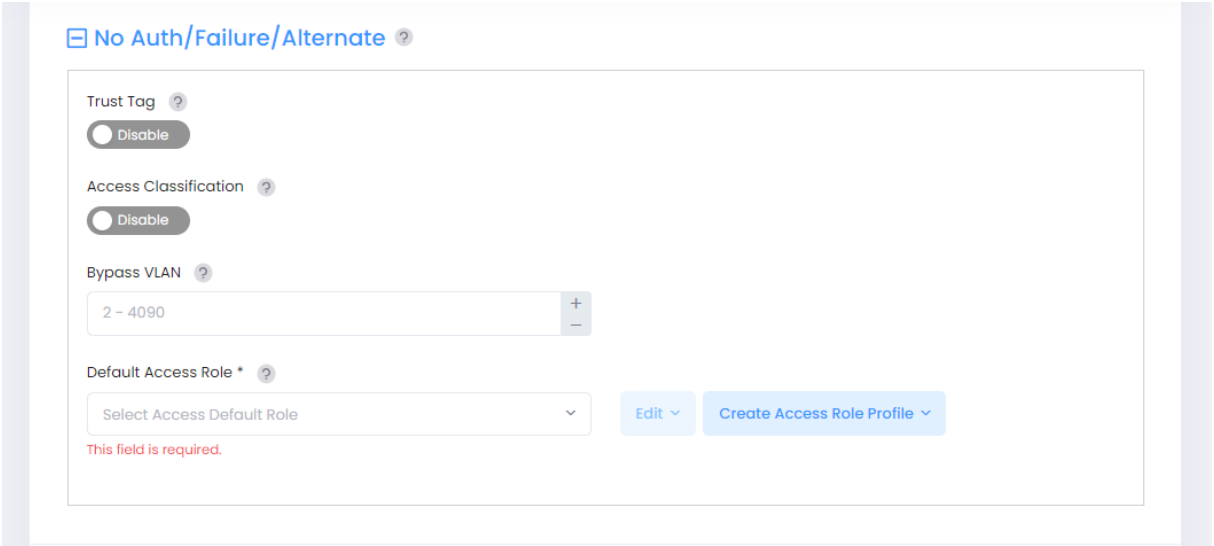


- **Profile Name** (required) - Specify a name to assign to the profile.
- **Port Bounce** - Enables/Disables Port Bounce. Always enabled on wireless devices. This feature is required to handle scenarios where a client is switched from one VLAN to another after a Change of Authorization (COA) request. When Port Bounce is enabled, the port is administratively shut down. This is to trigger DHCP renewal and re-authentication, if necessary.
- **MAC Authentication** - Enable/Disable MAC Authentication for the port.
- **802.1X Authentication** - Enable/Disable 802.1X Authentication for the port.
  - **Bypass Status (802.1X authentication only)** - Enable/Disable 802.1X bypass. When 802.1X Bypass is enabled, both MAC authentication and 802.1X authentication are performed - MAC authentication is performed first, then 802.1X authentication.
  - **MAC Allow EAP** - When 802.1X Bypass is enabled, select Pass, Fail, No-Auth or None for MAC Allow EAP.
    - **PASS** - 802.1X authentication is performed if MAC authentication passes.
    - **FAIL** - 802.1X authentication is performed if MAC authentication fails.
    - **NO-AUTH** - Allows 802.1X (EAP frame) authentication if there is no MAC authentication configured on the port.
    - **NONE** - It prevents 802.1X authentication. Only MAC authentication is performed on any device accessing this port.
- **AAA Server Profile** - Select an existing authentication, authorization, and accounting (AAA) Server Profile from the drop-down list. An AAA Server profile identifies the authentication servers and attributes that are used in an Access Authentication Profile. This field is required only if MAC or 802.1X authentication is enabled.
  - Click on **Edit** to modify settings for the selected AAA Server Profile.
  - Click on **Create AAA Server Profile** to create a new profile (see the AAA Server Profile online help).
- **Customer Domain ID** - Select a Customer Domain ID for the profile, if applicable.
- **Customer Domain Description** - Provide a description for Customer domain ID.

- **AP Mode** - Enables/Disables the Access Point Mode for the port. When enabled (the default), the Switch device automatically detects, learns, and manages a Stellar AP that is connected to the port. Wireless Client traffic is then forwarded from the AP to the Switch device onto the wired network.
- **Secure** - If the AP Mode is enabled, you can check this box to secure the AP Mode. The AP Mode is not secured by default (box is not checked). When an AP device is detected on a UNP port, the trust tag function is operationally enabled to trust the AP Client traffic. If the AP device fails authentication but is still learned as forwarding, the client traffic is still trusted and forwarded on the port. When the AP Mode is secured (box is checked), the trust tag function is not enabled for Client traffic until after the AP device successfully authenticates.

No Auth/Failure/Alternate

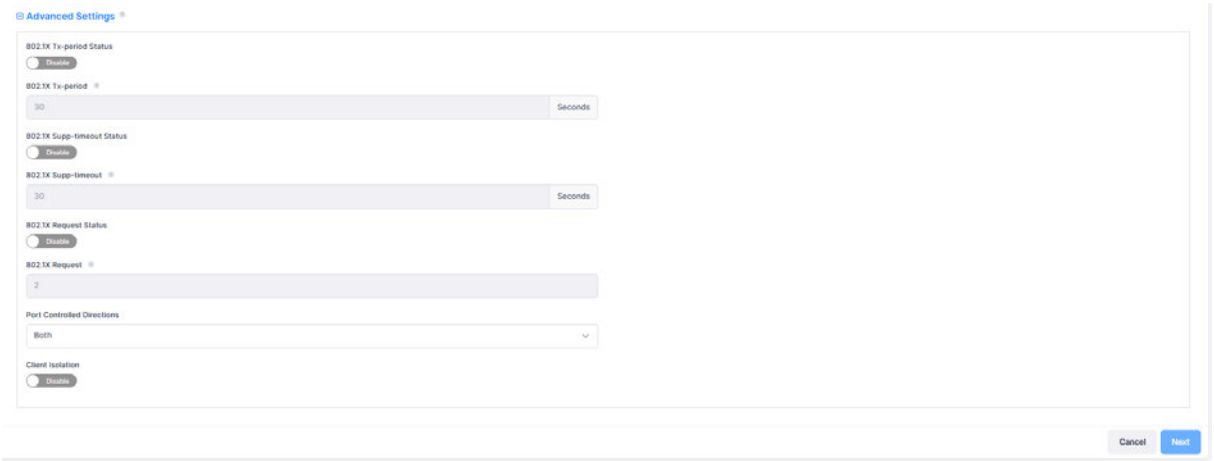
This section is used to configure alternate actions taken if MAC or 802.1X authentication was not enabled, authentication fails, or the returned role was not found.



- **Trust Tag** - Enable/Disable whether the VLAN ID of a tagged packet is trusted to determine how the packet is classified. Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic without the need to create specific classification rules for those profiles.
- **Access Classification** - Enable/Disable device classification. When enabled, device traffic is classified based on a classification rule (see the Access Classification online help).
- **Bypass VLAN** - Enter a Bypass VLAN ID (Range = 2 - 4094). The feature improves wired port forwarding performance by skipping the CPU process. When a Bypass VLAN is configured, traffic from the AP uplink port to the downlink port, or vice versa, is forwarded directly through without CPU intervention. The Bypass VLAN has higher priority than Trust Tag. Note that when Bypass VLAN is configured, Authentication/ACL/Policy etc. features cannot be applied to the traffic in the Bypass VLAN. When an Access Auth Profile is applied to an AP Group, OmniVista will pass the Bypass VLAN attribute to all APs in the AP Group. APs that support Bypass VLAN will accept it, other APs in the group will silently ignore this attribute.

- **MAC Pass Alt. Role (MAC authentication only)** - Select the Access Role Profile that is applied to clients that have passed MAC authentication but did not receive an Access Role Profile from the authentication server or the Access Role Profile was not found on the AP.
  - Click on **Edit** to modify settings for the selected Access Role Profile.
  - Click on **Create Access Role Profile** to create a new profile (see the Access Role Profiles (see page 514) online help).
- **802.1X Pass Alt. Role (802.1X authentication only)** - Select the Access Role Profile that is applied to clients that have passed 802.1X authentication but did not receive an Access Role Profile from the authentication server or the Access Role Profile was not found on the AP.
  - Click on **Edit** to modify settings for the selected Access Role Profile.
  - Click on **Create Access Role Profile** to create a new profile (see the Access Role Profiles (see page 514) online help).
- **Default Access Role** - Select the Default Access Role Profile that is applied to clients if authentication or classification methods fail to match traffic with any role. This is the last-resort role.
  - Click on **Edit** to modify settings for the selected Access Role Profile.
  - Click on **Create Access Role Profile** to create a new profile (see the Access Role Profiles (see page 514) online help).

Advanced Settings



This section is used to create the advanced 802.1X authentication settings for the Profile. The Client Isolation default value is disable.

- **802.1X Tx Period Status** - Enables/disables the Access Auth profile 802.1X Period Status. By default, it is disabled.
- **802.1X Tx Period** - Specifies the Access Auth Profile 802.1x Tx period, in seconds. (Note: Input a number between 1-65535 for AOS6 devices or 1-60 for AOS8/AOS5 devices).
- **802.1X Supp Timeout Status -** Enables/disables the 802.1X Authentication Support Timeout Status. By default, it is disabled.
- **802.1X Supp Timeout -** Specifies the 802.1X Authentication Support Timeout, in seconds. (Note: Input a number between 1-2147483647 for AOS6 devices or 1-120 for AOS8/AOS5 devices).

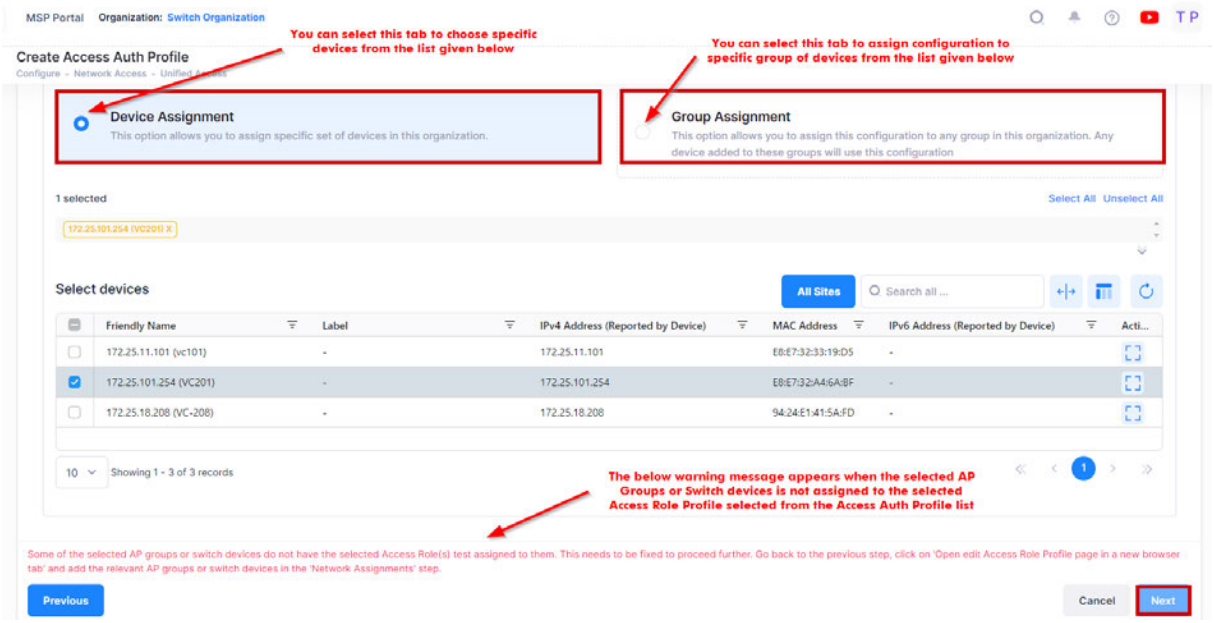
- **802.1X Request Status -** Enables/disables the 802.1X Authentication Max Request number Status. By default, it is disabled.
- **802.1X Request -** Specifies the 802.1X Authentication Max Request number. (Note: Input a number between 1-10 for AOS6 devices or 0-10 for AOS8/AOS5 devices).
- **Port Controlled Directions -** Configures whether Network Access control is applied to both incoming and outgoing traffic, or only applied to incoming traffic.
- **Client Isolation** - Enables/Disables Client Isolation (Default = Disabled). When enabled, traffic between Clients on the same AP in the SSID is blocked; Client traffic can only go toward the default gateway. You can create a list of device MAC addresses that a client can still access when Client Isolation is enabled.

> The **Client Isolation** advanced setting is only supported on Access Points and is not available for Switch devices.

7.1.1.1.2 2. Device Selection

The Device Selection tab is used to select the AP(s) or Switch devices from the available list of devices to which the Access Authentication Profile will be applied to devices within those groups. Complete the device selection as described below, then click **Next** to to the the next tab (Step 3).

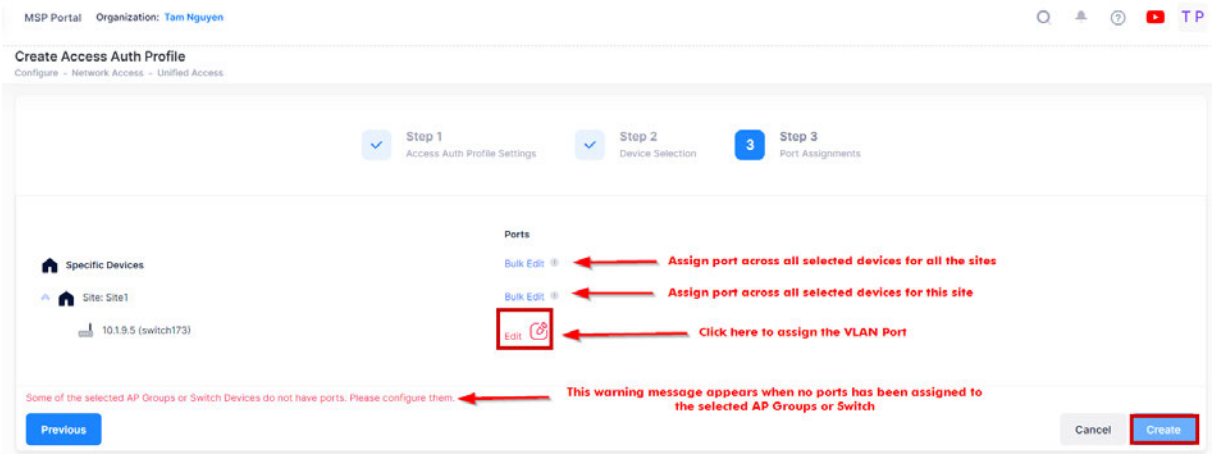
- **Device Assignment** - Select the specific set of Devices from the available list to assign the profile.
- **Group Assignment** - Select the specific group of Devices from the available list to assign the profile. The Access Authentication Profile is applied to the selected group of devices from the list.



Note: In case of failing to apply an Access Authentication Profile to devices, if you want to re-apply the profile with no change in the configuration, click on the Profile name to navigate to the device configuration detailed view. Then, select the Device configuration entry you want to reapply, click on edit button, and save the Profile without modifying any fields.

7.1.1.1.3 3. Port Assignments

The Port Assignments tab is used to select the port(s) to which OmniVista will apply the Access Authentication Profile. The profile is applied to client traffic received on the selected port(s).



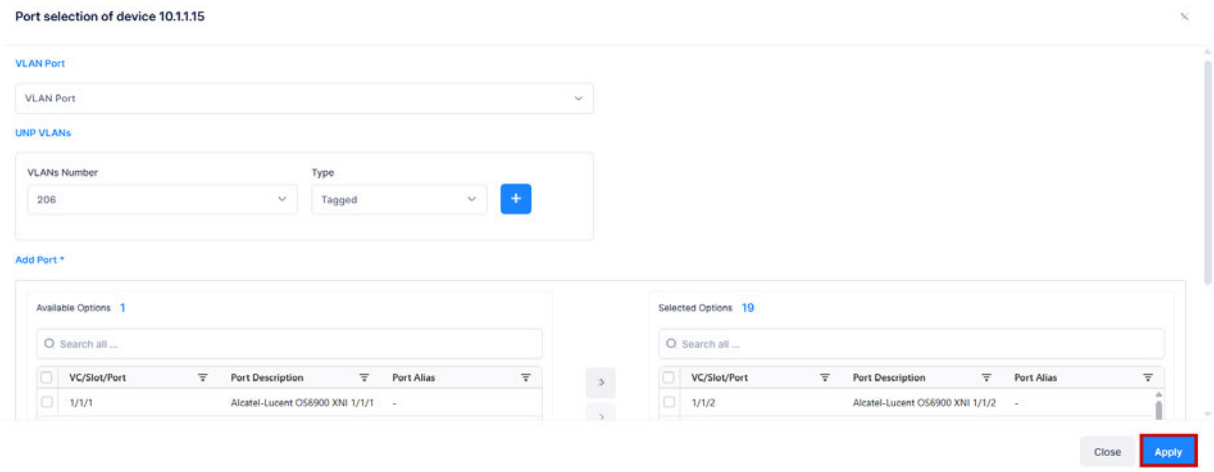
You can make a port selection for all AP Groups or Switch devices across all Sites in the Organization, for all AP Groups or Switch devices associated with a specific Site, or for the selected devices.

Consider the following use cases while selecting the Port assignments.

- Select different ports for different Access Authentication Profiles. No two different profiles can use the same ports.
- If any profile is using the selected switch port, then the other profile should be removed from that port.

Not all AP models have the same number of downlink ports (for example, some may have three and some may have four). If an AP Group contains an AP that does not support the selected downlink port(s), the AP will ignore the Access Authentication Profile configuration for that port and only apply the configuration to the available ports.

The downlink ports are displayed (Eth1, Eth2, Eth3, Eth4, USB0) on the Port Selection prompt, shown below, or next to the individual AP Group based on if you selected a **Bulk Edit** option or the individual AP Group to assign ports to the Access Authentication Profile.



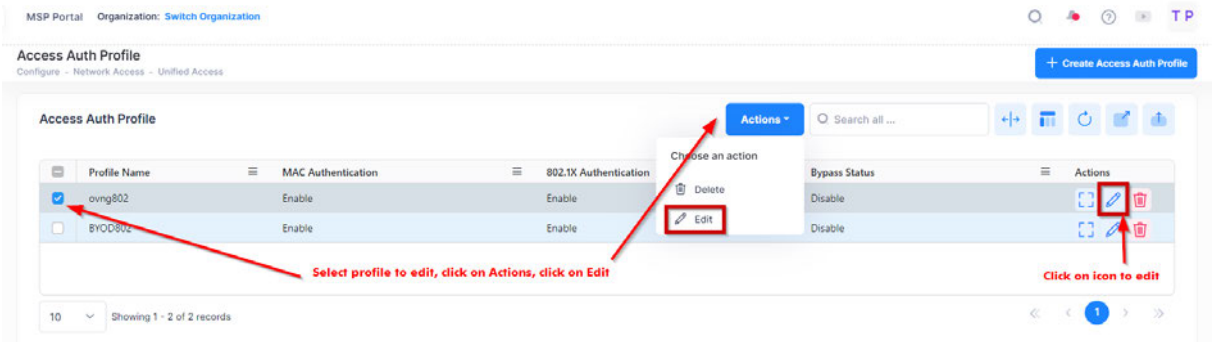
Complete the following field values:

- **Port Type** - The port type (VLAN Port, SPB Access Port, VXLAN Access Port).
- **UNP VLANs** - The VLANs configured for dynamically-created UNP VLANs. For 8.x Devices, select a traffic type (Tagged, Untagged).
- **Add Port** - The switch port(s) configured for the Profile.

When you are done selecting the device ports, click on **Apply**. The Access Authentication Profile is created and applied to client traffic received on the selected ports.

7.1.1.2 Editing an Authentication Access Profile

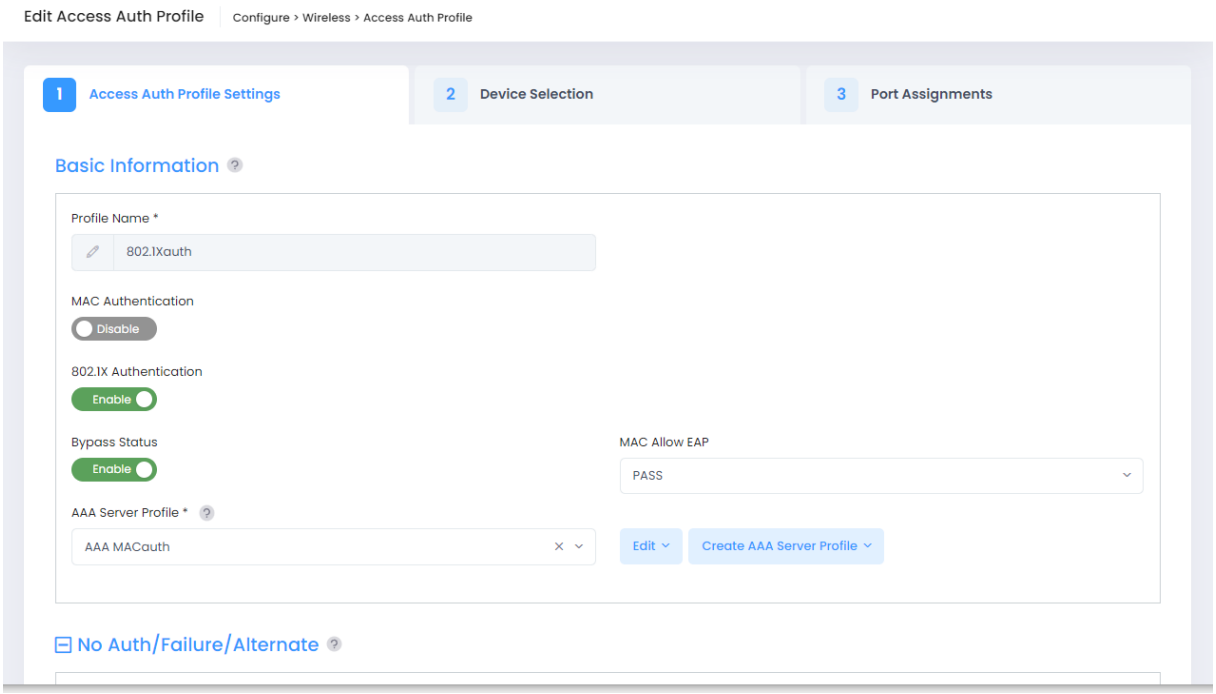
You can edit the parameter values for an existing Access Authentication Profile by accessing the Edit Access Auth Profile screen.



Use one of the following methods to access the Edit Access Auth Profile screen (as shown above):

- Select the profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the profile that you want to edit.

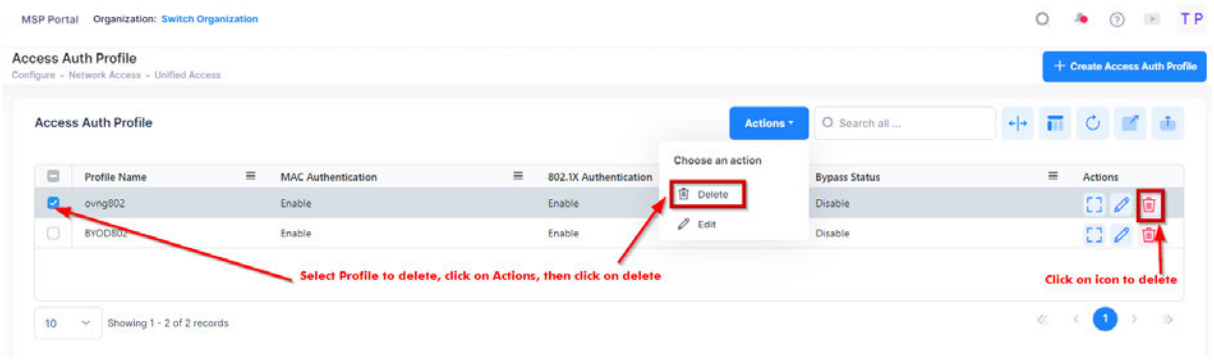
The following Edit Access Auth Profile screen displays. Edit the fields as described above (see page 483), then click on **Save**.



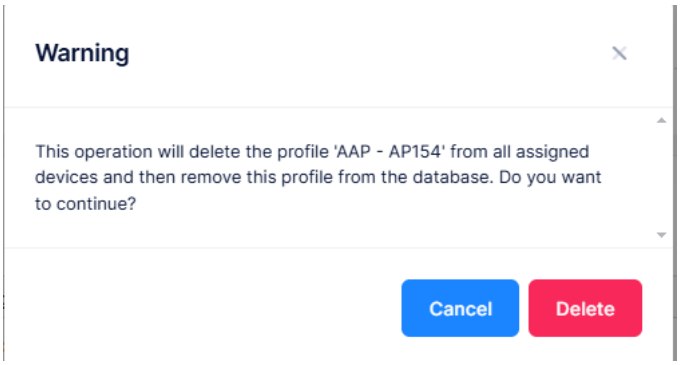
7.1.1.3 Deleting an Access Authentication Profile

To delete an Access Authentication Profile, use one of the following methods to select the profile you want to delete:

- Select the profile to delete by clicking on the checkbox next to the profile, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the profile that you want to delete.



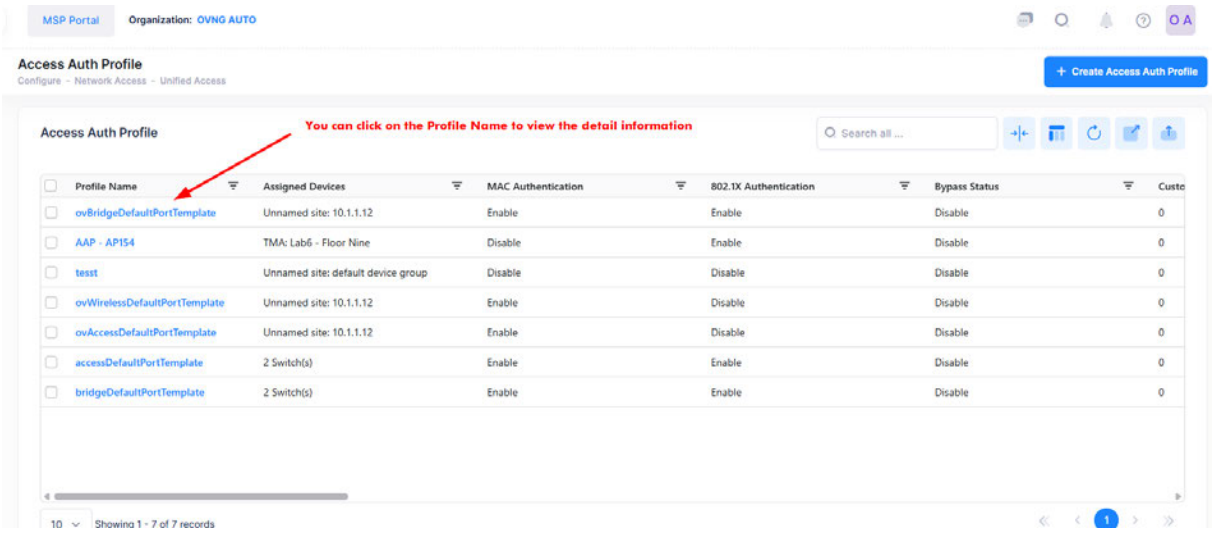
When you select the profile you want to delete, the following confirmation prompt appears:



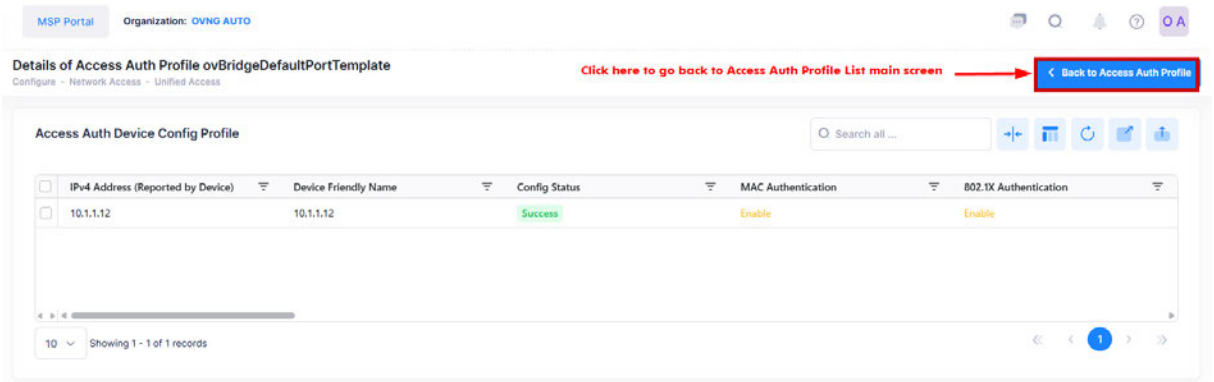
Click on **Delete** to confirm that you want to delete the Access Authentication Profile.

7.1.1.4 Display Assigned Switch Configuration Details

The Access Authentication Profile list displays information for the configured Access Authentication Profiles. To display assigned switch configuration detailed information about a specific Profile, click on the Profile Name as shown below.



The below screen will appears:



You can now view the current profile configuration for selected Switch that is assigned to an Access Authentication Profile. This screen also allows you to export, search and filter the data.

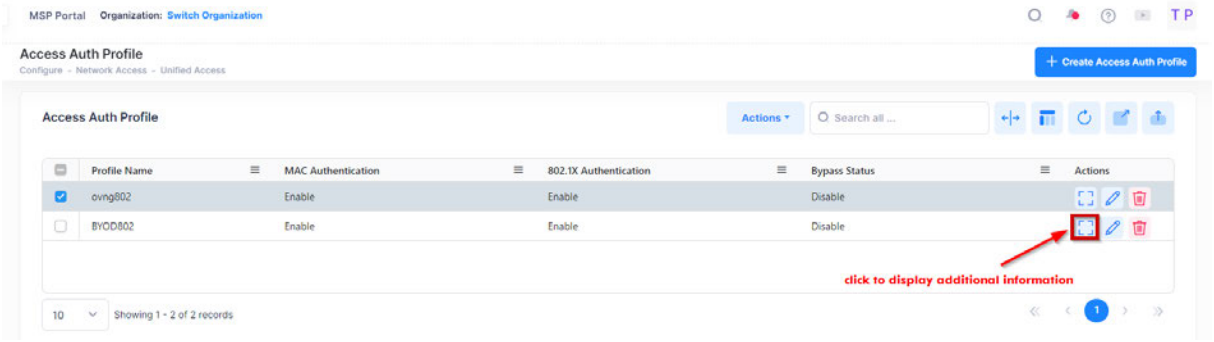
- **IPv4 Address** - The IPv4 address of the device.

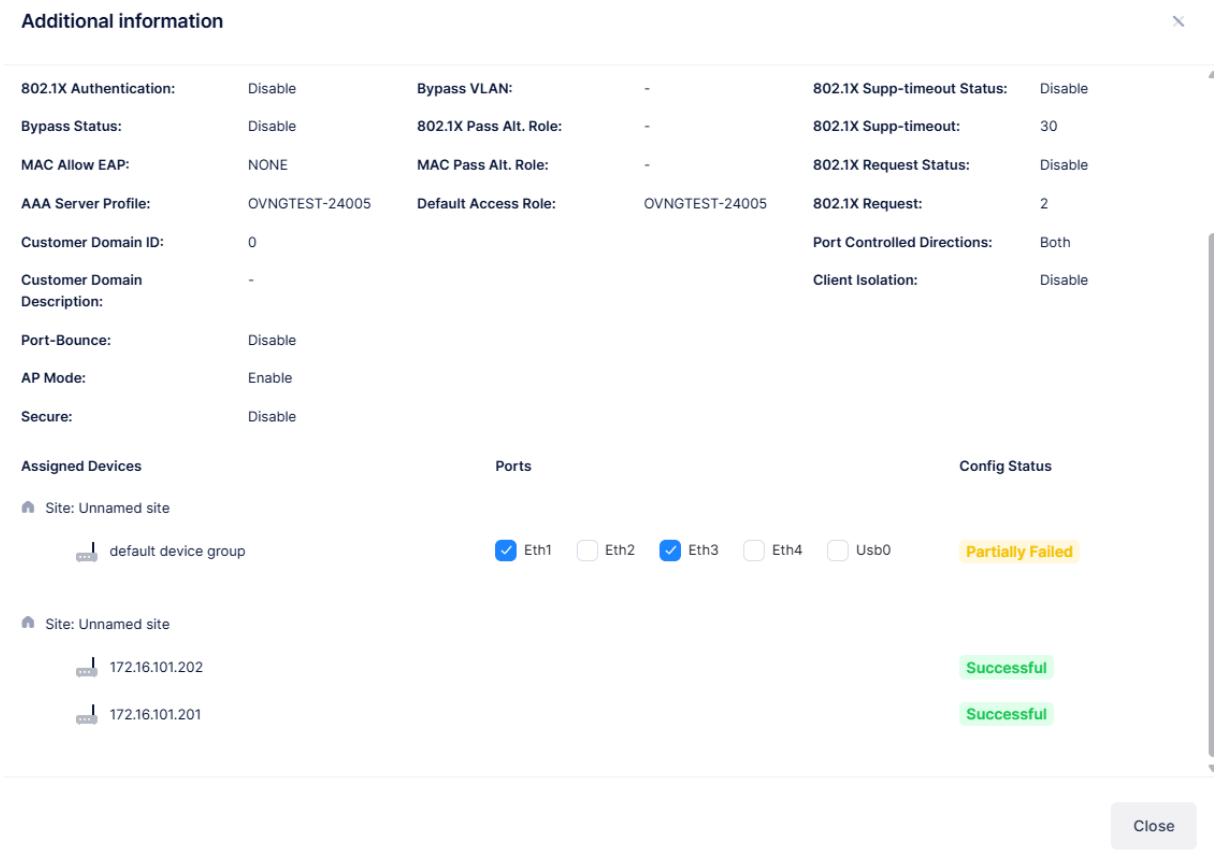
- **Device Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Config Status** - The configuration status of the device. (Successful or Failed or Pending).
  - **Pending** - The configuration is being pushed to the device and is still not receiving a response from the device.
  - **Failed** - The configuration failed to apply to the device. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to the device successfully.
- **MAC Authentication** - Enable/Disable MAC Authentication for the port.
- **802.1X Authentication** - Enable/Disable 802.1X Authentication for the port.

Note: You can now view the current profile configuration for each switch assigned to an Access Authentication Profile. You can edit the configuration on one or more assigned devices directly. If a device's configuration differs from the profile, the mismatched attributes will be highlighted, and you will have the option to synchronize them.

7.1.1.5 Display Access Authentication Profile Additional Information

You can click on Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.





The following information is displayed for each Access Authentication Profile:

- **Profile Name** - The name assigned to the Access Authentication Profile.

Basic Information

- **MAC Authentication** - The status of MAC authentication (Enable/Disable). When enabled, MAC authentication is applied with the profile.
- **802.1X Authentication** - The status of 802.1X authentication (Enable/Disable). When enabled, 802.1X authentication is applied with the profile.
- **Bypass Status** - The status of 802.1X bypass (Enable/Disable). Applies only when 802.1X authentication is enabled. When Bypass Status is enabled, the 802.1X authentication process is skipped and either MAC authentication or Access Classification is applied based on the profile configuration.
- **MAC Allow EAP** - Whether MAC Allow EAP is set to Pass or Fail (None). Applies only when 802.1X authentication and 802.1X bypass is enabled. If MAC Allow EAP is set to Pass, 802.1X authentication is performed only if MAC authentication passed.
- **AAA Server Profile** - The name of the authentication, authorization, and accounting (AAA) Server Profile assigned to the Access Authentication Profile.
- **Customer Domain ID** - Select a Customer Domain ID for the profile, if applicable.
- **Customer Domain Description** - Provide a description for Customer domain ID.

- **Port-Bounce** - Enables/Disables Port Bounce. Always Enabled on wireless devices. If port bounce is enabled, the port will be administratively put down.
- **AP Mode** - Enables/Disables the Access Point Mode for the port.
- **Secure** - If the AP Mode is enabled, you can check this box to secure the AP Mode. The AP Mode is not secured by default.

No Auth/Failure/Alternate

- **Access Classification** - The status of device classification (Enable/Disable). When enabled, classification rules are applied if other authentication methods are not enabled or fail.
- **Trust Tag** - The Trust Tag status (Enable/Disable). When enabled, the VLAN ID of tagged traffic is trusted to determine how traffic is classified if other authentication methods are not enabled or fail.
- **Bypass VLAN** - The Bypass VLAN ID specified for this profile.
- **802.1X Pass Alt. Role** - The Access Role Profile that is applied to clients that have passed 802.1X authentication but did not receive an Access Role Profile from the authentication server. Applies only when 802.1X authentication is enabled.
- **MAC Pass Alt. Role** - The Access Role Profile that is applied to clients that have passed MAC authentication but did not receive an Access Role Profile from the authentication server. Applies only when MAC authentication is enabled.
- **Default Access Role** - The Access Role Profile that is applied to clients if authentication or classification methods fail to match traffic with any role.

Assigned Devices

- **Site** - The AP Group(s), Switches and associated Sites to which the Access Authentication Profile is applied.

Ports

- **Eth1, Eth2, Eth3, Eth4, USB0** - The ports to which the Access Authentication Profile is applied via Port type VLAN_PORT. USB0 indicates an Ethernet-over-USB dongle. Switch ports are identified by *chassis/slot/port*.

Config Status

The status of applying the profile to devices (Successful, Failed, Pending, or Partially Failed).

- **Pending** - The configuration is being pushed to the devices and has still not received any response from any device.
- **Failed** - The configuration failed to apply to all the selected devices. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
- **Successful** - The configuration is pushed to all the selected devices successfully.
- **Partially Failed** - The configuration is pushed to some devices successfully, while to others it failed or remains in a pending state.

The table below displays the combinations of configuration status for all device configurations in the Profile template.

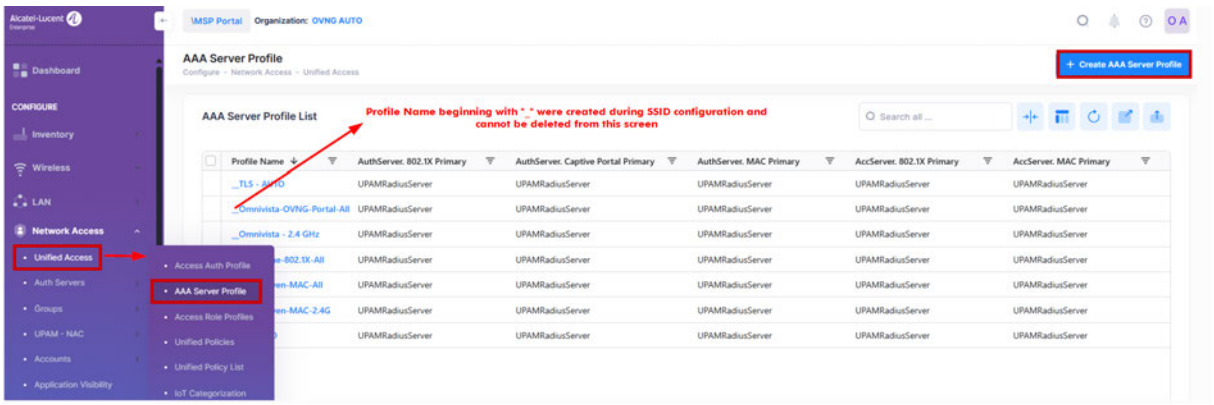
Device Configuration Status	Template
All Failed	Failed
All Successful	Successful
All Pending	Pending
Some failed, some successful	Partially Failed
Some pending, some successful	Pending
Some pending, some failed	Partially Failed
Some pending, some failed, some successful	Partially Failed

21 Oct 2025

7.1.2 AAA Server Profile

The AAA Server Profiles are used to define specific AAA parameters that can be used in an Access Authentication Profile or Captive Portal Profile. When an AAA Server Profile is assigned to a UNP Edge port through an Access Authentication Profile, the parameter values defined in the profile will override any existing global AAA configuration for users authenticating on that port.

Use the AAA Server Profile screen to display information (see page 509) about all of the configured AAA Server Profiles. This screen also allows you to create (see page 497), edit (see page 505), and delete (see page 506)profiles for Access Points on the network. To access the AAA Server Profile screen, click on **Network Access > Unified Access > AAA Server Profile** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.1.2.1 Creating an AAA Server Profile

The Create AAA Server Profile screen is used to configure the basic profile settings and advanced settings for Authentication Server, Accounting Server. it is also used to select the profile settings for 802.1X Authentication, MAC Authentication, Captive Portal Authentication and RADIUS Authentication for devices to which the profile is applied. To access this screen, click on **Create AAA Server Profile**.

Consider the following when configuring AAA Server Profile:

- You can unlink the AAA Server profile and that AAA Server profile will be deleted only if that profile isn’t used for any switches. The AAA Server profile template is retained in the AAA Server Profile List.
- The **Called Station ID** attribute value is not supported for switches, so when creating an AAA Server profile template or updating the table device configuration in OmniVista Terra 10, this attribute value is set to "AP-MAC-ADDRESS:SSID".
- The IPv6 would be available on the version 8.10.R03 on the switch.
- When Accounting Server has at least one server, the Syslog Accounting Server IP Address and Syslog Accounting Server UDP Port must be disabled.
- The Calling Station ID Type must be disabled when the Syslog Accounting Server IP Address is available. This attribute is available when you configure at least one server as the Accounting Server.
- When updating AAA Server Profile from aaa_profile_1 to aaa_profile_2, the aaa_profile_2 is pushed to Switch, and the aaa_profile_1 is not deleted from Switch.

- When deleting AAA Server Profile that does not link to any Access Auth Profile in OmniVista Terra 10, it would be deleted in Switch devices.
- Create a new NAS Client (see page 663) and configure the UPAMRadiusServer (see page 589) with the same shared secret that was used for the new NAS Client. The NAS Client and UPAMRadiusServer shared secret must match.
  Changing the shared secret on the UPAM Radius Server will affect all managed devices that authenticate through that UPAM Radius Server. This requires configuring the new shared secret for all NAS Client profiles to match the new shared secret for the UPAM Radius Server.

The Create AAA Server Profile screen provides the following step-by-step process for creating an AAA Sever Profile:

7.1.2.1.1 1. Basic Settings

- **Profile Name** - Configures the profile name.
- **Select Primary Authentication Server** - Select the Primary Authentication Server and the method of Authentication for the primary server to use (802.1X, MAC, Captive Portal).
- **Select Primary Accounting Server** - Select the Accounting Server and the method of Authentication for the primary server to use (802.1X, MAC, Captive Portal).

- The Select Primary Authentication Server field in the Basic Settings section only shows the RADIUS Server type.
- The Select Primary Accounting Server field in the Basic Settings section only shows RADIUS Server and LDAP Server type.
- When you click on the **Create Auth Server** button, the create RADIUS Server screen will open.
- An AP device supports one, and only one, TLS-enabled RADIUS server. As a result, you cannot have one TLS-enabled RADIUS server as Primary and another TLS-enabled RADIUS server as Secondary. If you have selected a TLS-enabled RADIUS Server as the Primary Server, do not select another TLS-enabled RADIUS Server as a Secondary or subsequent backup Server.

7.1.2.1.2 2. Advanced Settings

- **Authentication Server**- The Authentication Server section is used to select the Secondary, Third, and Fourth 802.1X, MAC and Captive Portal Authentication Servers to authenticate the network users.
- **Accounting Server**- The Accounting Server section is used to select the Secondary, Third, and Fourth 802.1X, MAC and Captive Portal Accounting Servers to use for user accounting.
- **802.1X Authentication Options**- This section is used to configure the advanced parameters of the 802.1X Authentication Protocol.
- **MAC Authentication Options**- This section is used to configure the advanced parameters of the MAC Authentication Protocol.

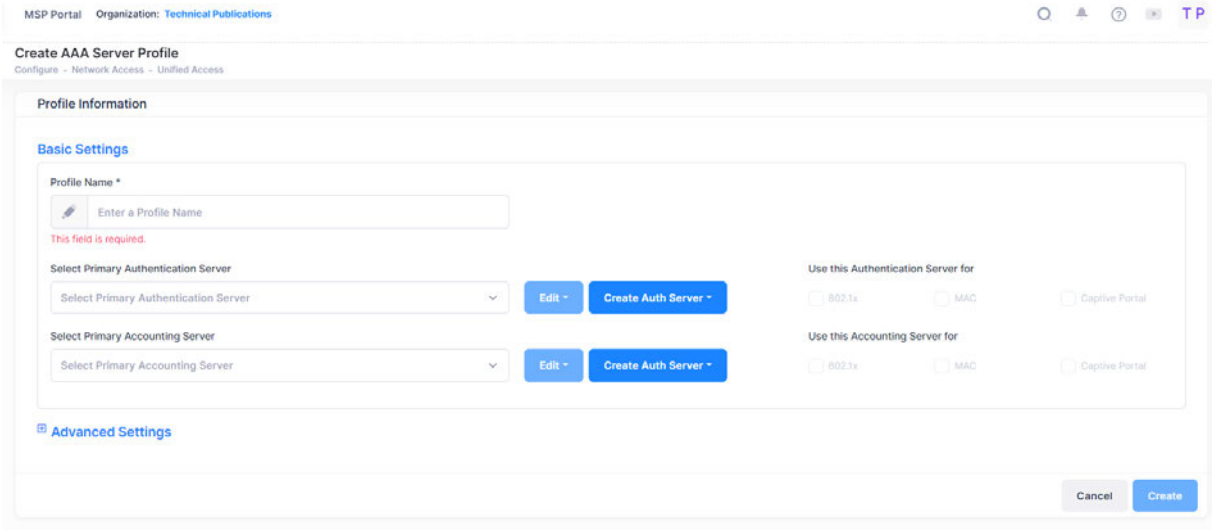
- **Captive Portal Authentication Options**- This section is used to configure the advanced parameters of the Captive Portal Authentication Protocol.
- **RADIUS Authentication Options**- This section is used to configure the advanced parameters of the RADIUS Authentication Protocol.

7.1.2.1.3 1. Basic Settings

Complete the fields for the Basic Settings section as described below, then go to Step 2.

Basic Settings

This section is used to configure basic settings for the AAA Server profile.



- **Profile Name** (required) - Specify a name to assign to the profile.
- **Select Primary Authentication Server** - Select the Primary Authentication Server from the drop-down menu or click on **Create Auth Server** to create a new Authentication Server. You can also click on **Edit** to open the Edit Auth Server screen and make changes to the selected profile. Select the type of Authentication method to use from the available options. (802.1X/MAC/ Captive Portal)
- **Select Primary Accounting Server** - Select the Primary Accounting Server from the drop-down menu or click on **Create Auth Server** to create a new Accounting Server. You can also click on **Edit** to open the Edit Auth Server screen and make changes to the selected profile. Select the type of Authentication method to use from the available options. (802.1X/MAC/Captive Portal)

7.1.2.1.4 2. Advanced Settings

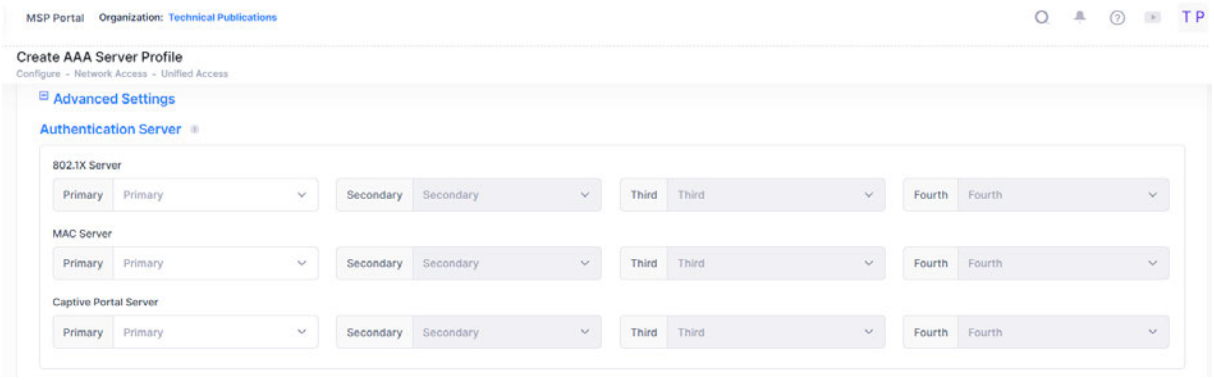
Complete the Advanced Settings sections as described below.

Authentication Servers

Select an Authentication Server for the Profile.

- **802.1X Server** - Select a Secondary, Third, and Fourth backup 802.1X Authentication Server for the Profile. Make sure you specify a different server for each backup server entry.

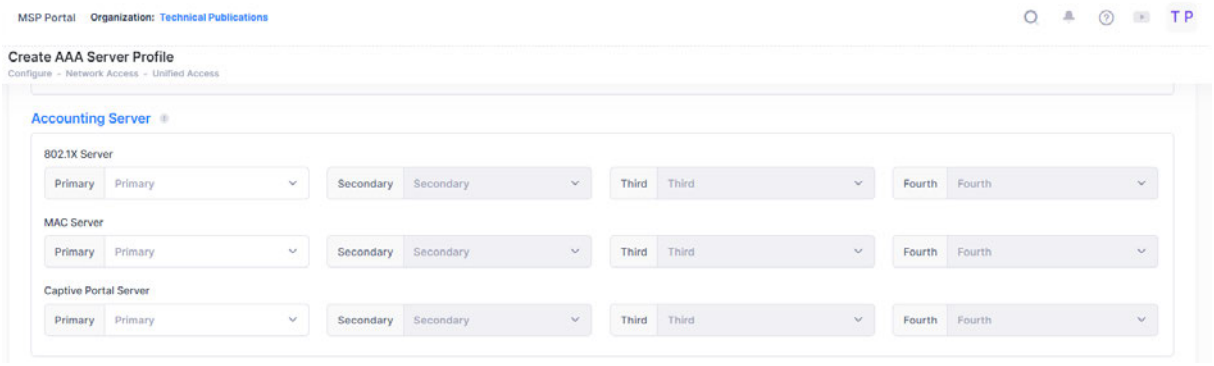
- **Captive Portal Server** - Select a Secondary, Third, and Fourth backup Captive Portal Server for the Profile. Make sure you specify a different server for each backup server entry.
- **MAC Server** - Select a Secondary, Third, and Fourth backup MAC Authentication Server for the Profile. Make sure you specify a different server for each backup server entry.



Accounting Servers

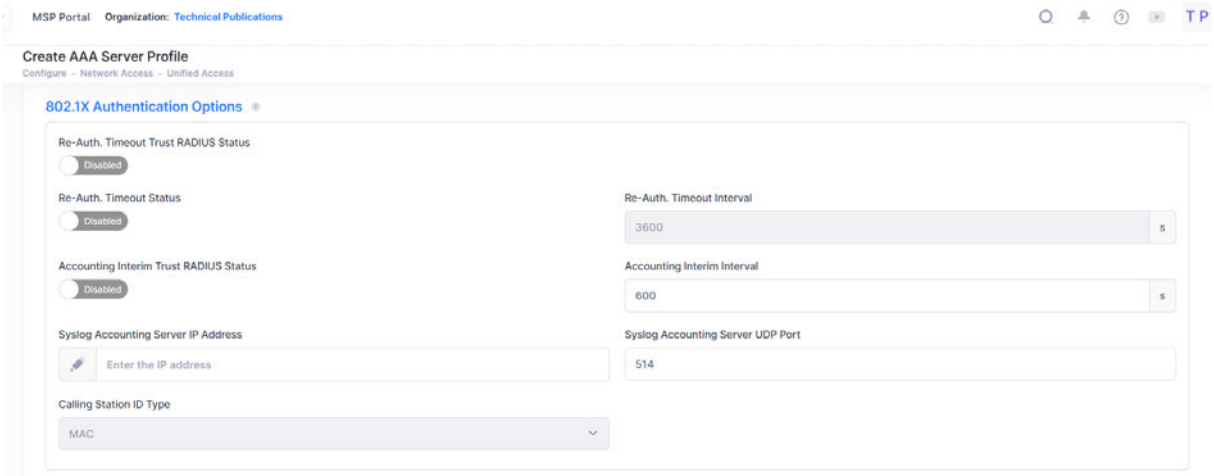
Select an Accounting Server for the Profile.

- **802.1X Server**- Select a Secondary, Third, and Fourth backup 802.1X Accounting Server for the Profile. Make sure you specify a different server for each backup server entry.
- **Captive Portal Server** - Select a Secondary, Third, and Fourth backup Captive Portal Accounting Server for the Profile. Make sure you specify a different server for each backup server entry.
- **MAC Primary** - Select a Secondary, Third, and Fourth backup MAC Accounting Server for the Profile. Make sure you specify a different server for each backup server entry.



802.1X Authentication Settings

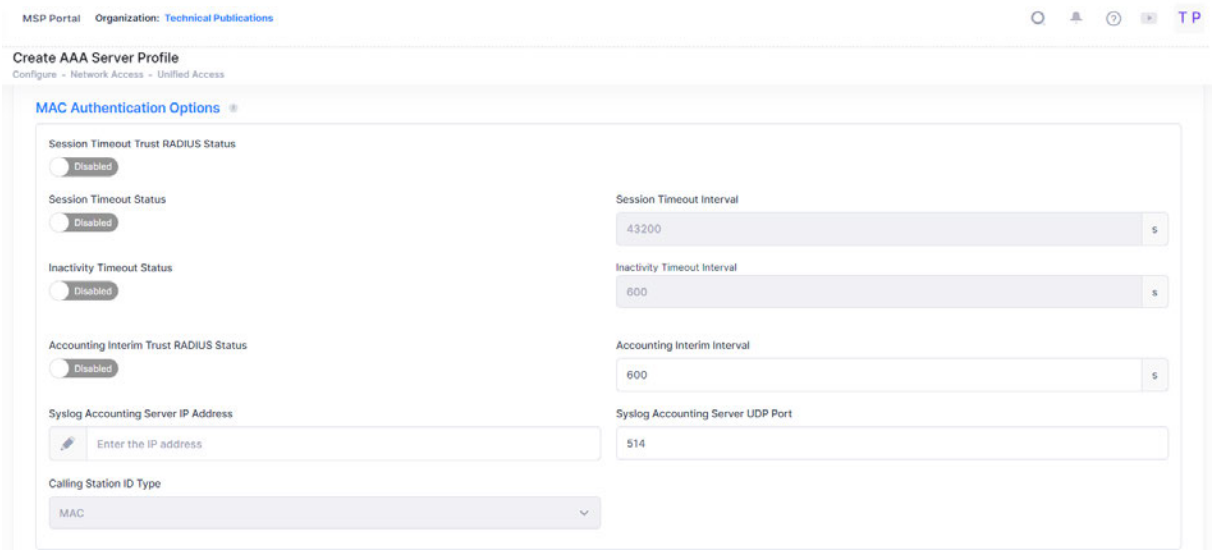
This section is used to configure the advanced parameters of the 802.1X Authentication Protocol. Complete the field values as described below.



- **Re-Authentication Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for 802.1X Authenticated users. If Enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch. (Default = Disabled).
- **Re-Authentication Timeout -** Enables/Disables the automatic re-authentication of authenticated 802.1X users (Default = Disabled).
- **Re-Authentication Interval -** The amount of time the switch waits, in seconds, before triggering re-authentication of 802.1X users. Note that when the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting. (Range = 600 - 7200, Default = 3600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for 802.1X authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for 802.1X accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

MAC Authentication Settings

This section is used to configure the advanced parameters of the MAC Authentication Protocol. Complete the field values as described below and **move to next tab**.

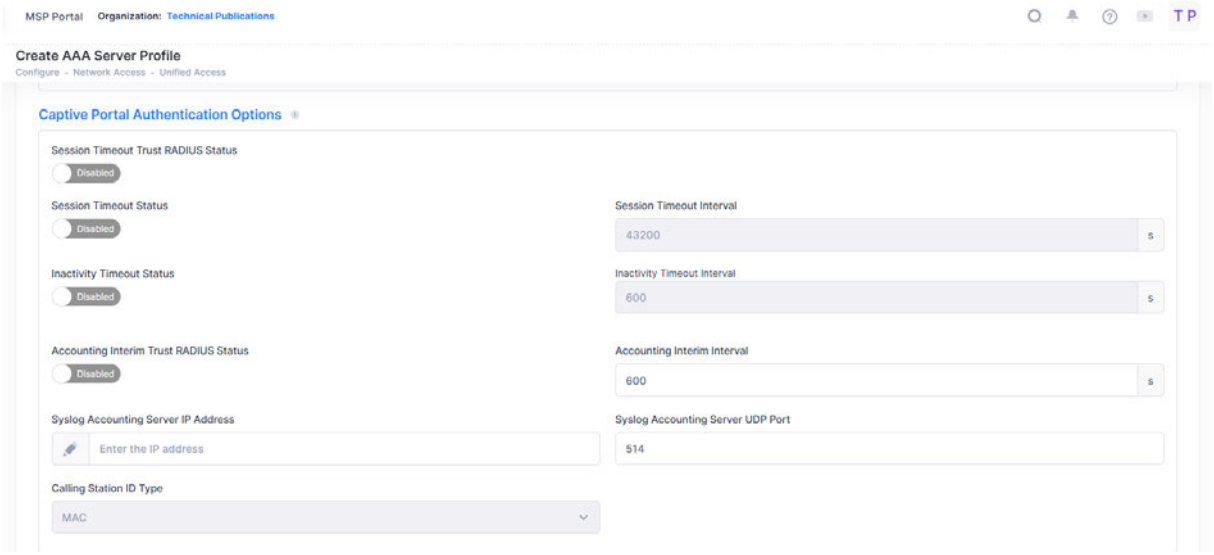


- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for MAC Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the Authentication Server in an Accept-Accept message. If Disabled, the switch uses the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 300 -172800, the 12000 - 86400 range is for AP ; 300 - 172800 range is for Switch, Default = 43200).
- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for MAC Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.(Range = 60 - 1200, Default = 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for MAC Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.

- **Accounting Interim Interval -** The amount of time between each interim accounting update for MAC accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

Captive Portal Authentication Settings

This section is used to configure the advanced parameters of the Captive Portal Authentication Protocol. Complete the field values as described below and **move to next tab**.

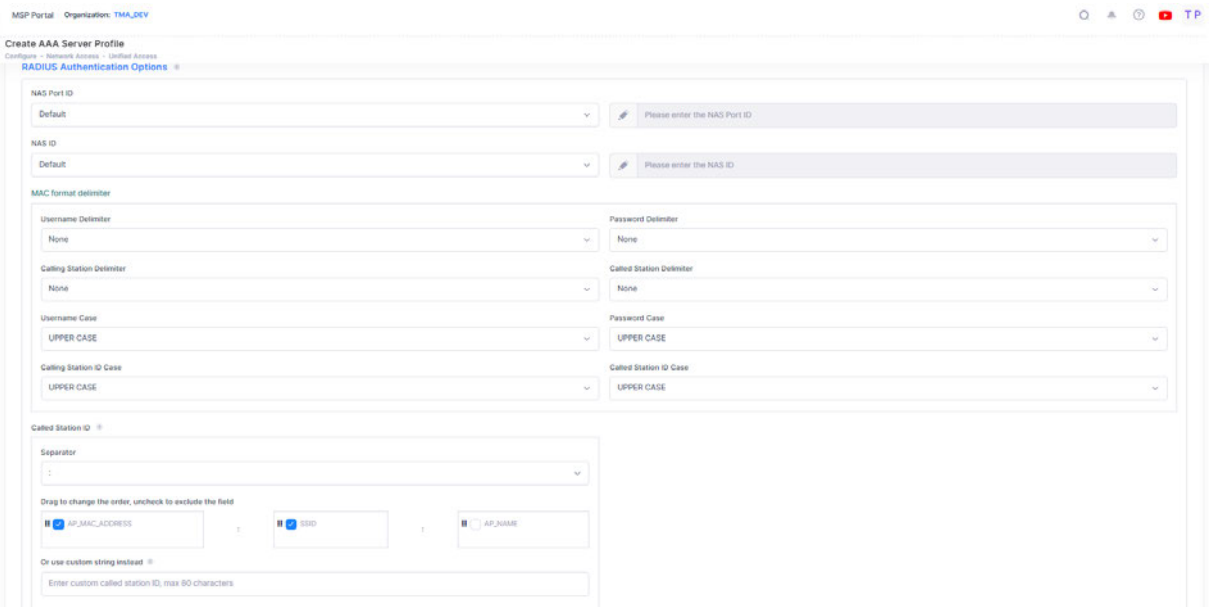


- **Session Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for Captive Portal Authenticated users. If Enabled, the switch will use the Session Timeout attribute received from the RADIUS server in an Accept-Accept message. If Disabled, the switch to use the locally configured timeout interval value (Default = Disabled).
- **Session Timeout Status -** Enables/Disables the Session Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Session Timeout Interval. (Default = Disabled).
- **Session Timeout Interval -** The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed. Note that when the Session Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again (Range = 300 -172800, the 12000 - 86400 range is for AP ; 300 - 172800 range is for Switch, Default = 43200).

- **Inactivity Timeout Status -** Enables/Disables the Inactivity Timeout option for Captive Portal Authenticated users. If Enabled, the user is automatically logged out of the network based on the configured Inactivity Timeout Interval (Default = Disabled).
- **Inactivity Timeout Interval -** The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value. Also note that when the Inactivity Timeout Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again. (Range = 60 - 1200, Default - 600)
- **Accounting Interim Trust Radius Status -** Enables/Disables the Accounting Interim Trust Radius option for Captive Portal Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value. Note that when the Accounting Interim Interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for Captive Portal accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).

RADIUS Authentication Options

This section is used to configure the advanced parameters of the Captive Portal Authentication Protocol. Complete the field values as described below.



- **NAS Port ID -** The RADIUS client NAS-Port attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to define a NAS-Port identifier for the NAS-Port

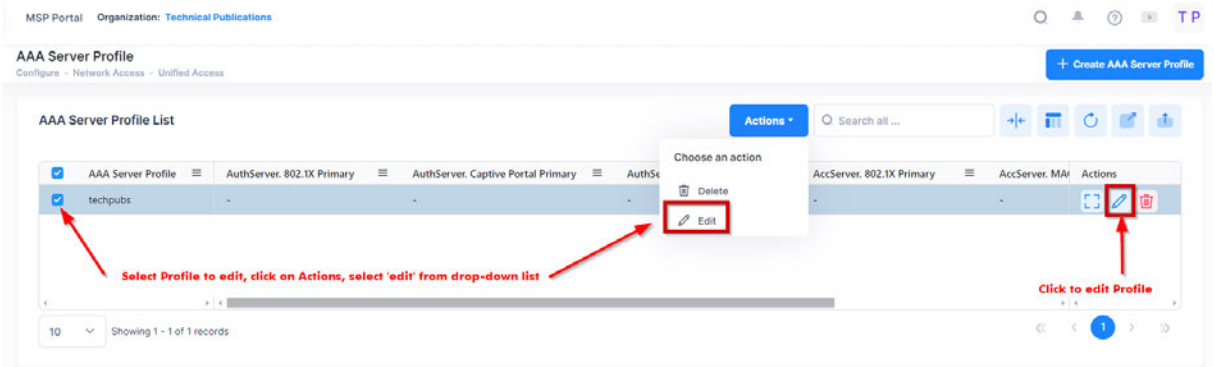
attribute. "Default" sets the NAS-Port attribute value to the chassis/slot/port of the user. The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages. (Default AP setting is wifi-2.4G/wifi-5G)

- **NAS ID -** The RADIUS client NAS-Identifier attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to identify the switch (RADIUS client) in the NAS-Identifier attribute. "Default" sets the NAS-Identifier attribute to the system name of the switch. The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages. (Default AP ID is AP WLAN name)
- **Username Delimiter -** The delimiter character used to separate fields within a RADIUS Server User Name.
- **Password Delimiter -** The delimiter character used to separate fields within a RADIUS Server Password.
- **Calling Station Delimiter -** The delimiter character used to separate fields within a Calling Station ID.
- **Called Station Delimiter -** The delimiter character used to separate fields within a Called Station ID.
- **Username Case -** Indicates if the RADIUS Server User Name must be in Upper Case or Lower Case.
- **Password Case -** Indicates if the RADIUS Server Password must be in Upper Case or Lower Case.
- **Calling Station ID Case -** Indicates if the Calling Station ID must be in Upper Case or Lower Case.
- **Called Station ID Case -** Indicates if the Called Station ID must be in Upper Case or Lower Case.
- **Called Station ID** - Customizing the Called Station ID only supports configuring on Access Points.

After completing the field values for **Basic Settings** and **Advanced Settings**, click on the **Create AAA Server Profile** button to create a new AAA Server Profile.

7.1.2.2 Editing an AAA Server Profile

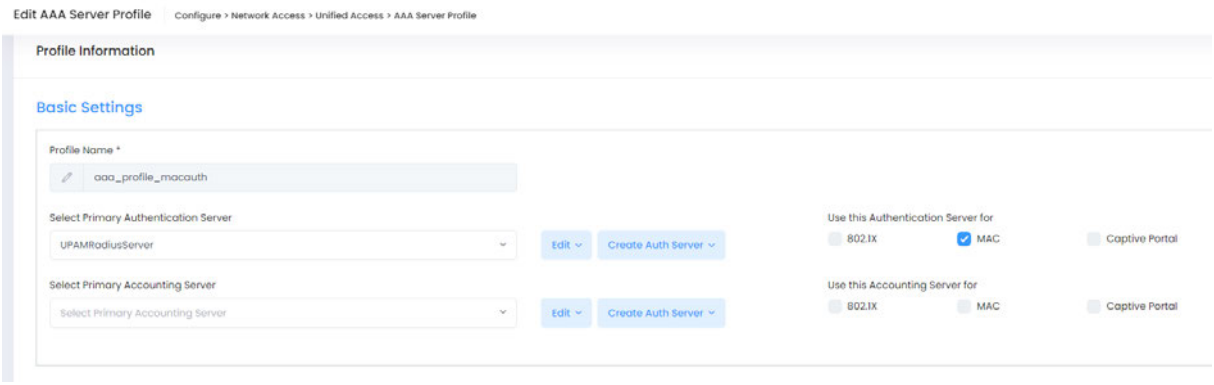
You can edit the parameter values for an existing AAA Server Profile by accessing the Edit AAA Server Profile screen.



Use one of the following methods to access the Edit AAA Server Profile screen (as shown above):

- Select the profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the profile that you want to edit.

The following Edit AAA Server Profile screen displays. Edit the fields as described above, then click on **Save**.

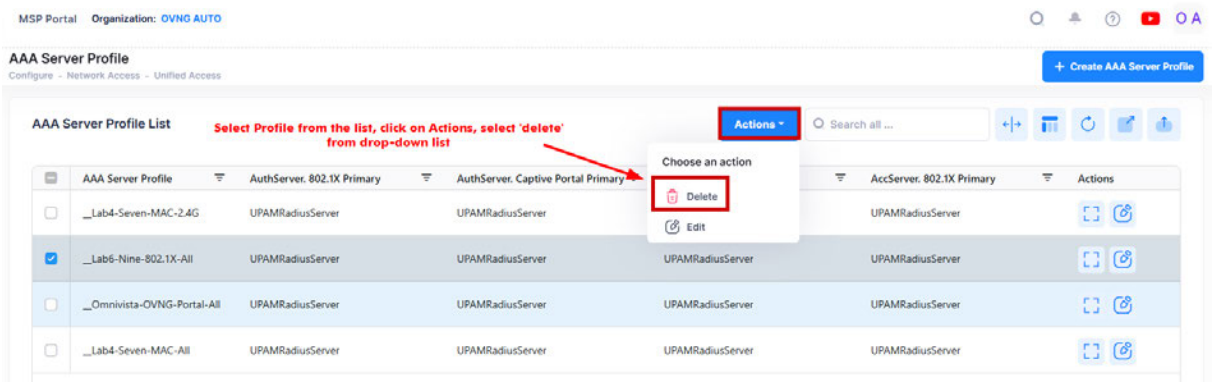


Note:

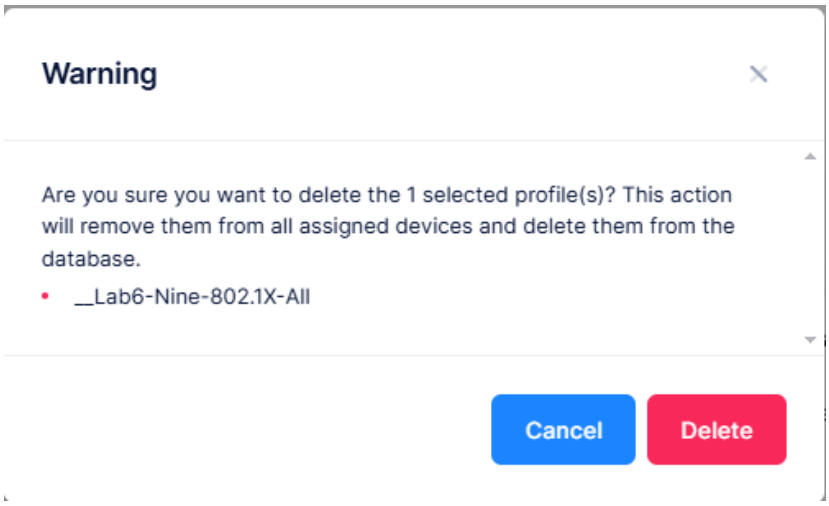
- If the AAA Server Profile has been applied to any devices through an Access Auth Profile or Captive Portal Profile, you will have to re-apply the associated Access Auth Profile or Captive Portal Profile to those devices to update the profile on the device(s).
- You can edit an existing AAA Server Profile that does not have the device configuration and verify that this AAA Server Profile is not pushed to Switch. The updated AAA Server profile would then push down to devices, which were on the device before.
- You can edit AAA Server profiles that were automatically generated through SSID configuration to add a secondary, third, and fourth AAA server for Authentication and Accounting.

7.1.2.3 Deleting an AAA Server Profile

To delete an AAA Server Profile, select the profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Delete** from the drop-down menu.



When you select the profile you want to delete, the following confirmation prompt appears:



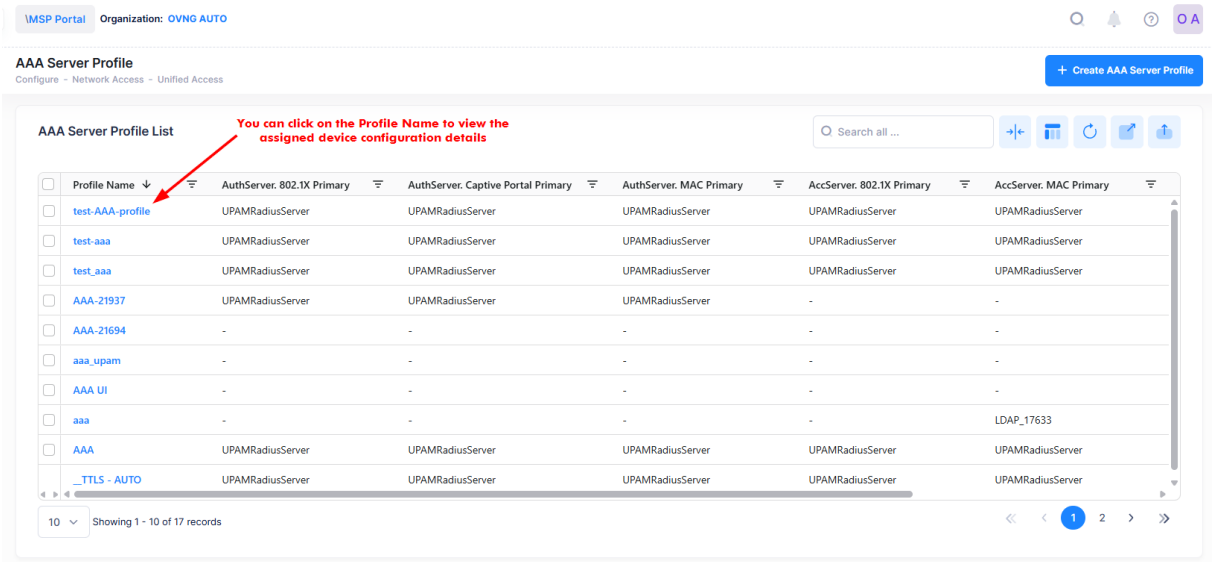
Click on **Delete** to confirm that you want to delete the AAA Server Profile.

Note:

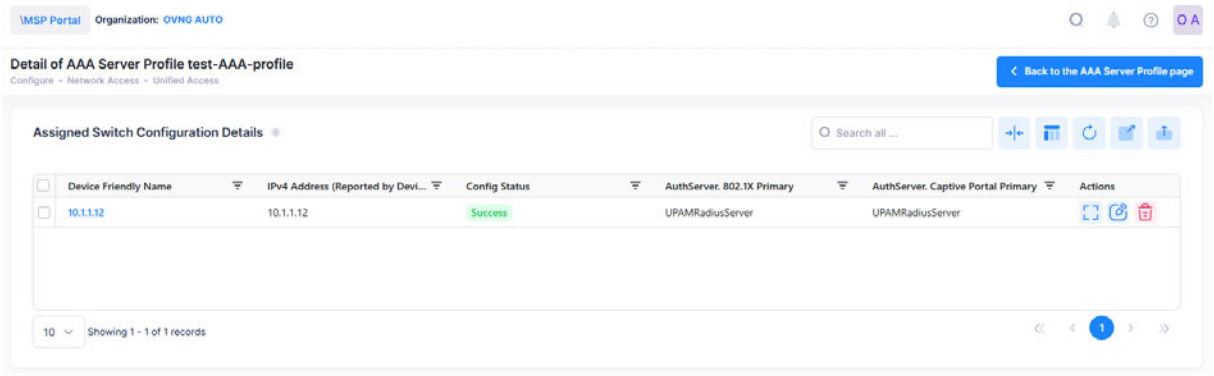
- If the profile has **not** been associated with an Access Auth Profile or Captive Portal Profile, the update will be applied and the status displayed. Click **OK** to return to the AAA Server Profile Screen.
- If the profile has been associated with an Access Auth Profile or Captive Portal Profile, the "**Delete AAA Server Profile**" confirmation prompt will appear listing any associated profiles. You must delete the AAA Server Profile from any associated profile(s) before returning to the AAA Server Profile Screen to delete the AAA Profile.
- You can delete the AAA server profile(s) that are not used anywhere in OmniVista Terra 10.
- When AAA server profile(s) are deleted on OmniVista Terra 10, they must be deleted on Switches.
- AAA Server profiles that were automatically generated through SSID configuration have a profile name beginning with an underscore (for example, “_guestuser”). You cannot delete this type of profile from the AAA Server Profile List.
- When you delete multiple AAA Server Profiles on Switch, one AAA Server Profiles failure will not affect other profiles.

7.1.2.4 Display Assigned Switch Configuration Details

The AAA Server Profile List displays information for the configured AAA Server Profiles. You can click on the Server Profile Name to view the assigned Switch configuration details of a specific profile as shown below.



The below screen will appears:



This screen also allows you to export, search and filter the data. You can click the back icon on the top right to navigate to the AAA Server Profile List page.

The following Device Configuration of the selected Profile is displayed.

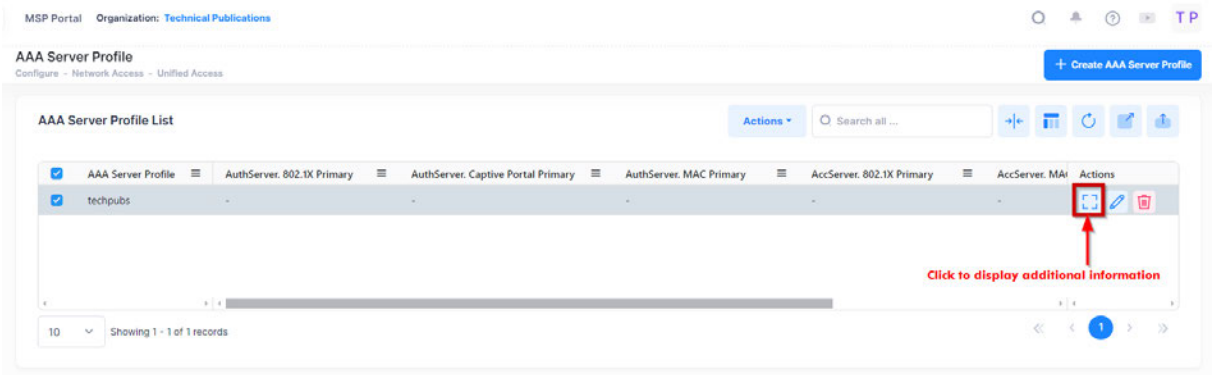
- **IPv4 Address** - The IPv4 address of the device.
- **Device Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Config Status** - The configuration status of the device. (Successful or Failed or Pending).
  - **Pending** - The configuration is being pushed to the device and is still not receiving a response from the device.
  - **Failed** - The configuration failed to apply to the device. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to the device successfully.
- **Authentication Server 802.1X Primary** - The name of the Primary Authentication 802.1X Server for the profile.

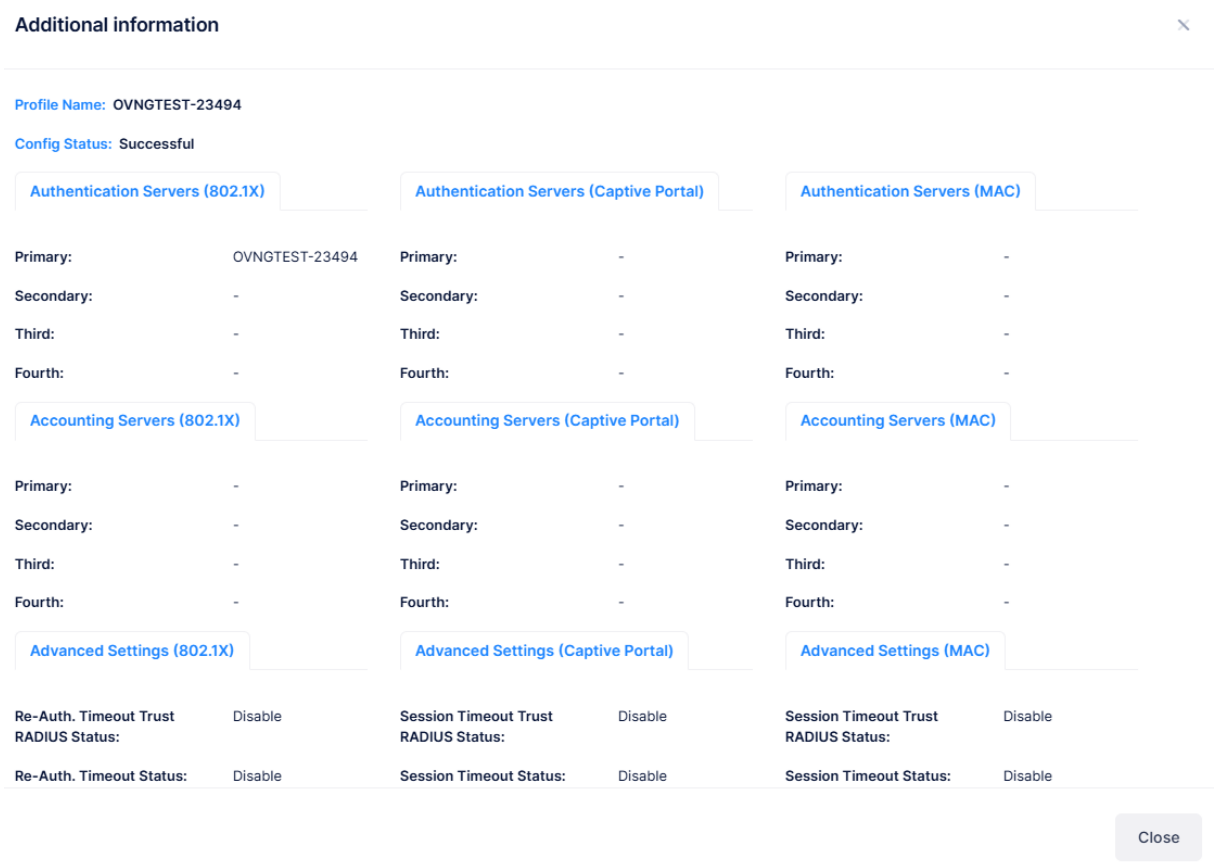
- **Authentication Server Captive Portal Primary** - The name of the Primary Authentication Captive Portal Server for the profile.
- **Authentication Server MAC Primary** - The name of the Primary Authentication MAC Server for the profile.
- **Accounting Server MAC Primary** - The name of the Primary Authentication MAC Server for the profile.
- **Accounting Server 802.1X Primary** - The name of the Primary Accounting 802.1X Server for the profile.
- **Accounting Server Captive Portal Primary** - The name of the Primary Authentication Captive Portal Server for the profile.

Note: You can now view the current profile configuration for each switch assigned to an AAA Server Profile. You can edit the configuration on one or more assigned devices directly. If a device's configuration differs from the profile, the mismatched attributes will be highlighted, and you will have the option to synchronize them.

7.1.2.5 Display AAA Server Profile Additional Information

To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column.





The following information is displayed for each of the AAA Server Profile:

- **Profile Name** - The name assigned to the AAA Server Profile.
- **Config Status** - The status of applying the profile to devices (Successful, Failed, Pending, or Partially Failed).
  - **Pending** - The configuration is being pushed to the devices and has still not received any response from any device.
  - **Failed** - The configuration failed to apply to all the selected devices. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to all the selected devices successfully.
  - **Partially Failed** - The configuration is pushed to some devices successfully, while to others it failed or remains in a pending state.

The table below displays the combinations of configuration status for all device configurations in the Profile template.

Device Configuration Status	Template
All Failed	Failed

Device Configuration Status	Template
All Successful	Successful
All Pending	Pending
Some failed, some successful	Partially Failed
Some pending, some successful	Pending
Some pending, some failed	Partially Failed
Some pending, some failed, some successful	Partially Failed

- **Authentication Server 802.1X Primary** - The name of the Primary Authentication 802.1X Server for the profile.
- **Authentication Server MAC Primary** - The name of the Primary Authentication MAC Server for the profile.
- **Authentication Server Captive Portal Primary** - The name of the Primary Authentication Captive Portal Server for the profile.
- **Accounting Server 802.1X Primary** - The name of the Primary Accounting 802.1X Server for the profile.
- **Accounting Server MAC Primary** - The name of the Primary Authentication MAC Server for the profile.
- **Accounting Server Captive Portal Primary** - The name of the Primary Authentication Captive Portal Server for the profile.
- **Session Timeout Trust RADIUS Status** - Enables/Disables the Session Timeout Trust Radius option for Captive Portal Authenticated users.
- **Session Timeout Status** - Enables/Disables the Session Timeout option for Captive Portal Authenticated users.
- **Session Timeout Interval** - The Session Timeout value, in seconds. When the Session Timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed.
- **Inactivity Timeout Status** - Enables/Disables the Inactivity Timeout option for Captive Portal Authenticated users.
- **Inactivity Timeout Interval** - The Inactivity Timeout value, in seconds. Make sure the configured value is value greater than the MAC address aging time for the switch. If the Timeout Value is exceeded, the user is not logged out of the network if the MAC address aging time expires before the configured timeout value.

- **Accounting Interim Trust RADIUS Status** - Enables/Disables the Accounting Interim Trust Radius option for Captive Portal Authenticated users. If Enabled, the Accounting Interim value received from the RADIUS server overrides the locally configured value.
- **Accounting Interim Interval -** The amount of time between each interim accounting update for Captive Portal accounting sessions, in seconds. (Range = 60 - 1200, Default - 600)
- **Syslog Accounting Server IP Address -** The IP address of the Syslog Accounting Server.
- **Syslog Accounting Server UDP Port -** The port used to communicate with the Syslog Accounting Server (Default = 514).
- **Calling Station ID Type -** The RADIUS Calling Station ID attribute for MAC accounting sessions (**MAC** - sets the Calling Station ID to the MAC address of the user. **IP** - sets the Calling Station ID to the IP address of the user).
- **NAS Port ID -** The RADIUS client NAS-Port attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to define a NAS-Port identifier for the NAS-Port attribute.
- **NAS ID -** The RADIUS client NAS-Identifier attribute for authentication and accounting sessions. A text string (up to 31 characters) is used to identify the switch (RADIUS client) in the NAS-Identifier attribute.
- **Username Delimiter -** The delimiter character used to separate fields within a RADIUS Server User Name.
- **Password Delimiter -** The delimiter character used to separate fields within a RADIUS Server Password.
- **Calling Station Delimiter -** The delimiter character used to separate fields within a Calling Station ID.
- **Called Station Delimiter -** The delimiter character used to separate fields within a Called Station ID.
- **Username Case -** Indicates if the RADIUS Server User Name must be in Upper Case or Lower Case.
- **Password Case -** Indicates if the RADIUS Server Password must be in Upper Case or Lower Case.
- **Calling Station ID Case -** Indicates if the Calling Station ID must be in Upper Case or Lower Case.
- **Called Station ID Case -** Indicates if the Called Station ID must be in Upper Case or Lower Case.
- **Re-Authentication Timeout Trust Radius Status -** Enables/Disables the Session Timeout Trust Radius option for 802.1X Authenticated users. If Enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch. (Default = Disabled).
- **Re-Authentication Timeout -** Enables/Disables the automatic re-authentication of authenticated 802.1X users (Default = Disabled).
- **Re-Authentication Interval -** The amount of time the switch waits, in seconds, before triggering re-authentication of 802.1X users. Note that when the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out

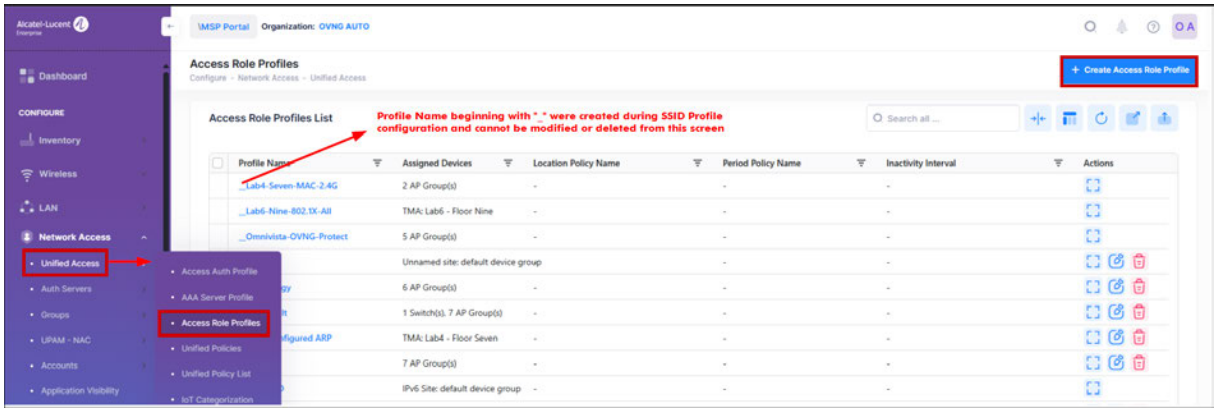
or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting. (Range = 600 - 7200, Default = 3600).

21 Oct 2025

7.1.3 Access Role Profiles

An Access Role Profile contains the various Unified Profile properties (such as QoS Policy List attached to the profile, Captive Portal Authentication) for users assigned to the profile. In a wireless-centric network, an Access Role Profile is considered as a user role with which every client in the wireless-centric network is associated.

Use the Access Role Profiles screen to display information (see page 530) about all configured Access Role Profiles. This screen is also used to create (see page 514), edit (see page 525), and delete (see page 526)Access Role Profiles. To access the Access Role Profiles screen, click on **Network Access > Unified Access > Access Role Profiles** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.1.3.1 Creating an Access Role Profile

The Create Access Role Profile screen is used to select profile settings, assign network devices, and configure the VLAN/tunnel mapping for the profile. To access this screen, click on **Create Access Role Profile**.

Consider the following when configuring Access Role Profile:

- Each switch maps to the Access Role profile by only one VLAN ID.
- The VLAN ID of the Switch must be an individual VLAN and in range of 1 to 4094.
- The VLAN ID of the Access Point must be ‘Untagged VLAN’ or in the range of 2 to 4090. You can input an individual VLAN (5) or VLAN range (10-20).
- You can select only AP Groups to apply the Access Role Profile.
- You can select only Switch devices to apply the Access Role Profile.
- You can select both AP Groups and Switch devices to apply Access Role Profile.
- If you configure the Max Ingress Depth without specifying the Max Ingress Bandwidth (null), the Access Role profile will be updated but the configuration will not be applied to the switch. An alert will be sent to you.
- If you configure the Max Egress Depth without specifying the Max Egress Bandwidth (null), the Access Role Profile will be updated but the configuration will not be applied to the switch. An alert will be sent to you.
- Common rule for overriding child profiles:

- When the child profile is an inline QoS profile, then the profile's latest configuration on the switch will be overridden.
- When the child profile is an existing QoS profile, it is sent to the device for the first time. If the profile has been sent before, the system will check its configuration status on the device. If the status is "Success," there is no need to resend it. However, if the status indicates anything other than "Success," such as "Failed," the profile will be resent.

The Create Access Role Profile screen provides the following step-by-step process to create an Access Role Profile:

1. Access Role Profile Settings

- **Profile Name** (see page 516) - Configures the Access Role Profile name.
- **Auth Flag** (see page 516) - Enables/Disables authentication (not supported on Steller AP).
- **Mobile Tag Status** (see page 516) - Enables/Disables classification of tagged packets received on mobile ports (not supported on Steller AP).
- **Redirect Status** (see page 516) - Enables/Disables Captive Portal Redirect (not supported on wireless devices and ignored when applied to those devices).
- **QoS/ACL** (see page 516) - Configures QoS policy rules that are used to filter device traffic assigned to the Access Role Profile.
- **Location Policy** (see page 519) - Defines the location from which a device is allowed to access the network.
- **Period Policy** (see page 519) - Defines the date and time during which a device is allowed to access the network.
- **Inactivity Interval** (see page 520) - Defines the amount of time, in seconds, before an authenticated device is automatically logged out of the network due to inactivity (MAC address for the device has aged out).
- **Bandwidth Control** (see page 520) - The ingress/egress bandwidth limit/depth applied to device traffic assigned to the Access Role Profile.
- **Walled Garden** (see page 520) - Selects social media vendors through which a wireless client can authenticate.
- **Client Isolation** (see page 521) - Defines the MAC Addresses of Allowed list of devices for an isolated Client.
- **Client Session Logging** (see page 521) - Enables/Disables client session logging.
- **Captive Portal Attributes** (see page 522) - Configures the type of Captive Portal authentication.
- **Others** (see page 522)- Enables/disables the DHCP Option 82 feature.

2. Network Assignments

- **Select Sites and Groups** (see page 523) - Select Access Point Groups or Switch devices from one or more Sites. The Access Role Profile is applied to the APs or Switch devices in the selected Sites/AP groups.

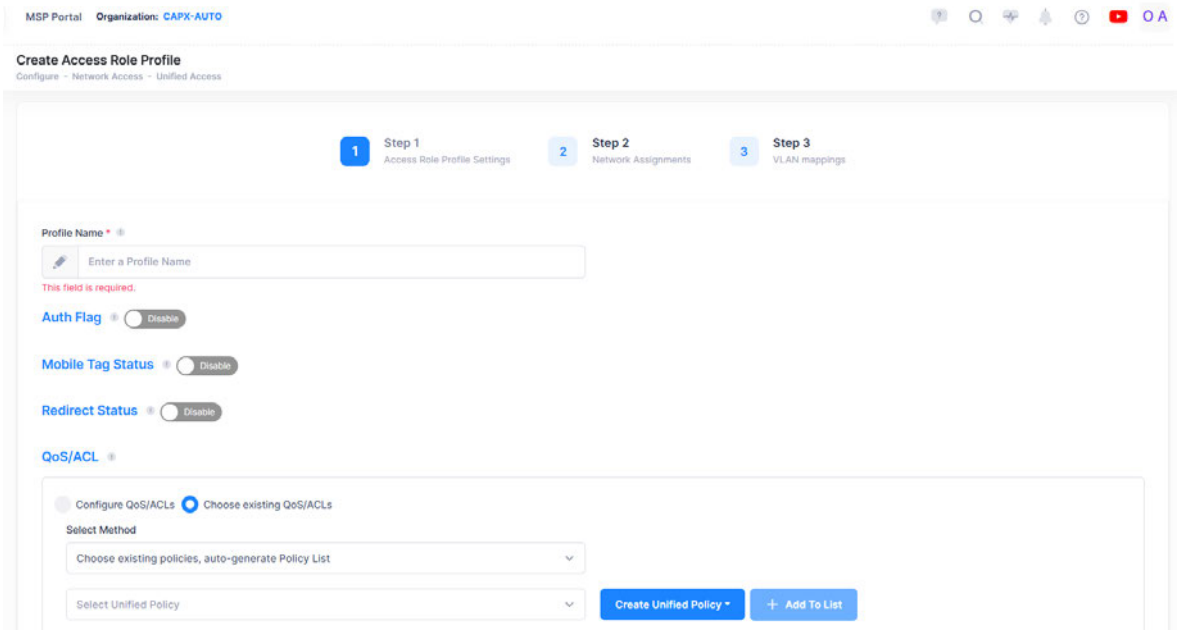
3. VLAN Mappings

- **VLAN/Tunnel Mapping** (see page 523) - Map the Access Role Profile to a VLAN or a Guest Tunnel ID. Traffic classified into the profile is forwarded on the selected VLAN or Tunnel.

7.1.3.1.1 1. Access Role Profile Settings

Complete the fields for the sections on the Access Role Profile Settings tab as described below, then click **Next** to move to the next tab (Step 2).

7.1.3.1.1.1 Profile Name, Auth Flag, Mobile Tag Status, Redirect Status

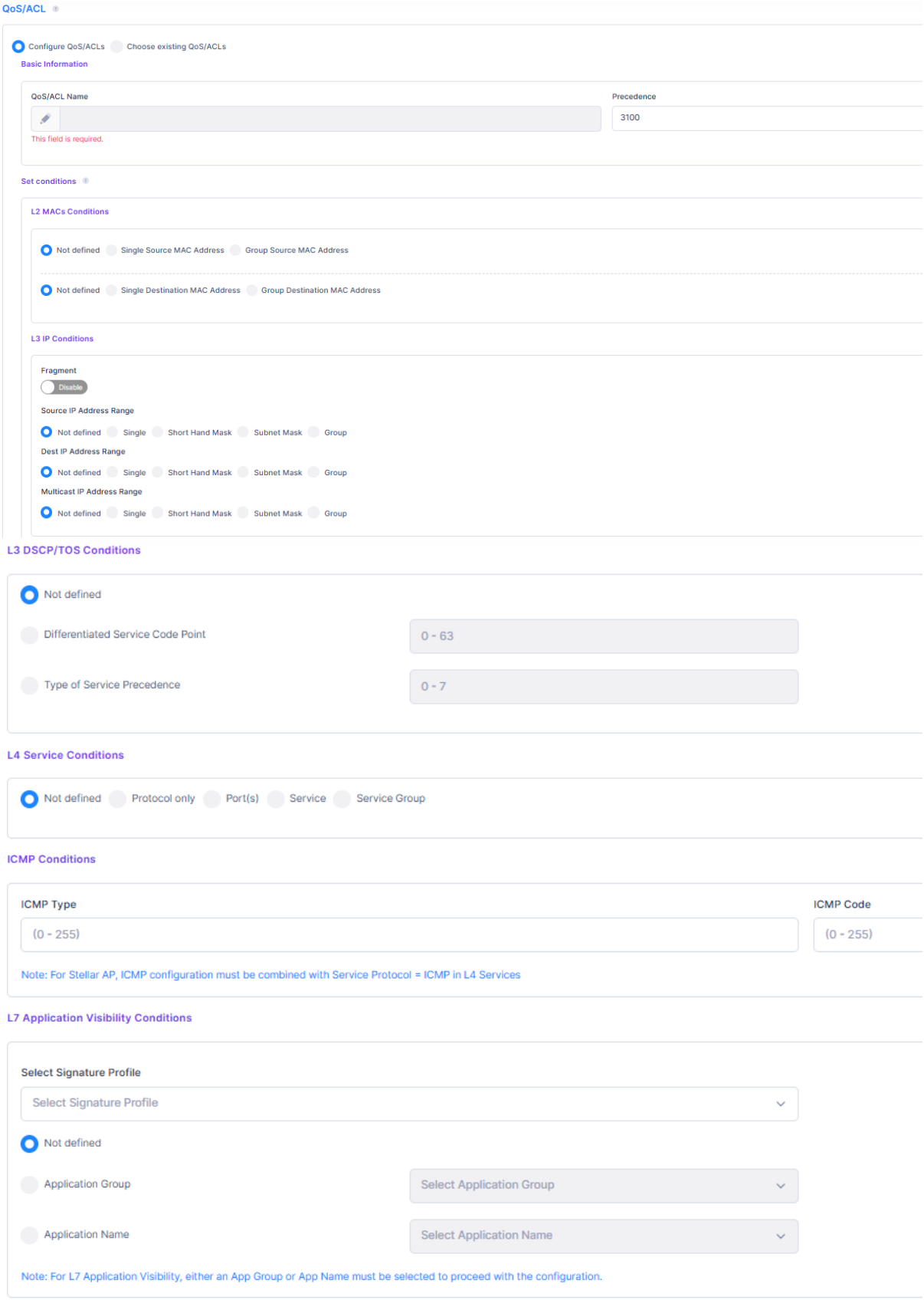


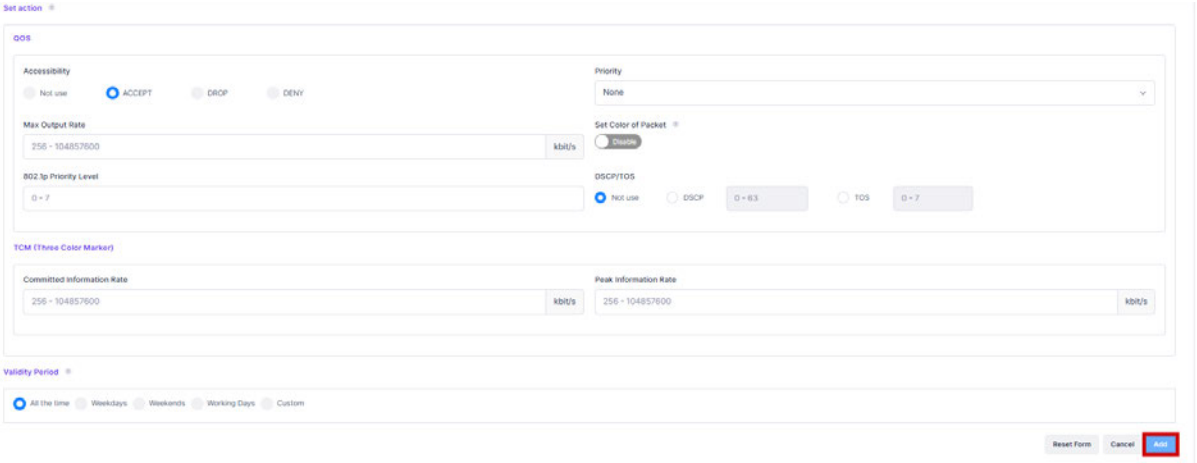
Complete the fields as described below to assign a name and QoS/ACLs to the profile:

- **Profile Name** - A unique name to identify the Access Role Profile.
- **Auth Flag** - Enables/Disables authentication (not supported on Steller AP).
- **Mobile Tag Status** - Enables/Disables classification of tagged packets received on mobile ports (not supported on Steller AP).
- **Redirect Status** - Enables/Disables Captive Portal Redirect (not supported on wireless devices and ignored when applied to those devices). Note that if Redirect Status is enabled, the Access Role Profile can only map to a VLAN when applying the profile to a device.

7.1.3.1.1.2 QoS/ACL

The QoS/ACLs are applied after you have joined the network. The QoS/ACLs have conditions to filter the traffic generated and actions taken on those generated traffics.


QoS/ACL
Configure QoS/ACLs
Choose existing QoS/ACLs
Basic Information
QoS/ACL Name
This field is required.
Precedence
3100
Set conditions
L2 MACs Conditions
Not defined
Single Source MAC Address
Group Source MAC Address
Not defined
Single Destination MAC Address
Group Destination MAC Address
L3 IP Conditions
Fragment
Disable
Source IP Address Range
Not defined
Single
Short Hand Mask
Subnet Mask
Group
Dest IP Address Range
Not defined
Single
Short Hand Mask
Subnet Mask
Group
Multicast IP Address Range
Not defined
Single
Short Hand Mask
Subnet Mask
Group
L3 DSCP/TOS Conditions
Not defined
Differentiated Service Code Point
0 - 63
Type of Service Precedence
0 - 7
L4 Service Conditions
Not defined
Protocol only
Port(s)
Service
Service Group
ICMP Conditions
ICMP Type
(0 - 255)
ICMP Code
(0 - 255)
Note: For Stellar AP, ICMP configuration must be combined with Service Protocol = ICMP in L4 Services
L7 Application Visibility Conditions
Select Signature Profile
Select Signature Profile
Not defined
Application Group
Select Application Group
Application Name
Select Application Name
Note: For L7 Application Visibility, either an App Group or App Name must be selected to proceed with the configuration.

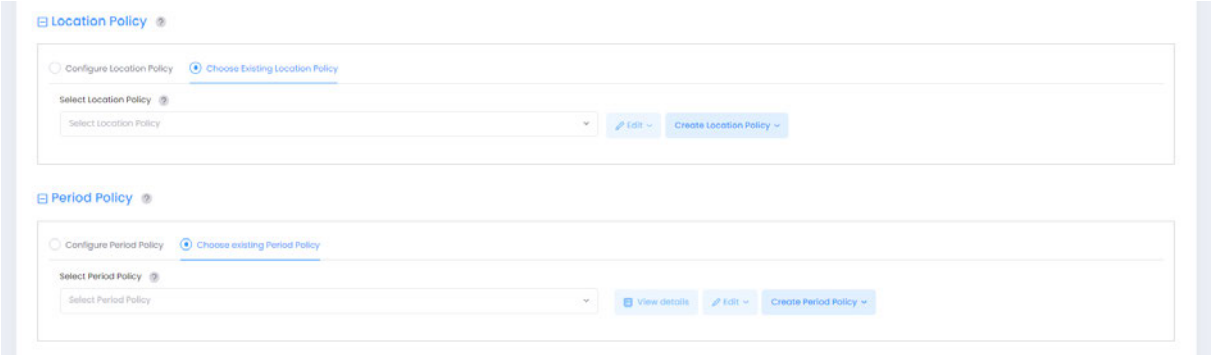


- **Configure QoS/ACLs** - Select this option to define a QoS Policy for the Access Role Profile. You can then customize the policy settings to define conditions/actions for the QoS policy by clicking on **Add more QoS/ACL** tab. Define the basic information and then define at least one condition to assign a QoS policy list. For more information regarding defining the various conditions, visit Unified Policies (see page 533) Online help.
- **Choose existing QoS/ACLs** - Select one of the following methods to assign a QoS policy list:
  - **Choose existing policies, auto-generated policy list** - Automatically generate a policy list by selecting existing policies for the list and/or click on **Create Unified Policy** to open the Create Unified Policy (see page 533) screen and create new QoS policies for the list. (**Note**: If the selected policies have already been successfully assigned to certain devices, their values will not be overridden on those devices. However, for the auto-generated policy list, the content will still be pushed to the assigned devices).
  - **Choose existing policy list** - Select an existing QoS policy list from the drop-down menu or click on **Create Unified Policies List** to open the Create Unified Policies List (see page 551) screen and create a new QoS policy list. You can also click on **View details** to view information about the selected list or click on **Edit** to open the Edit Unified Policies List screen to make changes to the selected list. (**Note:** If the selected policy list has been successfully assigned to certain devices, the values for those devices will not be overridden by that policy list).

Note: The 'Redirect Status' attribute value supports Switch devices only.

Note: To create a Quality of Service (QoS) policy for multiple applications, you can create a custom group within the Signature profile. By using the "Custom Application Group" feature, you can define a single policy that includes all applications in that group. This method is advantageous because any modifications to the applications within the custom group will not necessitate editing the policies or pushing updated policies to managed devices.

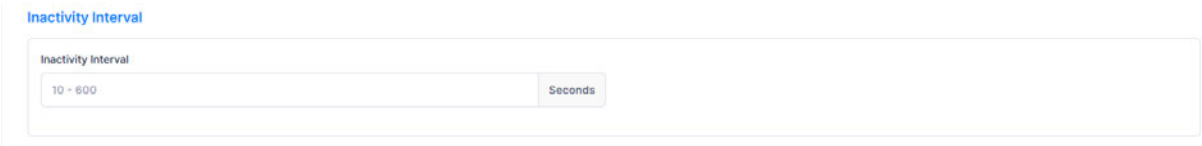
7.1.3.1.1.3 Location/Period Policy



- **Location Policy** - Defines a specific location from which a device can access the network. The Location Policy is applied to traffic classified into the Access Role Profile.
  - **Configure Location Policy** - Select this option to define a Location Policy to assign to the Access Role Profile. When you select this option, a Location Policy is automatically created with the Access Role Profile name.
    - **Save this as a distinct Location Policy, for reuse** - Select this option if you want the automatically created Location Policy to be available for use after the associated Access Role Profile has been deleted.
  - **Choose Existing Location Policy** - Select an existing Location Policy from the drop-down menu or click on **Create Location Policy** to open the Create Location Policy (see page 576) screen and create a new Location Policy. You can also click on **Edit** to open the Edit Location Policy screen and make changes to the selected policy.
- **Period Policy** - Specifies the days and times during which a device can access the network. The Period Policy is applied to traffic classified into the Access Role Profile.
  - **Configure Period Policy** - Select this option to define a Period Policy to assign to the Access Role Profile. When you select this option, a Period Policy is automatically created with the Access Role Profile name.
    - **Save this as a distinct Period Policy, for reuse** - Select this option if you want the automatically created Period Policy to be available for use after the associated Access Role Profile has been deleted.
  - **Choose Existing Period Policy** - Select an existing Period Policy from the drop-down menu or click on **Create Period Policy** to open the Create Period Policy (see page 585) screen and create a new Period Policy. You can also click on **View Details** to view information about the selected policy or click on **Edit** to open the Edit Period Policy screen and make changes to the selected policy.

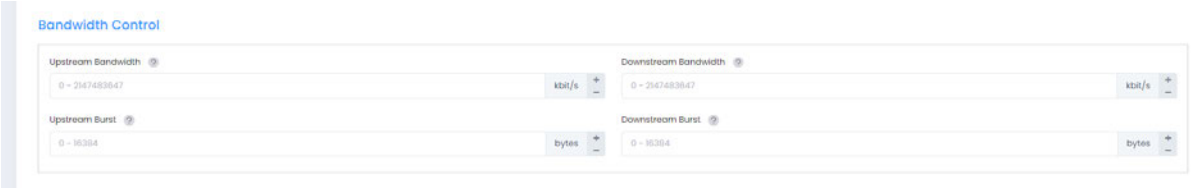
Note: The Location Policy and Period Policy does not support the Access Role Profile for Switch devices.

7.1.3.1.1.4 Inactivity Interval



- **Inactivity Interval** - Defines the amount of time, in seconds, before an authenticated device is automatically logged out of the network due to inactivity (MAC address for the device has aged out). This timer value applies only to devices learned in the profile.

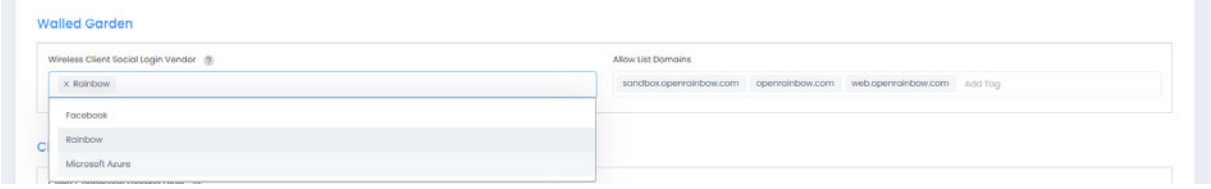
7.1.3.1.1.5 Bandwidth Control



- **Upstream Bandwidth -** The maximum bandwidth limit allocated for ingress traffic assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed.
- **Upstream Burst -** The maximum ingress depth value that is applied to traffic assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the device starts to drop packets.
- **Downstream Bandwidth -** The maximum bandwidth limit allocated for egress traffic assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed.
- **Downstream Burst -** The maximum egress depth value that is applied to traffic assigned to profile. This value determines how much the traffic can burst over the maximum egress bandwidth rate. The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the device starts to drop packets.

Bandwidth Control is supported only on the Switch devices OS6860, OS6865, and OS6900.

7.1.3.1.1.6 Walled Garden

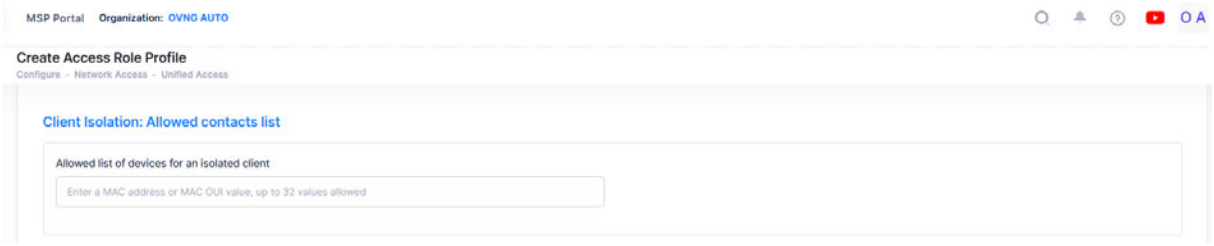


- **Wireless Client Social Login Vendor -** Select a vendor(s) from the drop-down menu to allow a wireless client to authenticate through a social media vendor (Facebook, Rainbow, and Microsoft Azure are supported). OmniVista will automatically configure the Allow List Domains

for the selected vendor(s). This will allow the user to connect over the Internet to the selected vendor(s) for authentication.

- **Allow List Domains -** In addition to Facebook, Rainbow, and Microsoft Azure login, you can enter any domain name to allow a user to connect to sites over the Internet without authentication. For example, a hotel may want to allow a guest to connect to their website without authentication. Enter the domain name directly into the Allow List Domain field to allow access to the site. Repeat to add additional domains. Domains must be entered in Fully Qualified Domain Name (FQDN) format (for example, www.marriot.com, www.bbc.com). IP Addresses and HTTP/HTTPS prefixes should **not** be used.

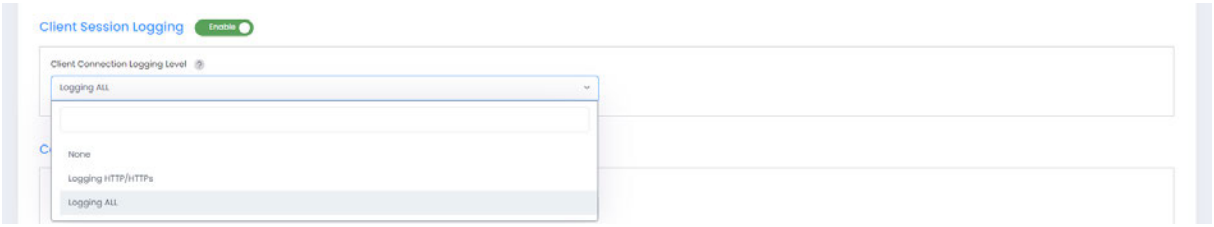
7.1.3.1.1.7 Client Isolation



When Client Isolation is enabled for the client SSID or the Access Authentication Profile for the Switch port to which the AP is connected, traffic between clients on the same AP in the SSID is blocked; client traffic can only go toward the default gateway. To identify the devices a client is allowed to contact when Client Isolation is enabled, enter the MAC address for each device. You can manually specify or copy and paste the device MAC address using any of the following formats:

- 00:80:0f:33:33:24
- 00-80-0f-33-33-24
- 00800f333324
- 008.00f.333.324
- 00800f.333324
- 00:d0:95* (trailing wildcard character "*" specifies all MAC addresses beginning with 00:d0:95) This wildcard format is particularly useful for entering a vendor OUI only and not the full MAC address for all the vendor devices.

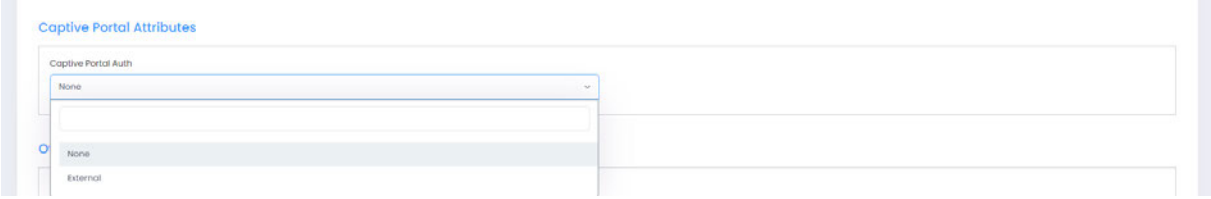
7.1.3.1.1.8 Client Session Logging



- **Client Session Logging -** Enables/Disables client session logging. When enabled, select one of the following from the Client Connection Logging Level drop-down menu:
  - **None** - Log only client online/offline behavior, without session details.
  - **Logging HTTP/HTTPs -** Log only the HTTP/HTTPs web session of wireless clients.

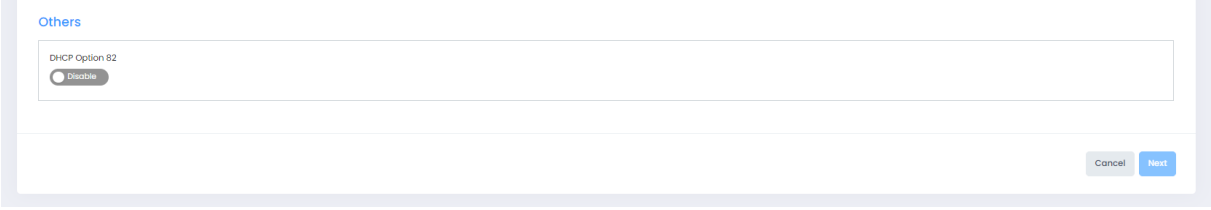
- **Logging ALL -** Log all sessions of wireless clients, including HTTP/HTTPs.

7.1.3.1.1.9 Captive Portal Attributes



- **Captive Portal Auth** - Select the Captive Portal Authentication method from the drop-down menu:
  - **None** - No Captive Portal authentication.
  - **External** - Select this method to redirect device traffic to an external Captive Portal Server for authentication. Complete the following fields to provide the information needed to redirect traffic to the external server:
    - **Portal Server** - The FQDN/IP address of the external captive portal server.
    - **Redirect URL** - The redirect URL for the captive portal authentication.
    - **HTTPS Redirection** - Specify whether the redirect portal page is using HTTPS protocol.
    - **AAA Server Profile** - The AAA Server used for Captive Portal Authentication. Select an existing AAA Server Profile from the drop-down menu or click on **Create AAA Server Profile** to open the Create AAA Server Profile screen and create a new AAA Server Profile to use. You can also click on **Edit** to open the Edit AAA Server Profile screen and make changes to the selected profile. (See the AAA Server Profile (see page 497) online help for more information.)
    - **Custom Profile** - The External Captive Portal Configuration file used for communication between APs and the external Captive Portal Server. Select an existing External Captive Portal Configuration file from the drop-down menu or click on **Create External Captive Portal Config File** to open the New External Captive Portal Config File screen and create a custom external config file. You can also click on **Edit** to open the Edit External Captive Portal Config File screen and make changes to the selected config file. (See the External Captive Portal (see page 409) online help for more information.)

7.1.3.1.1.10 DHCP Option 82

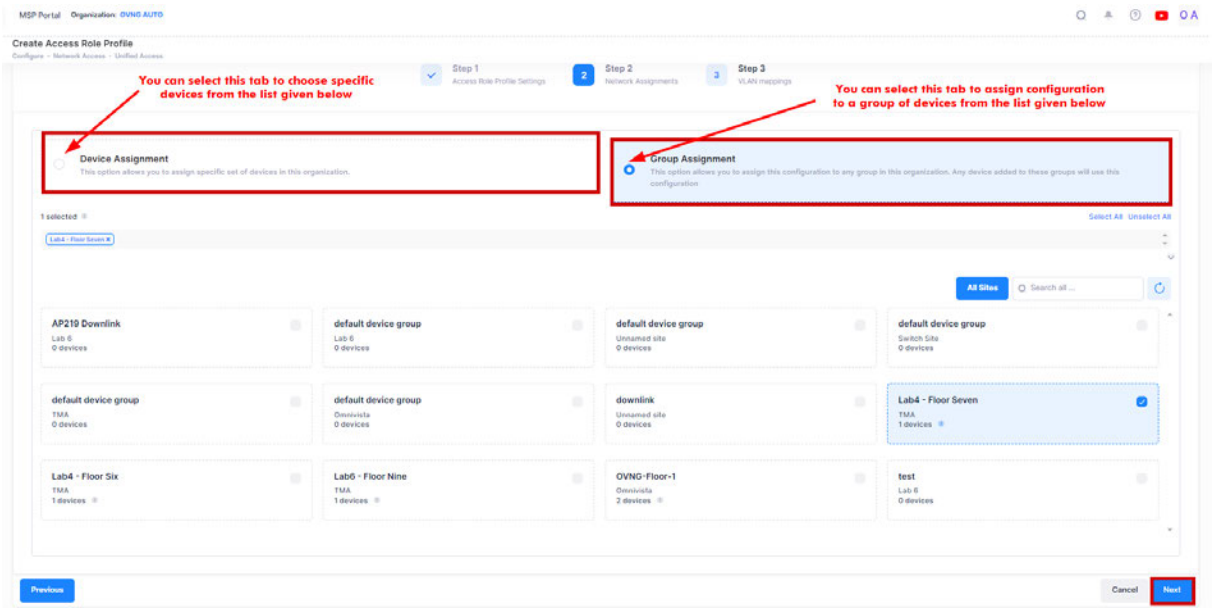


- **DHCP Option 82** - Enable/disable DHCP Option 82 for the Access Role Profile.

7.1.3.1.2 2. Network Assignments

The Network Assignment tab is used to select the AP(s) or Switch devices from the available list of devices to which the Access Role Profile will be applied to devices within those groups. Complete the network assignment as described below, then click **Next** to to the the next tab (Step 3).

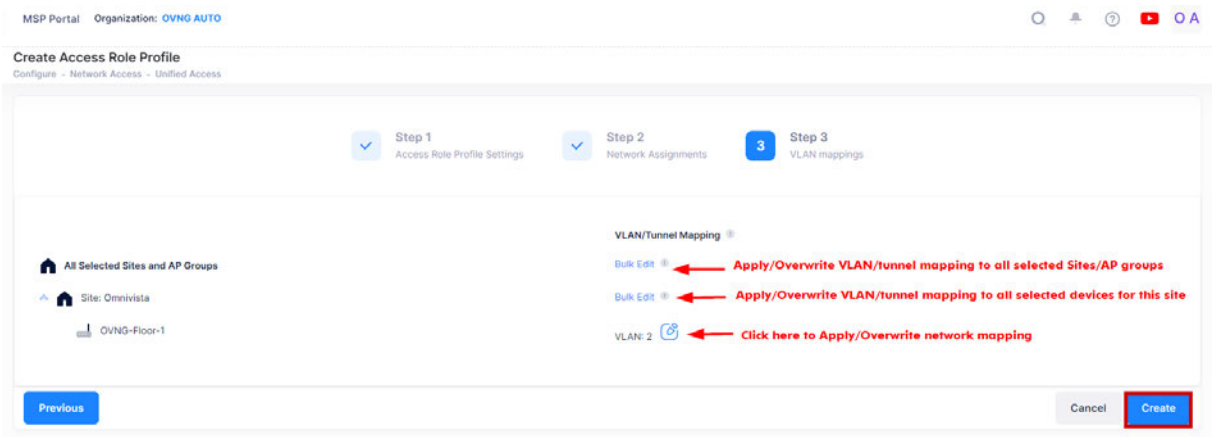
- **Device Assignment** - Select the specific set of Devices from the available list to assign the profile.
- **Group Assignment** - Select the specific group of Devices from the available list to assign the profile. The Access Role Profile is applied to the selected group of devices from the list.



Note: In case of failing to apply an Access Role Profile to devices, if you want to re-apply the profile with no change in the configuration, click on the Profile name to navigate to the device configuration detailed view. Then, select the Device configuration entry you want to reapply, click on edit button, and save the Profile without modifying any fields.

7.1.3.1.3 3. VLAN Mappings

The VLAN Mappings tab is used to map a VLAN or a Tunnel service to the Access Role Profile. Traffic classified into the profile will be forwarded on the mapped VLAN or Tunnel service. Note that you can only select one mapping method per Access Role Profile.

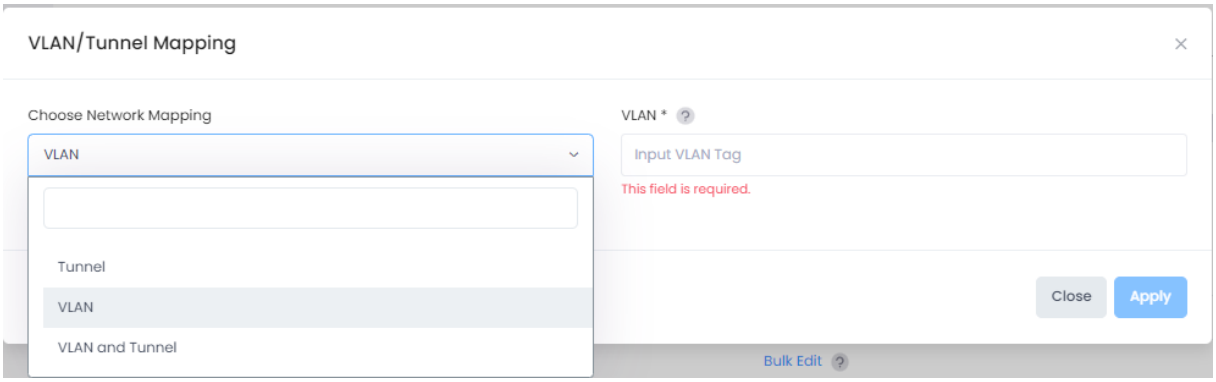


You can configure a VLAN/Tunnel mapping for all AP Groups or Network devices across all Sites in the Organization, for all AP Groups/devices associated with a specific Site, or for the selected AP Group or Network Devices.

The ability to bind up to 256 VLANs to a WLAN/SSID on the AP13xx/AP14xx models is supported. However, not every AP model can accommodate 256 VLANs for all the configured SSIDs. The limitations are outlined below:

- AP1301H can support 256 VLANs on a maximum of 2 SSIDs, with a total of 512.
- AP1311/AP1301/AP1431/AP1411 can support 256 VLANs on a maximum of 4 WLANs/SSIDs, with a total of 1024.
- AP1320/AP1331/AP1351/AP1451 can accommodate 256 VLANs on a maximum of 7 WLANs/SSIDs, with a total of 1792.

When you click on the **Bulk Edit** option or the **Edit** option for an individual AP Group/device, the following VLAN/Tunnel Mapping screen opens:



Select one of the following network mapping options from the drop-down menu:

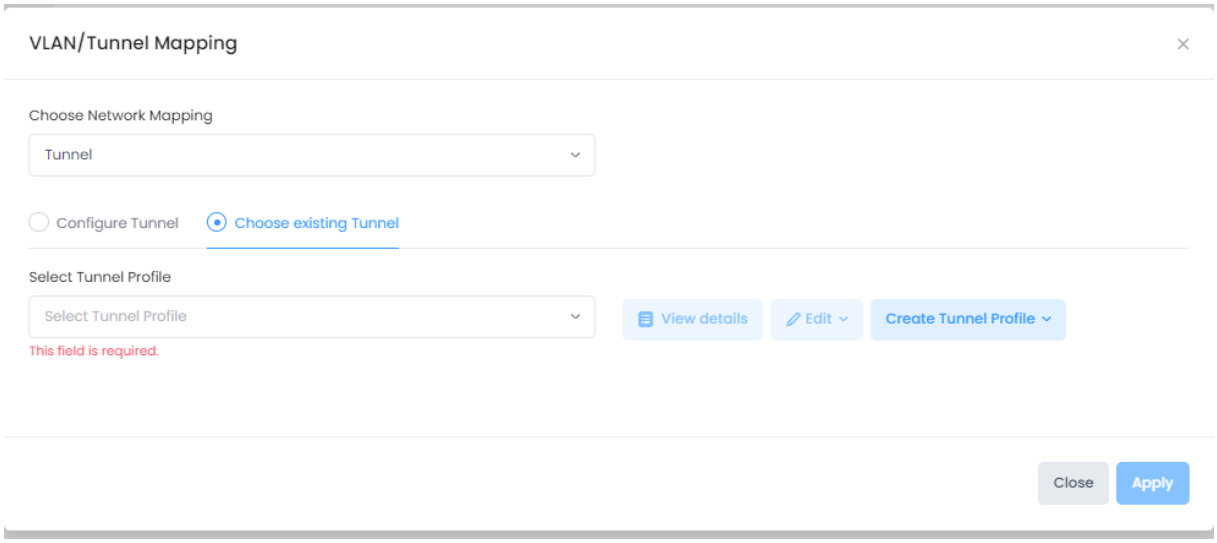
- **VLAN**- Maps the profile to a specific VLAN ID tag on network devices.
  - **For Access Point**: You can enter multiple VLAN ID tags in this field by specifying an Untagged VLAN (0), a range of VLAN IDs (10-20), individual VLAN IDs (25), or both (10-20, 25). Note that after each VLAN ID entry, you must press the tab key before making the next entry. For example, enter “10-20” press tab key, then enter “21” press tab key, then enter

"22" press tab key, and so on. You can also click outside of this field after each entry, instead of pressing the tab key. VLAN 1 is not supported.

- **For Switch**: You can enter one VLAN ID within a range of 1 to 4094.

- **Tunnel -** Maps the profile to a Guest Tunnel.
- **VLAN and Tunnel -** Maps the profile to a VLAN and a Tunnel, allowing VLAN tagging inside the GRE.

When you select the Tunnel mapping option, the following fields are displayed on the VLAN/Tunnel Mapping screen:

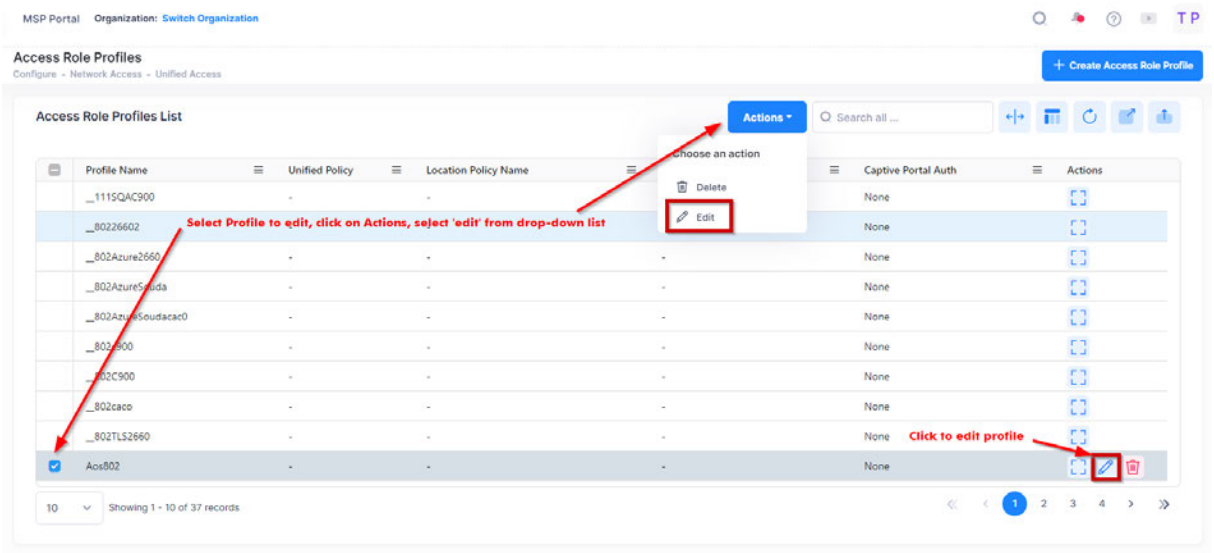


- **Configure Tunnel** - Select this option to define a Guest Tunnel service to assign to the Access Role Profile.. When you select this option, a Tunnel Profile is automatically created with the Access Role Profile name.
  - **Save this as a distinct Tunnel Profile, for reuse** - Select this option if you want the tunnel mapping to be available for use after the associated Access Role Profile has been deleted. When you click on this option, you will be prompted to enter a Tunnel Profile name.
- **Choose Existing Tunnel** - Select an existing Guest Tunnel Profile from the drop-down menu or click on **Create Tunnel Profile** to open the Create Tunnel Profile screen and create a new Guest Tunnel Profile. You can also click on **View Details** to view information about the selected Tunnel Profile or click on **Edit** to open the Edit Tunnel Profile screen and make changes to the selected Tunnel Profile.

When you are done configuring the VLAN/Tunnel mappings, click on **Create Access Role Profile**. The Access Role Profile is created and applied to users assigned to the profile.

7.1.3.2 Editing an Access Role Profile

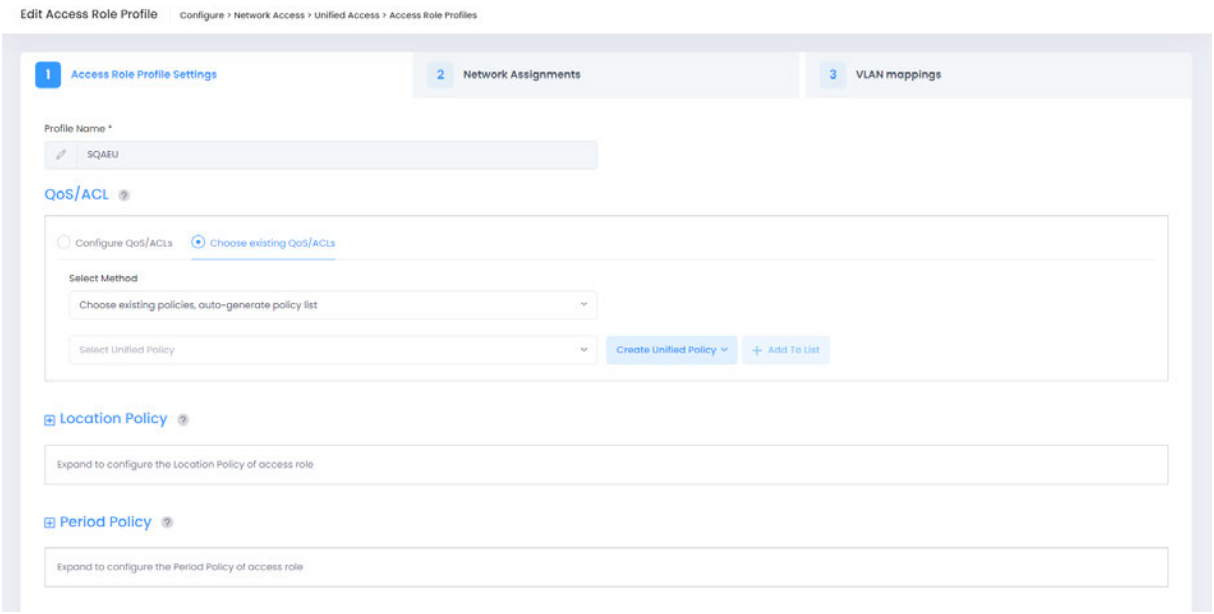
You can edit the Access Role Profile attributes by accessing the Edit Access Role Profile screen.



Use one of the following methods to access the Edit Access Role Profile screen (as shown above):

- Select the profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the profile that you want to edit.

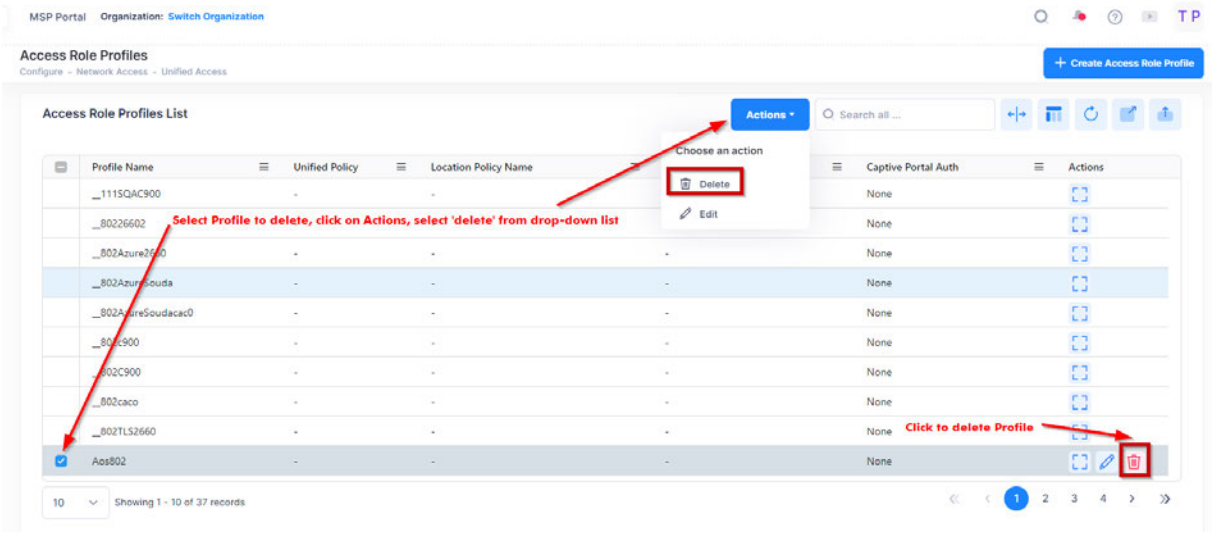
The following Edit Access Role Profile screen displays. Edit the fields as described above (see page 514), then click on **Save**.



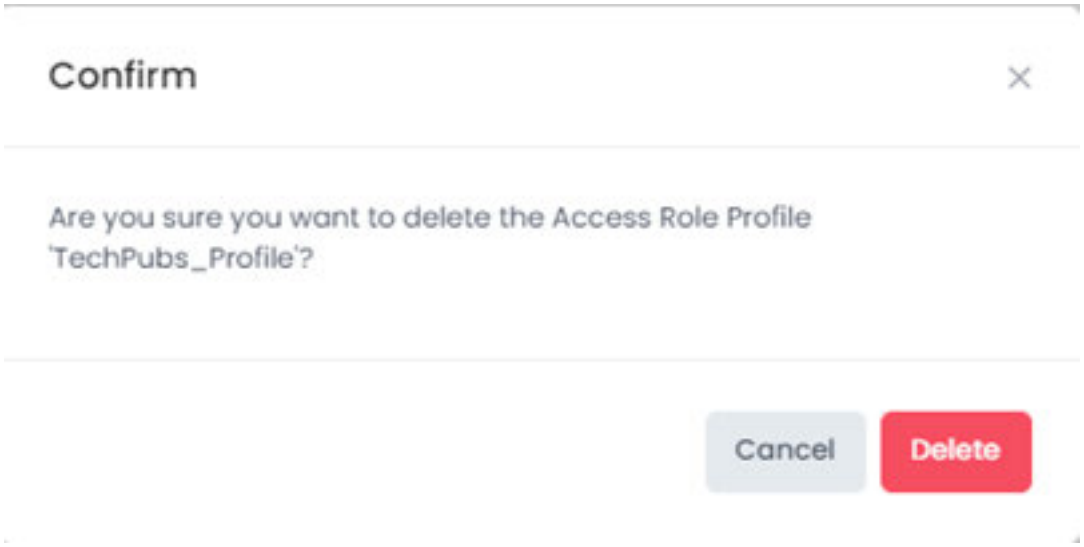
7.1.3.3 Deleting an Access Role Profile

To delete an Access Role Profile, use one of the following methods to select the profile you want to delete:

- Select the profile to delete by clicking on the checkbox next to the profile, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the profile that you want to delete.



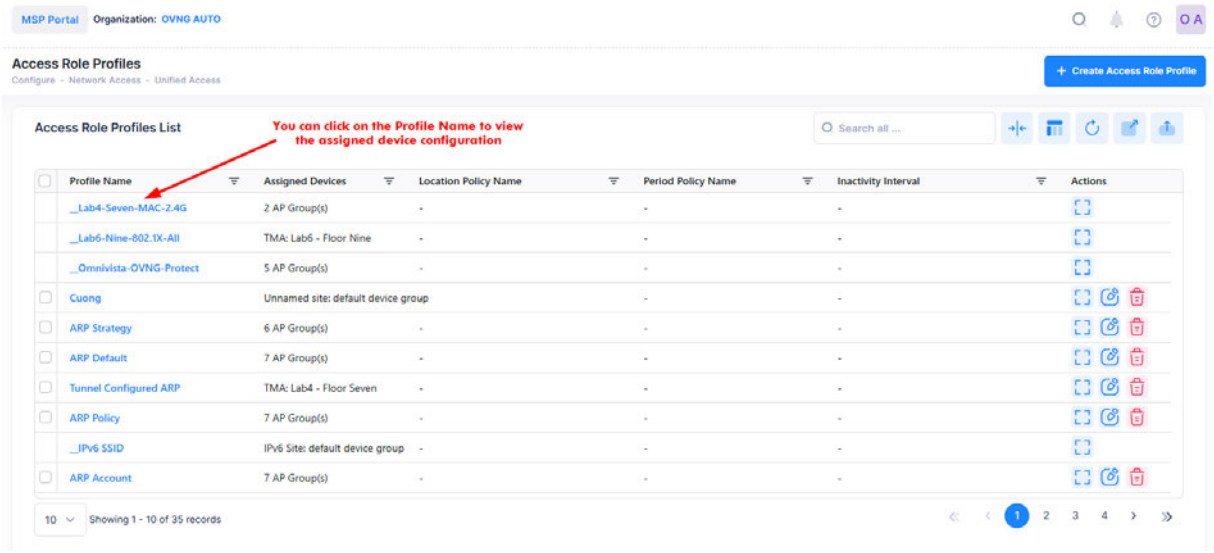
When you select the profile you want to delete, the following confirmation prompt appears:



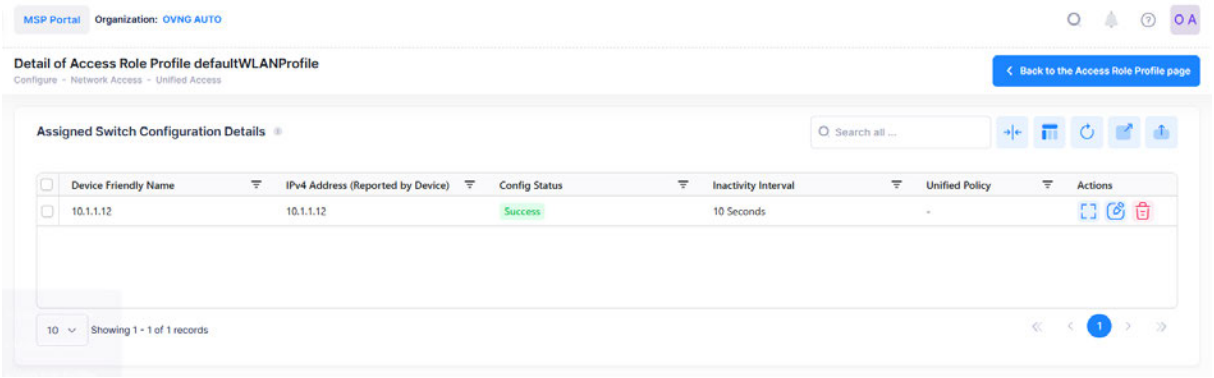
Click on **Delete** to confirm that you want to delete the Access Role Profile.

7.1.3.4 Display Assigned Switch Configuration Details

The Access Role Profile list displays information for the configured Access Role Profiles. You can click on the Profile Name to view the assigned Switch configuration details of a specific Profile as shown below.



The below screen will appears:



This screen also allows you to export, search and filter the data. You can click the back icon on the top right to navigate to the Access Role Profile List page.

The following Device Configuration of the selected Profile is displayed.

- **IPv4 Address** - The IPv4 address of the device.
- **Device Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Config Status** - The configuration status of the device. (Successful or Failed or Pending).
  - **Pending** - The configuration is being pushed to the device and is still not receiving a response from the device.
  - **Failed** - The configuration failed to apply to the device. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to the device successfully.

- **Inactivity Interval** - Defines the amount of time, in seconds, before an authenticated device is automatically logged out of the network due to inactivity.
- **Upstream Bandwidth -** The maximum bandwidth limit allocated for ingress traffic assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed.
- **Downstream Bandwidth -** The maximum bandwidth limit allocated for egress traffic assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed.
- **Upstream Burst -** The maximum ingress depth value that is applied to traffic assigned to the profile.
- **Downstream Burst -** The maximum egress depth value that is applied to traffic assigned to profile.
- **Unified Policy -** The name of the Policy List assigned to the profile.
- **Captive Portal Auth -** The type of Captive Portal Authentication (**None**, or **External**).
- **Redirect Status** - Enables/Disables Captive Portal Redirect (not supported on wireless devices and ignored when applied to those devices).
- **Auth Flag** - Enables/Disables authentication (not supported on Steller AP).
- **Mobile Tag Status** - Enables/Disables classification of tagged packets received on mobile ports (not supported on Steller AP).

7.1.3.4.1 Editing an Assigned Switch Configuration Details

Consider the following while editing an assigned Switch Configuration details for Access Role Profile:

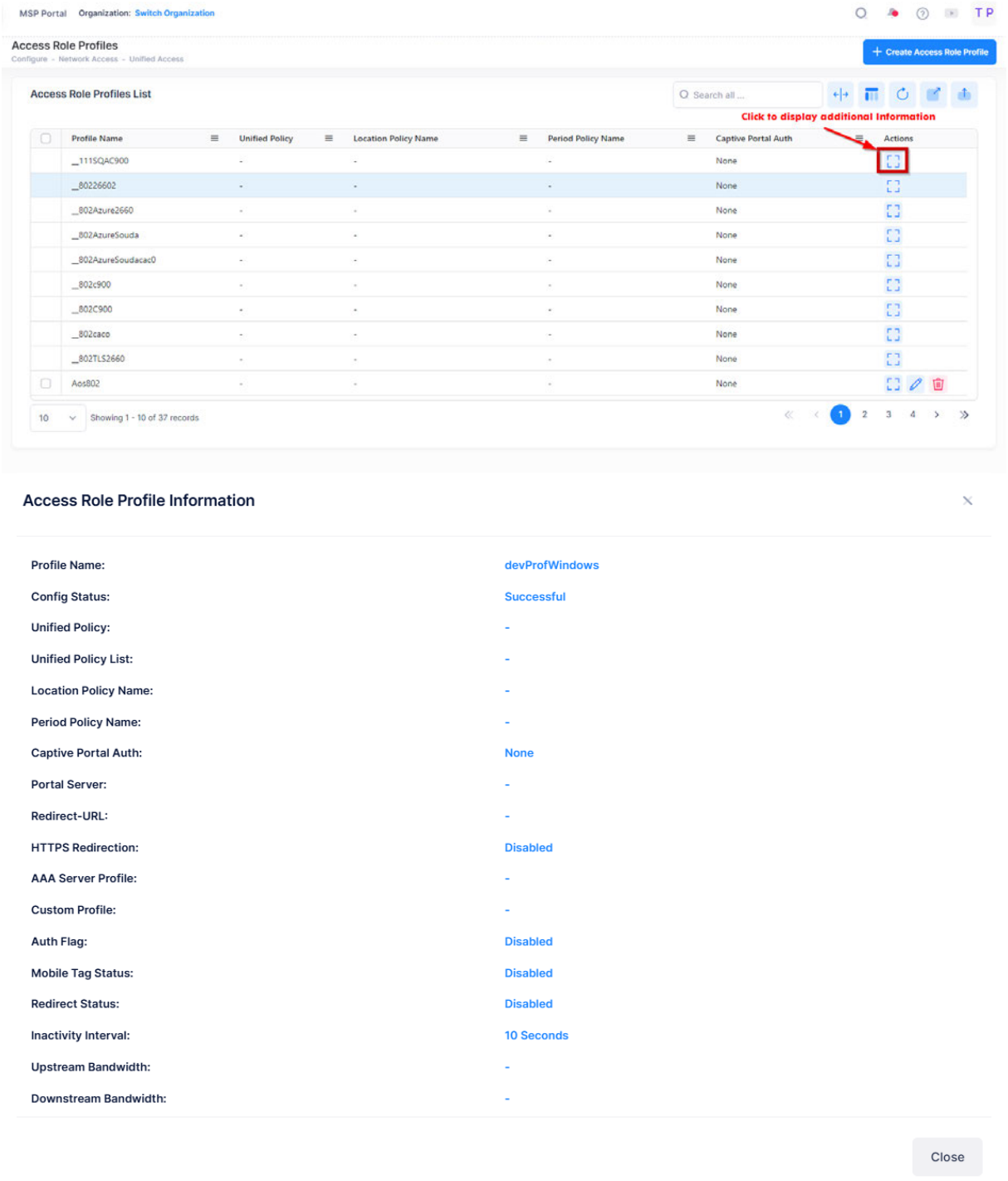
- You can edit the configuration settings for one or multiple devices at the same time.
- When you choose to edit a single device, the configuration screen will display the unique, current settings for that device.
- If you opt to edit multiple devices simultaneously, the system will automatically fill the configuration fields with values from the original Access Role Profile template, establishing a common baseline for your bulk modifications.
- If you select a child profile, such as a "policy list," and that specific configuration has a "Config Status" of "Success" on the device, the system will not overwrite the new value on the device. It helps to prevent conflicts or unnecessary overwrites.

Note: You can remove the Access Role Profile device configuration from one or multiple devices. This action will send a notification message to the device to remove that specific Access Role Profile from its configuration.

Note: You can now view the current profile configuration for each switch assigned to an Access Role Profile. You can edit the configuration on one or more assigned devices directly. If a device's configuration differs from the profile, the mismatched attributes will be highlighted, and you will have the option to synchronize them.

7.1.3.5 Display Access Role Profile Additional Information

To display additional information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



The following information is displayed for each Access Role Profile:

- **Profile Name** - The name assigned to the Access Role Profile.

- **Config Status** - The status of applying the profile to devices (Successful, Failed, Pending, or Partially Failed).
  - **Pending** - The configuration is being pushed to the devices and has still not received any response from any device.
  - **Failed** - The configuration failed to apply to all the selected devices. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to all the selected devices successfully.
  - **Partially Failed** - The configuration is pushed to some devices successfully, while to others it failed or remains in a pending state.

The table below displays the combinations of configuration status for all device configurations in the Profile template.

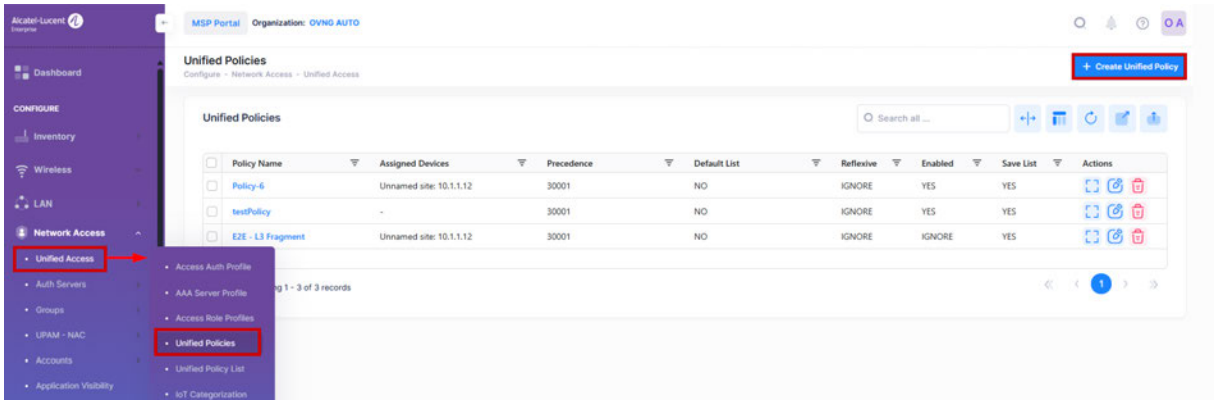
Device Configuration Status	Template
All Failed	Failed
All Successful	Successful
All Pending	Pending
Some failed, some successful	Partially Failed
Some pending, some successful	Pending
Some pending, some failed	Partially Failed
Some pending, some failed, some successful	Partially Failed

- **Unified Policy -** The name of the Policy List assigned to the profile. The set of rules within the Policy List are applied to the traffic that passes though devices. Only one Policy List is allowed per profile, but multiple profiles may use the same Policy List.
- **Location Policy Name -** The name of the Location Access Policy assigned to the profile.
- **Period Policy Name -** The name of the Period Policy assigned to the profile..
- **Captive Portal Auth -** The type of Captive Portal Authentication (**None**, or **External**).
- **Portal Server -** The FQDN/IP address of the external captive portal server.
- **Redirect URL -** The redirect URL for the captive portal authentication.
- **HTTPS Redirection -** Specify whether the redirect portal page is using HTTPS protocol.
- **AAA Server Profile -** The AAA Server used for Captive Portal Authentication.

- **Custom Profile -** The External Captive Portal Config File used for communication between APs and the External Portal Server.
- **Upstream Bandwidth -** The maximum bandwidth limit allocated for ingress traffic assigned to the profile. If the maximum ingress bandwidth value is set to zero, all ingress traffic is allowed.
- **Downstream Bandwidth -** The maximum bandwidth limit allocated for egress traffic assigned to the profile. If the maximum egress bandwidth value is set to zero, all egress traffic is allowed.
- **Upstream Burst -** The maximum ingress depth value that is applied to traffic assigned to the profile. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the device starts to drop packets.
- **Downstream Burst -** The maximum egress depth value that is applied to traffic assigned to profile. This value determines how much the traffic can burst over the maximum egress bandwidth rate. The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the device starts to drop packets.
- **DHCP Option 82 -** Enables/Disabled the DHCP Option 82 Feature.
- **Client Isolation** - Defines the MAC Addresses of Allowed list of devices for an isolated Client
- **Client Session Logging -** Enables/Disables client session logging.
- **Client Connection Logging Level:**
  - **Logging HTTP/HTTPs -** Log only the HTTP/HTTPs web session of wireless clients.
  - **Logging ALL -** Log all sessions of wireless clients, including HTTP/HTTPs.
  - **None -** Log only client online/offline behavior, without session details.
- **Wireless Client Social Login Vendor -** The vendor(s) selected to allow a wireless client to authenticate through a social media vendor (Facebook, Rainbow, and Microsoft Azure are supported). OmniVista automatically configures the Allow List Domains for the selected vendor(s). This allows the user to connect over the Internet to the selected vendor(s) for authentication.
- **Allow List Domains -** Facebook, Rainbow, Microsoft Azure login, or any user-specified Allow List Domain that allows a user to connect to sites over the Internet without authentication. For example, a hotel may want to allow a guest to connect to their website without authentication. Domains must be in Fully Qualified Domain Name (FQDN) format (for example,, http:// www.marriot.com , http://www.bbc.com). IP Addresses and HTTP/HTTPS prefixes should **not** be used.
- **Assigned Devices:**
  - **Assigned Devices** - The AP Groups, Switches and associated Sites to which the Access Role Profile is applied.
  - **VLAN/Tunnel Mapping** - The VLAN ID or Tunnel service ID mapped to the profile.

7.1.4 Unified Policies

Unified Policies are QoS Policies that can be applied to devices. Use the Unified Policies screen to display information (see page 547) about all of the configured Unified Policies. This screen also allows you to create (see page 533), edit (see page 546), and delete (see page 547)Unified Policies on the network. To access the Unified Policies screen, click on **Network Access > Unified Access > Unified Policies** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.1.4.1 Creating a Unified Policy

The Create Unified Policy screen is used to configure the Unified Policy Settings and Network Assignment settings for a unified policy. To access the Create Unified Policy screen, click on **Create Unified Policy** at the top of the Unified Policies screen, as shown above.

Consider the following use cases when configuring Unified Policies:

1. OmniVista Terra does not use LDAP, so any Unified Policies created on a Switch via LDAP are not discovered; only policies configured through the Switch CLI are discovered. As a result, the Unified Policies screen displays only policies configured through the Switch CLI.
2. Child policy profiles (action, condition, validity period) can be shared among policy rules.

Example:

- policy rule r1 condition r1 action r1 validity-period r1
- policy rule r2 condition r1 action r1 validity-period r1

  In this complex case, when you try to delete policy rule r2, only rule r2 will be deleted on both OmniVista Terra devices and the applied Switch devices. The child profiles (condition r1, action r1, validity period r1) will be retained because they are used by policy rule r1. They will only be deleted when no policies are using them. If you edit the child profile of policy rule r1, policy rule r2 will be affected because they are sharing the child profile.

3. If there are two policies with the same name but different child profiles between two Switch devices, there will be a mismatch between the profile template and device configuration.

Example:

- Switch A has policy rule r1 condition r1 action r1 validity-period r1
- Switch B has policy rule r1 condition r2 action r2 validity-period r2

Assuming that Switch A will report the polling data before Switch B, you should save the profile template of policy rule r1 with the child profile condition r1, action r1, and validity period r1. Subsequently, when Switch B reports the polling data for policy rule r1 but with a different child profile, you should only update the assignment for policy rule r1 instead of updating the profile with the new child profile. As a result, there will be a mismatch between policy rule r1 and Switch B. (**Note:** If rule r1 is edited without changing the device selection, the configuration on both Switch A and Switch B will be updated).

4. There are two platform types for the Switch devices: QoS1 and QoS2.
   - The QoS1 platform includes the following models: OS6860, OS6865, and OS6900-TOR, which require at least one configuration when creating a policy condition.
   - The QoS2 platform includes the following models: OS9900, OS6860N, OS6900-Yukon, OS6560, OS6465, OS6360, and OS6570, which allow the creation of a policy condition without any configuration.

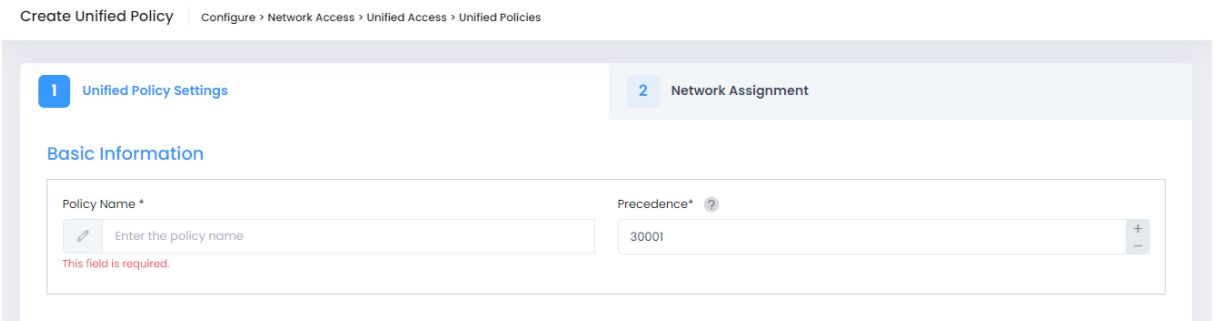
As a result, you cannot apply a policy condition without criteria on the QoS1 platform.

5. The modification of Policy Rule which contains only a single L3 condition to another L3 condition is not allowed. If you want to add a condition with the existing condition, then first delete and re-create the policy with the new L3 condition.
6. The Switch device does not allow combining the L3 Condition Multicast IP with L2 Condition Source MAC, L3 Condition Source IP, L3 Condition DSCP/TOS, L4 Condition Service, L4 Condition Service Group, or Policy Action CIR.

The Create Unified Policy screen provides the following step-by-step process for creating an Unified Policy:

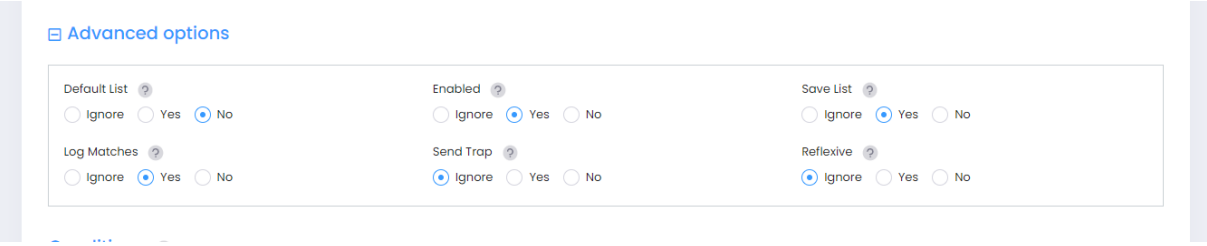
7.1.4.1.1 1. Unified Policy Settings

7.1.4.1.2 Basic Information



- **Policy Name** - The name of the policy. The field must have at most 22 characters. The use of two special characters(/ or \) is not allowed for the Policy name.
- **Precedence** - The Precedence value of the Policy (0 - 65535).

7.1.4.1.3 Advanced Options



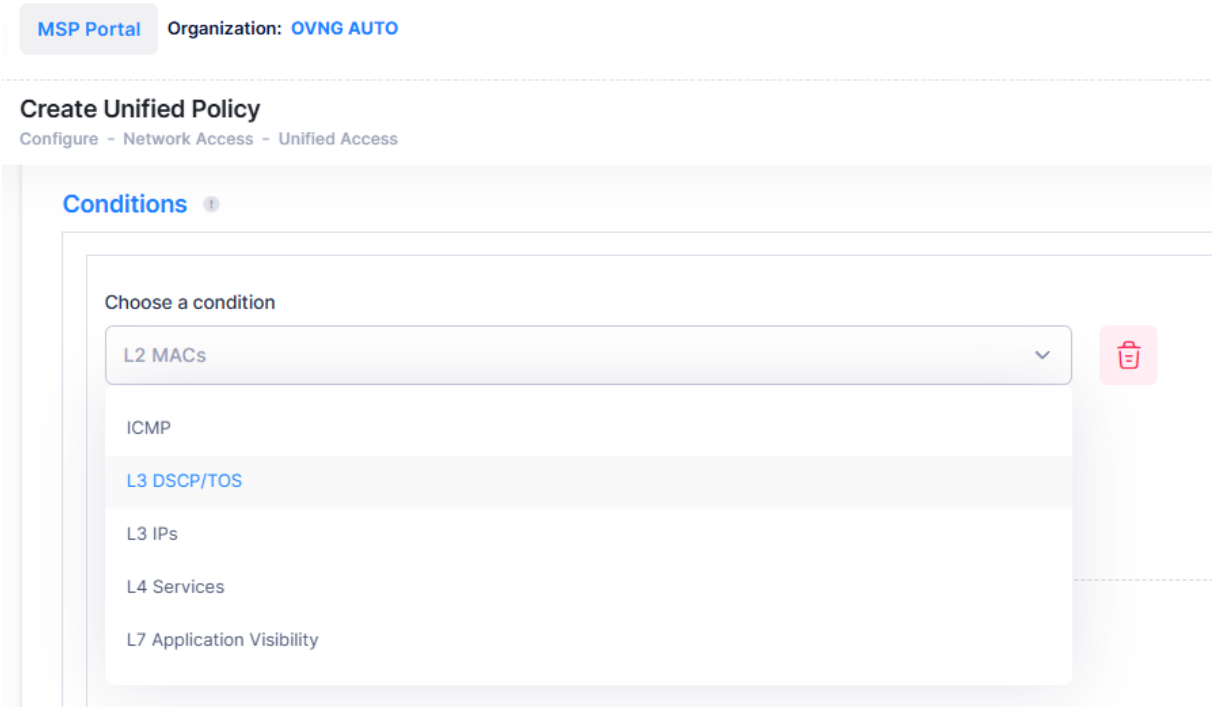
Click on Advanced options to display and configure the following options:

- **Default List** - Adds the rule to the default policy list.
- **Enabled** - Enables the policy.
- **Save List** - Marks the policy rule so that it may be captured as part of the switch configuration.
- **Log Matches** - Configures the switch to log messages about specific flows coming into the switch that match this policy rule.
- **Send Trap** - Enables or disables traps for the rule. By default, it is set to Ignore. Since the Switch devices no longer support this option, therefore enabling it will have no effect on the Switch devices.
- **Reflexive** - Enables support for Reflexive for the policy. Reflexive policies allow specific return connections that would normally be denied. Since the Switch devices no longer support this option, therefore enabling it will have no effect on the Switch devices.

7.1.4.1.4 Conditions

A Unified Policy is applied to client traffic that matches the condition(s) configured for the policy. At least one condition is mandatory. When multiple conditions are specified, all conditions must match for the policy to be applied to the client traffic.

When you create a Condition, the Condition(s) you configure must be true before traffic is allowed to flow. Click on **Add Condition** and select the Condition you want to configure from the “Choose a condition” drop-down menu. The configuration options for the selected Condition will display.



A brief description of each Condition is provided below. Click the hyperlink for each Condition for detailed configuration instructions.

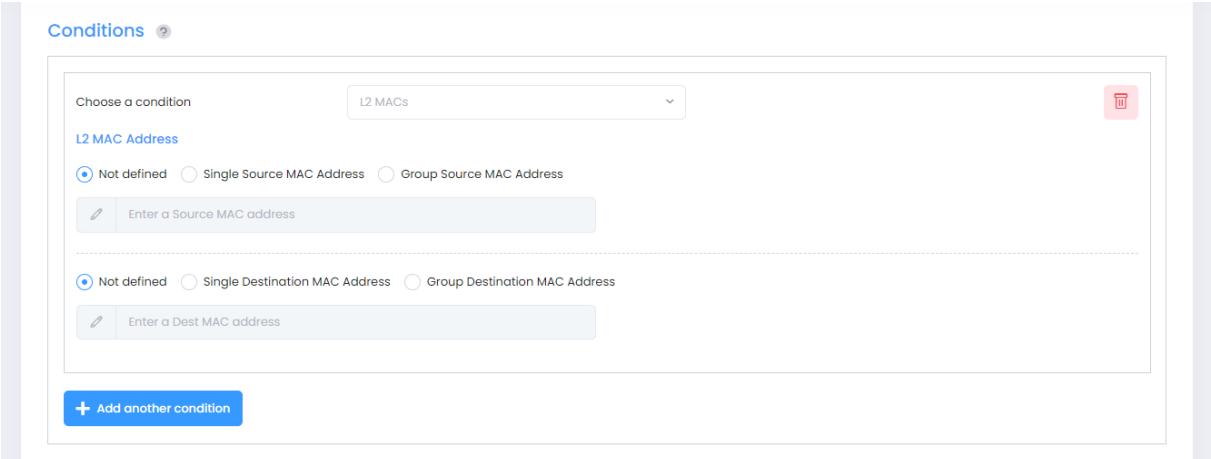
- **L2 MACs** (see page 536) - Create a Condition that applies the policy to traffic originating from a MAC address/group or to traffic flowing to a MAC address/group. (Note that, MAC Addresses cannot contain wildcard characters for both Access Points and Switches).
- **L3 IPs** (see page 538) - Create a Condition that applies the policy to traffic originating from an IP address/network group or to traffic flowing to an IP address/network group. (Note that any IP address can be masked).
- **L3 DSCP/TOS** (see page 539) - Create a Condition that applies the policy to traffic with a specified value in either the DSCP (Differentiated Services Code Point) byte or in the IP TOS (IP Type of Service) byte. Both DSCP and IP TOS are mechanisms used to convey QoS information in the IP header of frames.
- **L4 Services** (see page 540) (see page 533)- Create a Condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port. You can also create a Condition using an existing service/ service group.
- **ICMP** (see page 541) **-** Create a Condition that applies the policy to traffic with a specified ICMP Type or Code value.
- **L7 Application Visibility** (see page 541) **-** Create a Condition that applies the policy to traffic flowing to and from an Application Group or Application.

L2 MACs

A MAC Condition applies the Policy to traffic flowing from/to a MAC Address/Group. Note that Layer 2 Conditions (conditions that specify MAC Addresses) are "lost" when traffic passes through a router.

For this reason, it may be advisable to specify other types of Conditions (such as a Layer 3 Condition, which specifies IP Addresses) when traffic is expected to travel more than one router hop.

When you select the L2 MACs condition, the following parameters to configure a single/group source MAC address or a single/group destination MAC address will display.



Select the parameter(s) you want to configure by selecting the applicable radio button. For Source/Destination MAC Address, click on **Single Source/Destination MAC Address** to configure a single MAC Address or click on **Group Source/Destination MAC Address** to configure a MAC Address Group. If you select the Group option, you will then be prompted to select an existing MAC Address Group or create a new group (see page 605).

- **Not defined** - This option specifies that there is no criteria for the policy.
- **Single Source MAC Address/Group** - Configuring a Source MAC Address/Group Condition restricts the policy to traffic that flows from this MAC Address/Group only. If you do not select this option, you are effectively stating that the Source MAC Address/Group traffic is not a criterion for the policy.
- **Single Destination MAC Address/Group** - Configuring a Destination MAC Address/Group Condition restricts the policy to traffic that flows to this MAC Address only. If you do not select this option, you are effectively stating that the Destination MAC Address/Group traffic is not a criterion for the policy.

Notes:

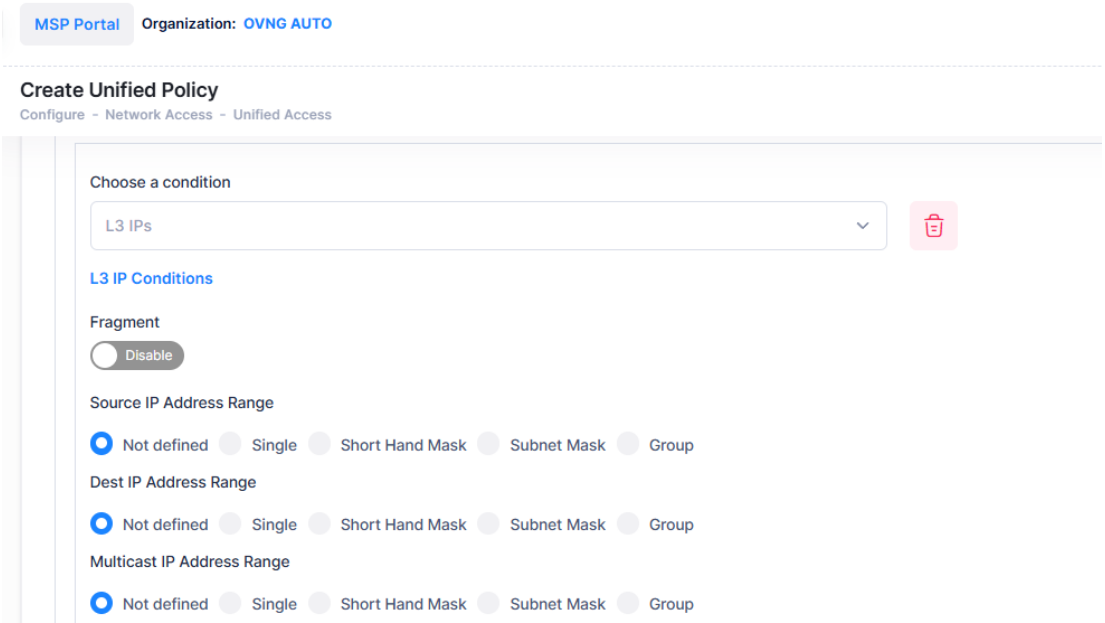
- Conditions that specify both a source and a destination MAC address may be rejected by some devices as invalid. However, if you wish to create policies for both source and destination traffic, you can create one policy for the source traffic and a second policy for the destination traffic.
- The following MAC address ranges are assigned to Alcatel-Lucent Enterprise voice devices and Alcatel-Lucent Enterprise IP phones.
  - Voice Devices
    - 00809F3A0000 - 00809F3AFFFF
    - 00809F3B0000 - 00809F3BFFFF
    - 00809F3C0000 - 00809F3CFFFF

- IP Phones
  - 00809F3D0000 - 00809F3DFFFF
- Multi-Media Devices
  - 00809F3E0000 - 00809F3EFFFF
  - 00809F3F0000 - 00809F3FFFFF

L3 IPs

An IP Condition applies the Policy to traffic originating from, or flowing to, an IP Address/IP Network group. Any IP Address can be masked. Note that a Condition that specifies both a Source and Destination IP Address/Network Group will be rejected by the device as invalid. However, if you wish to create policies for both Source and Destination traffic, you can create one policy for the Source traffic and a second policy for the Destination traffic.

When you select the L3 IPs condition, the following parameters to configure a single/group source IP address or a single/group destination IP address will display.



Select the parameter(s) you want to configure by selecting the applicable radio button. For Source/Destination/Multicast IP Address, click on **Single** to configure a single IP Address (and **Shorthand** or **Subnet Mask**, if applicable), or click on **Group** to configure an IP Group. If you select the Group option, you will then be prompted to select an existing IP Group or create a new group (see page 608).

- **Fragment** - Select this checkbox to restrict the policy to TCP packet fragments. (Note: This option is available only for Switch devices configuration).
- **Not defined** - This option specifies that there is no criteria for the policy.

- **Single Source IP Address -** Configuring a Source IP Address/Group Condition restricts the policy to traffic that flows from this IP Address only. If you do not select this option, you are effectively stating that the Source IP Address/Group traffic is not a criterion for the policy.
- **Single Destination IP Address** - Configuring a Destination IP Address/Group Condition restricts the policy to traffic that flows to this IP Address only. If you do not select this option, you are effectively stating that the Destination IP Address/Group traffic is not a criterion for the policy.
- **Single Multicast IP Address** - Configuring a Multicast IP Address/Group Condition restricts the policy to traffic that flows to this IP Multicast Address Group only. If you do not select this option, you are effectively stating that the Destination IP Multicast Address/Group or Subnet Mask/Group traffic is not a criterion for the policy.

When configuring an IP Address Condition, you can also click either the **Shorthand Mask** or **Subnet Mask** button to configure a Subnet Mask. If you are using a Shorthand Mask, select a value from the Shorthand Mask drop-down list. If you are using a full Subnet Mask, select a value from the Subnet Mask drop-down list. Note that the * wildcard character is not allowed in IP addresses.

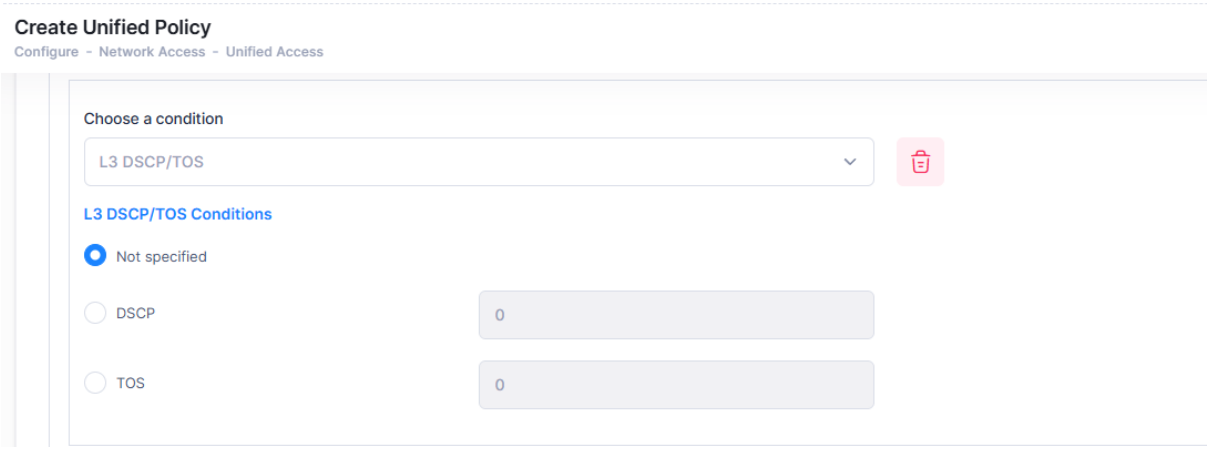
Important Note:

1. When creating an IP Condition for a **NAT** Action, you must specify an IP Network Group in the Condition. NAT will only work when both the Condition and Action specify network groups. To create a "One-to-Many" Condition and action, create a Network Group with a single entry for the Condition.
2. If you configure L3 IP Conditions with Source IP Address Range and Destination IP Address Range with **Short Hand Mask** set to 0, the Switch will reflect the Source or Destination IP address as **“ANY”**.

L3 DSCP/TOS

A DSCP/TOS Condition applies the Policy to incoming traffic that has a specified value in either the DSCP (Differentiated Services Code Point) byte or in the TOS (Type of Service) byte. Both DSCP and TOS are mechanisms used to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive - you can use either DSCP or TOS but not both.

When you select the L3 DSCP/TOS condition, the following parameters to configure a single/group source IP address or a single/group destination IP address will display.

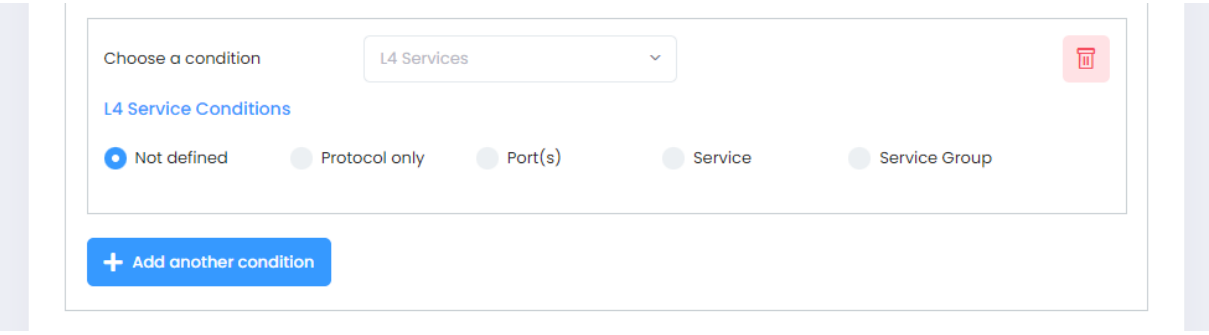


Click on the applicable radio button (DSCP or TOS) and enter a value.

- **Not specified** - There is no criteria for the policy.
- **Differentiated Service Code Point** - Defines the QoS treatment a frame is to receive from each network device. This is referred to as per-hop behavior. If you are using DSCP, you can define any value in the range 0 - 63 as the DSCP value in the IP header of the frame. Traffic that contains this value will match this condition.
- **Type of Service Precedence**- A TOS value creates a condition that applies the policy to traffic that has the specified TOS value in the IP header of frames. Enter any value from 0 - 7 to specify the value of the precedence field in the TOS byte that will match this condition. A value of 7 has the highest precedence and a value of 0 has the lowest.

L4 Services

A Service Condition applies the policy to Service Protocol traffic (TCP or UDP) flowing from/to two TCP or UDP ports, or to traffic flowing from/to a TCP or UDP Service or Service Group. When you select the L4 Services condition, the following parameters to configure the type of Service Condition will display:



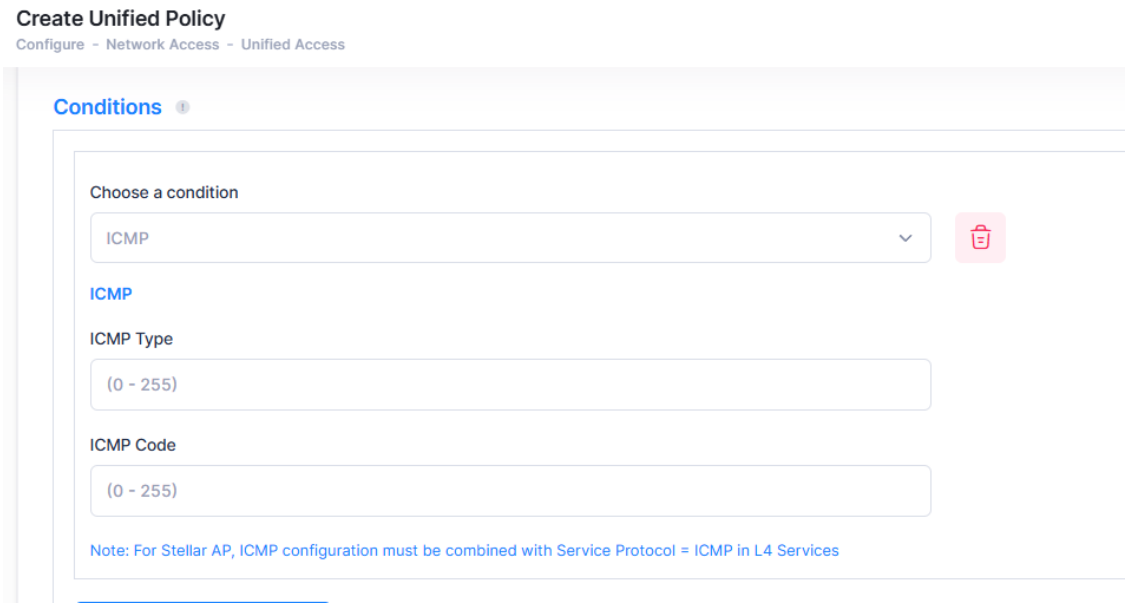
Select a type of Service Condition you want to configure, then configure the parameter(s) as described below.

- **Not defined** - This option specifies that there is no criteria for the policy.
- **Protocol Only -** Select **TCP**,**UDP** or **ICMP** to create a condition for a Service Protocol only.
- **Port(s) -** To configure the Condition for a specific Service Port, select a **Source** and **Destination** Port from the drop-down menu to specify a specific port for the service you selected. You can also click on **Add New** to create new Service Ports (see page 616).

- **Service -** Select a Service from the drop-down menu. You can also click on **Add New** to create a new Service (see page 610).
- **Service Group -** Select a Service Group from the drop-down menu. You can also click on Add New to go create a new Service Group (see page 610).

ICMP

An ICMP Condition applies the policy to traffic with the specified ICMP Type/Code value. Traffic that contains this value will match this condition. When you select the ICMP condition, the following parameters to configure the type of Condition will display:



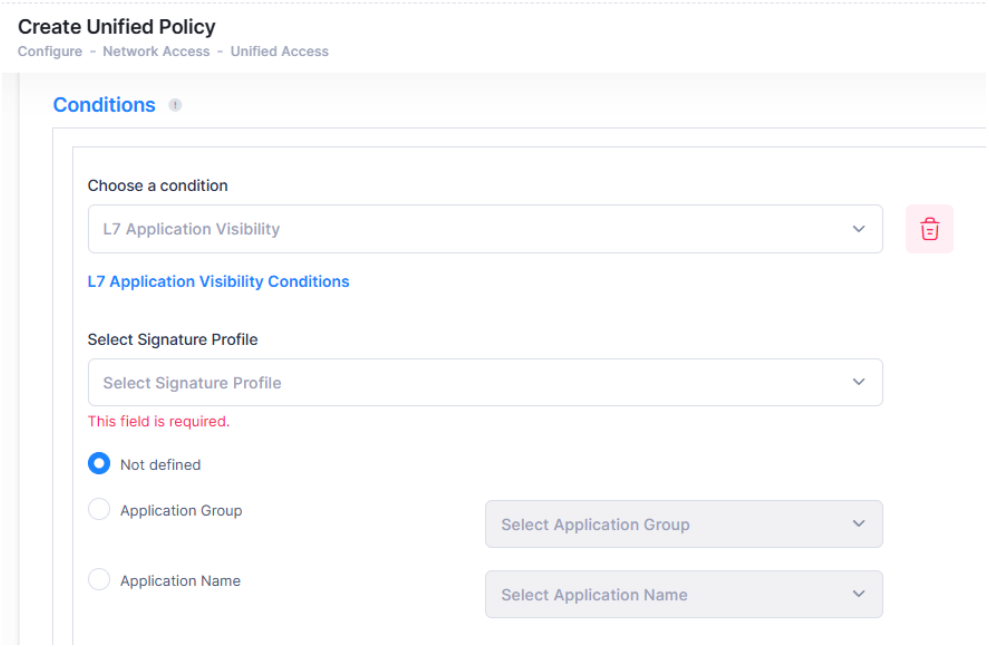
You can configure the parameter(s) as described below.

- **ICMP Type** - Enter any value between 0 - 255 for the ICMP Type.
- **ICMP Code** - Enter any value between 0 - 255 for the ICMP Code.

Note: For Steller Access Points, ICMP configuration must be combined with Service protocol = ICMP in L4 Services.

L7 Application Visibility

An Application Visibility Condition applies the policy to traffic flowing to and from an Application Group or Application. When you select the L7 condition, the following parameters to configure the type of Condition will display:



Select a type of L7 Condition you want to configure, then configure the parameter(s) as described below.

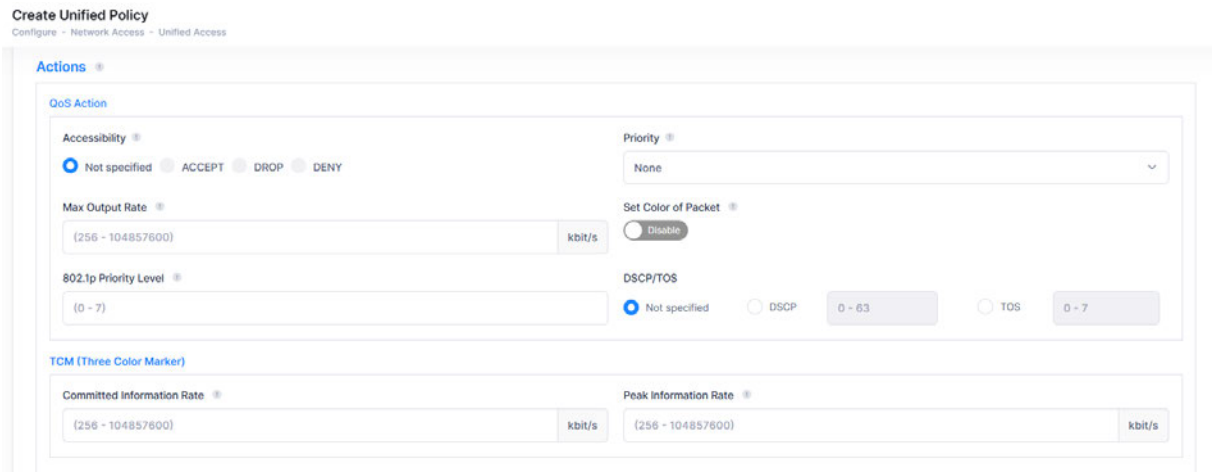
- **Select Signature Profile** - Select a signature profile from the drop-down menu.
- **Not defined** - This option specifies that there is no criteria for the policy.
- **Application Group -** Select an Application Group from the drop-down menu.
- **Application Name -** Select an Application from the drop-down menu.

Note: The drop-down menus are populated with the Application Groups/Applications contained in the Signature Profile for the selected Stellar APs. If you select multiple APs, only those Application Groups/Applications common to all APs will be displayed.

Note: To create a Quality of Service (QoS) policy for multiple applications, you can create a custom group within the Signature profile. By using the “Custom Application Group" feature, you can define a single policy that includes all applications in that group. This method is advantageous because any modifications to the applications within the custom group will not necessitate editing the policies or pushing updated policies to managed devices.

7.1.4.1.5 Actions

A Unified Policy Action enables you to specify the treatment traffic receives when it flows. This includes the priority the traffic will receive, its minimum and maximum output rates, and the values to which specified bits in the frame headers will be set upon egress from the device. When the conditions specified by the Unified Policy Condition are true, traffic will flow as specified by the Unified Policy Action.



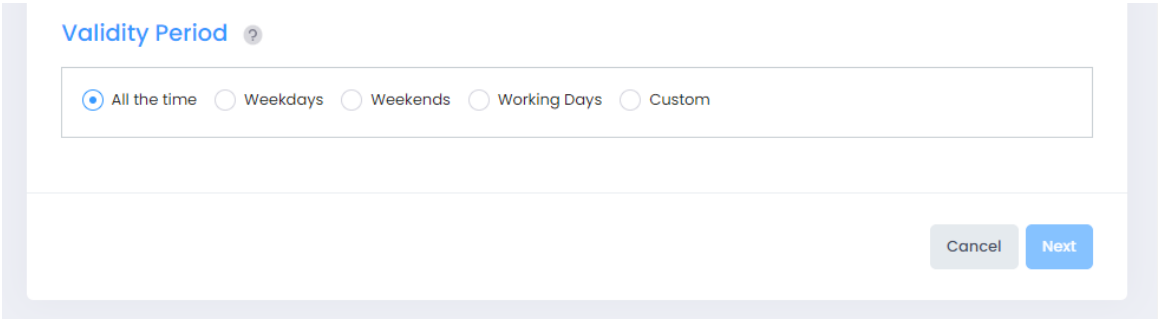
A brief description of each Action is provided below. Click the hyperlink for each Action for detailed configuration instructions.

- QoS (see page 543) - Create an Action to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.
- TCM (see page 544) - Create an Action to specify Tri-Color Marking (TCM) actions to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a device interface. TCM meters traffic based on user-configured packet rates and burst sizes and "marks" the metered packets as green, yellow, or red based on whether the traffic meets the configured rates. This "color marking" determines the packet's precedence when congestion occurs.
- **QoS** - The QoS Policy Action option enables you to specify QoS actions to impose on traffic that meets the configured policy condition(s). When the conditions specified by the policy are true, traffic will flow as specified by the policy action.
  - **Accessibility** - Set the Action to Accept, Drop or Deny traffic that meets the configured condition(s). The Deny option will only be available for Switch devices.
    - **Accept**- Specifies that the switch should accept the flow.
    - **Drop**- Specifies that the switch should silently drop the flow.
    - **Deny**- Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as drop; that is, the flow is silently dropped.
  - **Priority** - Specify QoS priority the traffic will receive if it meets the configured condition(s).
    - **Platinum** priority provides the highest quality of service (and maps to a firmware priority of 7).
    - **Gold** provides the next-highest quality of service (and maps to a firmware priority of 5).
    - **Silver** provides the next-highest quality of service (and maps to a firmware priority of 3).

    - **Bronze** provides the same quality of service as best effort (and maps to a firmware priority of 1). A separate egress queue is maintained in the hardware for traffic of each different priority.
  - **Max Output Rate** - Specify the maximum amount of traffic, in kilobits-per-second, which is guaranteed to be transmitted. Even if no other traffic exists, the output will be limited to the rate specified here.
  - **802.1p Priority Level** - If you want outgoing packets tagged with an 802.1b priority level, set the 802.1p Priority Level field value between 0 to 7 to specify the desired outgoing 802.1p priority for the traffic. A value of 7 indicates the highest priority and a value of 0 indicates the lowest priority.
  - **Set Color of Packet** - Enables/Disables Three Color Marking (TCM) for output traffic flows. This parameter is not supported on Access Point devices and is ignored when applied to those devices.
  - **DSCP/TOS** - Enable/Disable DSCP/TOS Precedence.
- **TCM (Three Color Marker)** - The TCM Policy Action option enables you to specify Three-Color Marking (TCM) actions action to impose on traffic that meets the configured policy condition(s). TCM provides a mechanism for policing network traffic by limiting the rate at which traffic is sent or received on a switch interface.
  - **Committed Information Rate** - The guaranteed bandwidth in bits-per-second, for all traffic that ingresses on the port.
  - **Peak Information Rate -** The peak bandwidth in bits-per-second, for all traffic that ingresses on the port.

7.1.4.1.6 Validity Period

The Validity Period enables you to add a validity period to a condition by specifying the time periods when the policy is active and enforced.



Select a validity period for the Unified Policy.

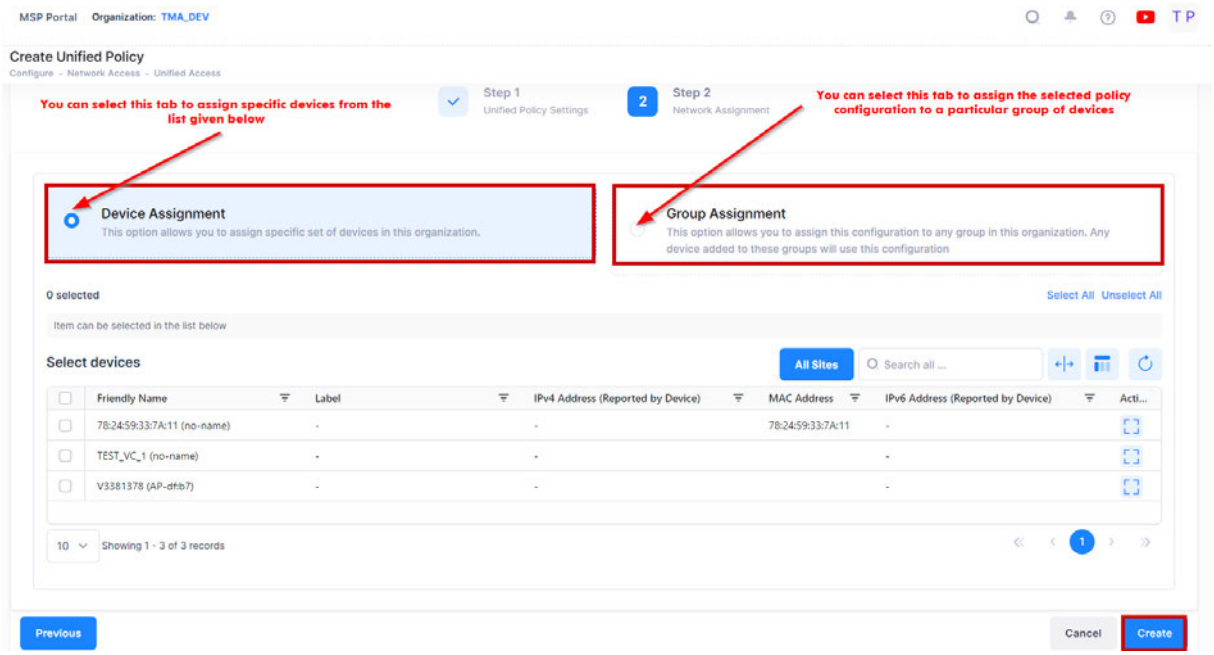
- **All The Time -** The policy will be enforced all days of the week, all months of the year, and all hours of the day.
- **Weekdays** - The policy will be enforced on weekdays (Monday - Friday), all months of the year. Each weekday is 24 hours (midnight to midnight).
- **Weekends -** The policy will be enforced on Saturday and Sunday, all months of the year. Each Saturday and Sunday is 24 hours (midnight to midnight).

- **Working Days -** The policy will be enforced on weekdays (Monday - Friday), from 9:00 a.m. to 5:00 p.m., all months of the year.
- **Custom -** Select to create a custom validity period by specifying specific days, months, and times.

Click on **Next** button to configure Network Assignments for the Unified policy.

7.1.4.1.7 2. Network Assignments

The Network Assignments tab is used to select the AP Group(s) within a Site(s) and specific Switch devices to which the Unified Policy will be applied to devices within those groups. Complete the network assignments as described below, then click on **Create** to create the Unified Policy.



- **Device Assignment** - Select the specific set of Devices from the available list to assign the policy.
- **Group Assignment** - Select the specific group of Devices from the available list to assign the policy. The Unified Policy will be applied to the selected group of devices from the list.

Note: If a Unified Policy fails to apply to devices, re-apply the policy without changing the configuration. Edit the profile (or a linked profile that supports device assignment) to remove the devices, then re-add the devices in the device assignment tab.

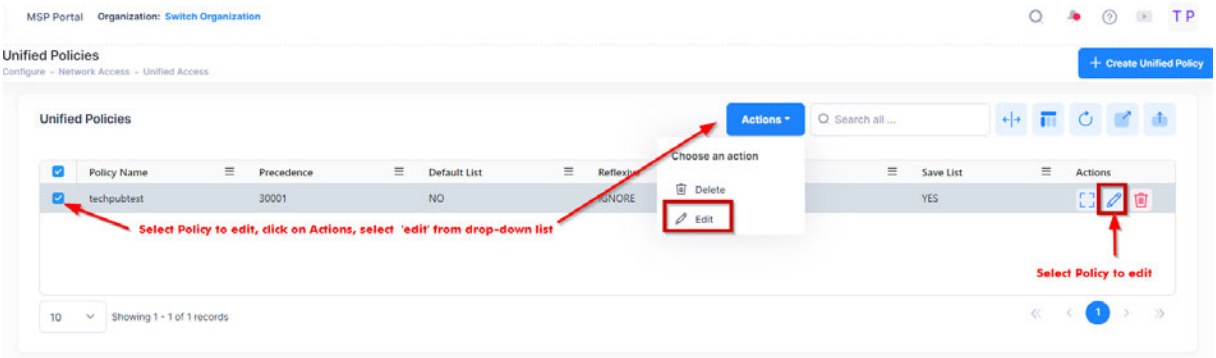
Note: For the selection of an AP Group or Device, follow the below criteria:

1. You can define a Unified Policy without selecting an AP Group or Device
2. You can select only AP Groups to apply the Unified Policy

3. You can select only Switch devices to apply the Unified Policy
4. You can select both AP Groups and Switch devices to apply the Unified Policy
5. You can filter the Switch devices based on labels.
6. When you type characters in the device list field, the list of devices matching the typed characters will be displayed.

7.1.4.2 Editing a Unified Policy

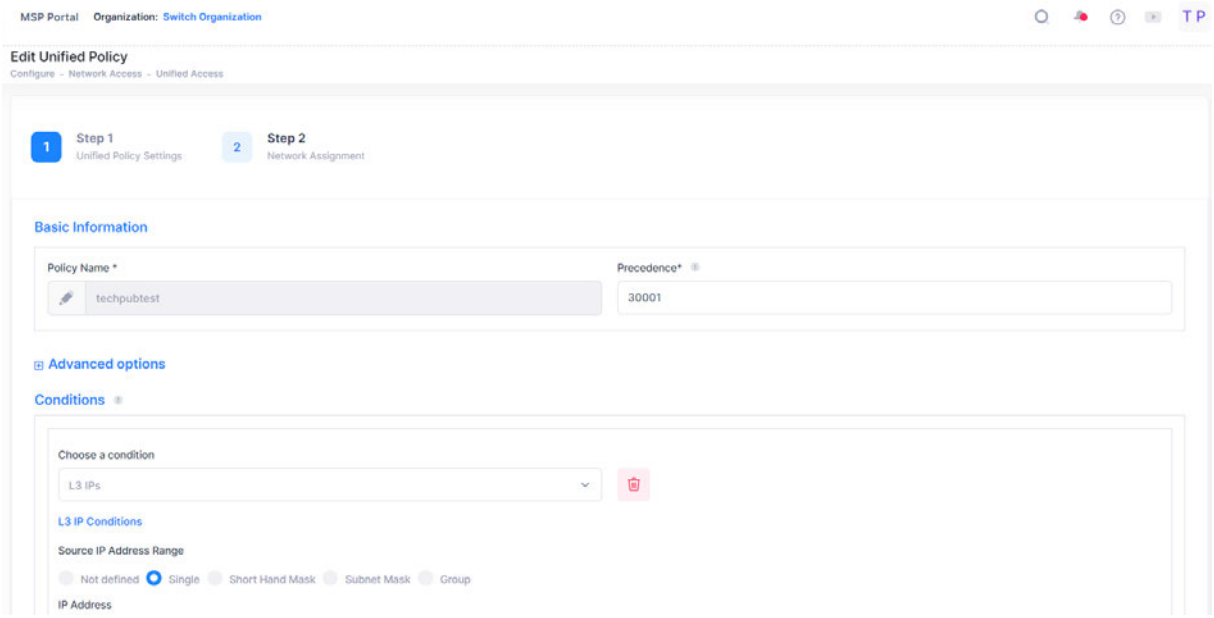
Select the policy in the Unified Policy list and click on the Edit icon to bring up the Edit Unified Policy screen.



Use one of the following methods to access the Edit Access Role Profile screen (as shown above):

- Select the profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the profile that you want to edit.

The following Edit Access Role Profile screen displays. Edit the fields as described above (see page 534), then click on **Save**.

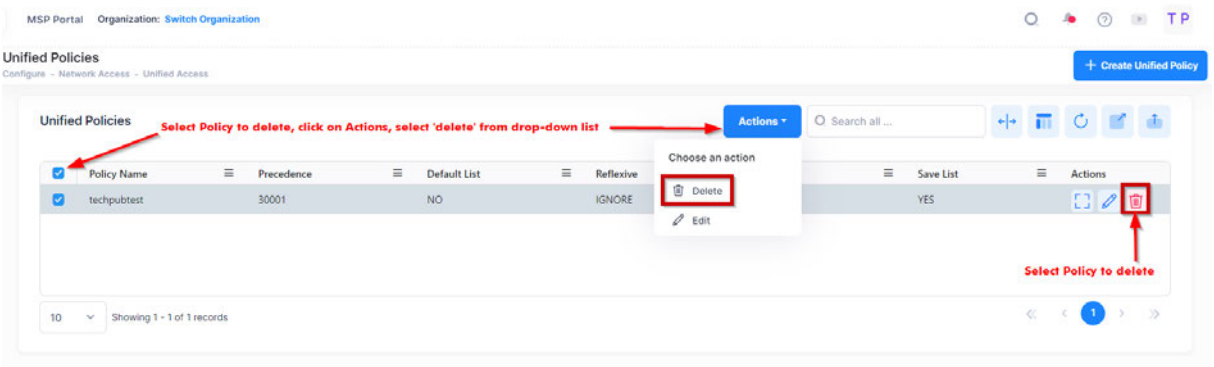


Note: If a Unified Policy fails to apply to devices, re-apply the policy without changing the configuration. Edit the profile (or a linked profile that supports device assignment) to remove the devices, then re-add the devices in the device assignment tab.

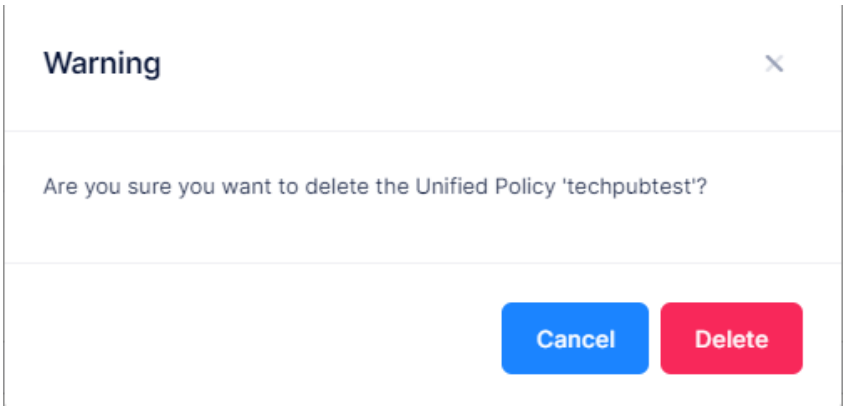
7.1.4.3 Deleting a Unified Policy

To delete an Unified Policy, use one of the following methods to select the policy you want to delete:

- Select the profile to delete by clicking on the checkbox next to the profile, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the profile that you want to delete.



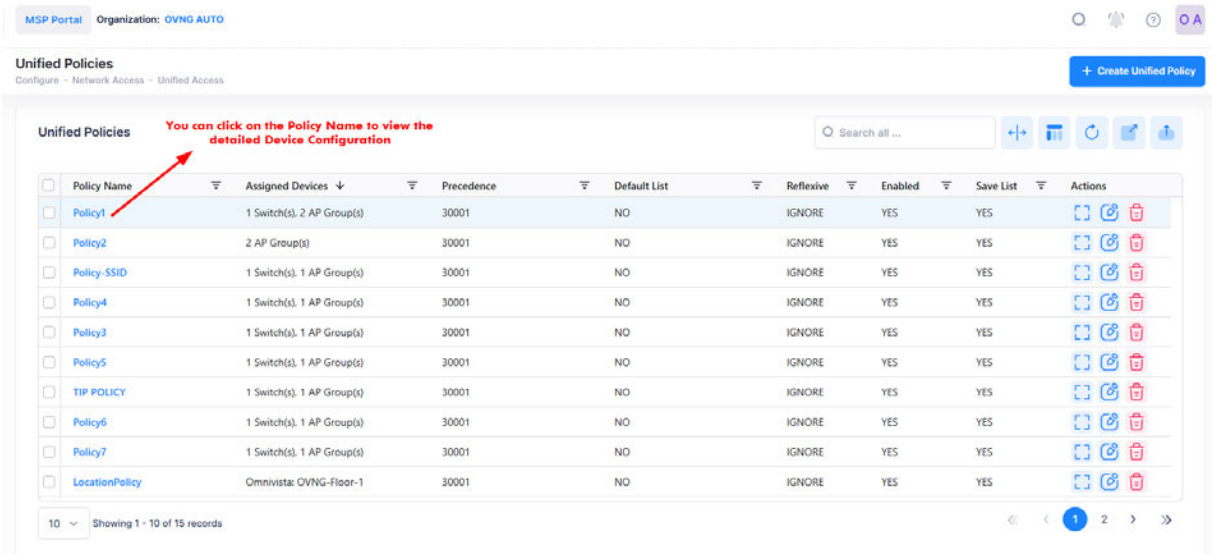
When you select the profile you want to delete, the following confirmation prompt appears:



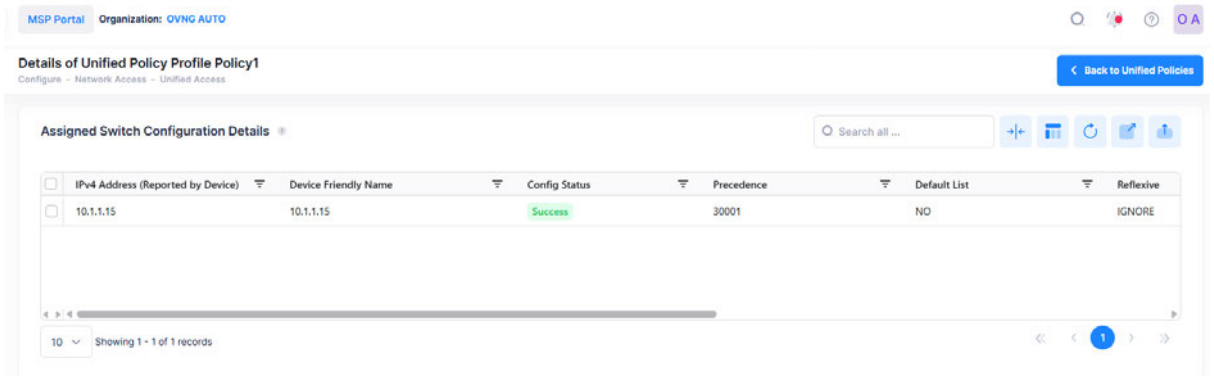
Click on **Delete** to confirm that you want to delete the Unified Policy.

7.1.4.4 Display Assigned Switch Configuration Details

The Unified Policies displays information for the configured Unified Policies. You can click on the Policy Name to view the assigned Switch configuration details of a specific Policy as shown below.



The below screen appears:



This screen also allows you to export, search and filter the data. You can click the back icon on the top right to navigate to the Unified Policy page.

The following Device Configuration of the selected Policy is displayed.

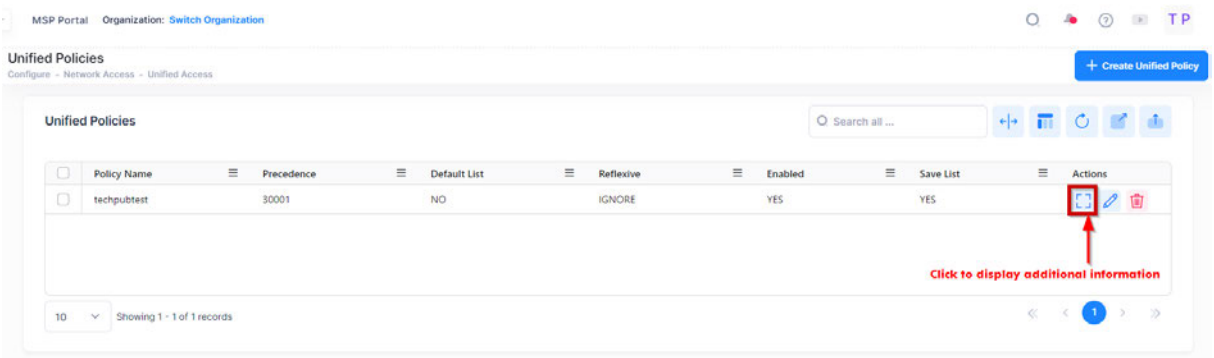
- **IPv4 Address** - The IPv4 address of the device.
- **Device Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Config Status** - The configuration status of the device. (Successful or Failed or Pending).
  - **Pending** - The configuration is being pushed to the device and is still not receiving a response from the device.
  - **Failed** - The configuration failed to apply to the device. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to the device successfully.
- **Precedence** - The Precedence value of the Policy (0 - 65535).

- **Enabled -** Indicates whether or not the Policy is enabled.
- **Log Matches -** Indicates whether or not matches to this rule are logged in the QoS Log.
- **Reflexive -** Indicates whether or not the Policy is reflexive. Reflexive Policy Rules allow specific return connections that would normally be denied (Yes/No).
- **Default List-** Indicates whether or not the Policy is saved to the Default Policy List. By default, a Policy Rule is added to this list when it is created. A Policy Rule remains a member of the Default List even when it is subsequently assigned to additional Policy Lists.
- **Save List -** Indicates whether or not the rule will be recorded during a snapshot command.
- **Send Trap -** Indicates whether or not an SLA Policy Trap is configured for the policy.

Note: You can now view the current policy configuration for each switch assigned to a Unified Policy. You can edit the configuration on one or more assigned devices directly. If a device's configuration differs from the policy, the mismatched attributes will be highlighted, and you will have the option to synchronize them.

7.1.4.5 Display Unified Policy Additional Information

To display detailed information about a specific policy, you can click on the Additional Information icon under the “Actions” column.



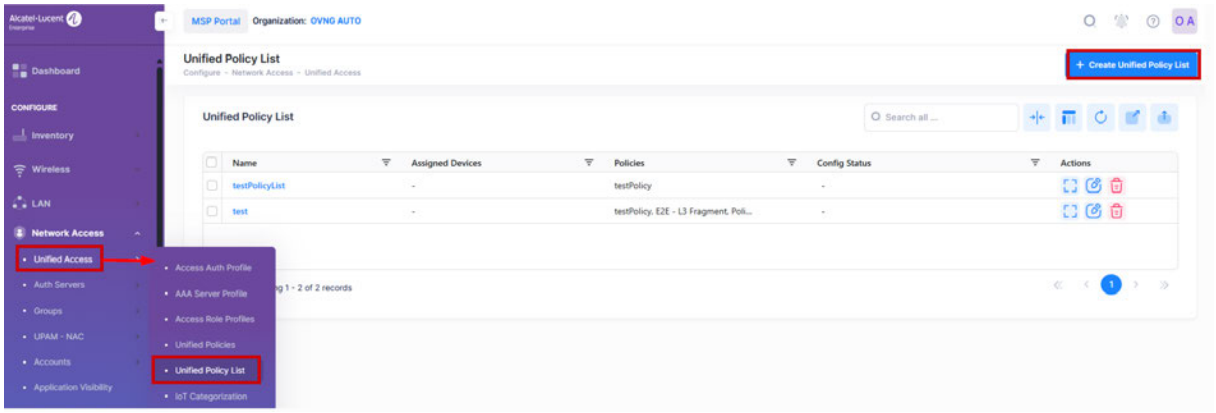
Additional information
Policy Name: OVNGTEST-21027-2
Config Status: Successful
Precedence: 30001
Default List: NO
Enabled: YES
Save List: YES
Log Matches: YES
Send Trap: IGNORE
Reflexive: IGNORE
Policy Condition: __OVNGTEST-21027-2
Service Protocol: TCP
Source Port Range: DNS (53)
Destination Port Range: LDAP (389)
Policy Action: __OVNGTEST-21027-2
Priority: 0
Validity Period: All The Time
Assigned Devices:
Sites
Assigned Groups and Devices
Config Status
Close

21 Oct 2025

7.1.5 Unified Policies List

A Unified Policy List is a set of Unified Policies (see page 533) that are grouped together and assigned to devices as a group. You can also assign a Unified Policy List to an Access Policy. The policies in the list are applied to devices that are assigned to the Access Policy (see page 621).

Use the Unified Policies List screen to display information (see page 555) about all of the configured Unified Policies Lists. This screen also allows you to create (see page 551), edit (see page 554), and delete (see page 554)Unified Policies Lists on the network. To access the Unified Policies List screen, click on **Network Access > Unified Access > Unified Policies List** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.1.5.1 Create Unified Policy List

The Create Unified Policy List screen is used to select policies for the list and assign network devices to which the policy list is applied. To access this screen, click on **Create Unified Policy List**.

Consider the following use cases when configuring Unified Policies List:

1. OmniVista Terra does not use LDAP, so any Unified Policies created on a Switch via LDAP are not discovered; only policies configured through the Switch CLI are discovered. As a result, the Unified Policies List screen displays only policies configured through the Switch CLI. In case, you want to "restore" the set of policies that they had previously configured on the Switch via LDAP or any other interface, you should use the mechanism of Golden Configuration from OmniVista Terra to restore all the configuration on the switch (and not just Policies).
2. OmniVista Terra only supports polling policy lists created from type UNP. When receiving profiles not created from type UNP, it will ignore these profiles and will not save them to the OVNG database, so you will not be able to view them in the User Interface screen.
3. If there are two policy list with the same name but different child profiles between two Switch devices, there will be a mismatch between the profile template and device configuration.

The Create Unified Policy List Screen appears and provides the following step-by-step process for creating a Unified Policy List:

1. **Policy List Configuration** (see page 552)

- **Name** - Configures the name for the Unified Policy List. The field must have at most 22 characters. The use of two special characters(/ or \) is not allowed for the Policy name.

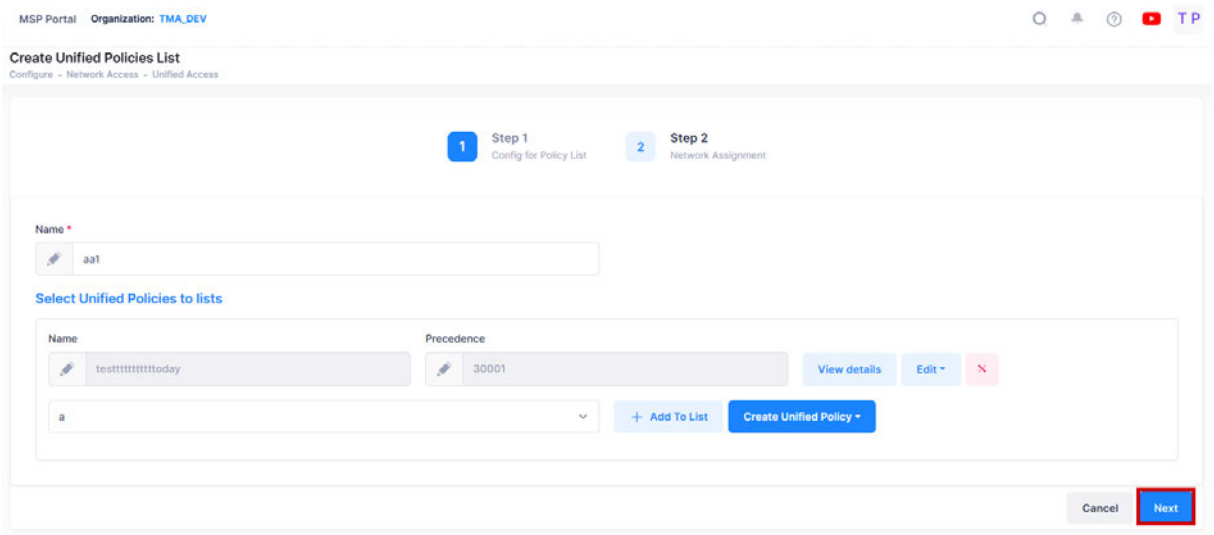
- **Select Unified Policies to lists** - Configures the Unified Policies you want to include in the list. You must have at least one Unified Policies selected from the list.

2. **Network Assignments** (see page 553)

- **Select Sites and Groups** - Select Access Point Groups or Switch devices from the available list of devices for one or more Sites. The Unified Policy List is applied to the devices in the selected Sites/AP groups.

7.1.5.2 1. Policy List Configuration

Complete the fields on the following Config for Policy List tab, as described below.

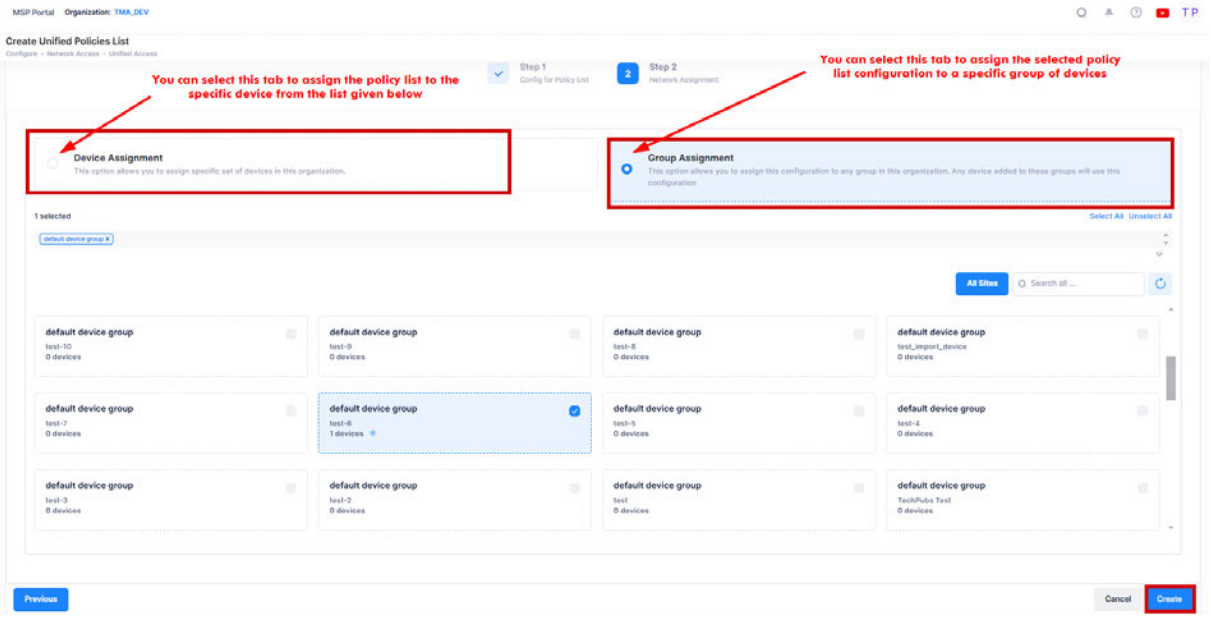


- **Name** - The name of the policy. The field must have at most 22 characters. The use of two special characters(/ or \) is not allowed for the Policy name.
- **Select Unified Policies to list** - Select an existing Unified Policy from the drop-down menu or click on **Create Unified Policy** to open the Create Unified Policy screen and create a new policy to select. After you have selected a policy, click on **Add to List**. The policy that you just added appears in this section with the following options:
  - **View Details** - Click on this option view additional details about the selected policy.
  - **Precedence** - The Policy precedence. By default, the precedence field is pre-filled with the lowest unused precedence value. A higher number indicates higher precedence. (Range = 0 - 65535)
  - **Edit** - Click on this option to open the Edit Unified Policy screen and make any changes to the policy.
  - **Remove** - Remove the selected policy; it will not be added to the Unified Policy List.

  Continue to select and add more policies, as necessary. Once you have selected all of the policies that you want to add to the Unified Policy List, click on **Next** to go to the next tab (Step 2).

7.1.5.3 2. Network Assignments

The Network Assignments tab is used to select the AP Group(s) within a Site(s) or Switch devices to which the Unified Policy List will be applied to devices within those groups. Complete the network assignments as described below, then click on **Create**.



- **Device Assignment** - Select the specific set of Devices from the available list to assign the policy list.
- **Group Assignment** - Select the specific group of Devices from the available list to assign the policy list. The Unified Policy will be applied to the selected group of devices from the list.

Note: In case of failing to apply an Unified Policy List to devices, if you wants to re-apply the policy with no change in the configuration, you needs to edit the profile (or the profile that links to it and supports device assignment) to remove the devices then edit to re-add the devices into the device assignment tab.

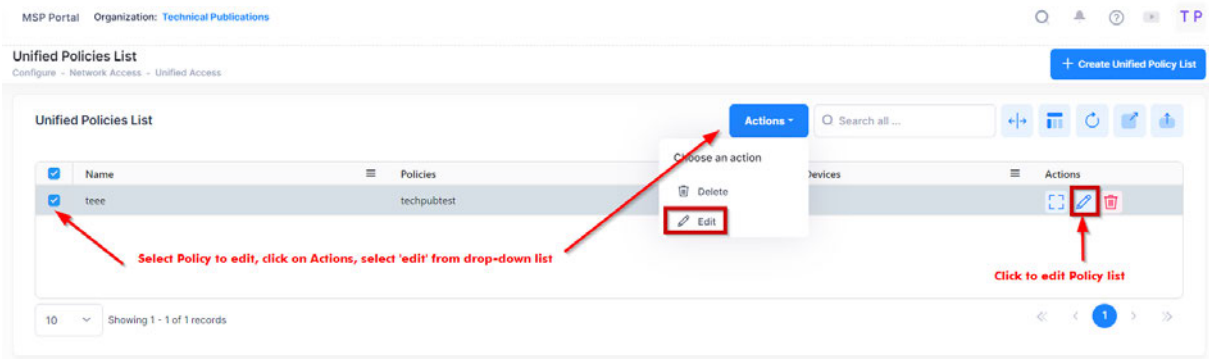
Note: For the selection of an AP Group or Device, follow the below criteria:

1. You can define a Unified Policy List without selecting an AP Group or Device.
2. You can select only AP Groups to apply the Unified Policy List.
3. You can select only Switch devices to apply the Unified Policy List.
4. You can select both AP Groups and Switch devices to apply the Unified Policy List.
5. You can filter the Switch devices based on labels.
6. When you type characters in the device list field, the list of devices matching the typed characters will be displayed.

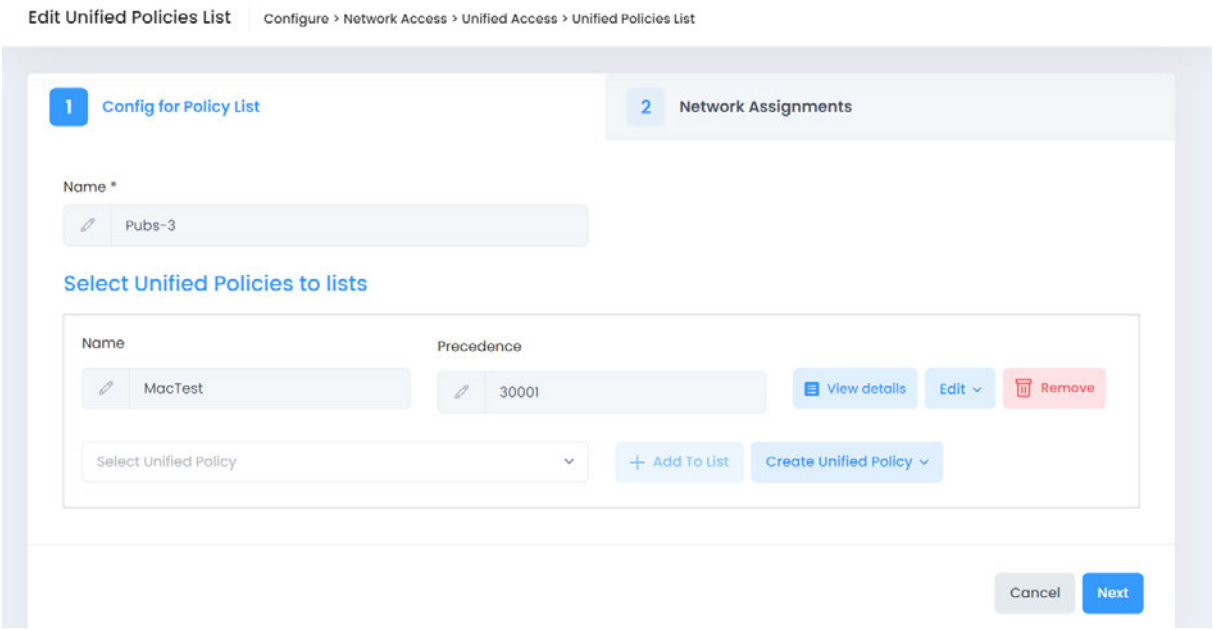
7.1.5.4 Editing a Unified Policy List

You can edit a Unified Policy List by accessing the Edit Unified Policy List screen. Use one of the following methods to access the Edit Edit Unified Policy List screen:

- Select the list to edit by clicking on the checkbox next to the list, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the list that you want to edit.



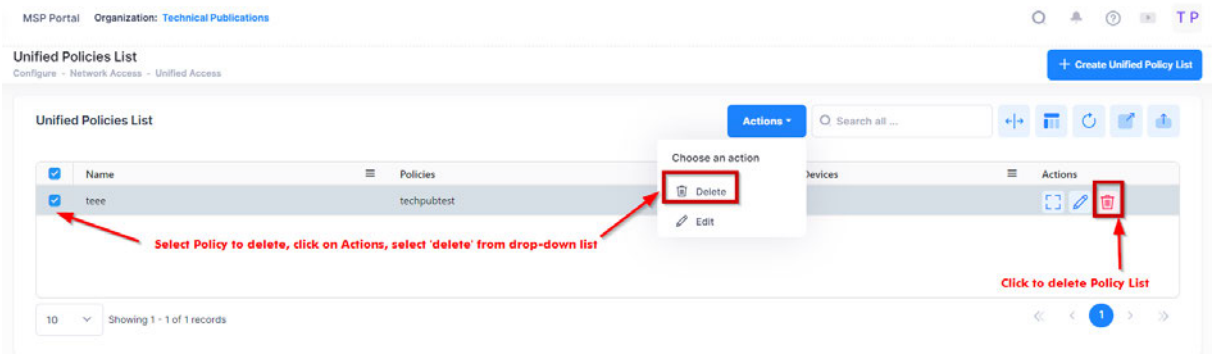
The following Edit Unified Policy List screen displays. Edit the fields as described above (see page 552)then click on **Save** to save the changes.



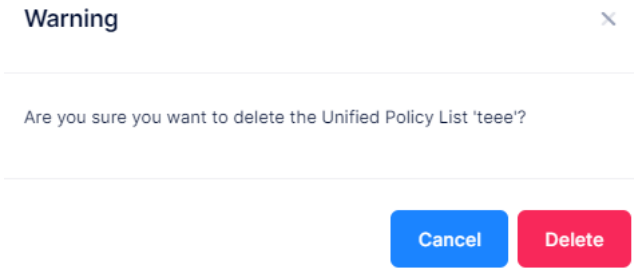
7.1.5.5 Deleting a Unified Policy List

To delete a Unified Policy List, use one of the following methods to select the list you want to delete:

- Select the List to delete by clicking on the checkbox next to the list, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the list that you want to delete.

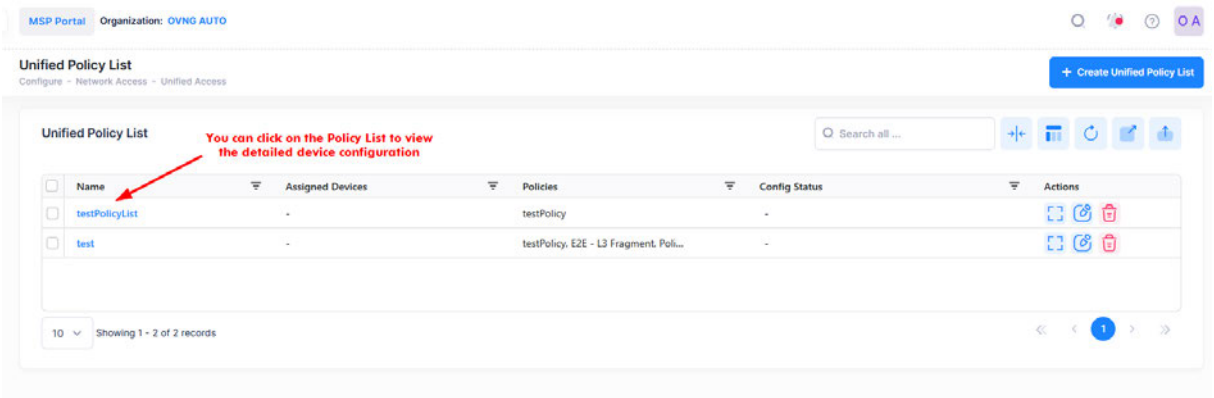


Click **Delete** on the confirmation prompt.

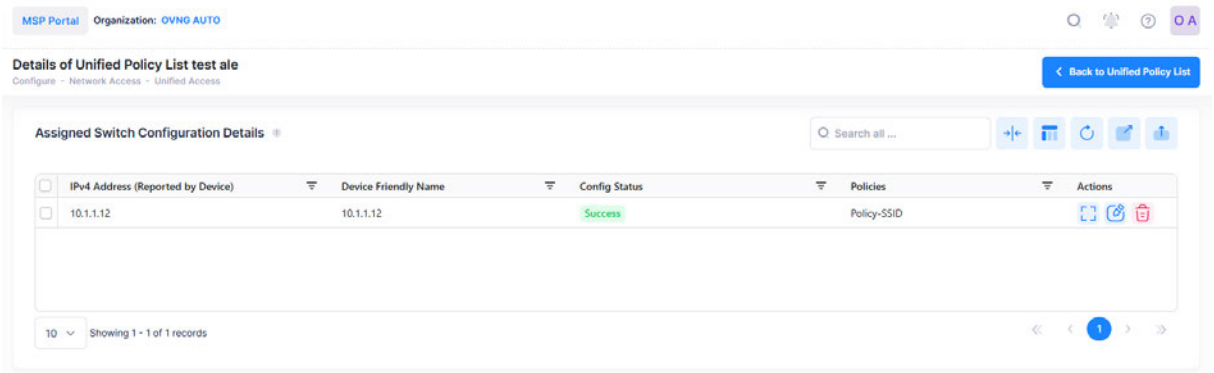


7.1.5.6 Display Assigned Switch Configuration Details

The Unified Policy list displays information for the configured Unified Policies. You can click on the Policy List Name to view the assigned Switch configuration details of a specific Policy as shown below.



The following screen appears:



This screen also allows you to export, search and filter the data. You can click the back icon on the top right to navigate to the Unified Policy List page.

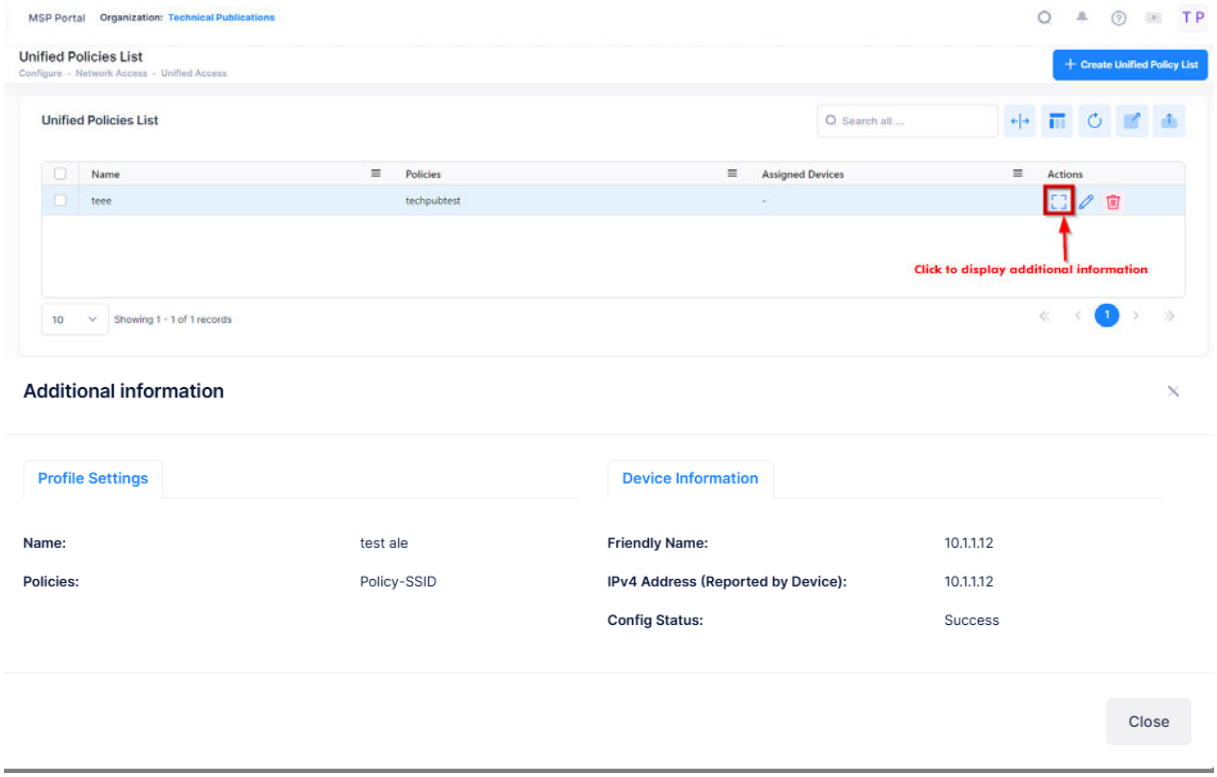
The following Device Configuration of the selected Policy List is displayed.

- **IPv4 Address** - The IPv4 address of the device.
- **Device Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Config Status** - The configuration status of the device. (Successful or Failed or Pending).
  - **Pending** - The configuration is being pushed to the device and is still not receiving a response from the device.
  - **Failed** - The configuration failed to apply to the device. Possible reasons include a timeout while applying the configuration due to the device being unreachable or a network issue, or the configuration being invalid and rejected by the device. Check alerts to identify the specific reason.
  - **Successful** - The configuration is pushed to the device successfully.
- **Policies** - The assigned Unified policy to device.

Note: You can now view the current profile configuration for each switch assigned to an Unified Policy List. You can edit the configuration on one or more assigned devices directly. If a device's configuration differs from the Policy List, the mismatched attributes will be highlighted, and you will have the option to synchronize them.

7.1.5.7 Display Unified Policy List Additional Information

You can click on the Additional Information icon to view additional information of a Unified Policy List.


MSP Portal
Organization: Technical Publications
TP
Unified Policies List
Configure - Network Access - Unified Access
Create Unified Policy List
Unified Policies List
Search all ...
Name
Policies
Assigned Devices
Actions
teee
techpubtest
Click to display additional information
10
Showing 1 - 1 of 1 records
1
Additional information
Profile Settings
Device Information
Name:
test ale
Policies:
Policy-SSID
Friendly Name:
10.1.1.12
IPv4 Address (Reported by Device):
10.1.1.12
Config Status:
Success
Close

21 Oct 2025

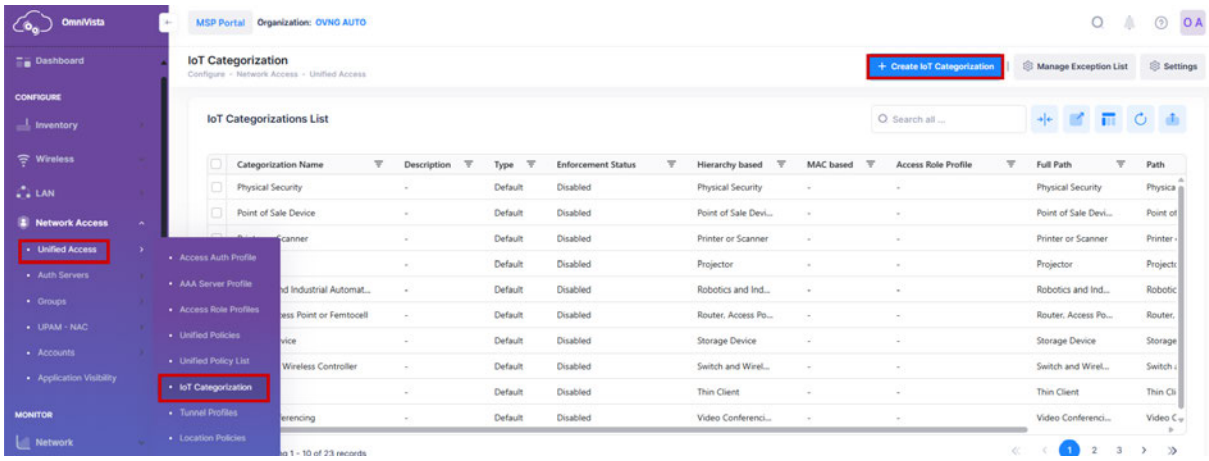
7.1.6 IoT Categorization

OmniVista Terra monitors network packets to determine the types of client devices connected to an IoT-enabled Access Point and interfaces with a Device Fingerprinting Service to categorize them. Categories are hierarchical. Default Categories are the top-level categories and are provided and listed by default. When a device is initially categorized, it will be assigned one of these top-level categories (e.g., Phone, Tablet or Wearable). As OmniVista monitors packets and learns more about a device, the category assigned to the device will become more specific. For example, a device may initially be categorized as "Phone, Tablet or Wearable". As OmniVista learns more about the device, the device may be categorized as an "Apple Mobile Device", and then an "Apple iPhone". As OmniVista Terra learns these new categories, they are added to the List of Categories.

- The Default Categories provided cannot be deleted, but can be edited to assign an Access Role Profile to the category.
- In addition to the default set of hierarchical categories, you can create custom categories that you can edit and delete. There are two types of custom categories: hierarchy and MAC-based.
  - A custom hierarchy category specifies the hierarchy categorization a device must match to be associated with the custom category.
  - A custom MAC-based category specifies the MAC address a device must have to be associated with the custom category.
- Category-based device authentication is configurable by assigning an Access Role Profile to a category (default or custom) with the option of Automatic Enforcement.

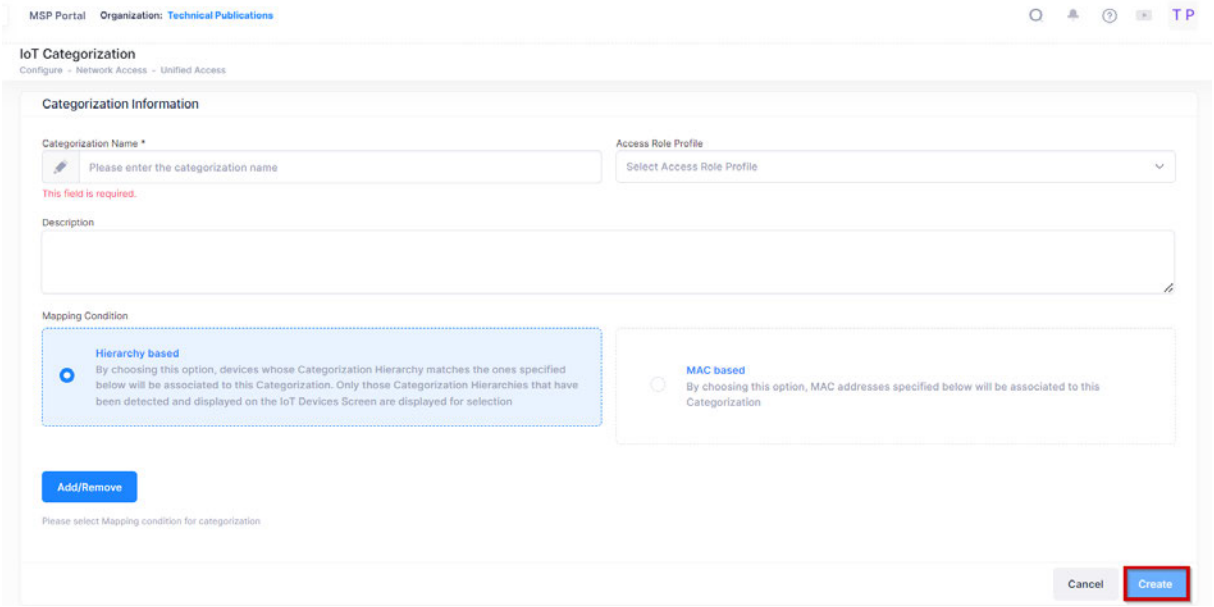
The IoT Categorization screen displays information (see page 560) about device categories and is used to create (see page 558), edit (see page 559), and delete (see page 561)an IoT Categorization list entry. This screen is also used to configure category-based authentication using IoT Enforcement (see page 561).

To access the IoT Categorization screen, click on **Network Access > Unified Access > IoT Categorization** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.1.6.1 Creating an IoT Category

Click on the **Create IoT Categorization** icon and complete the fields as described below.



- **Categorization Name -** A name for the Custom Category.
- **Description -** An optional description for the category.
- **Access Role Profile -** Select the required Access Role Profile.
- **Mapping Conditions** - You can create a Custom Category based on an existing category (Hierarchy Based) or create a Custom Category based on MAC Address (MAC Based).
  - **Hierarchy Based -** Click on the **Add/Remove** button to bring up a list of categories. Only those category hierarchies that have been detected and displayed on the Inventory Screen are displayed for selection. Add/Remove categories to create the Custom Category.
  - **MAC Based -** Enter a MAC Address of the categorization and click on the Add icon (+). Repeat to add additional MAC Addresses. Click on the Delete icon (x) to remove a MAC Address from the Custom Category.

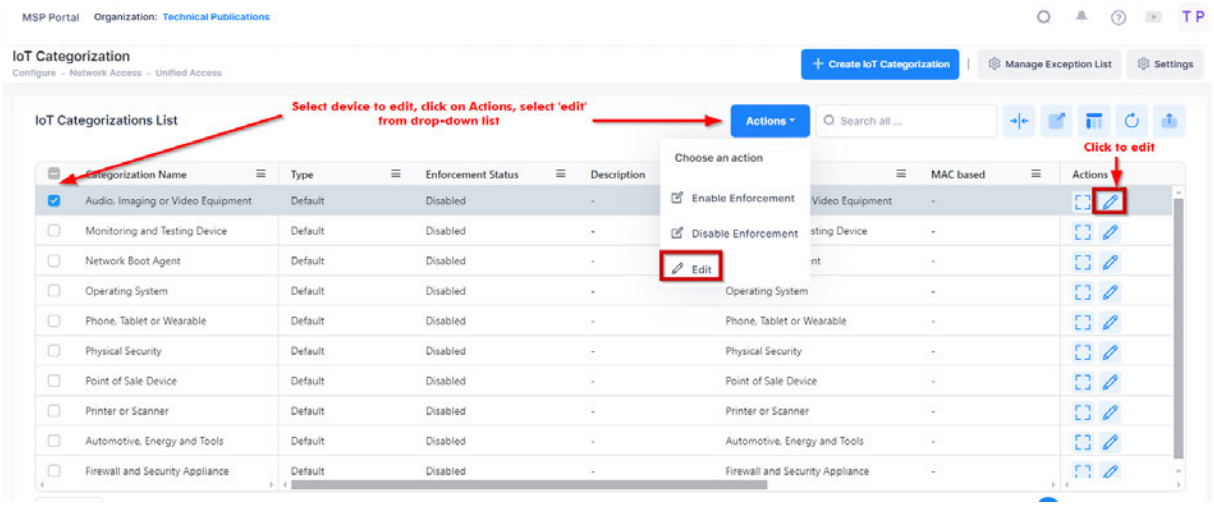
The new Custom Category will appear at the bottom of the Category List. The Custom Category will be displayed for any online devices in the Inventory List matching the new category.

When you are finished, click on the **Create** button.

- DHCP should be enabled on Client for IoT Categorization.
- Device Categorization depends on the Fingerbank API, which requires Internet connectivity. In the absence of Internet access, client devices may not be categorized.

7.1.6.2 Editing an IoT Category

Select an IoT Category name in the list and click on the Edit icon to bring up the Edit IoT categorization Screen . Edit the field(s) as described above, and click on the **Save** button.



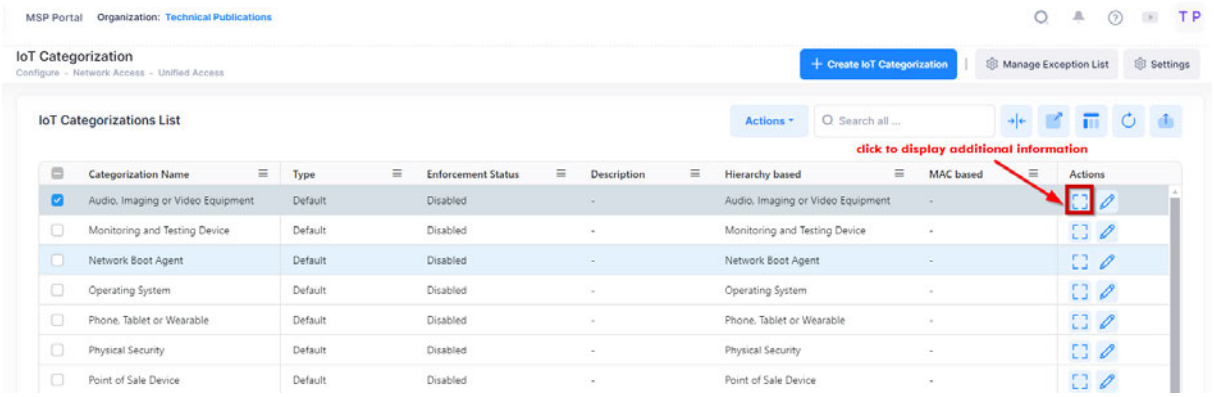
Use one of the following methods to access the Edit IoT categorization screen (as shown above):

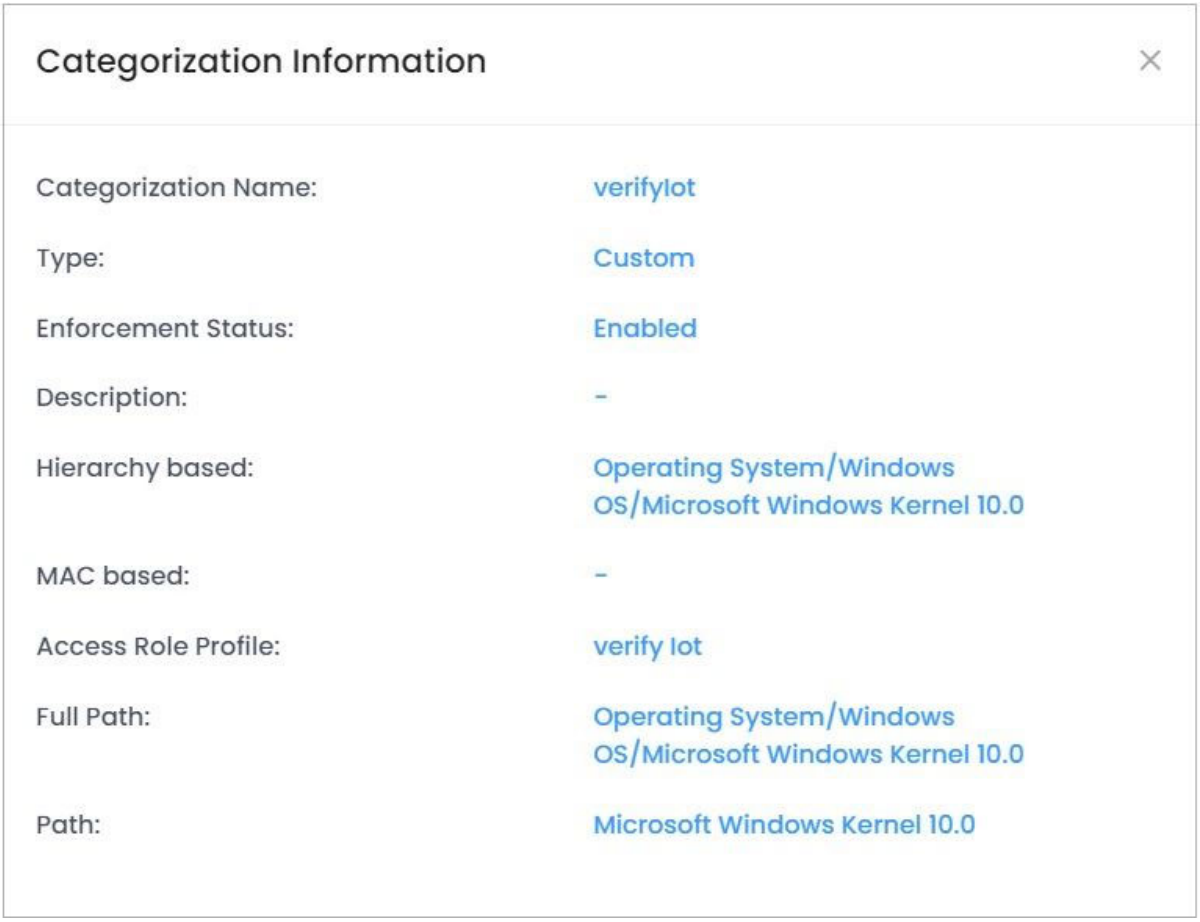
- Select the name to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the name that you want to edit.

Edit the fields as described above (see page 559), then click on **Save**.

7.1.6.3 View Additional Information of an IoT Category

Select the IoT Category name in the list and click on the Additional Information icon to view additional information of the IoT Category data.





7.1.6.4 Deleting an IoT Category

Select an IoT Category name and click on the Delete icon. Click **Delete** at the Confirmation Prompt. Any devices matching the deleted Custom Category in the Inventory List will revert to the applicable default category.

7.1.6.5 Configuring IoT Enforcement

The IoT Enforcement feature enables you to authenticate devices by associating a Category with an Access Role Profile. Once a device accesses the network and is categorized, the assigned Access Role Profile is applied to the device. You can associate different Access Role Profiles with different categories; and you can enable automatic (see page 562)or manual (see page 563)enforcement Categories.

You can also specify exceptions (see page 563) for specific devices by SSID, MAC address, AP Group, or IP address. When a device matching one of these exceptions is categorized, it will not be subject to IoT enforcement configured for its category.

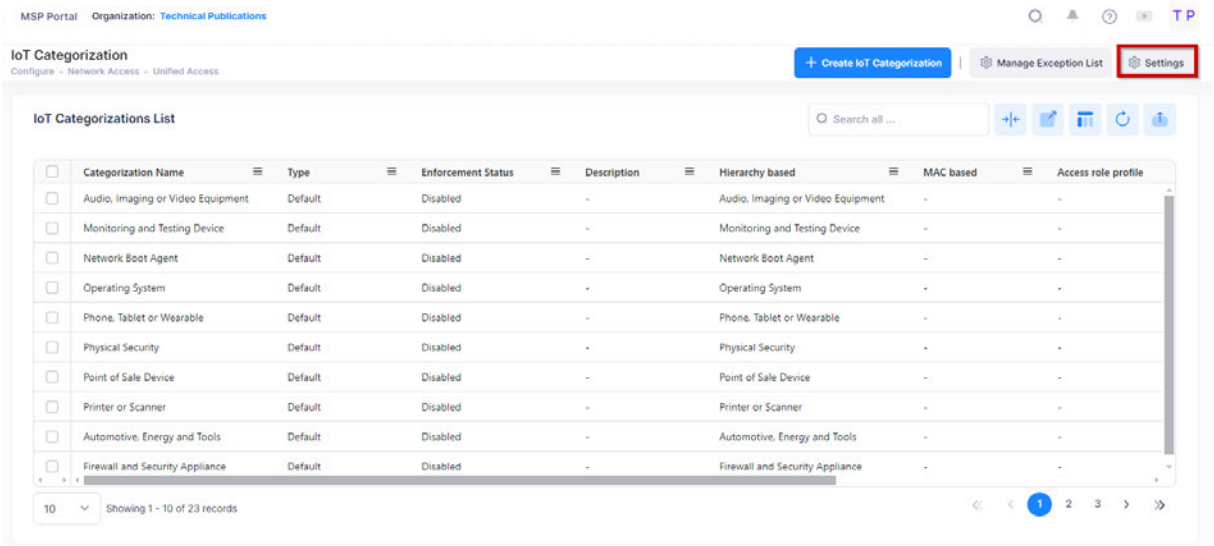
Consider the following while configuring the IoT Enforcement:

- For MAC and 802.1X Authentication, Omni Vista Terra will apply IoT Enforcement only if the authentication is successful.

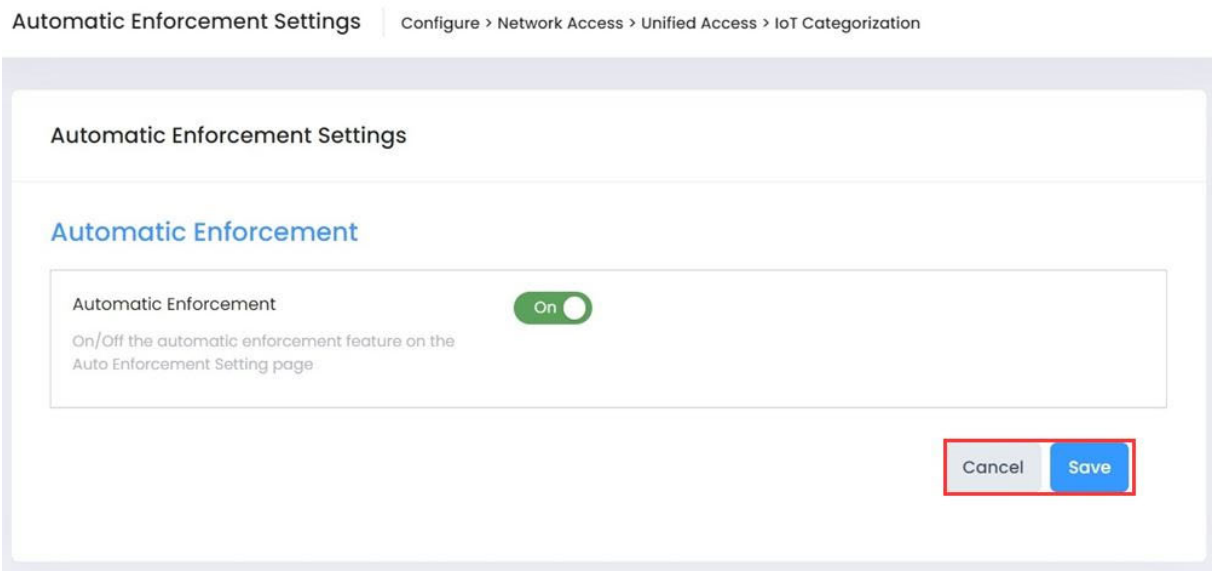
- The IoT based profile will not be applied if authentication fails.
- The above two criteria do not apply to Captive Portal authentication.

7.1.6.5.1 Automatic IoT Enforcement

Automatic Enforcement can be set from the **Settings** button at the top of the IoT Categorizations List screen.



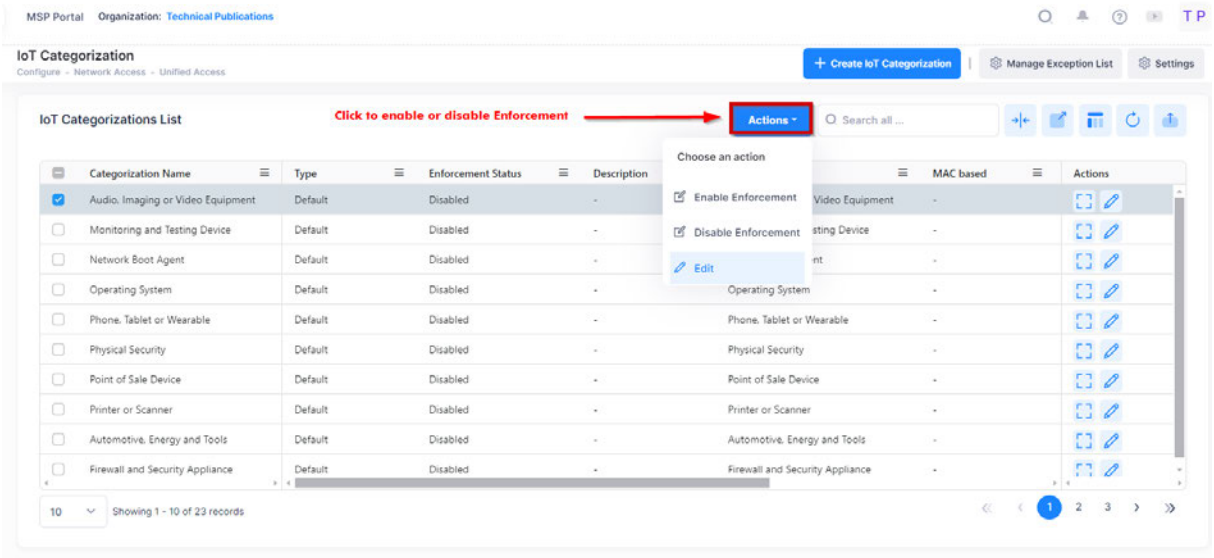
Enable Automatic Enforcement and click on **Save** button to enable automatic enforcement.



If you change Automatic Enforcement from "On" to "Off", enforcement will continue for any device on which enforcement was previously enabled, unless you manually disable enforcement for the Category used for the device, or if the device re-initializes or roams to another AP. If you change Automatic Enforcement from "Off" to "On", Automatic Enforcement will only be applied to devices that connect to the network and match a configured Enforcement Category after you enable Automatic Enforcement. If you delete a Category/ARP mapping, the new mapping configuration will be applied the next time an endpoint reconnects to an AP.

7.1.6.5.2 Manual IoT Enforcement

If Automatic Enforcement is disabled (Off), Access Role Profiles assigned to Categories are not applied to devices. However, you can manually enable IoT Enforcement for specific Categories. With the **Automatic Enforcement** button at the top of the screen set to "Off", select a Category(ies) and click on the **Action** button at the top of the Category List and select **Enable Enforcement**. The Enable Enforcement window will appear. Click on **OK** to Enable Enforcement.

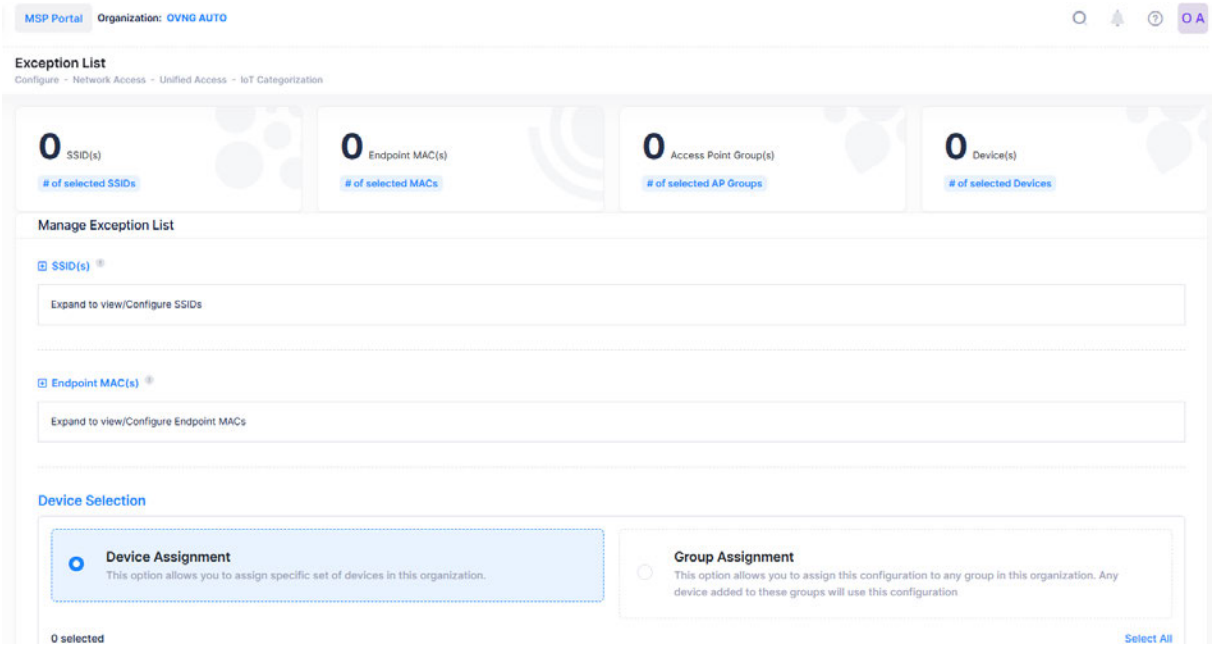


- Manual Enforcement is applied to currently-connected clients only. If Automatic Enforcement is "Off", you must apply enforcement manually whenever IoT-based enforcement is desired.
- After enabling manual enforcement for a Category(ies), if an endpoint roams to another AP or re-initializes, there will be no IoT Enforcement for that Category. You must disable Enforcement of the Category and enable it again to apply IoT enforcement manually to currently-connected endpoints.

7.1.6.5.3 Configuring IoT Enforcement Exceptions

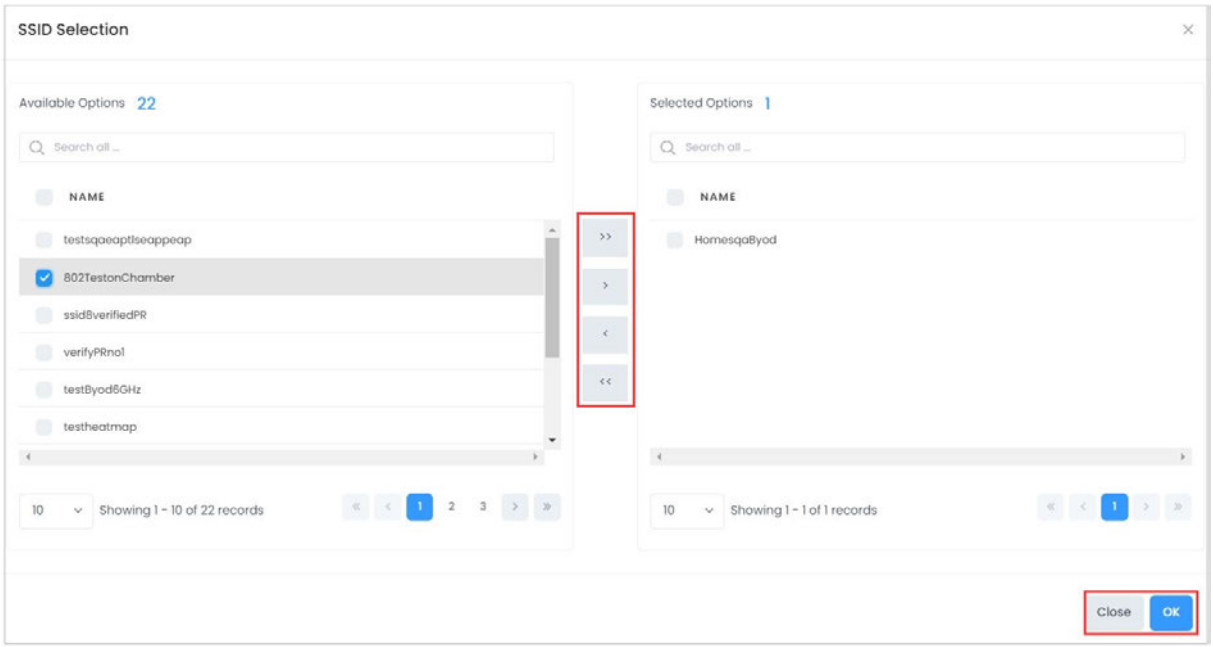
You can specify exceptions for specific devices by SSID, MAC address, AP Group, or Device. When a device matching one of these exceptions is categorized, it will not be subject to IoT enforcement configured for its category. To create IoT Enforcement exceptions, click on the **Manage Exception List** button at the top of the screen to bring up the Exception List Screen. Add SSID(s), MAC address(es), AP Group(s), or Device(s) to the exception list as described below and click on the **Save** button.

If an endpoint is initially configured for Enforcement and later added to the Exception List, the endpoint can remain assigned to the Enforcement Access Role Profile because the AP will cache the Enforcement Access Role Profile and reapply it to the endpoint if it reconnects. To add a device that was assigned to an Enforcement Access Role Profile to the Exception List, first remove Enforcement from the endpoint, then add it to the Exception List.



The Summary at the top of the Exception List displays the number of SSID(s), Endpoint MAC(s), AP Group(s), and Device(s) that have been added to the Exception List. Click on one of the items or scroll down to add/remove devices from the Exception List.

7.1.6.5.4 SSID(s)

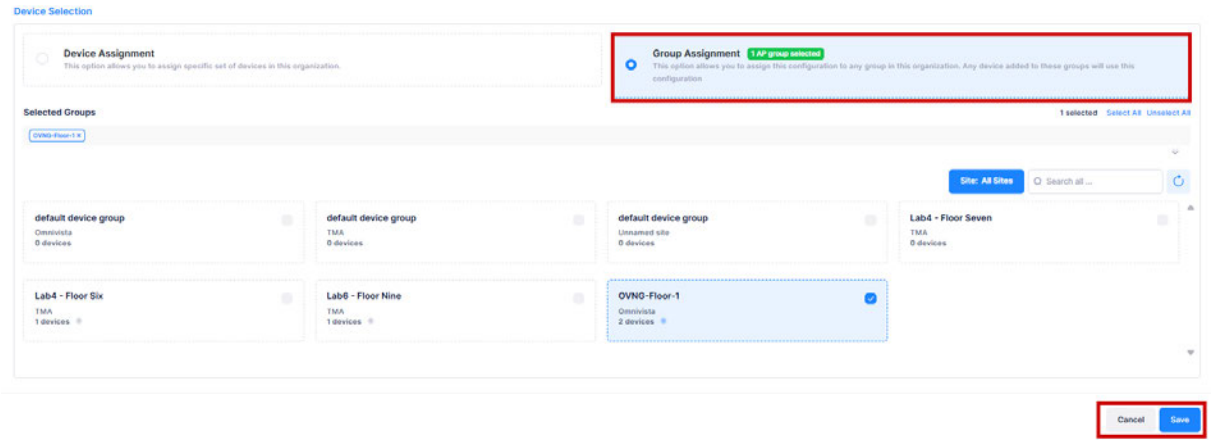


To add devices associated with an SSID to the Exception List, click on the **Change Selection** button to bring up the SSID Selection window. Select an SSID(s) and click on the **Arrow** button, then click on **OK** to add the SSID(s) to the Exception List. To remove an SSID(s) click on the **Change Selection** button to bring up the SSID Selection window. Select an SSID(s) and click on the **Arrow** button, then click on **OK** to remove the SSID(s) from the Exception List.

7.1.6.5.5 Endpoint MAC(s)

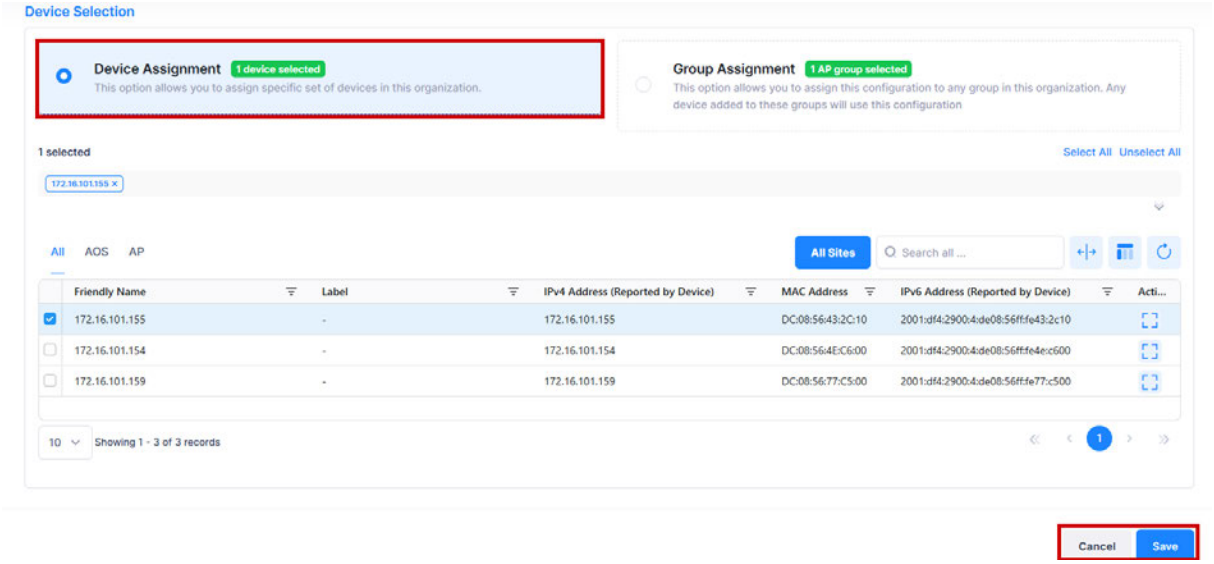
To add devices by MAC address to the Exception List, click on the **Change Selection** button to bring up the MAC address Selection window. Select an MAC address and click on the **Arrow** button, then click on **OK** to add the MAC address to the Exception List. To remove a MAC address click on the **Change Selection** button to bring up the MAC address Selection window. Select an MAC address and click on the **Arrow** button, then click on **OK** to remove the MAC address from the Exception List.

7.1.6.5.6 AP Group(s)



To add devices associated with APs in an AP Group to the Exception List, click on the **Group Assignment** tab and select AP Group from the available list to assign this configuration to the group associated with the Organization.

7.1.6.5.7 Device Selection



To add a specific device or set of devices to the Exception List, click on the **Device Assignment** tab and select device(s) from the available list to assign the specific device(s) to this Organization.

21 Oct 2025

7.1.6.6 IoT - FAQs/Troubleshooting

7.1.6.6.1 IoT is enabled for the switch and the IoT record appears in the IoT Devices page but the record does not include Category, EndPoint Name, or Manufacturer.

Check if DHCP is enabled for the Endpoint device. If a static IP is assigned, enable DHCP and reconnect the device to the switch.

7.1.6.6.2 I have deleted a Category but the device which I connected before deleting the category is still categorized as the deleted category.

After deleting the IoT Category, reconnect the device to categorize the device again.

7.1.6.6.3 ARP is not enforced, even though ARP is selected in IoT Category and IoT devices are categorized to the same category.

To enforce the ARP, configure the endpoint connected port as a UNP port and UNP should be applied on switch/AP. ARP enforcement works only on switch UNP ports.

7.1.6.6.4 I created an IoT category, connected the device, and device is categorized, but only the category and endpoint name are shown; the Manufacturer information is absent.

Manufacturer information may be absent for some devices.

7.1.6.6.5 I have configured the UNP Port but ARP is still not enforced.

Check the IoT Category Manage exception list to see if the switch or endpoint MAC address is selected.

7.1.6.6.6 I changed the running directory on an IoT-enabled switch but IoT is not showing any records for that switch.

Disable and Enable IoT for that switch.

7.1.6.6.7 Endpoint is not showing Enforced after Manual Enforcement and endpoint reconnect.

Manual Enforcement only applies enforcement for that moment. It is not applied for subsequent connections.

7.1.6.6.8 IoT endpoints are not seen after connecting endpoints to AP.

Verify in device catalog AP activation status is ‘OV managed’.
Verify the IoT status is enabled for the AP from device catalog.
Once verified, refresh the IoT devices page and check whether correct date filter is applied.
Related config and logs in AP to troubleshoot:

- /tmp/config/iot.conf

- /tmp/log/iot.log

7.1.6.6.9 I am unable to see some column for IoT devices.

Display of columns in table is depending upon the ‘view’ option selected. Verify what ‘view’ option is selected.
If not sure, select ‘**All**’ option to display all columns.

7.1.6.6.10 I am not able to see enforcement status or update enforcement status of category.

Manual update of enforcement status is not allowed when automatic enforcement is enabled. Disable the automatic enforcement from settings, you will be able to see enforcement status column and can update the status manually.

7.1.6.6.11 Hierarchy not listed while creating custom category.

The listed category hierarchies that have been detected from the connected endpoint and displayed for selection.

7.1.6.6.12 Why enforcement is not applied to device endpoint.

Verify the automatic enforcement is **ON**.
Verify the endpoint mapped to correct category. Then try reconnecting the device.

7.1.6.6.13 UNP not getting updated after deleting UNP.

Disconnect the connected endpoint and reconnect.

21 Oct 2025

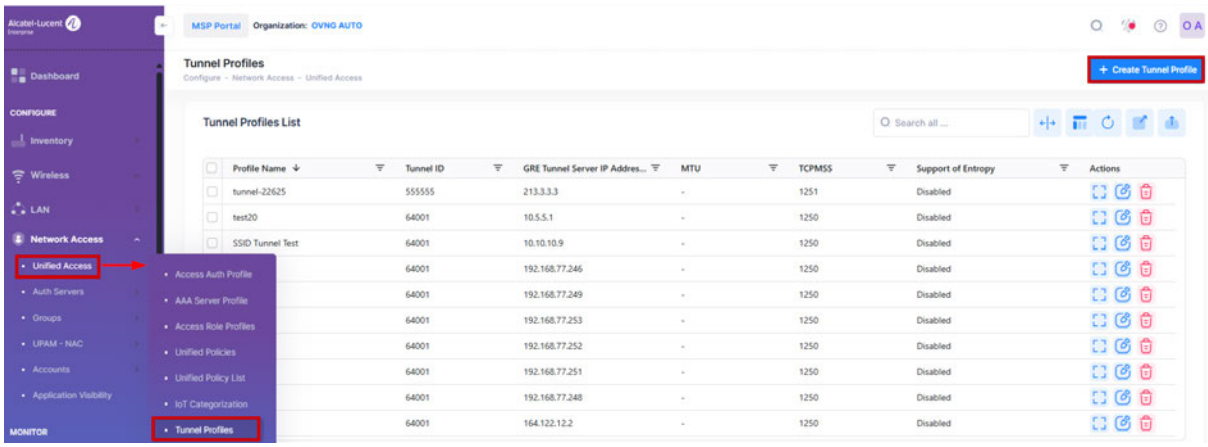
7.1.7 Tunnel Profiles

The Tunnel Profile Screen displays (see page 572)information about configured Tunnel Profiles and is used to create (see page 569), edit (see page 571), and delete (see page 574)GRE Tunnel Profiles or Data VPN Tunnel Profiles. A Tunnel Profile defines whether GRE or Data VPN encryption is used to securely forward traffic.

- A GRE Tunnel is typically used to tunnel Guest traffic from an AP to an AOS Switch. The AOS Switch acts as a Guest Tunnel Termination Switch.
- A Data VPN Tunnel is used to tunnel Guest traffic from an AP to a Data VPN Server.

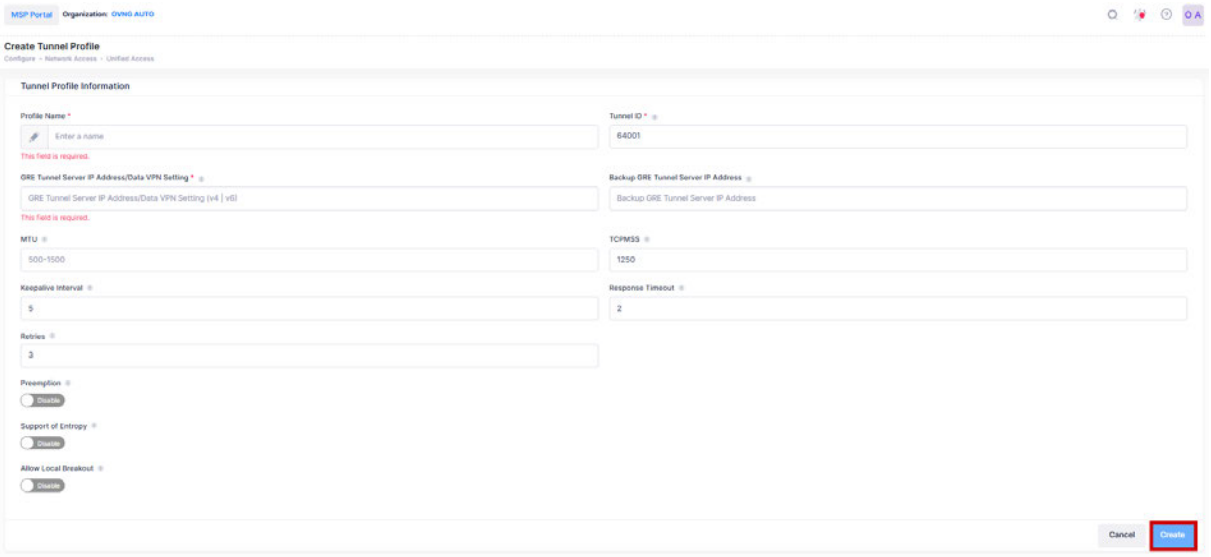
When you create an Access Role Profile to authenticate a Guest Client, you specify the Tunnel Profile to use for forwarding Client traffic that is mapped to the Access Role Profile.

To create a Tunnel Profile, navigate to the Tunnel Profile screen by clicking on **Network Access > Unified Access > Tunnel Profile** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Tunnel Profile screen displays.



7.1.7.1 Creating a Tunnel Profile

Click on **Create Tunnel Profile** and complete the fields as described below. When you are finished, click on the **Create** button. Each tunnel should have a unique Tunnel ID - GRE Tunnel Server/Data VPN Server pairing.



- **Profile Name -** The Tunnel Profile name.
- **Tunnel ID -** The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
- **GRE Tunnel Server IP Address/Data VPN Setting** - Enter the IP address of the Tunnel Termination Switch (GRE Tunnel Server) or select a Data VPN Server Setting (see page 414) from the drop-down list.
- **Backup GRE Tunnel Server IP Address** - The IP address of a backup GRE Tunnel Server to provide GRE tunnel redundancy between an AP and GRE Tunnel Server. Select a switch from the drop-down or enter an IP address. When the primary GRE Tunnel Server IP address goes down, the backup Tunnel Server takes over.
- **MTU -** Enter the MTU value. The recommended value is 1476 for RAW GRE and 1416 for GRE over wire guard interface. Leave it blank if you do not want to set a specific value.
- **TCPMSS** - The TCP Maximum Segment Size (TCP MSS) attribute can be used to control the maximum size of packets going out through a connection. Specifically, it will cause the AP and VPN Server to choose a smaller TCP window and frame size to avoid fragmentation as much as possible. This is especially useful for Dual-stack Lite(DS-Lite) ISP connections. You can configure or adjust the TCPMSS value on the Tunnel profile for Access Role configuration. The default value is 1250. The range is from 500 to 1460.
- **Keepalive Interval** - The time interval, in seconds, for APs to check the status of the far-end IP address for the GRE Tunnel Server. (Range = (2 to 5) seconds, Default = 5 seconds).
- **Response Timeout** - The amount of time, in seconds, to wait for a response from the GRE Tunnel Server to keepalive requests. (Default = 2 seconds).
- **Retries** - The number of times to retry after a failed Keepalive request. (Range = 3 - 5, Default = 3). A failover to the backup GRE Tunnel Server IP address occurs after the last retry has failed.
- **Preemption** - Enables/Disables whether to go back to the primary GRE Tunnel Server. (Default = Disabled). When enabled:
  - **Preemption Countdown Timer** - Specify the amount of time to wait, in seconds, after a failover to the backup GRE Tunnel Server before attempting to go back to the primary GRE

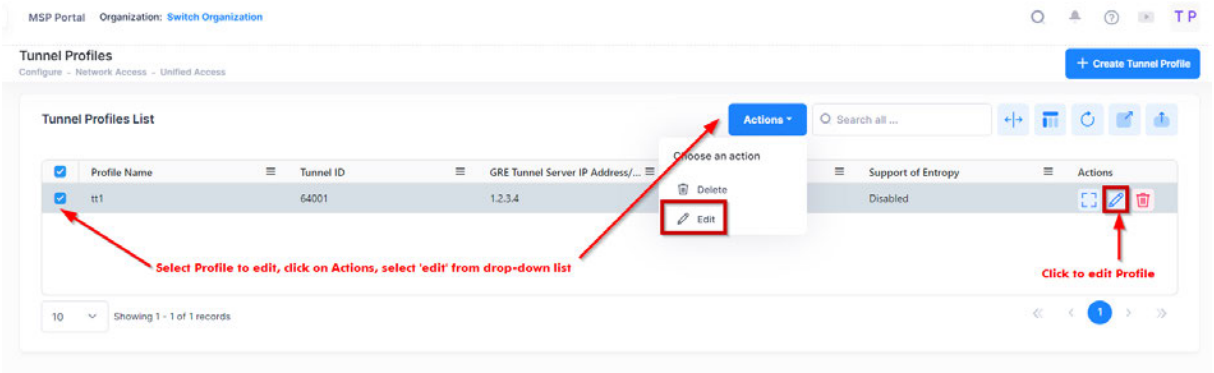
Tunnel Server. The countdown timer restarts on every switchover to the backup server. (Default = 300 seconds)

- **Support of Entropy -** Enables/Disables entropy. An ALE switch acting as a GRE Tunnel Server requires Entropy; however, some third-party GRE Tunnel Servers (e.g., Linux) do not require Entropy.
- **Allow Local Breakout -** Enables/Disables Local Breakout on the tunnel. If enabled, enter the Static Route(s) to be used for entering the Tunnel. All other traffic will go out through the local network. Make sure you have applied the relevant Data VPN Server to AP Groups in the SSID **before** choosing Data VPN Server as the Tunnel endpoint. To apply a Data VPN Server to an AP Group, go to the Provisioning Configuration (see page 313) (Inventory- Provisioning Configuration) associated with the AP Group and edit the Data VPN Setting. Note that only one VLAN inside the tunnel (tunnel ID different from 0 if tagged, 0 if untagged) can be enabled with Local Breakout.
  - **Static Routes -** Specify the static routes to be used for entering the tunnel. All other traffic will go out through the local network.
    - Avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the Tunnel. For example, if VLAN ID = 41 is specified to be carried within the Tunnel and if the network subnet that corresponds to VLAN 41 is 192.168.41.0, the AP will automatically set up this route and make sure traffic destined for 192.168.41.0 will enter the Tunnel. The AP will automatically set up this route and make sure traffic with VLAN ID = 41 will enter the Tunnel. **Do not specify an explicit Route** with Destination = 192.168.41.0, as that will confuse the AP and lead to poor performance.
    - The static routes specified will be accumulated on an AP across all SSIDs assigned to the AP. For example, if you have two SSIDs configured on the same AP and configure SSID1 to use Tunnel Profile T1 with Static Routes A and B, and configure SSID2 to use Tunnel Profile T2 with Static Routes C and D, all of the routes (A, B, C, and D) will be applicable for SSID 1 and SSID 2.
    - Across all of the routes applied on an AP from the different SSIDs, make sure any destination IP subnet is specified only once. Each route applied on an AP should be for a different IP subnet, even across the SSIDs. Also, avoid specifying static routes pertaining to the VLAN ID of the traffic that enters the tunnel. The AP will automatically set up such routes. If a route to IP subnet X already exists in an SSID and that SSID is applied to an AP, another route to the same IP subnet X must not be specified in the same or a different SSID that is applied to the same AP.

If you create two tunnel profiles with the same Remote IP and Tunnel ID, the "Support of Entropy" status **must** be the same on both tunnels (both must be "enabled" or "disabled"). Choose the value based on what use case you plan to deploy.

7.1.7.2 Editing a Tunnel Profile

Select the profile in the Tunnel Profile List and click on the Edit icon to bring up the Edit Tunnel Profile Screen. Edit the fields as described above then click on the **Save** button to save the changes. Note that you cannot edit the profile name.



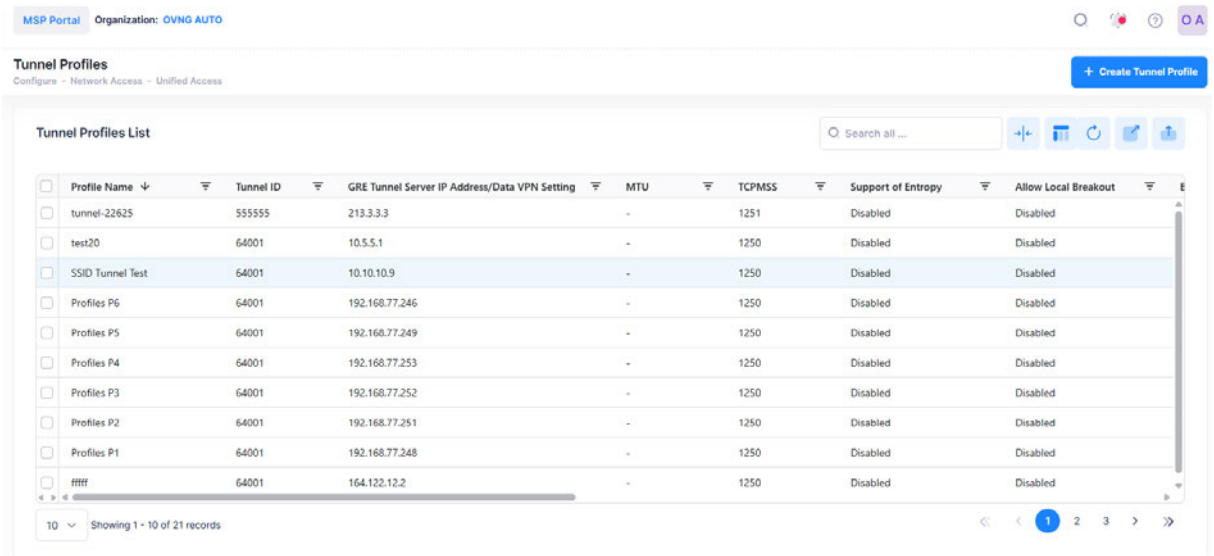
Use one of the following methods to access the Edit Tunnel Profile screen (as shown above):

- Select the profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the profile that you want to edit.

Edit the fields as described above (see page 570), then click on **Save**.

7.1.7.3 Display Information of a Tunnel Profile

The Tunnel Profiles list displays information for the configured Tunnel Profiles.

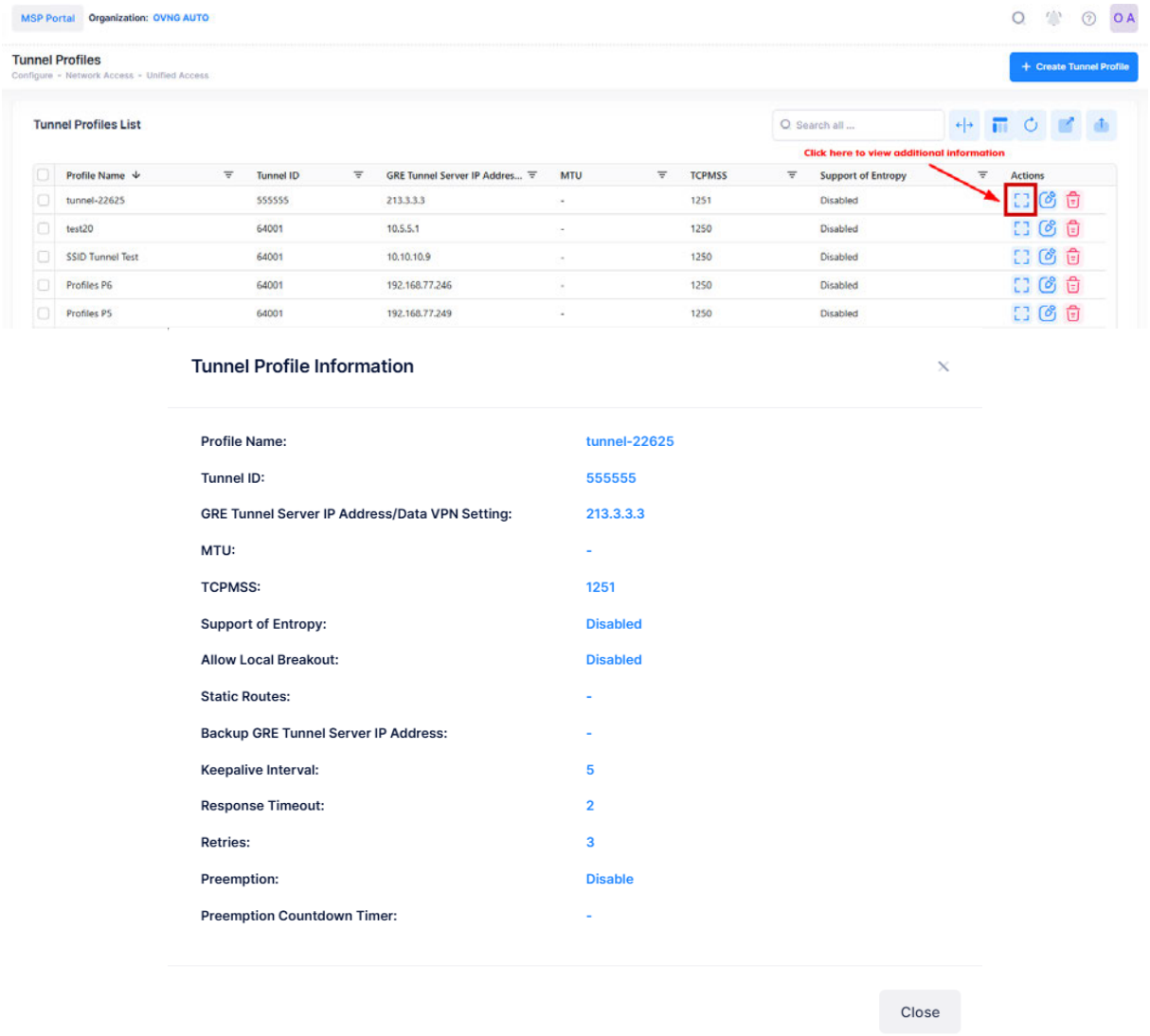


The following information is displayed. This screen also allows you to export, search and filter the data.

- **Profile Name** - The Tunnel Profile name.
- **Tunnel ID** - The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
- **GRE Tunnel Server IP Address/Data VPN Setting** - The IP address of the Tunnel Termination Switch (GRE Tunnel Server).
- **MTU** - The MTU value.

- **TCPMSS** - The TCPMSS value on the Tunnel profile for Access Role configuration. The default value is 1250. The range is from 500 to 1460.
- **Support of Entropy** - Enables/Disables entropy. An ALE switch acting as a GRE Tunnel Server requires Entropy; however, some third-party GRE Tunnel Servers (e.g., Linux) do not require Entropy.

You can click on Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



The following information is displayed for each Tunnel Profile:

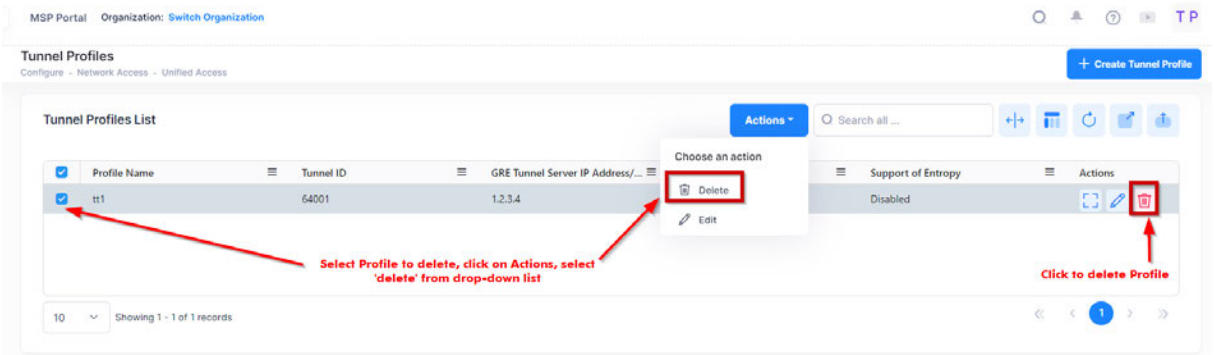
- **Profile Name** - The Tunnel Profile name.
- **Tunnel ID** - The VPN ID used for Access Role Profile mapping. (Range = 0 - 16777215, suggested range of 64001 - 65000). If the Tunnel ID is set to "0", no GRE Key is sent.
- **GRE Tunnel Server IP Address/Data VPN Setting** - The IP address of the Tunnel Termination Switch (GRE Tunnel Server).
- **MTU** - The MTU value.

- **TCPMSS** - The TCPMSS value on the Tunnel profile for Access Role configuration. The default value is 1250. The range is from 500 to 1460.
- **Support of Entropy** - Enables/Disables entropy. An ALE switch acting as a GRE Tunnel Server requires Entropy; however, some third-party GRE Tunnel Servers (e.g., Linux) do not require Entropy.
- **Allow Local Breakout** - Enables/Disables Local Breakout on the tunnel. If enabled, enter the Static Route(s) to be used for entering the Tunnel.
- **Static Routes -** Specify the static routes to be used for entering the tunnel. All other traffic will go out through the local network.
- **Backup GRE Tunnel Server IP Address** - The IP address of a backup GRE Tunnel Server to provide GRE tunnel redundancy between an AP and GRE Tunnel Server.
- **Keepalive Interval** - The time interval, in seconds, for APs to check the status of the far-end IP address for the GRE Tunnel Server. (Range = (2 to 5) seconds, Default = 5 seconds).
- **Response Timeout** - The amount of time, in seconds, to wait for a response from the GRE Tunnel Server to keepalive requests. (Default = 2 seconds).
- **Retries** - The number of times to retry after a failed Keepalive request. (Range = 3 - 5, Default = 3). A failover to the backup GRE Tunnel Server IP address occurs after the last retry has failed.
- **Preemption** - Enables/Disables whether to go back to the primary GRE Tunnel Server. (Default = Disabled).
- **Preemption Countdown Timer** - Specify the amount of time to wait, in seconds, after a failover to the backup GRE Tunnel Server before attempting to go back to the primary GRE Tunnel Server. The countdown timer restarts on every switchover to the backup server. (Default = 300 seconds).

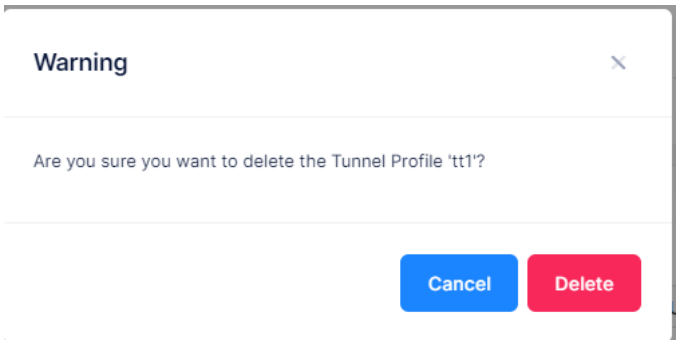
7.1.7.4 Deleting a Tunnel Profile

To delete a Tunnel Profile, use one of the following methods to select the profile you want to delete:

- Select the profile to delete by clicking on the checkbox next to the profile, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the profile that you want to delete.



When you select the profile you want to delete, the following confirmation prompt appears:



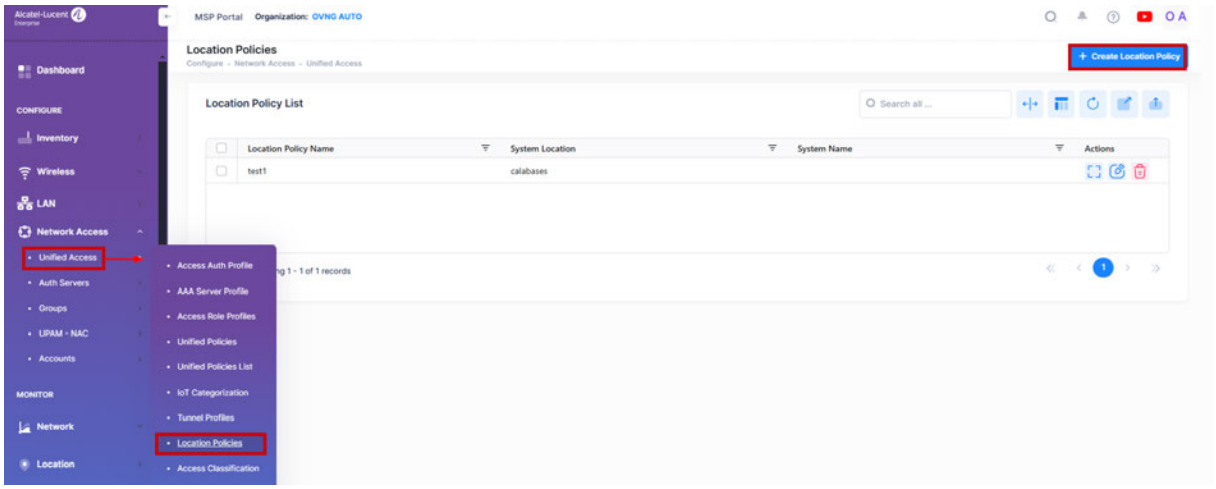
Click on **Delete** to confirm that you want to delete the Tunnel Profile.

21 Oct 2025

7.1.8 Location Policies

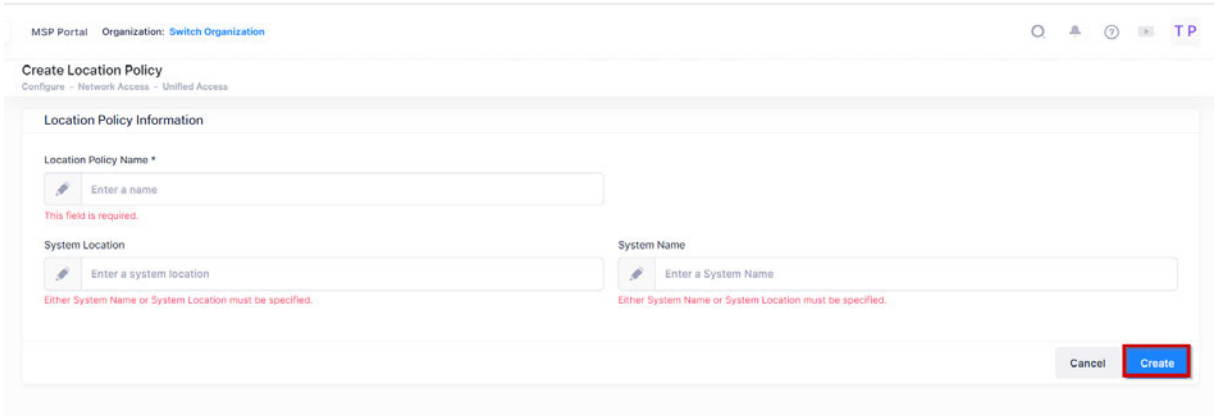
The Unified Profile Location Policy Screen displays all configured Location Policies that is used to **create** (see page 576), **edit** (see page 577), and **delete** (see page 577) Location Policies. A Location Policy defines a specific location where a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

To create a Location Policy, navigate to the Location Policy Information screen by clicking on **Network Access > Unified Access > Location Policies** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Location Policies Information screen displays.



7.1.8.1 Creating a location Policy

The Create Location Policy screen is used to configure the Location Policy Settings and Network Assignment settings for a location policy. To access the Create Location Policy screen, click on **Create Location Policy** at the top of the Location Policies screen, as shown above and complete the fields as described below.

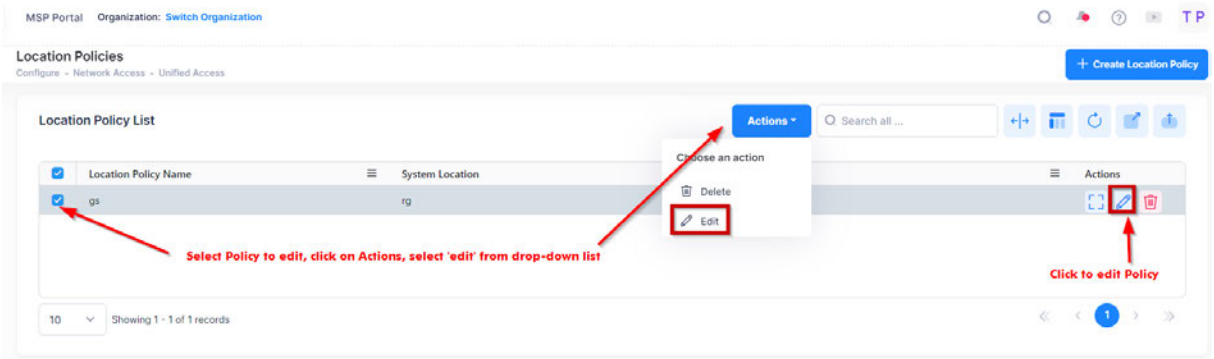


- **Location Policy Name** - User-configured Location Policy Name.
- **System Location** - The configured system location for the switch from which the device can access the network.
- **System Name** - The configured system name from which the device can access the network

When you are finished, click on the **Create** button.

7.1.8.2 Editing a Location Policy

Select the policy in the Location Policy List and click on the Edit icon to bring up the Edit Location Policy Screen.



Use one of the following methods to access the Edit Location Policy screen (as shown above):

- Select the policy to edit by clicking on the checkbox next to the policy, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the policy that you want to edit.

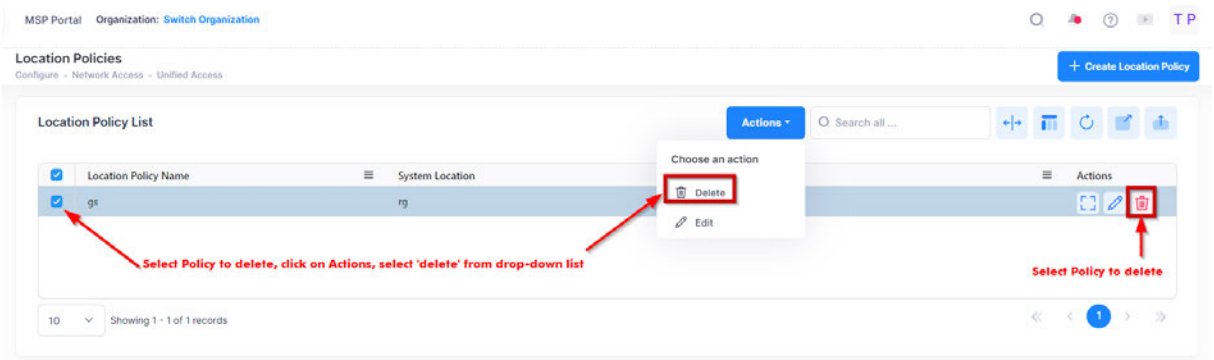
Edit the fields as described above (see page 576), then click on **Save**.

> **Note:** You cannot edit the policy name.

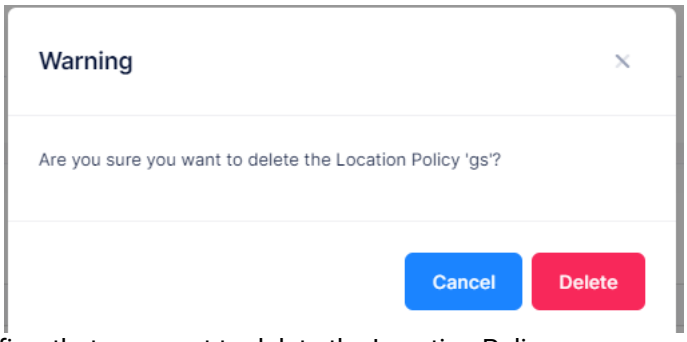
7.1.8.3 Deleting a Location Policy

To delete a Location Policy, use one of the following methods to select the policy you want to delete:

- Select the policy to delete by clicking on the checkbox next to the policy, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the policy that you want to delete.



When you select the policy you want to delete, the following confirmation prompt appears:



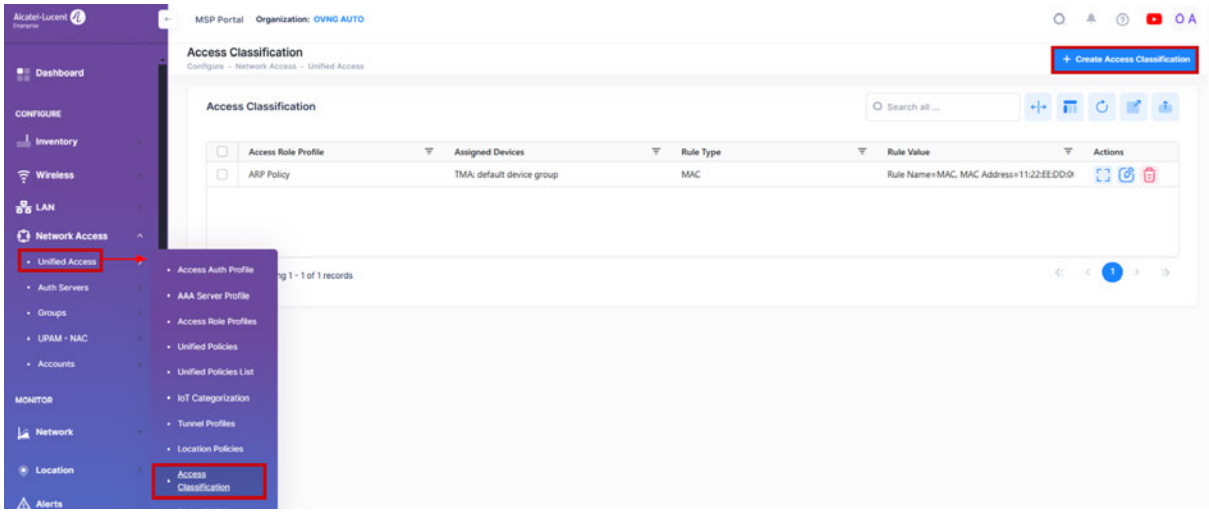
Click on **Delete** to confirm that you want to delete the Location Policy.

21 Oct 2025

7.1.9 Access Classification

Access Classification Rules are defined and associated with an Access Role Profile to provide an additional method for classifying a device into an Access Role Profile. If authentication is not available or does not return a profile name for whatever reason, Access Classification rules are applied to determine the profile assignment.

Use the Access Classification screen to display information (see page 583) about all Access Classification Rules configured for Access Role Profiles. This screen is also used to create (see page 579) edit (see page 581), and delete (see page 582) Access Classification Rules. To access the Access Classification screen, click on **Network Access > Unified Policies > Access Classification** under the "Configure" section of the OmniVista Terra Menu (see page 45).



7.1.9.1 Creating an Access Classification Rule

The Create a New Access Classification screen is used to select the type of rule (SSID or MAC address) to configure and assign the rule to an Access Role Profile and network devices. To access this screen, click on **Create Access Classification**.

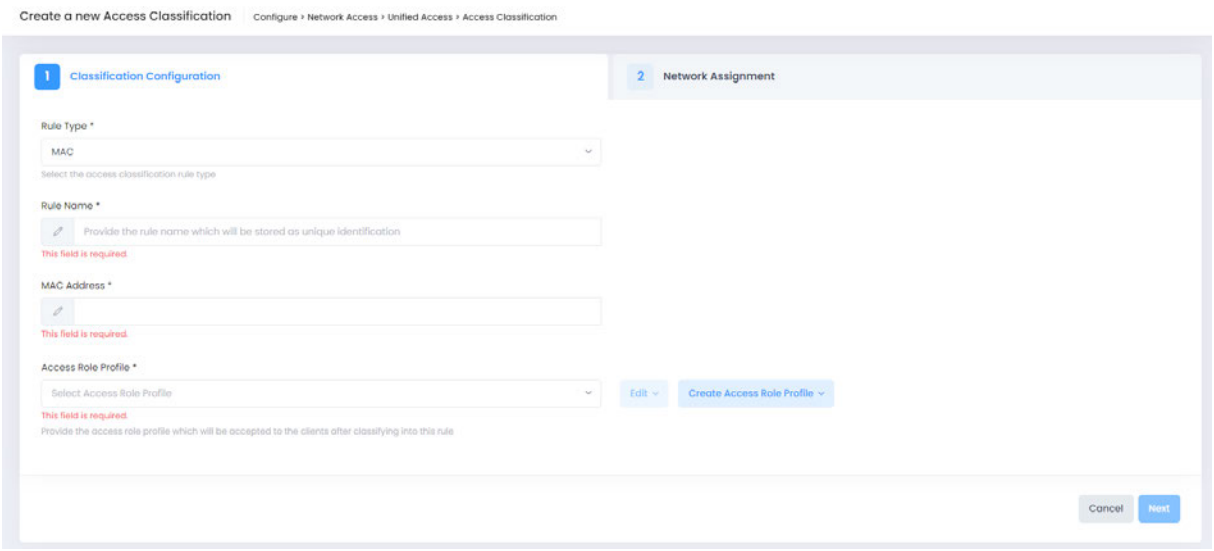
The Create a New Access Classification screen provides the following step-by-step process to create an an Access Classification Rule:

1. Classification Configuration (see page 579) - Specify the type of rule, a name for the rule, and the Access Role Profile to which the rule is assigned. The Access Role Profile is applied to traffic that matches the Access Classification Rule.

2. Network Assignment (see page 580) - Selects Access Point (AP) Groups from one or more Sites. The Access Classification Rule is applied to the APs in the selected Sites/AP groups.

7.1.9.1.1 1. Classification Configuration

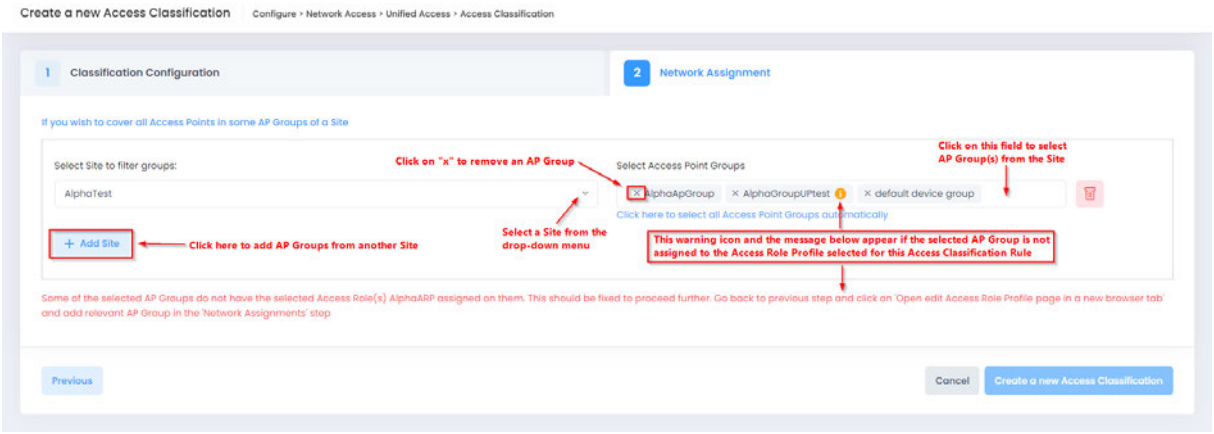
Complete the fields on the Classification Configuration tab, as described below, then click **Next** to go to the next tab (Step 2).



- **Rule Type** - Click on this field and select the type of rule to configure (MAC or SSID) from the drop-down menu.
  - **SSID** - Defines an SSID for the specified Access Role Profile. The specified Access Role Profile will be applied if the SSID of AP (which client is associating) matches with the defined SSID in the rule.
    - **SSID Value -** The SSID of AP.
  - **MAC** - Defines a MAC Address Access Classification Rule for the specified Access Role Profile. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified Access Role Profile is applied. Note that when a MAC Access Classification Rule is removed or modified, all MAC addresses classified with that rule are flushed.
    - **MAC Address** - The MAC address to use for the rule.
- **Rule Name** - Specify a name to identify the rule.
- **Access Role Profile** - Select an existing Access Role Profile to use for the rule from the drop-down menu or click on **Create Access Role Profile** to open the the Create Access Role Profile screen and create a new profile. You can also click on **Edit** to open the Edit Access Role Profile and make changes to the selected profile.

7.1.9.1.2 2. Network Assignment

The Network Assignments tab is used to select the AP Group(s) within a Site(s) to which the Access Classification rule will be applied to devices within those groups. Complete the network assignments as described below, then click **Create a New Access Classification**. The Access Classification Rule is created and used to determine the Access Role Profile assignment for a device.

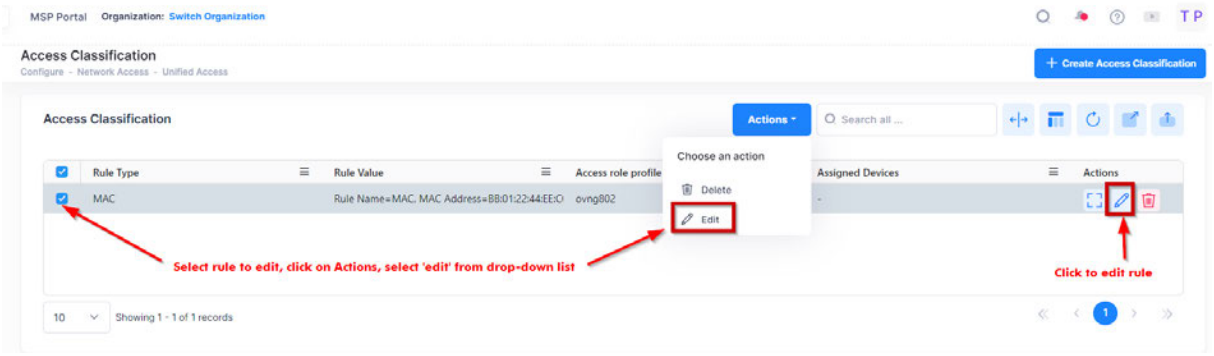


- **Select Site to Filter Groups** - Select the Site from which you want to select AP Group(s).
- **Select Access Point Groups** - Select the Access Point Group(s) associated with the selected Site. The Access Role Profile is applied to devices in the AP Group(s).

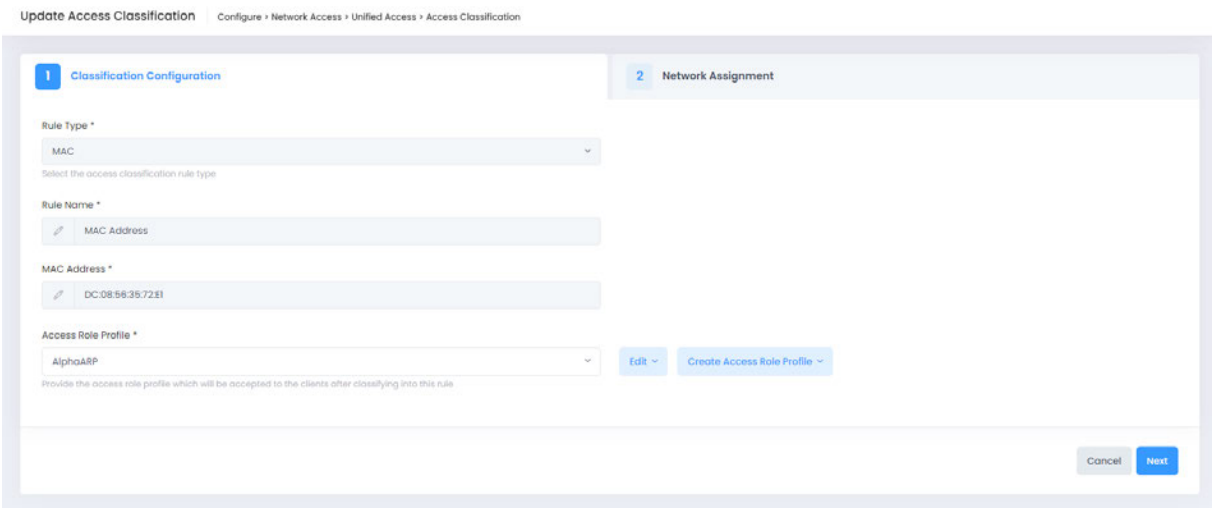
7.1.9.2 Editing an Access Classification Rule

You can edit the values for an existing Access Classification Rule by accessing the Update Access Classification screen. Use one of the following methods to access the Update Access Classification screen:

- Select the rule to edit by clicking o the checkbox next to the rule, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the rule that you want to edit.



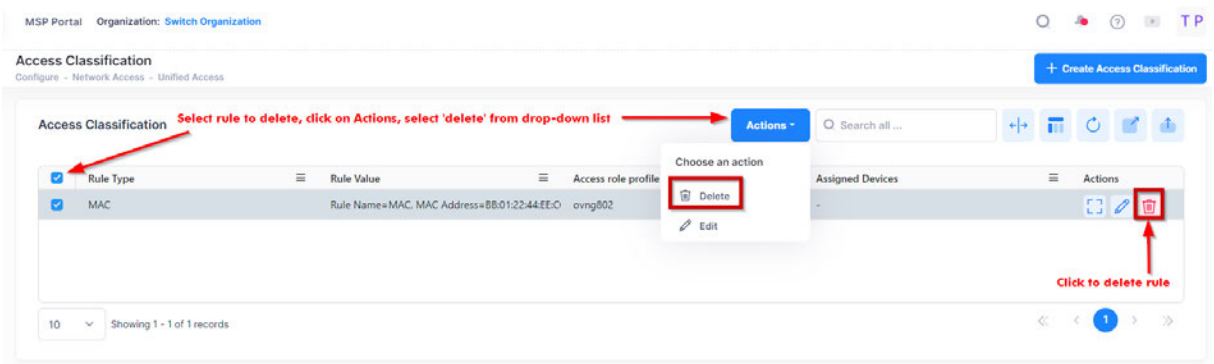
The following Update Access Classification screen displays. Edit the fields as described above (see page 579), then click on **Update Access Classification**.



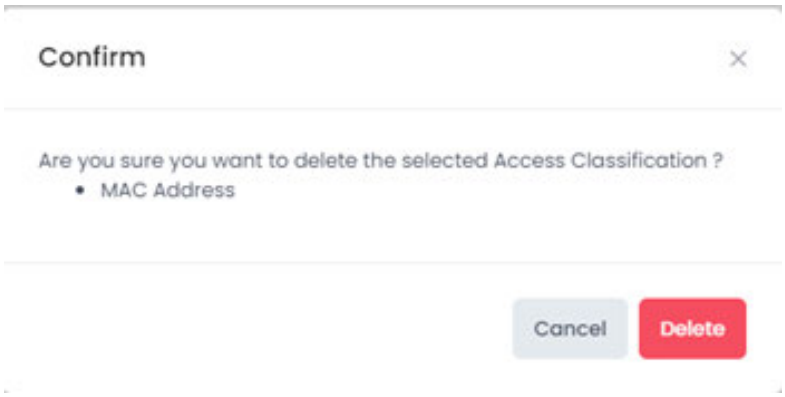
7.1.9.3 Deleting an Access Classification Rule

To delete an Access Classification Rule, use one of the following methods to select the rule that you want to delete:

- Select the rule to edit by clicking on the checkbox next to the rule, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the rule that you want to delete.



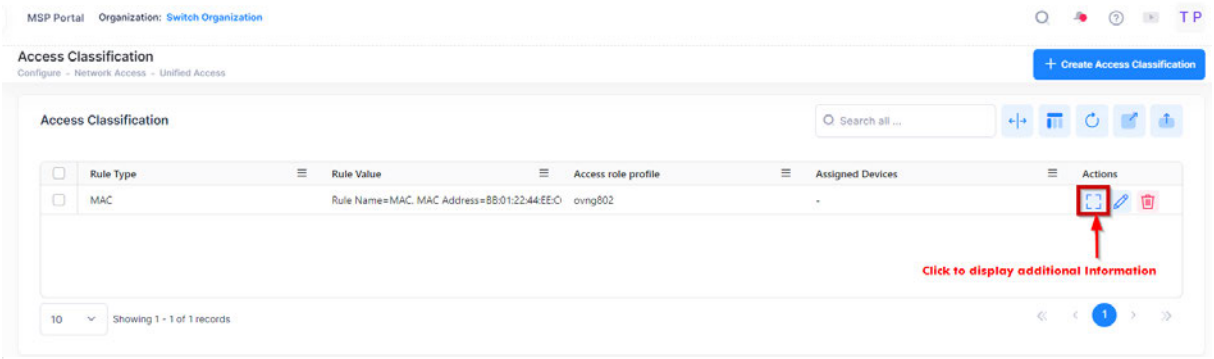
When you select the Access Classification Rule that you want to delete, the following confirmation prompt appears:

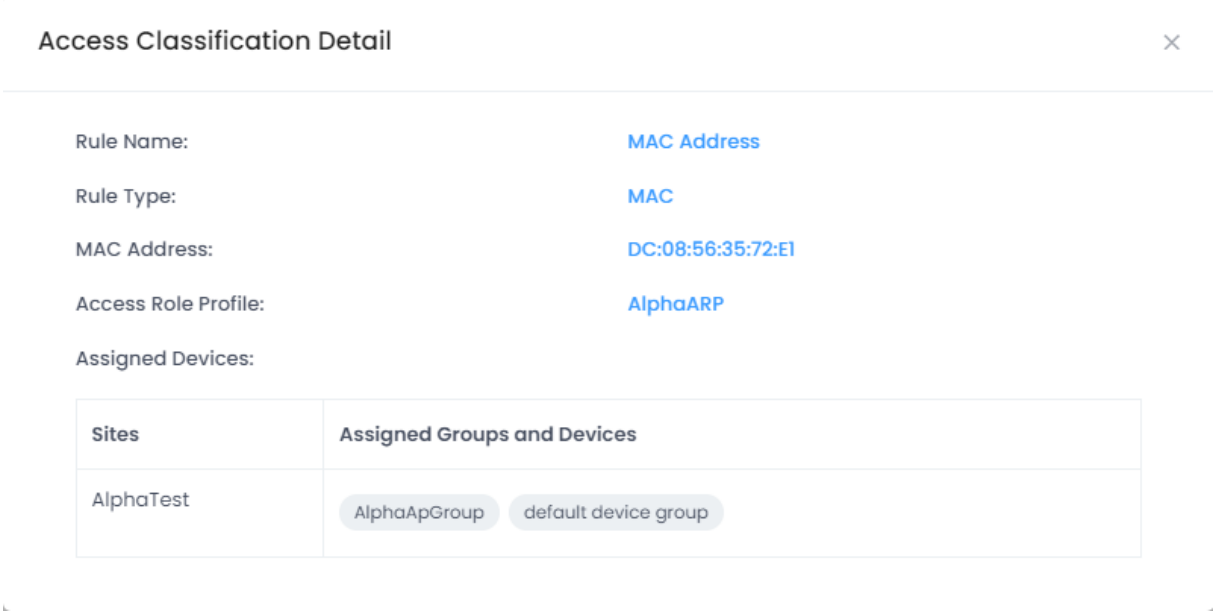


Click on **Delete** to confirm that you want to delete the selected rule(s).

7.1.9.4 Display Access Classification Detail

The Access Classification list displays information for the configured Access Classification Rules. To display detailed information about a specific rule, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.





The following information is displayed for each Access Classification Rule:

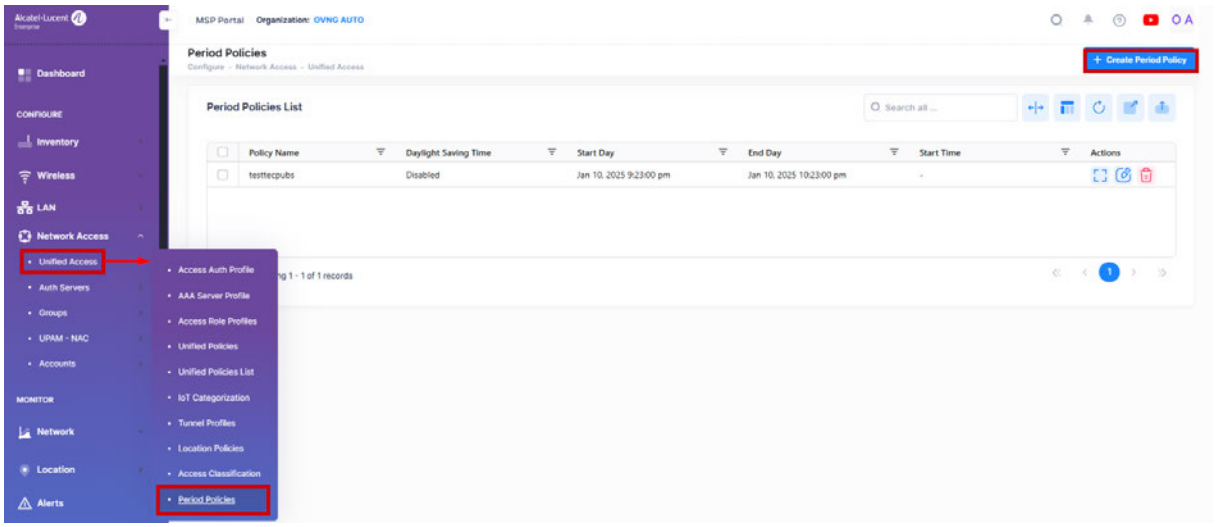
- **Rule Name** - The name assigned to identify the classification rule.
- **Rule Type** - The type of rule (MAC or SSID).
- **MAC Address** - If the rule type is set to MAC, this field displays the MAC address to match for this rule.
- **SSID** - If the rule type is SSID, this field displays the SSID to match for this rule.
- **Access Role Profile** - The name of the Access Role Profile assigned to this rule. The profile is applied to traffic that matches the classification rule parameters.
- **Assigned Devices** - The Organization Site(s) and AP Group(s) to which the Access Classification Rule is applied to devices within the selected groups.

21 Oct 2025

7.1.10 Period Policies

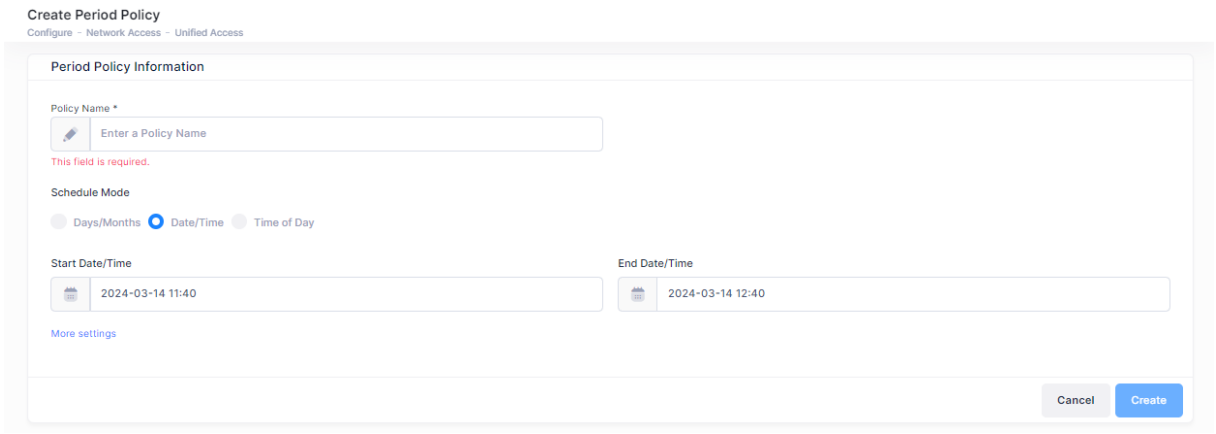
The Unified Access Period Policy screen displays all configured Period Policies and is used to **create** (see page 585), **edit** (see page 586), and **delete** (see page 587) Period Policies. A Period Policy specifies the days and times during which a device can access the network. The policy is associated with an Access Role Profile and applied to devices classified into the Access Role Profile.

To create a Period Policy, navigate to the Period Policy screen by clicking on **Network Access > Unified Access > Period Policies** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Period Policies Information screen displays.



7.1.10.1 Creating a Period Policy

Click on **Create Period Policy** and complete the fields as described below. When you are finished, click on **Create**.



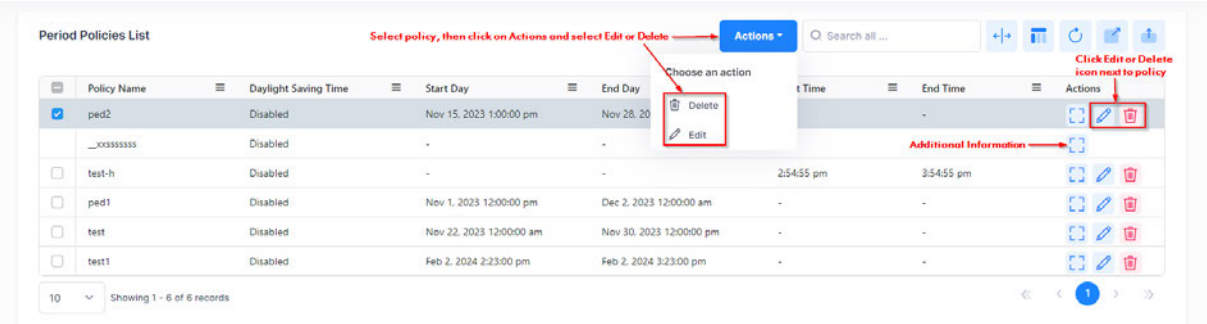
- **Policy Name -** User-configured Period Policy Name.
- **Scheduled Mode -** Configure the time schedule for the policy period. The time schedule determines when devices can access the network.
  - **Days/Months** - Select the days and months for the policy period.
  - **Date/Time** - Specify a start date/time and an end date/time during for the policy period.

- **Time of Day** - Specify a start and end date/time and the days/months for the policy period.

- **Timezone -** Select the timezone in which the Period Policy is active.
- **Daylight Saving Time -** Select to enable or disable daylight saving time.

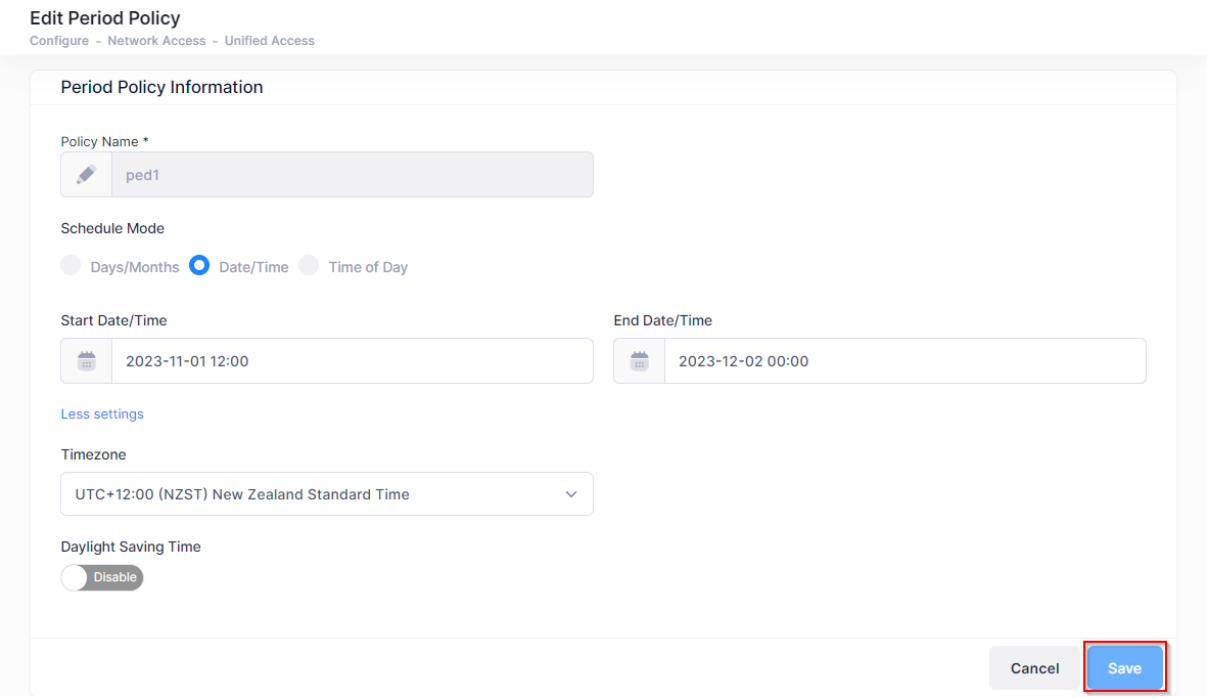
7.1.10.2 Editing/Deleting a Period Policy

You can edit (see page 586)or delete (see page 587)a Period Policy from the Period Policy List as shown below.



7.1.10.2.1 Editing a Period Policy

To modify a Period Policy, select an existing policy and click on the Edit icon under the “Actions” column or select Edit from the **Actions** drop-down menu to bring up the Edit Period Policy screen. Edit the fields as described above then click on **Save** to save the changes. Note that you cannot change the Period Policy name.

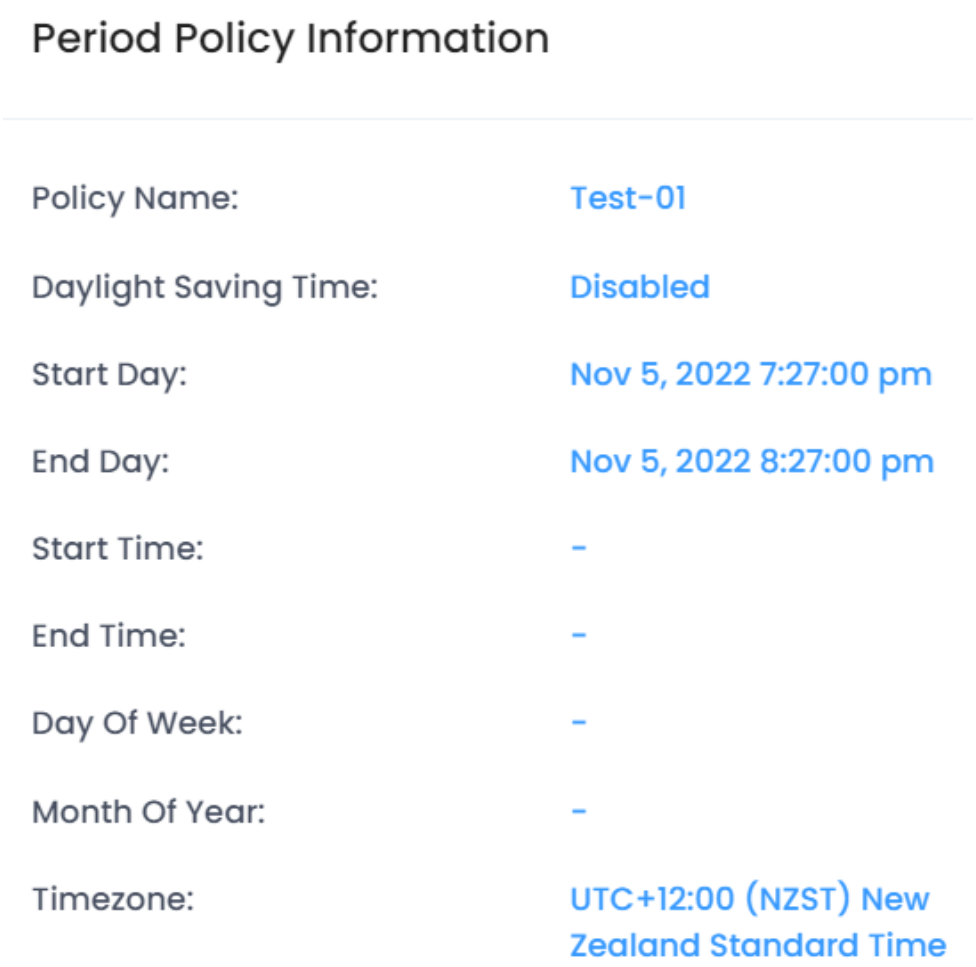


7.1.10.2.2 Deleting a Period Policy

To delete a Period Policy, select an existing policy and click on the Delete icon under the “Actions” column or select Delete from the **Actions** drop-down menu. You are then prompted with a Warning message to confirm your delete request. Click on **Delete** to confirm that you want to delete the Period Policy(s) listed in the Warning message.

7.1.10.3 View Additional Period Policy Information

Select the policy in the Period Policy List and click on the Additional Information icon to view additional information about the period policy.



21 Oct 2025

7.2 Authentication Servers

The Authentication Servers application enables you to create, modify, and delete authentication servers in OmniVista Terra. An authentication server could be an LDAP or RADIUS Server. Any authentication server that you want to use, other than the default OmniVista LDAP Server or the default UPAM RADIUS Server, must be added to OmniVista. Adding a server to OmniVista basically informs OmniVista that the server exists. OmniVista does not search the network to locate available authentication servers, so any server that you add to OmniVista should actually exist (or should exist in the near future). When you add a server, you can also specify other information such as:

- Operating parameters for devices that will use the server for authentication, such as the number of retries the device will attempt while communicating with the server.
- The user name and password used to login to the server (if applicable).
- The location of the server to be used as a "backup" server if the added server becomes unavailable.

To access the Authentication Servers application, navigate to **Network Access > Auth Servers** under the “Configure” section of the OmniVista Terra Menu (see page 45), then select one of the following Authentication Servers:

- RADIUS Servers (see page 589) - Displays information about all RADIUS Servers known to OmniVista Terra. You can also use this screen to add, edit, and delete RADIUS Servers.
- LDAP Servers (see page 597) - Displays information about all Lightweight Directory Access Protocol (LDAP) Servers known to OmniVista Terra. You can also use this screen to add, edit, and delete LDAP Servers.

21 Oct 2025

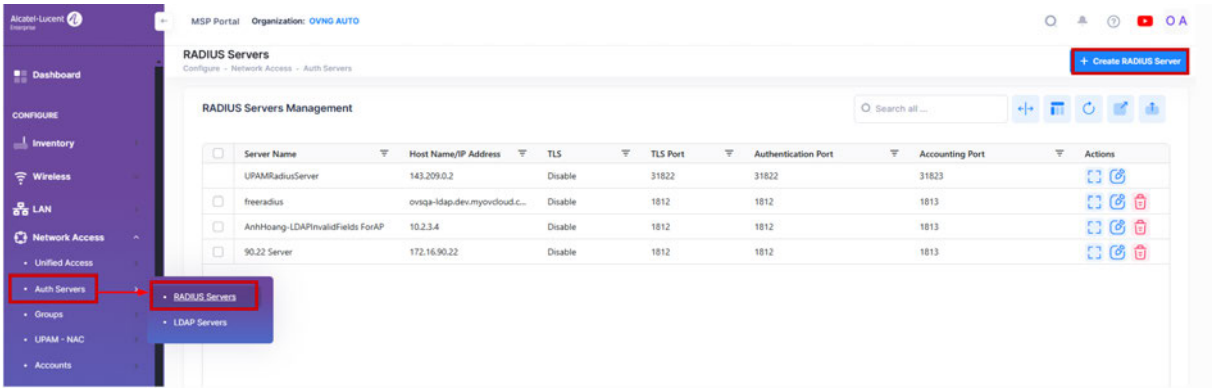
7.2.1 RADIUS Server Management

The Authentication Servers RADIUS Server Management screen displays all RADIUS Servers known to OmniVista Terra. It also enables you to add (see page 589), edit (see page 592), and delete (see page 595) RADIUS Servers from the list of RADIUS Servers known to OmniVista Terra. A built-in RADIUS Client is available on the device. A RADIUS Server that supports Vendor Specific Attributes (VSAs) is required. VSAs carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. Refer to "Managing Authentication Servers" in your Network Configuration Guide for specific information on the VSAs required. Before you add a RADIUS Server to the list of RADIUS Servers known to OmniVista, you must first install and configure the RADIUS Server.

- You cannot add, modify, or delete users and user privileges from RADIUS Servers in OmniVista Terra.
- RADIUS Server Management supports both Switch and wireless devices; however certain attributes may not be supported on wireless devices. See the configuration fields below (see page 589) for more information.
- If you change the Shared Secret of the UPAM RADIUS Server, then you must also update the Shared Secret of the NAS Clients (see page 663). The UPAM RADIUS Server and the NAS Clients must use the same Shared Secret.
- OmniVista Terra converts an IPv6 address to its compressed form before saving the address to the database.

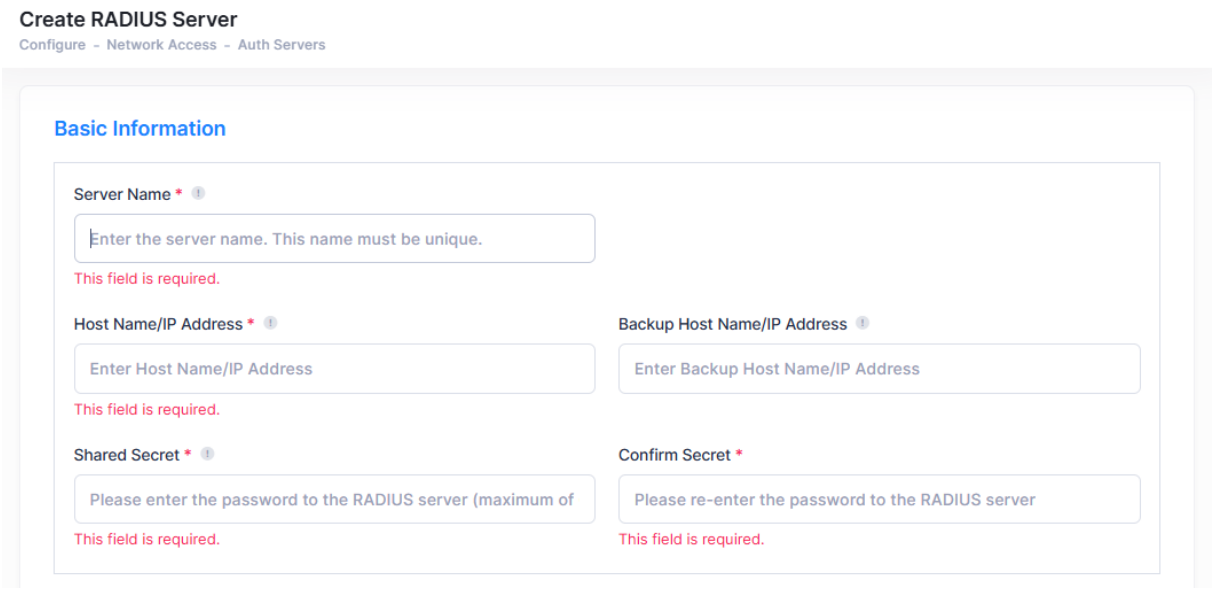
7.2.1.1 Adding a RADIUS Server

After configuring a RADIUS Server, you must add it to the list of RADIUS Servers known to OmniVista Terra. To add a new RADIUS Server, navigate to the RADIUS Servers Management screen by clicking on **Network Access > Auth Servers > RADIUS Servers** under the “Configure” section of the OmniVista Terra Menu (see page 45). The RADIUS Servers Management screen displays.



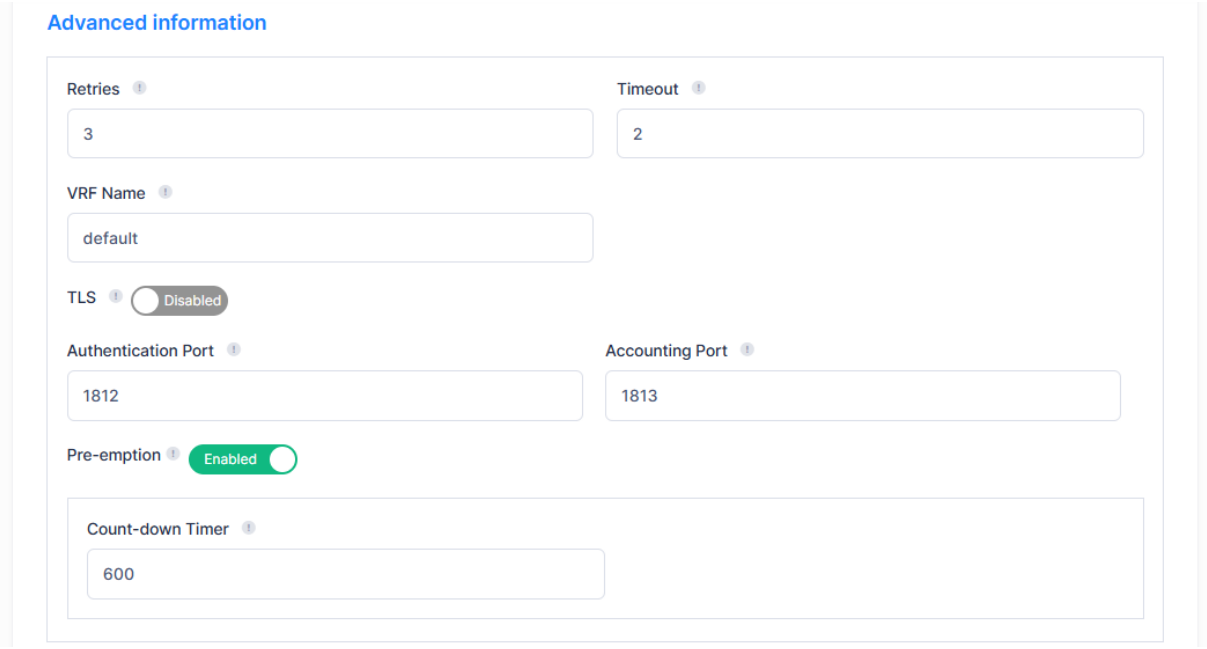
A default RADIUS Server (“UPAMRadiusServer”) is provided for OmniVista UPAM RADIUS authentication. You can edit the information for this server, but you cannot delete the server entry.

To add a new RADIUS Server, click on **Create RADIUS Server** and complete the fields as described below. When you are finished, click on **Create**.



7.2.1.1.1 Basic Information

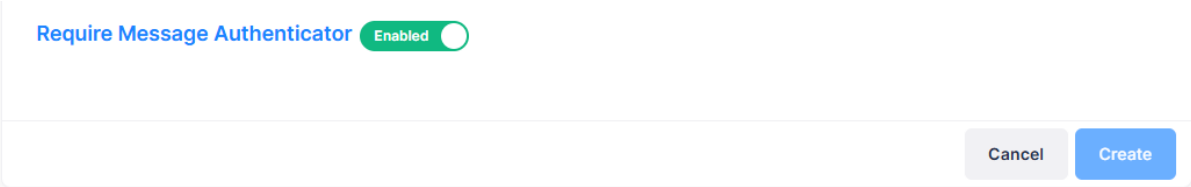
- **Server Name -** Unique name for the RADIUS Server. This name will be used by OmniVista and the device to identify the Server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the Server is located.
- **Backup Host Name/IP Address -** Each RADIUS Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup Server is located.
- **Shared Secret -** The password to the RADIUS Server (AP: 1-64 characters, Switch: 1-63 characters). The "Shared Secret" is essentially the server password. Note that the password you enter must be configured identically on the RADIUS Server. In addition, if you use a remote RADIUS Server with a Shared Secret greater than 16 characters, OmniVista only supports PAP and CHAP authentication.
- **Confirm Secret -** Re-enter the Shared Secret.



7.2.1.1.2 Advanced Information

- **Retries -** The number of retries that you want the device to attempt when trying to contact the RADIUS Server (AP Range = 1-3, Switch Range = 1-32, Default = 3).
- **Timeout** - The number of seconds that you want the device to wait before a request to the RADIUS Server is timed out (Range = 1 - 30, Default = 2).
- **VRF Name** - The name of the VRF instance associated with the RADIUS Server, if applicable. A RADIUS Server can be configured on any VRF instance including the default VRF instance. However, all of the servers (for example, all the RADIUS servers) must reside on the same VRF instance. Default value is "default". (Not supported on wireless devices and ignored when applied to those devices.)
- **TLS** - Enable/disable the use of the Transport Layer Security encryption method. Enable the TLS option to allow the RADIUS Server to use RadSec (RADIUS-over-TLS). Note that an AP can only support one RadSec Server. If you set up multiple RadSec (TLS-Enabled Radius) servers in OmniVista, make sure that all SSIDs within an AP Group are configured to use the same RadSec server. In addition, an AP does not support MAC authentication or External Captive Portal using RadSec. (Applies only to Access Point configuration.)
  - **TLS Port** - The TLS port number for the RADIUS Server (Range = 1 - 65535, Default = 2083).
- **Authentication Port -** The port to access the Server (Range = 1 - 65535, Default = 1812).
- **Accounting Port -** The port for accounting information (Range = 1 - 65535, Default = 1813).
- **Pre-emption -** If Pre-emption is enabled, the device will switch back to primary RADIUS server at the end of Count-Down Timer. If Pre-emption is disabled, then the device will switch to use the primary RADIUS server only if the backup RADIUS server is timed out. By default Pre-emption is Enabled. (Applies only to Access Point configuration.)

- **Count-down Timer -** Enter the number of seconds for the device to adhere with the Secondary server, before moving back to Primary (Default is 600 seconds). (Applies only to Access Point configuration.)



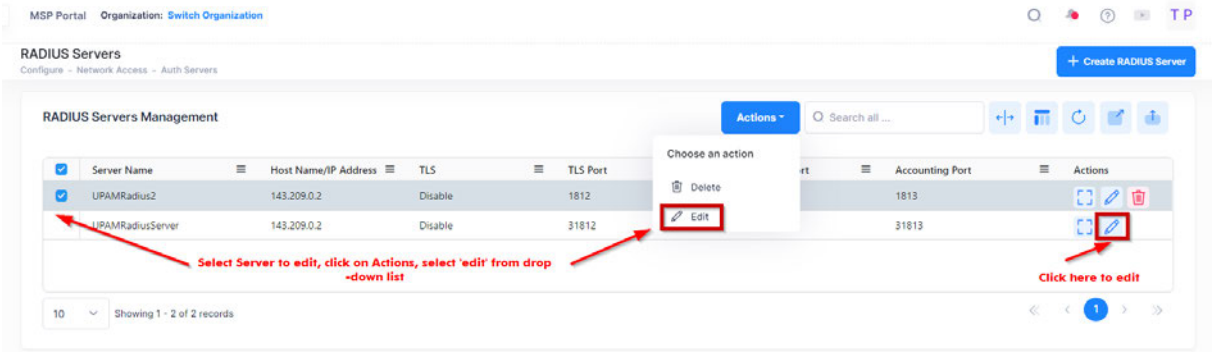
7.2.1.1.3 Require Message Authenticator

- **Require Message Authenticator** - Enables/Disables checking for the Message-Authenticator attribute in RADIUS response packets coming from the RADIUS Authentication server. Enabling the Require Message Authenticator check is the recommended setting to prevent attempts to forge authentication responses by spoofing UDP-based RADIUS response packets. Checking for this attribute is also configurable when defining a UPAM NAS Client and a UPAM External RADIUS server. Refer to Require Message Authenticator Use Cases (see page 704) for more information.
  - **Enabled** - Checks for the Message-Authenticator attribute and drops any response packets that do not contain this attribute. Access Points running >= AWOS 5.0.2 check for the Message-Authenticator attribute; however, you must use the **aaa radius message-authenticator** CLI command to enable an OmniSwitch to check for this attribute.
  - **Disabled** - Does not check for the Message-Authenticator attribute in RADIUS response packets. Note that this attribute is not checked by Access Points running less than AWOS 5.0.2.

- If the TLS option is enabled for the RADIUS Server, the Require Message Authenticator option is not available.
- Require Message Authenticator is:
  - enabled by default when you are adding a RADIUS Server.
  - enabled for the existing UPAMRadiusServer on a fresh installation.
  - disabled by default for existing servers that were created in OVC 10.4.3. This ensures that devices managed in OVC 10.4.3 can still pass RADIUS authentication after an upgrade to OVT 10.5.1.

7.2.1.2 Editing a Radius Server

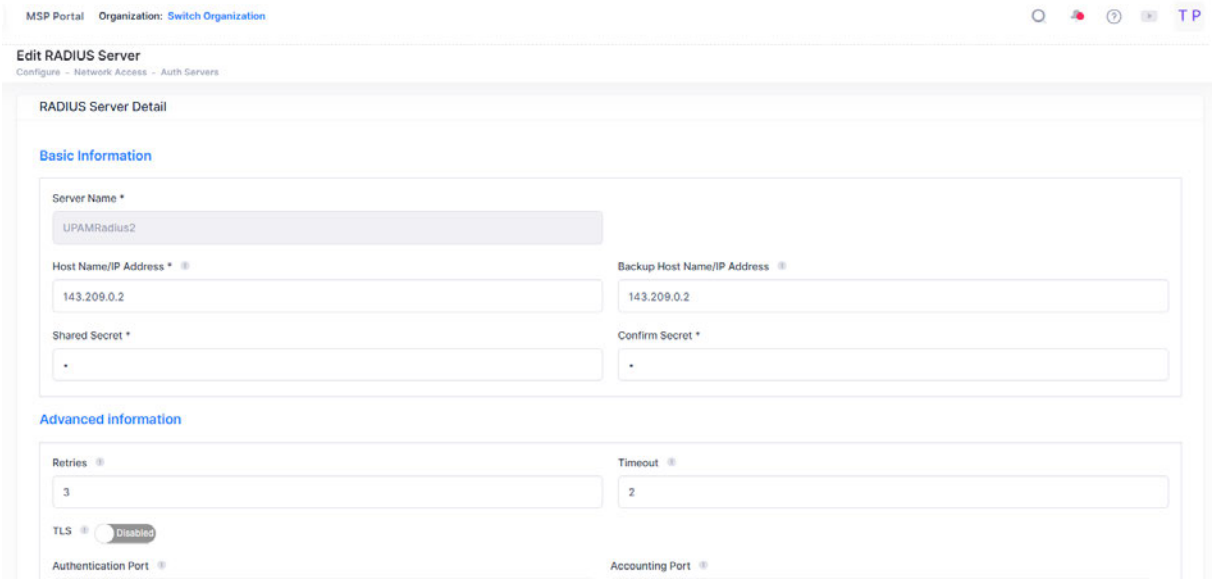
Select a RADIUS Server in the list and click on the Edit icon. It is important to note that you cannot modify values indiscriminately. The values must match those of the actual RADIUS Server. For example, if you want to change the RADIUS Authentication port, you must first use the tools provided by your RADIUS Server's vendor to change the port on the RADIUS Server itself. You can then inform OmniVista that the port number has changed by modifying the **Authentication Port** field.



Use one of the following methods to access the Edit RADIUS Servers screen (as shown above):

- Select the server to edit by clicking on the checkbox next to the server name, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the server name that you want to edit.

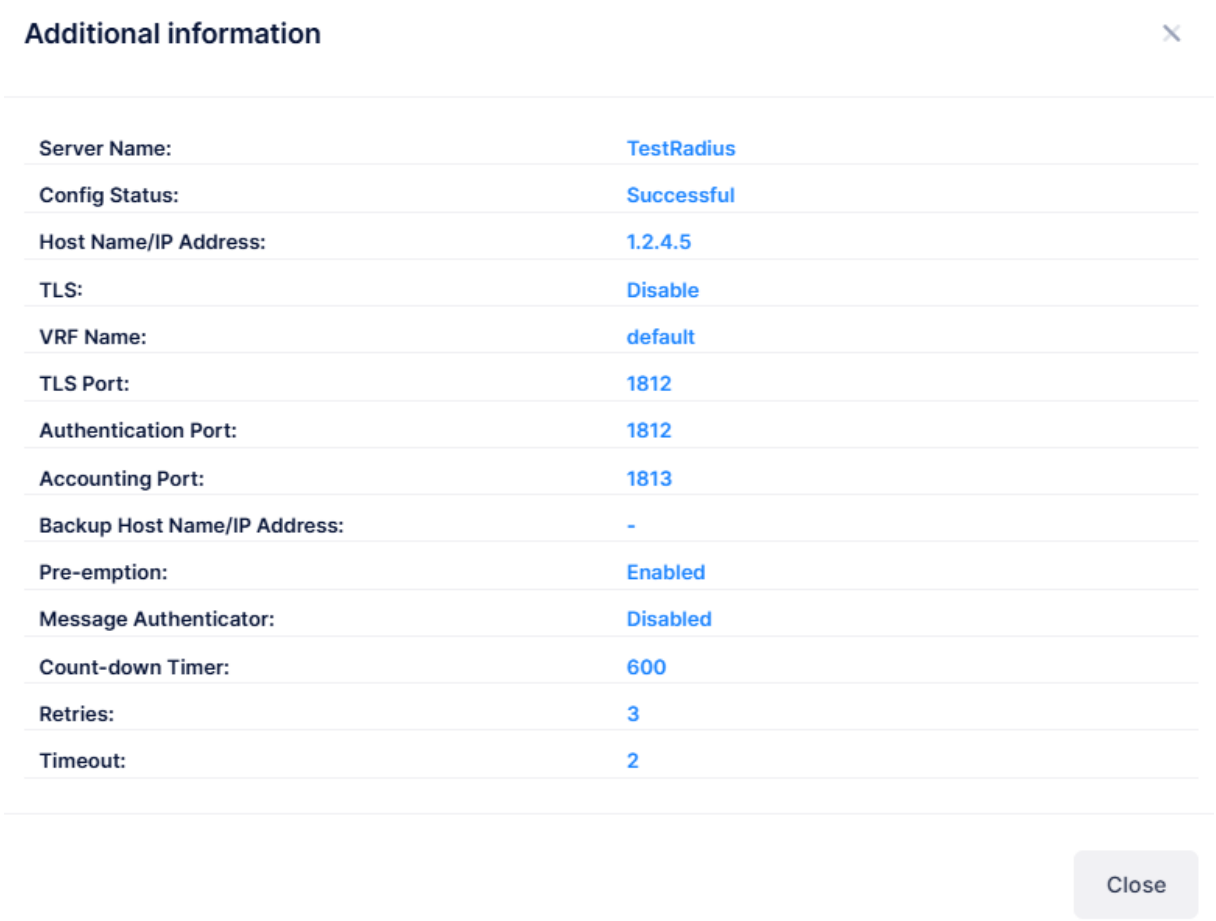
The following Edit RADIUS Server screen displays. Edit the fields as described above (see page 589), then click on **Save**.



A default “UPAMRadiusServer” is provided. This default server cannot be deleted. In addition, you **can not** enable TLS on this server. This functionality is not needed between an AP and the UPAM RADIUS Server.

7.2.1.3 View Additional RADIUS Server Information

Select the RADIUS Server in the list and click on the Additional Information icon to view additional information about the selected RADIUS Server.



- **Server Name** - Unique name for the RADIUS Server. This name will be used by OmniVista and the switch to identify the Server.
- **Config Status** - The configuration status of the RADIUS Server.
- **Host Name/IP Address** - The name of the computer where the server is located OR the IP address of the computer where the Server is located.
- **TLS** - Whether the TLS encryption method is enabled or disabled.**Authentication Port** - The port you to access the Server (Range = 1 - 65535, Default = 1812).
- **VRF Name** - The name of the VRF instance associated with the RADIUS Server.
- **TLS Port** - The TLS port number, when TLS is enabled.
- **Authentication Port** - The port to access the RADIUS Server.
- **Accounting Port** - The port for accounting information (Range = 1 - 65535, Default = 1813).
- **Backup Host Name/IP Address -** Each RADIUS Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup Server is located. (Not supported on wireless devices and ignored when applied to those devices.)
- **Pre-emption -** If Pre-emption is enabled, Access Point (AP) will switch back to primary RADIUS server at the end of Count-Down Timer. If Pre-emption is disabled, then AP will switch to use the

primary RADIUS server only if the backup RADIUS server is timed out. By default Pre-emption is Enabled.

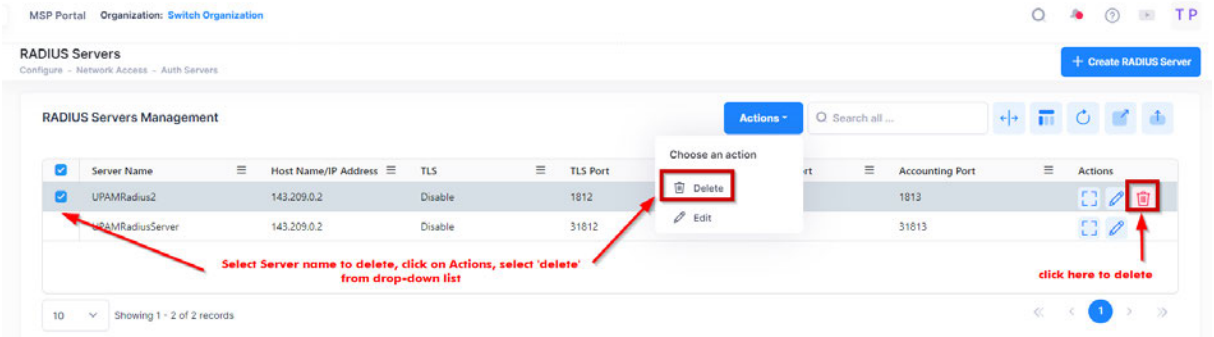
- **Message Authenticator** - Whether the check for the Message-Authenticator attribute in RADIUS response packets is enabled or disabled.
- **Count-down Timer -** The number of seconds for the AP to adhere with the Secondary server, before moving back to Primary (Default is 600 seconds).
- **Retries -** The number of retries that you want the switch to attempt when trying to contact the RADIUS Server (AP Range = 1-3, Switch Range = 1-32, Default = 3).
- **Timeout -** The number of seconds that you want the switch to wait before a request to the RADIUS Server is timed out (Range = 1 - 30, Default = 2).

7.2.1.4 Deleting a RADIUS Server

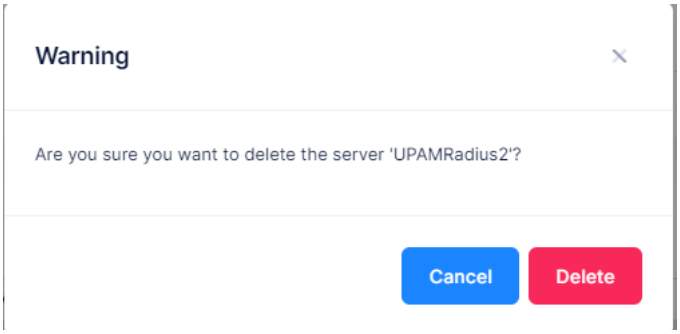
To delete a RADIUS Server, use one of the following methods to select the Server Name you want to delete:

- Select the RADIUS Server to delete by clicking on the checkbox next to the server name, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the server name that you want to delete.

Note that when deleting an RADIUS Server known to OmniVista Terra, it will send a delete alert message to the Switch if it has not been used in another profile.



When you select the server you want to delete, the following confirmation prompt appears:



Click on **Delete** to confirm that you want to delete the RADIUS Server.

21 Oct 2025

7.2.2 LDAP Servers Management

Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The protocol was developed as a way to use directory services over TCP/IP and to simplify the Directory Access Protocol (DAP) defined as part of the Open Systems Interconnection (OSI) effort. Originally, LDAP was a front-end for X.500 DAP.

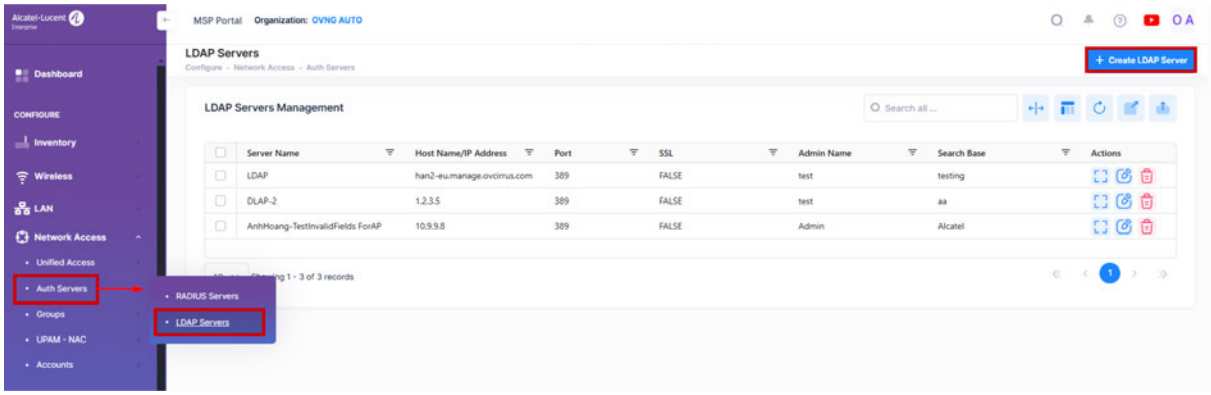
The LDAP protocol synchronizes and governs the communications between the LDAP Client and the LDAP Server. The protocol also dictates how database information, which is normally stored in hierarchical form, is searched from the root directory down to distinct entries. In addition, LDAP has its own format that permits LDAP-enabled Web browsers to perform directory searches over TCP/IP.

The OmniVista Terra LDAP Server is automatically installed in OmniVista Terra. You cannot modify or delete it. However, if you want to use a different LDAP V3 server, you must add it to OmniVista Terra. OmniVista Terra only manages the built-in LDAP Server, other authentication servers must be managed outside of OmniVista. You can assign devices to such servers, but the Authentication Servers application does not allow you to add, modify, or delete users and user privileges in the LDAP database of such servers. This is because an LDAP Server's database must be configured for the specific schema used to manage users and there is no public API for configuring LDAP schemas.

- LDAP Server Management supports both Switch and wireless devices; however, certain attributes may not be supported on wireless devices. See the configuration fields below for more information.
- OmniVista Terra converts an IPv6 address to its compressed form before saving the address to the database.

The LDAP Servers Management screen displays (see page 600)all LDAP Authentication Servers known to OmniVista. It also enables you to add (see page 598), modify (see page 601), and delete (see page 602)LDAP Servers from the list of LDAP Servers.

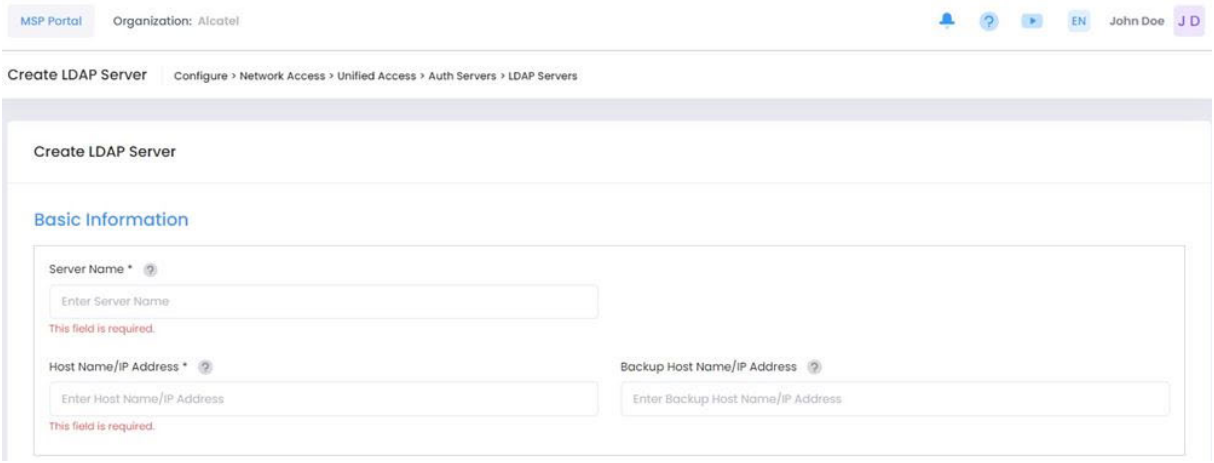
To access the LDAP Servers Management screen, click on **Network Access > Auth Servers > LDAP Servers** under the “Configure” section of the OmniVista Terra Menu (see page 45). The LDAP Servers Management screen displays.



7.2.2.1 Adding an LDAP Server

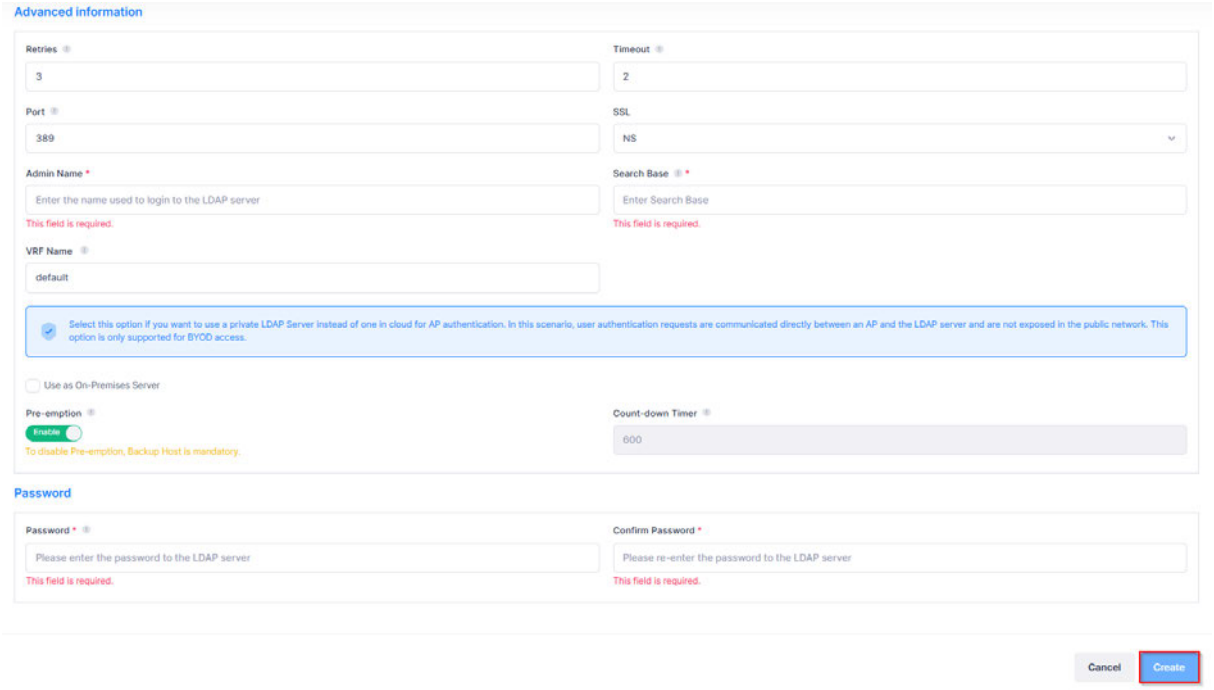
The OmniVista Terra LDAP Server is automatically installed in OmniVista Terra and known to OmniVista Terra. However, if you have configured a new LDAP Server, you must add it to the list of LDAP Servers known to OmniVista Terra.

To add a new LDAP Server, click on **Create LDAP Server** and complete the fields as described below. When you are finished, click on **Create** to add the new LDAP Server.



7.2.2.1.1 Basic Information

- **Server Name -** A unique name for the LDAP Authentication Server. This name will be used by OmniVista and the device to identify the server.
- **Host Name/IP Address -** The name of the computer where the server is located OR the IP address of the computer where the server is located.
- **Backup Host Name/IP Address -** Each LDAP Server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.



7.2.2.1.2 Advanced Information

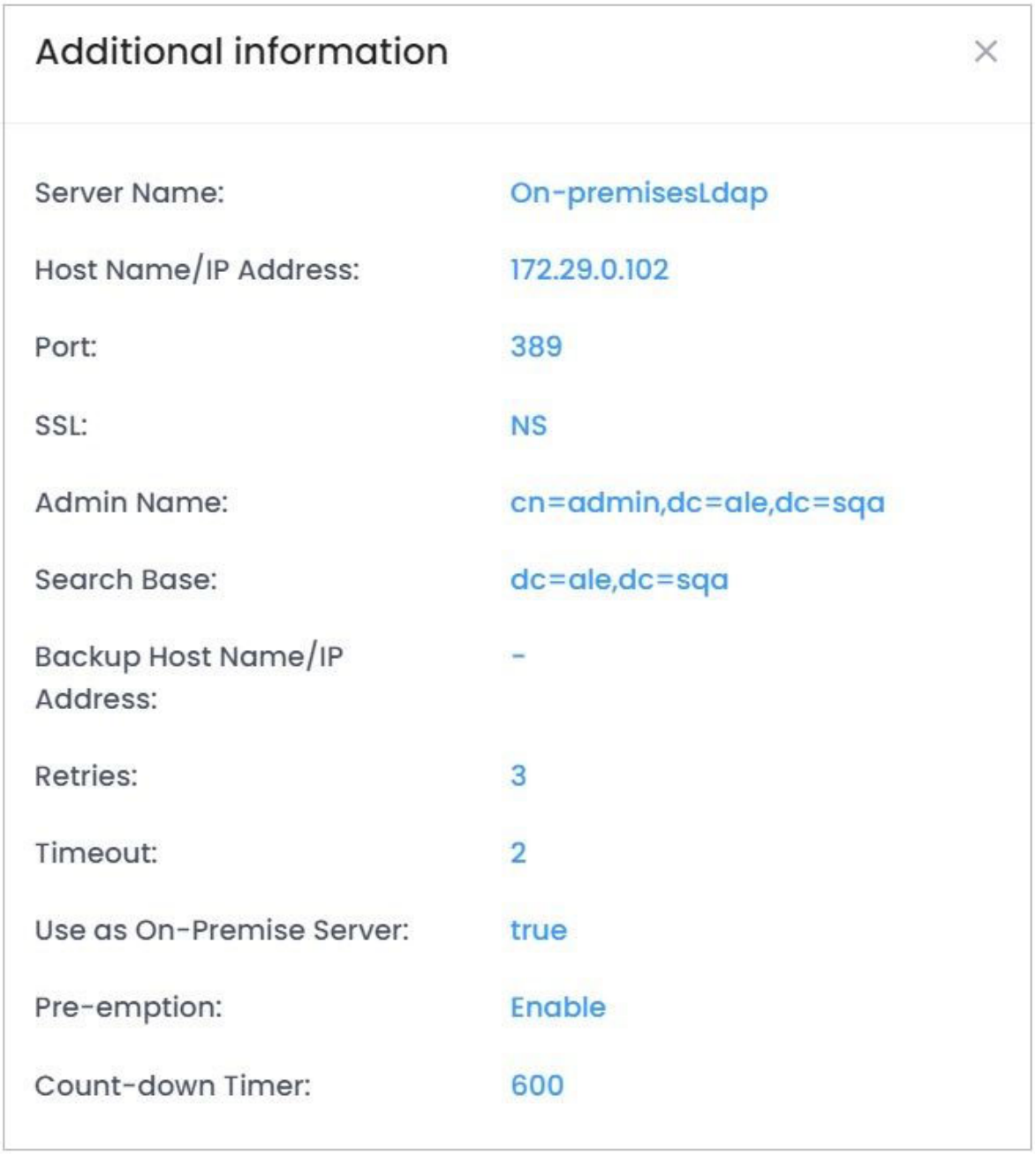
- **Retries -** The number of retries that you want the device to attempt when trying to contact the LDAP Server (AP Range = 1-3, Switch Range = 1-32, Default = 3).
- **Timeout -** The number of seconds that you want the device to wait before a request to the LDAP authentication server is timed out (Range = 1 - 30, Default = 2).
- **Port -** The port number used as the LDAP port address. This is the port at which the LDAP Server "listens". By default, the port number is 389. However, note that the switch automatically sets the port number to 636 when SSL is enabled. (Port number 636 is typically used on LDAP Servers for SSL.) The port number on the switch must match the port number configured on the server.
- **SSL -** Set this field to **True** or **False** to inform the device whether SSL (Secure Socket Layer) is enabled or disabled on the LDAP authentication server. SSL can be set up on the server for additional security. (This usually involves adding digital certificates to the server.) When SSL is enabled, the server's identity will be authenticated. Refer to "Managing Authentication Servers" in your *Network Configuration Guide* and to the instructions provided by the LDAP Server's vendor for further information on setting up SSL on the LDAP Server. (Not supported on wireless devices and ignored when applied to those devices.)
- **Admin Name -** The Administrator's name used to login to the LDAP Server.
- **Search Base -** The search base in the LDAP Server where authentication information can be found (e.g., o=alcatel.com).
- **Use As an On-Premise Server -** Select this option if you want to use a private LDAP Server instead of one in the cloud for AP authentication. In this scenario, user authentication requests are communicated directly between an AP and the LDAP server, and are not exposed in the public network. This option is only supported for BYOD authentication (see the BYOD Access

Strategy (see page 658) online help for certified LDAP Server versions).
Note: Only one On-Premise Server is permitted per organization. To configure a new server, please edit the existing server and uncheck the 'Use as On-Premises Server' option.

- **Pre-emption -** Enable or Disable Pre-emption to configure whether the AP should move back to the primary LDAP Server, after it has switched to a secondary LDAP Server. By default Pre-emption is Enabled. (Applies only to Access Point configuration.)
- **Count-down Timer -** Enter the number of seconds for the AP to adhere with the secondary server before moving back to primary server (Range=600 seconds, (5 minutes) to 3600 seconds (60 minutes), Default = 600 seconds). (Applies only to Access Point configuration.)
- **Password -** Password used to login to the LDAP Server (AP Range = 1-128 characters, Switch Range = 1-31 characters).
- **Confirm Password -** Re-enter the LDAP Server password.

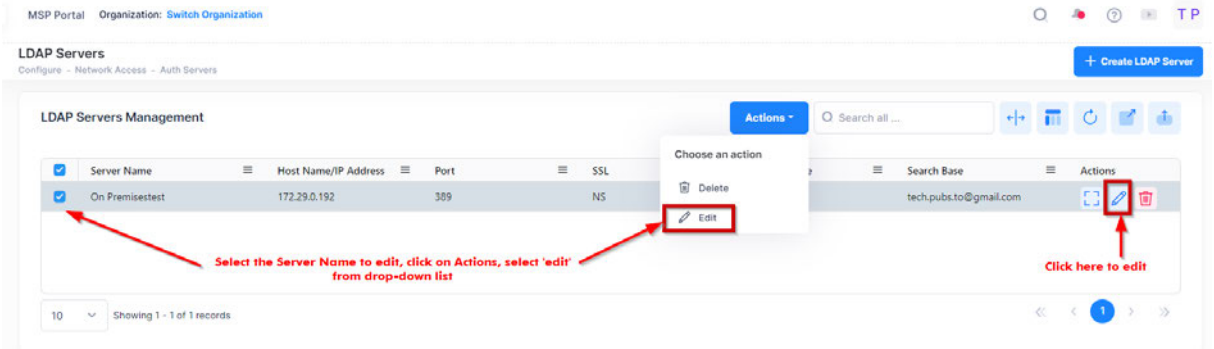
7.2.2.2 View Additional LDAP Server Information

Select the LDAP Server in the list and click on the Additional Information icon to view additional information about the LDAP Server.



7.2.2.3 Editing an LDAP Server

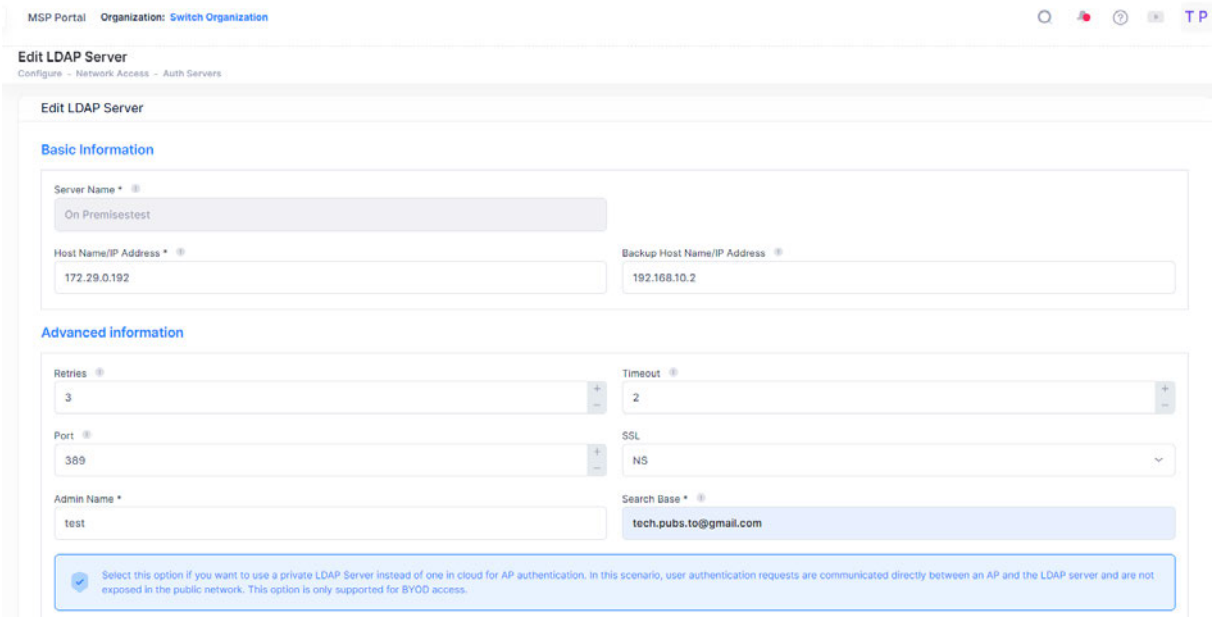
Select an LDAP Server in the list and click on the Edit icon. It is important to note that you cannot modify values indiscriminately. The values must match those of the actual LDAP Server. For example, if you want to change the LDAP port address, you must first use the tools provided by your LDAP Server's vendor to change the port on the LDAP Server itself. You can then inform OmniVista Terra that the port number has changed by modifying the **Port** field. Also note that you cannot edit an LDAP Server's name. You must delete it and create a new one.



Use one of the following methods to access the Edit LDAP Servers screen (as shown above):

- Select the server to edit by clicking on the checkbox next to the server name, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the server name that you want to edit.

The following Edit LDAP Server screen displays. Edit the fields as described above (see page 598), then click on **Save**.



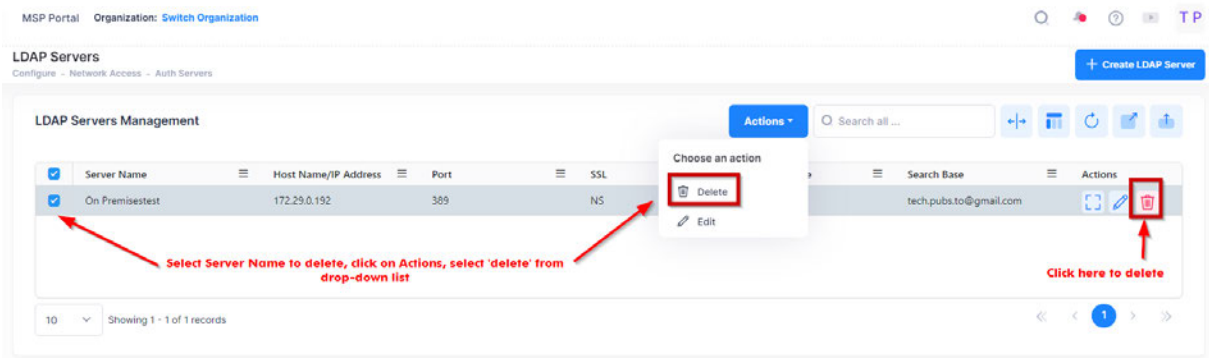
> You cannot delete an LDAP Server that is currently being used by OmniVista.

7.2.2.4 Deleting an LDAP Server

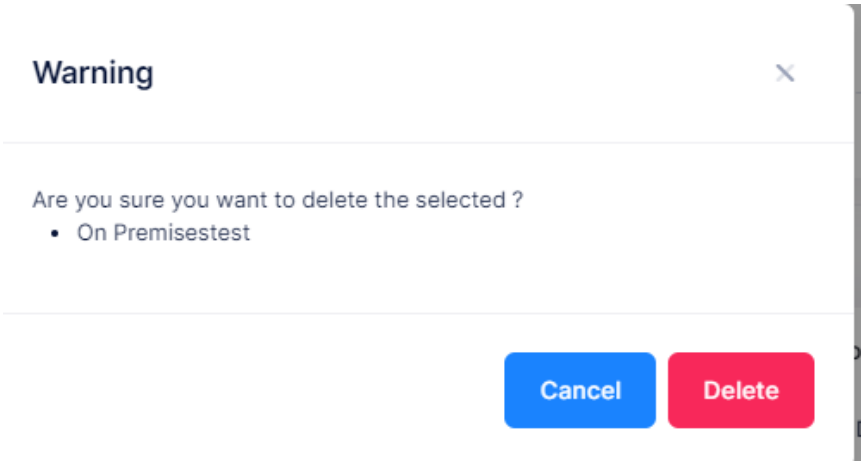
To delete a LDAP Server, use one of the following methods to select the Server Name you want to delete:

- Select the LDAP Server to delete by clicking on the checkbox next to the server name, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the server name that you want to delete.

Note that when deleting an LDAP Server, known to OmniVista Terra, it will send a delete alert message to the Switch if it is not been used in another profile.



When you select the server you want to delete, the following confirmation prompt appears:



Click on **Delete** to confirm that you want to delete the LDAP Server.

21 Oct 2025

7.3 Groups

The Groups application enables you to create the following groups, which can be used in various policy conditions:

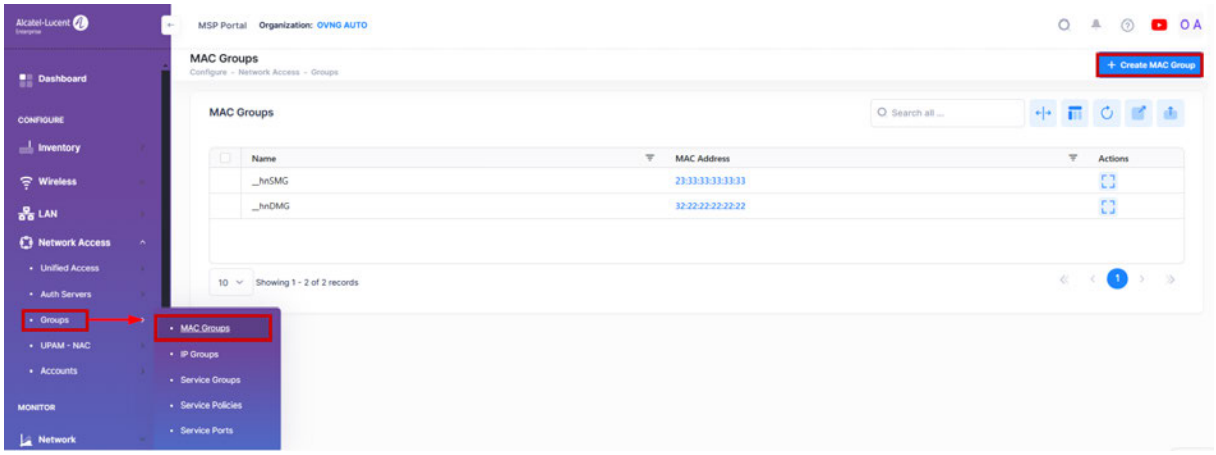
- MAC Groups (see page 605) - Displays all configured MAC Groups. The screen is used to create, edit, and delete MAC Groups, which can be used in creating various policy conditions, such as source MAC group condition and destination MAC group condition.
- IP Groups (see page 608) - Displays all configured IP Groups. The screen is used to create, edit, and delete IP Groups, which can be used in creating various policy conditions.
- Service Groups (see page 610) - Displays all configured Service Groups. The screen is used to create, edit, and delete Service Groups, which can be used in creating various policy conditions.
- Service Policies (see page 612) - Displays all configured Service Policies, which are assigned to a Service Group. This screen is used to create, edit, and delete Service Policies.
- Service Ports (see page 616) - Displays all configured Service Ports, which are assigned to Service Policies. By default, the TCP radio button is selected and TCP Services are displayed. Click on the UDP radio button to display UDP Services. The screen is used to create, edit, and delete Service Ports.

21 Oct 2025

7.3.1 MAC Groups

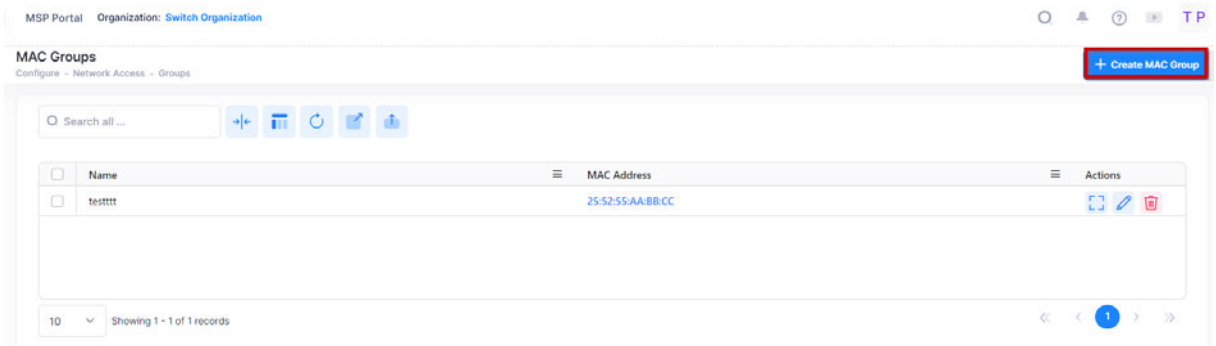
The Groups MAC Groups Screen displays all configured MAC Groups. MAC Groups screen is used to **create** (see page 605), **edit** (see page 606), and **delete** MAC Groups, which can be used in creating various policy conditions, such as source MAC group condition and destination MAC group condition.

To access the MAC Groups screen, navigate to the MAC Group screen by clicking on **Network Access > Groups > MAC Groups** under the “Configure” section of the OmniVista Terra Menu (see page 45).

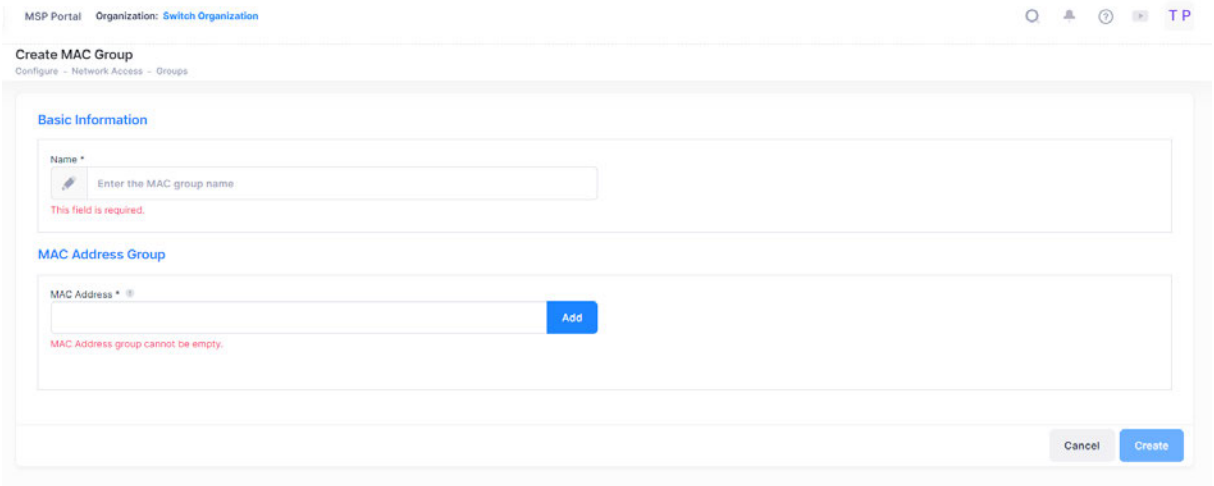


7.3.1.1 Creating a MAC Group

To create a MAC Group, Click on the **Create MAC Group** icon from the available MAC Groups List.



The following screen will appears.



Enter a Name for the MAC Group. Enter a MAC Address and click on the Add icon. Repeat to add additional addresses. When you are done, click on the **Create** button. The MAC Group will appear in MAC Groups List.

Note: You must enter at least one MAC Address.

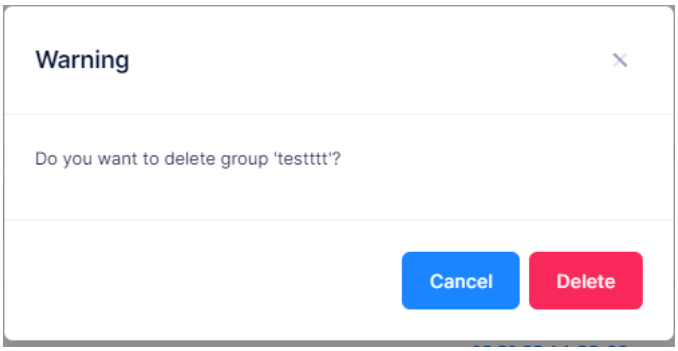
7.3.1.2 Editing a MAC Group

Click on the MAC Group that you want to edit to view the MAC Addresses in the MAC Group. Note that you cannot edit a MAC Group name. To edit a MAC Group name you must delete the MAC Group and create a new one.

- To **add** a MAC Address to the Group, enter the MAC Address, then click on the Add icon. Repeat to add additional addresses. When you are done, click on **Save** button.
- To **edit** a MAC Address, click on the Edit icon, edit the address, then click on the Save icon. Repeat to edit additional addresses. When you are done, click on the **Save** button.
- To **delete** a MAC Address, click on the Delete icon next to the MAC Address you want to delete. Repeat to delete additional addresses. When you are done, click on the **Save** button.

7.3.1.3 Deleting a MAC Group

To delete a MAC Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **Delete** at the confirmation prompt.



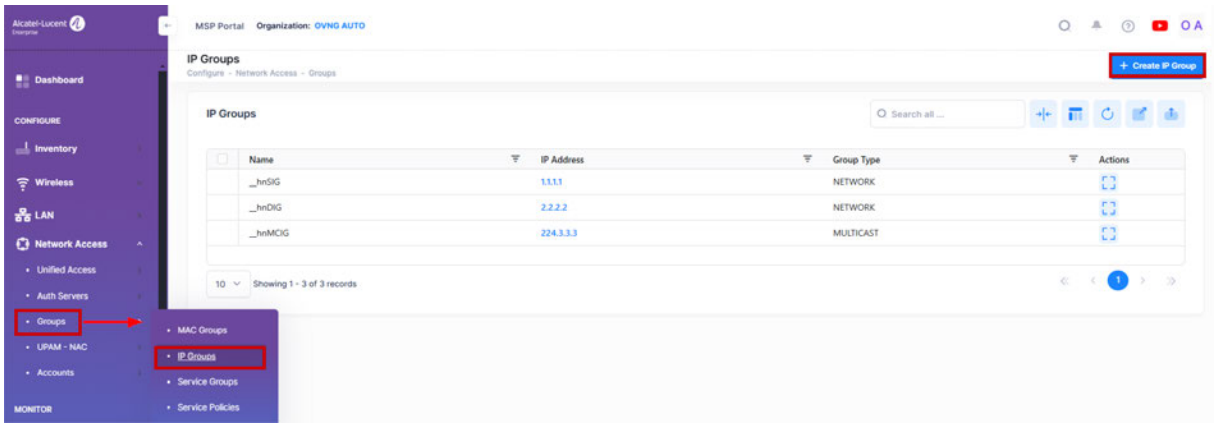
MAC Groups that are in use by policy conditions cannot be deleted. To delete these MAC groups, remove them from the policy conditions.

21 Oct 2025

7.3.2 IP Groups

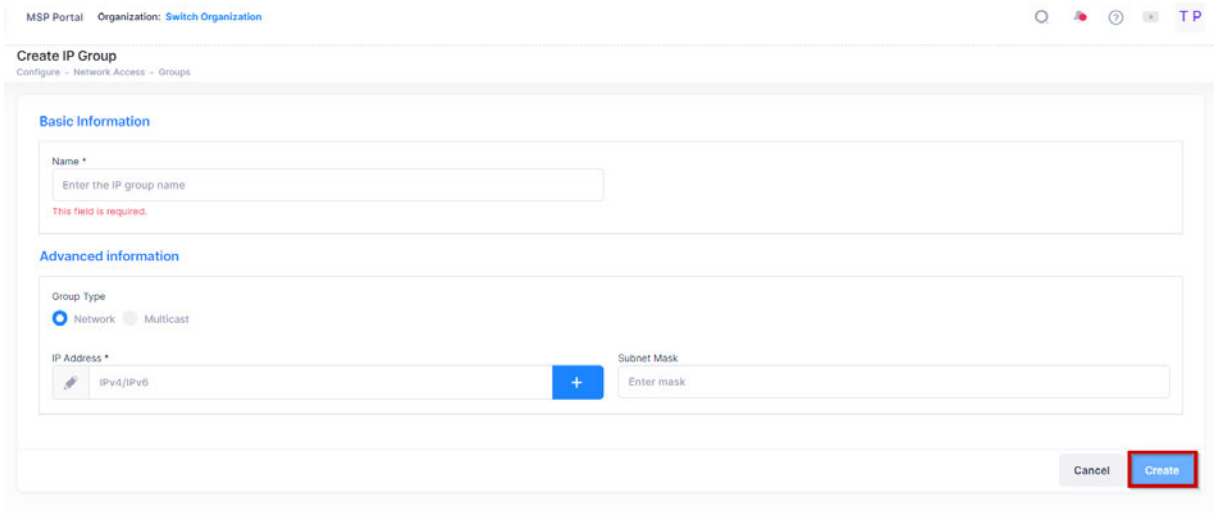
The Groups IP Groups Screen displays all configured Network Groups. The screen is used to **create** (see page 608), **edit** (see page 608), and **delete** (see page 609) Network Groups.

To access a IP Group, navigate to the IP Group screen by clicking on **Network Access > Groups > IP Groups** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.3.2.1 Creating a IP Group

To create a IP Group, click on the **Create IP Group** icon. The following screen appears.



Enter a Name for the IP Group. Enter a Subnet IP/Subnet Mask and click on the Add icon. Repeat to add additional subnets. When you are finished, click on the **Create** button. The IP Group will appear in IP Groups List. Note that you must enter at least one Subnet IP/Subnet Mask.

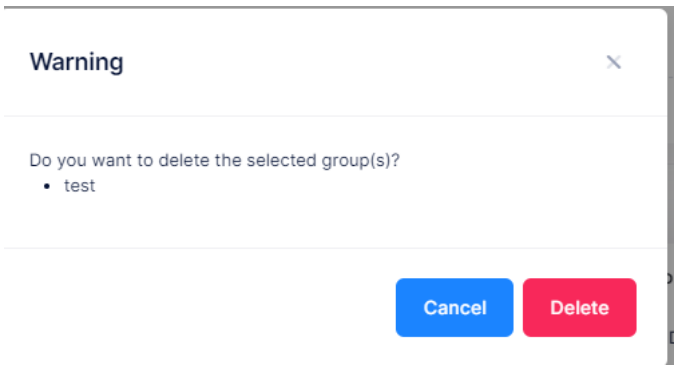
7.3.2.2 Editing a IP Group

Click on the IP Group that you want to edit to view the Subnets in the IP Group. Note that you cannot edit a IP Group name. To edit a IP Group name you must delete the IP Group and create a new one.

- To **add** a Subnet Address to the Group, enter a Subnet IP/Subnet Mask and click on the Add icon. Repeat to add additional subnets. When you are finished, click on the **Save** button.
- To **delete** a Subnet, click on the Delete icon next to the Subnet you want to delete. Repeat to delete Subnets. When you are done, click on the **Save** button.

7.3.2.3 Deleting a IP Group

To delete a IP Group(s), select the checkbox next to the group(s) in the list, click on the Delete icon, then click **Delete** at the confirmation prompt.

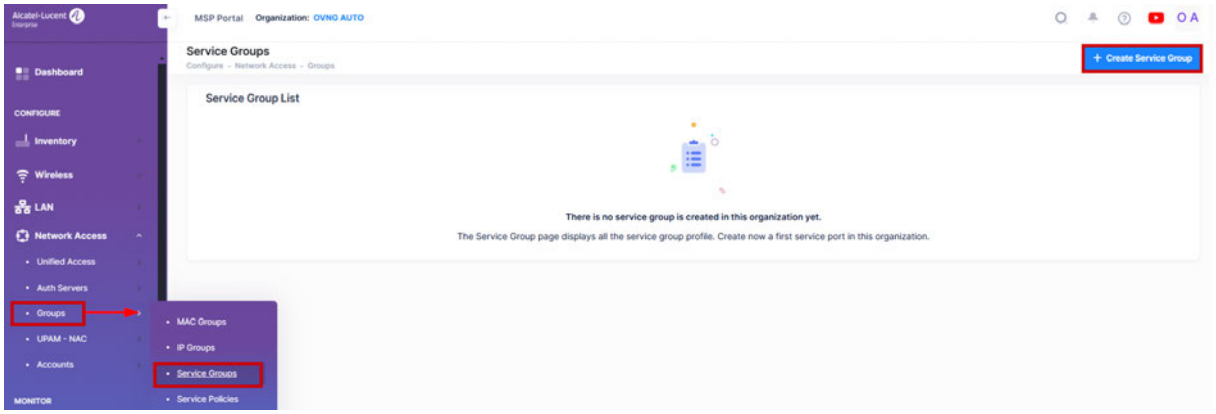


IP Groups that are in use by policy conditions cannot be deleted. To delete these IP groups, remove them from the policy conditions.

21 Oct 2025

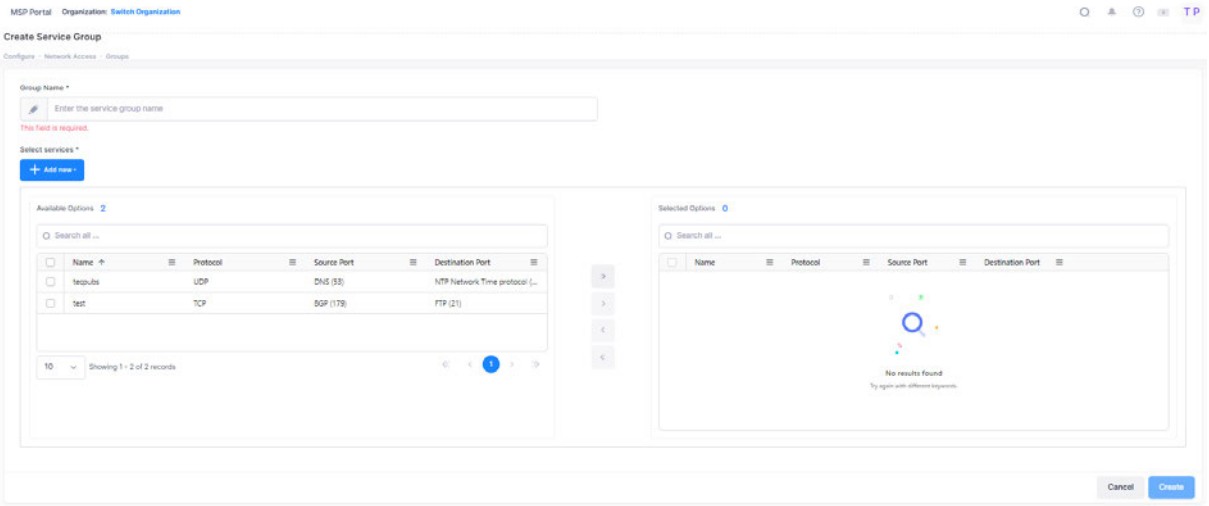
7.3.3 Service Groups

The Service Groups Screen displays all configured Service Groups. The screen is used to **create** (see page 610), **edit** (see page 611), and **delete** (see page 611) Service Groups.
To access Service Group, navigate to the Service Groups List screen by clicking on **Network Access > Groups > Service Groups** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Service Groups List screen displays.



7.3.3.1 Creating a Service Group

To create a Service Group, Click on the **Create Service Group** icon from the available Service Groups List. The following screen appears.



Enter a logical Group Name for the Service Group. Select a Service(s) and click on the **Create** button. If you want to create a new Service, click on the **Add New** Icon to go to the Services Screen and create the Service. When you click on the Create button on the Services Screen you will be returned to the Create Service Group Screen to finish creating the Service Group.

Note: You must enter at least one service policy to create a service group. Also, you cannot use Source and Destination Services in group.

7.3.3.2 Editing a Service Group

Click on the Service Group that you want to edit, then click on the **Edit** Icon. Add or remove Services from the group as described above then click on the **Save** button. You cannot edit a Service Group name. To edit a Service Group name you must delete the Service Group and create a new one.

7.3.3.3 Deleting a Service Group

To delete a Service Group(s), select the checkbox next to the group(s) in the list, click on the **Delete** icon then click **Delete** at the confirmation prompt.

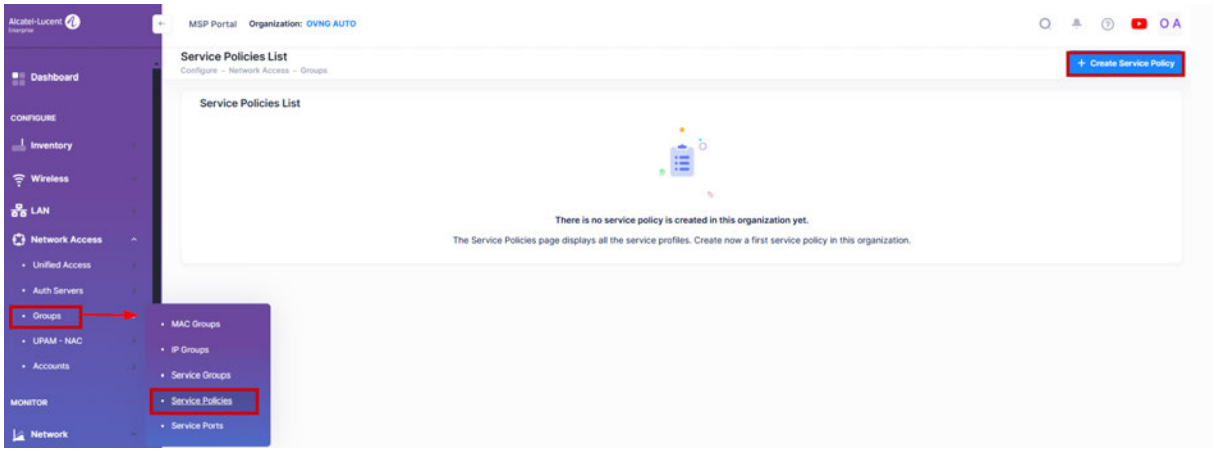
Service Groups that are in use by policy conditions cannot be deleted. To delete these Service Groups, remove them from the policy conditions.

21 Oct 2025

7.3.4 Service Policies List

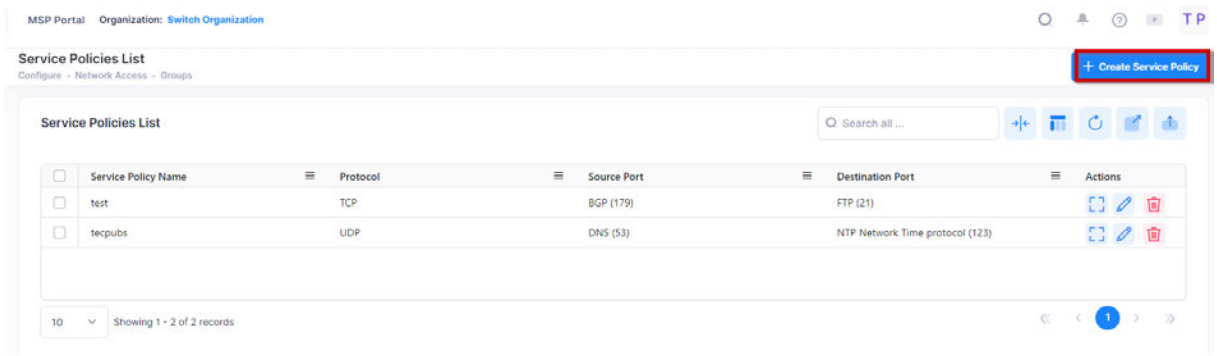
The Groups Services Policies List Screen displays all configured Services, which are used to create Service Policy Groups. The screen is used to **create** (see page 612), **edit** (see page 613), and **delete** (see page 614) Service Policy.

To access the Service Policy screen, navigate to the Service Policy List screen by clicking on **Network Access > Groups > Service Policies** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Service Policies List screen displays.

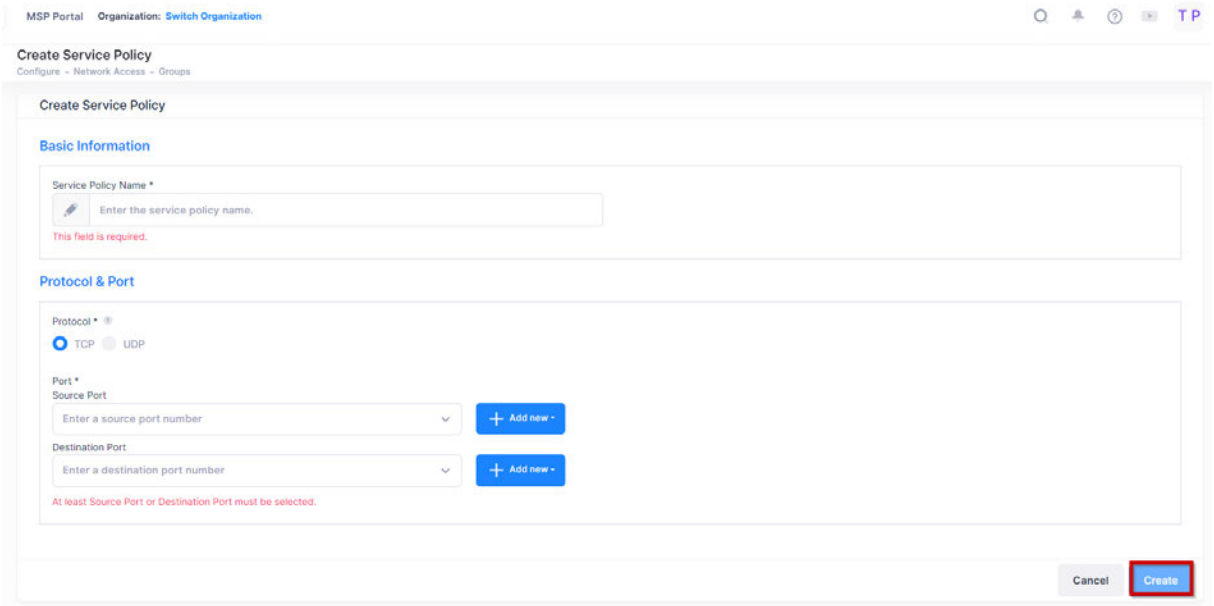


7.3.4.1 Creating a Service Policy

To create a new Service Policy, click on the **Create Service Policy** icon as shown below.



The following screen appears.



Complete the fields as described below, then click on the **Create** button.

- **Service Policy Name** - User-configured name for the Service.
- **Protocol** - Select a protocol for the Service. By default, the TCP radio button is selected and TCP ports are displayed. Click on the UDP radio button to display UDP ports.
- **Source Port** - Select a source port from the Source Port drop-down list. The drop-down box includes a list of well-known TCP or UDP ports. Select a port(s) from the drop down menu (you can also select "Check All" to select all ports. Click "Uncheck All" to deselect the ports and start over). If you want to create a new port, click on the Add Icon to go to the Service Port Screen and create a new port.
  When you click on the **Create Service Policy** button on the Service Port Screen you will be returned to the Create Service Screen to finish creating the Service. Note that you can specify a Source Port, a Destination Port, or both.
- **Destination Port** - Select a destination port from the Destination Port drop-down list. The drop-down box includes a list of well-known TCP or UDP ports. Select a port(s) from the drop down menu (you can also select "Check All" to select all ports. Click "Uncheck All" to deselect the ports and start over). If you want to create a new port, click on the Add Icon to go to the Service Port Screen and create a new port. When you click on the Create button on the Service Port Screen you will be returned to the Create Service Screen to finish creating the Service.

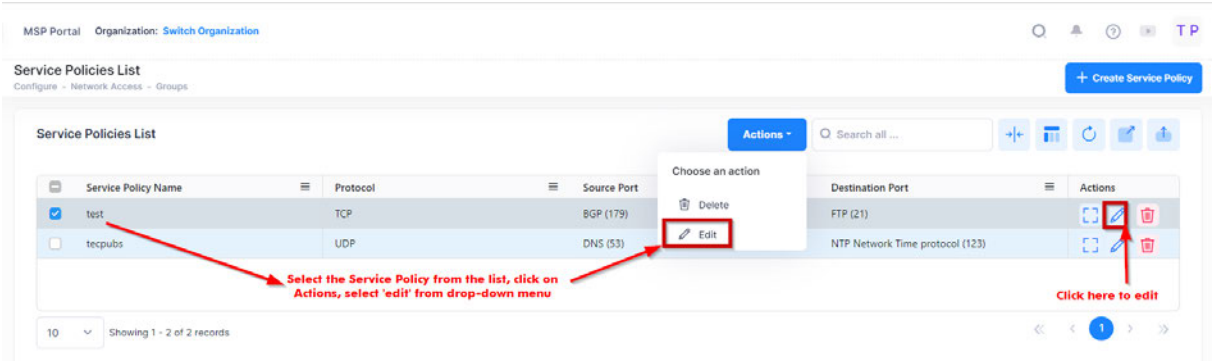
Note: You can specify a Source Port, a Destination Port, or both.

7.3.4.2 Editing a Service Policy

Use one of the following methods to access the Edit a Service Policy screen (as shown above):

- Select the Service Policy to edit by clicking on the checkbox next to the Service Policies List, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the Service Policies that you want to edit.

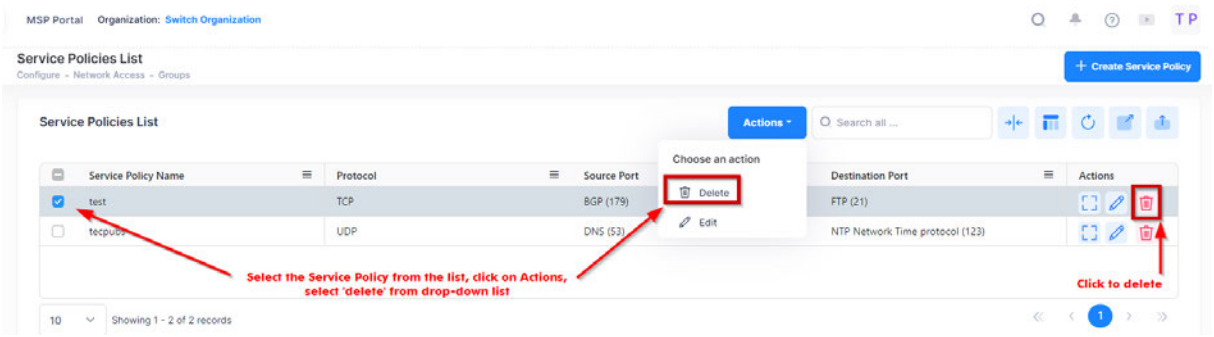
Edit the fields as described above, then click on **Save**.



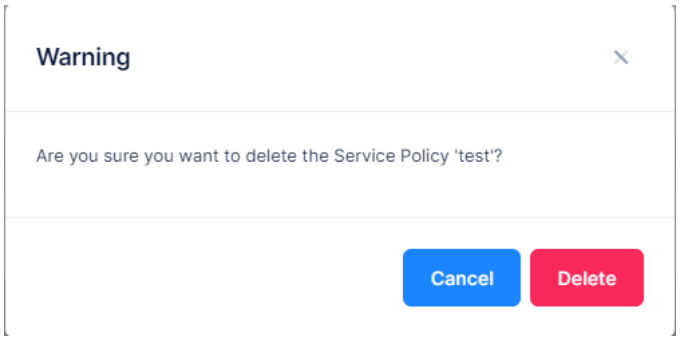
7.3.4.3 Deleting a Service Policy

To delete a Service Policy(s), use one of the following methods to select the Service Policy you want to delete:

- Select the Service Policy to delete by clicking on the checkbox next to the List, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash icon under the “Actions” column next to the Service Policy that you want to delete. (as shown below).



When you select the Service Policy you want to delete, the following confirmation prompt appears:



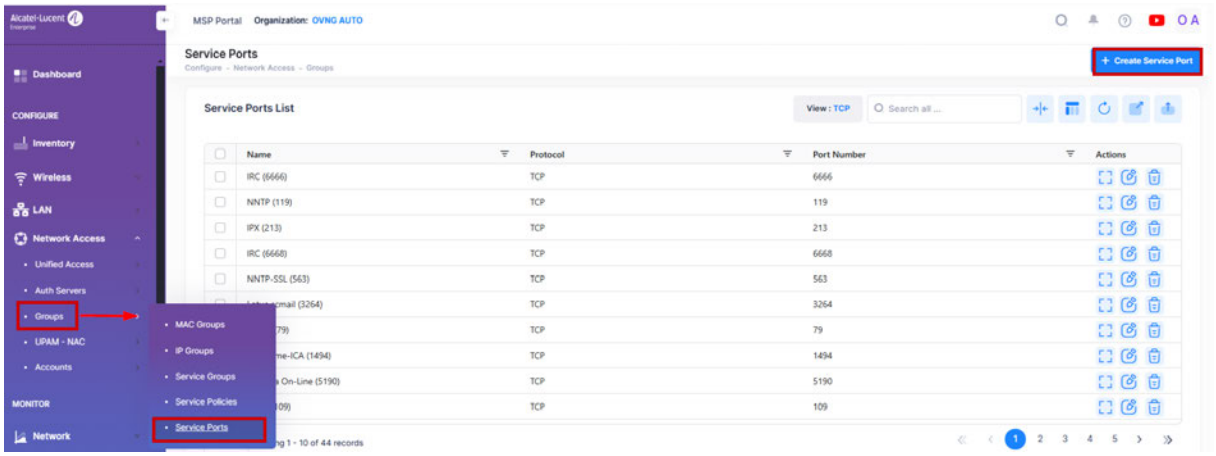
Services that are in use by policy conditions cannot be deleted. To delete these Services, remove them from the policy conditions.

21 Oct 2025

7.3.5 Service Ports List

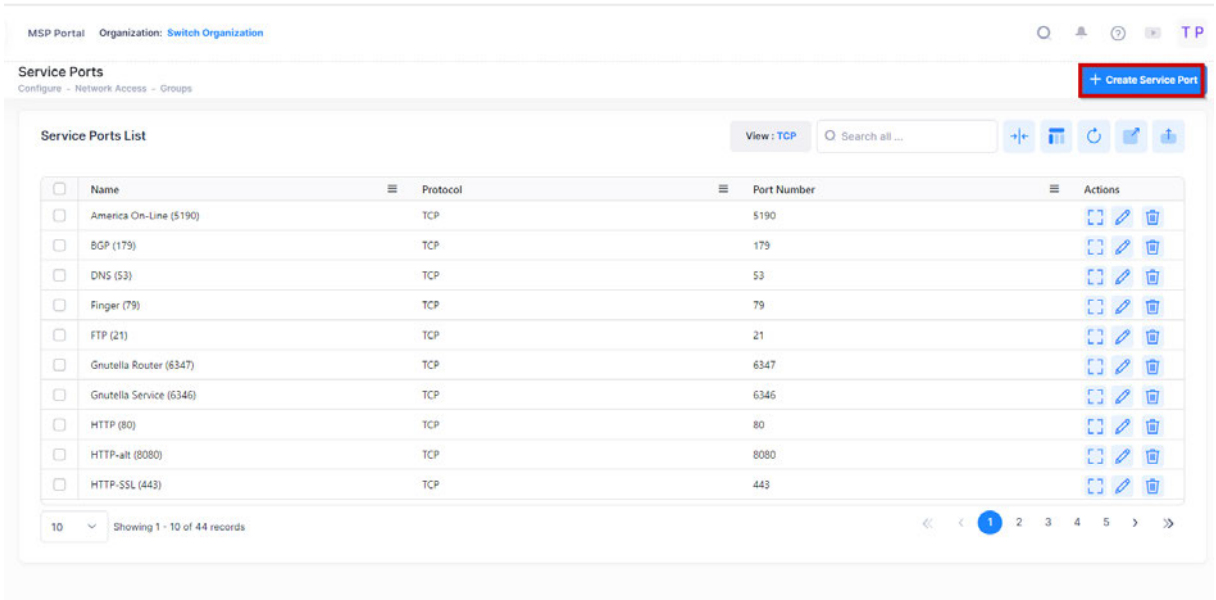
The Groups Service Port List Screen displays all configured Service Ports, which are used to create Services. By default, the TCP radio button is selected and TCP Services are displayed. Click on the UDP radio button to display UDP Services. The screen is used to **create** (see page 616), **edit** (see page 617), and **delete** (see page 617)Service Ports.

To access the Service Port List, navigate to the Service Port List screen by clicking on **Network Access > Groups > Service Ports** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Service Port List screen displays.

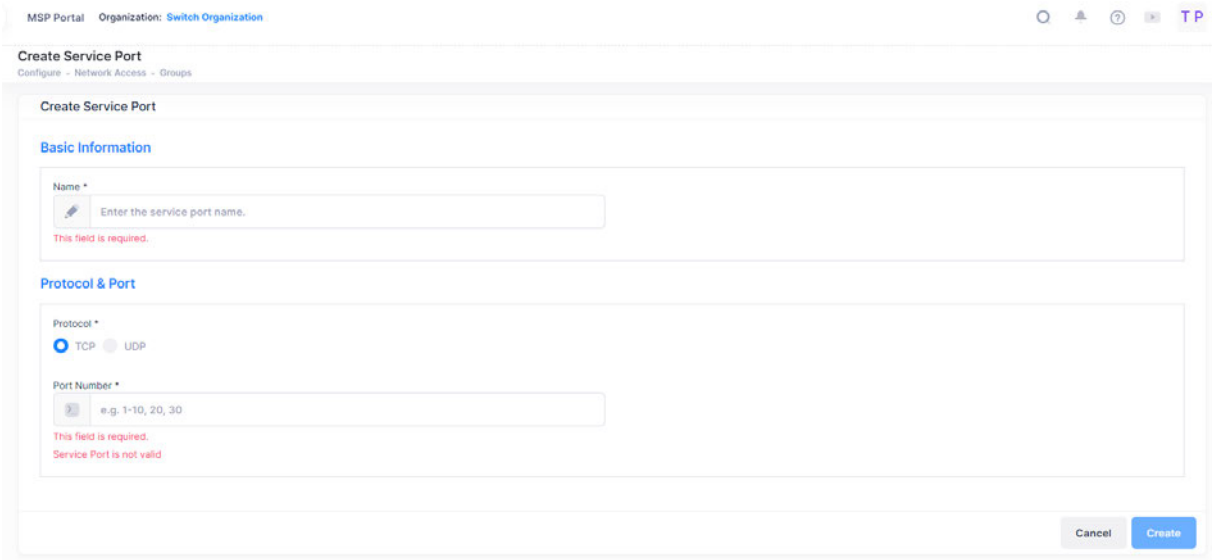


7.3.5.1 Creating a Service Port

To create a Service Port, click on the **Create Service Port** icon.



The following screen appears.



Complete the fields as described below, then click on the **Create** button.

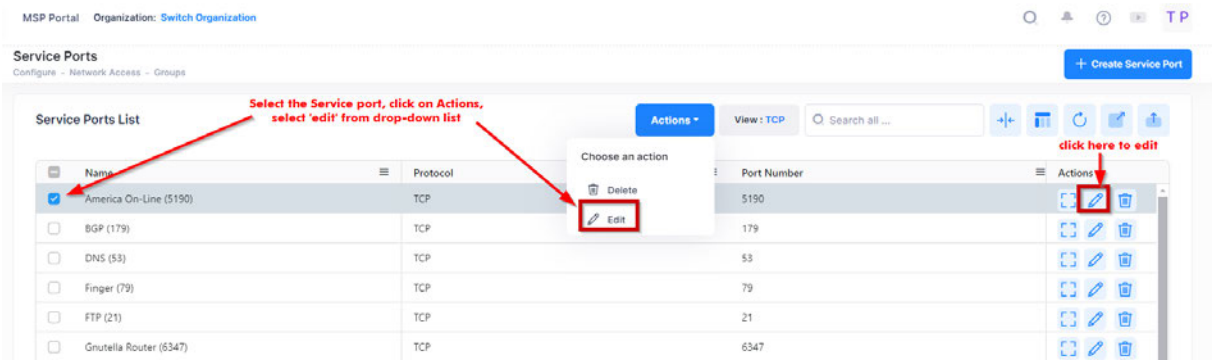
- **Name** - User-configured name for the Service Port.
- **Protocol** - Select TCP or UDP protocol.
- **Port Number** - Enter a Service Port number.

7.3.5.2 Editing a Service Port

Use one of the following methods to access the Edit a Service Port screen (as shown above):

- Select the Service Port to edit by clicking on the checkbox next to the Service Ports List, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the Service Port that you want to edit.

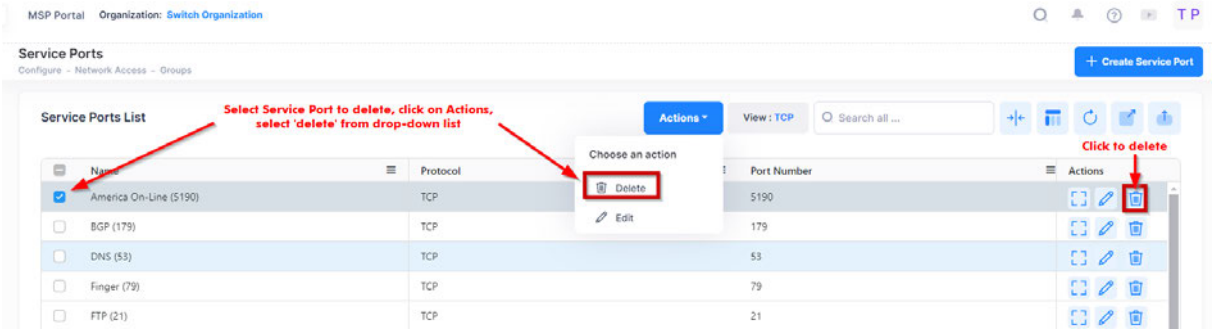
Edit the fields as described above, then click on **Save**.



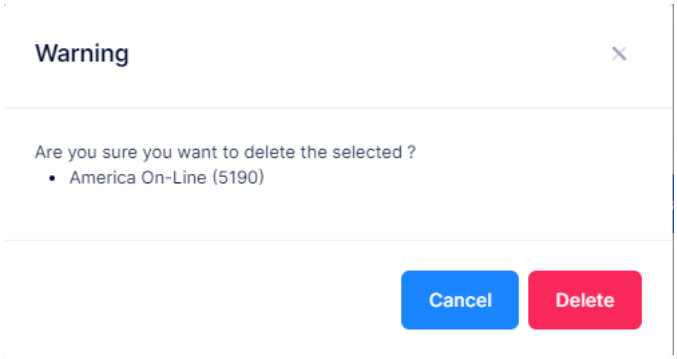
7.3.5.3 Deleting a Service Port

To delete a Service Port(s), use one of the following methods to select the Service Port you want to delete:

- Select the Service Port to delete by clicking on the checkbox next to the List, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash icon under the “Actions” column next to the Service Port that you want to delete. (as shown below).



Click **Delete** at the confirmation prompt.



Note: Service Ports that are in use by Services cannot be deleted. To delete these Service Ports, remove them from the Service.

21 Oct 2025

7.4 UPAM - NAC

The Unified Policy Authentication Manager (UPAM) is a unified access management platform for Stellar AP Series devices. UPAM supports both Captive Portal server and RADIUS server; and can be used to implement MAC authentication and Captive Portal authentication. User Profiles can be supported in the OmniVista database or on external servers. The following applications are used to configure and monitor the UPAM platform and are accessible by clicking on **Network Access > UPAM-NAC** under the "Configure" section of the OmniVista Terra Menu (see page 45):

- **Access Policies** (see page 621) - Displays information about configured UPAM Access Policies and is used to create, edit, and delete Access Policies. Access Policies define the mapping conditions for an authentication strategy. Through Access Policy configuration, an authentication strategy can be applied to different user groups, which can be divided by SSID or other attributes.
- **Guest Access** - The UPAM Guest Access application is used to manage guest users accessing the network. Guest Access service is based on the captive portal authentication. The following screens are used to monitor and configure the Guest Access application:
  - **Guest Access Strategy** (see page 633) - Displays information about configured Guest Access Strategies and is used to configure access attributes for guest users.
  - **Guest Accounts** (see page 727) - Display all configured Guest accounts in the UPAM network and is used to create the login accounts for the Guest users. If self-registration is not enabled, you can manually create a login account for a guest user and relay the information to the guest user.
  - **Guest Devices** - Displays all authenticated online devices as well as all devices that were previously on the network and are stored in UPAM.
  - **Self-Registration Requests** - Displays a list of self-registration requests from Guest users and is used to review, approve or reject self-registration requests.
  - **Guest Operators** (see page 745) - Displays a list of Guest Operators and is used to configure the Guest Operators in the UPAM network. A Guest Operator is a network operator who manages the guest user network access.
- **BYOD Access Strategy** (see page 658) - Displays information about configured BYOD Access Strategies to configure access attributes for BYOD users. The screen can be used to create, edit, and delete BYOD Access Strategies. The UPAM BYOD Access application is used to manage employee BYOD devices. BYOD service is based on Captive Portal authentication.
- **NAS Clients** (see page 663) - Displays information about configured NAS Clients and is used to create, edit, and delete NAS Clients. NAS acts as a gateway to guard access to a network resource. A client connects to the NAS, and the NAS then connects to an AAA Server to determine whether or not the client's supplied credentials are valid. The NAS then allows or denies access to the network resource. The network device in the infrastructure attaching with wireless clients will act as a NAS client, communicating to UPAM which acts as a AAA Server.
- **Role Mapping for On-Premises LDAP** (see page 669) - Displays information about configured mappings and is used to create, edit, and delete mappings. The Role Mapping for On-Premises LDAP screen allows you to assign different Access Role Profiles and Policy Lists to different sub-user groups by creating mapping rules based on user attributes. For example, you could assign a Premium Access Role Profile with larger bandwidth to the VIP group in LDAP.

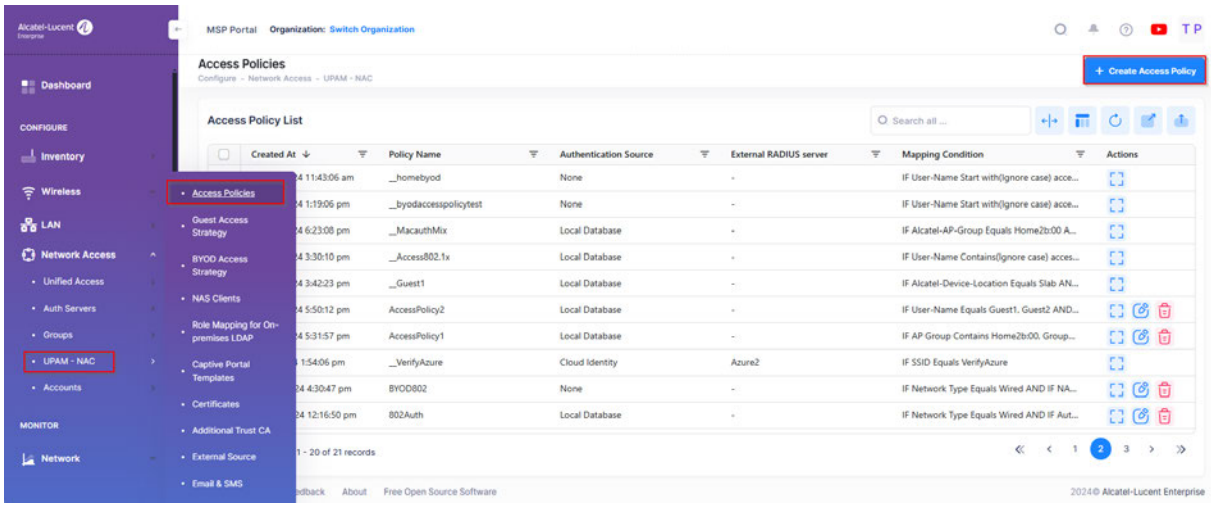
- **Captive Portal Templates** (see page 675) - Displays all configured Captive Portal templates and is used to create, edit, and delete Captive Portal templates. A Captive Portal template defines the login page that is presented to the user for Guest and BYOD login.
- **Certificates** (see page 682)- Displays information about UPAM RADIUS Server certificates and RadSec client certificates. The Certificates screen is also used to add, download, and delete certificates in the UPAM RADIUS Server for 802.1X or TLS authentication.
- **Additional Trust CA** (see page 688) - Displays information about all RADIUS Trust CAs and RadSec Trust CAs in the UPAM Trust RADIUS Store. This screen is also used to add, download, and delete Trust CAs for client authentication.
- **External Source** - The following screens are used to configure External RADIUS Servers and Cloud Identity integration.
  - **External RADIUS Server** (see page 692) - Displays information about External RADIUS Servers that are configured for UPAM to use for authentication. The External RADIUS Server screen can be used to create, edit, and delete external RADIUS servers.
  - **Cloud Identity** (see page 698) - Displays information about Cloud Identities that are configured for UPAM integration with Azure AD. The Cloud Identities screen can be used to create, edit, and delete Cloud Identities.
- **Email & SMS** (see page 702) **-** The SMS and Email for Guest Access Strategy screen lists the pre-defined content templates used for SMS text messages and Emails sent from OmniVista Terra. Emails/messages are sent during certain user-interactions, such as self-registration or the user forgot their password.

21 Oct 2025

7.4.1 Access Policies

Access Policies are used to define the mapping conditions for an authentication strategy. Through Access Policy configuration, authentication strategy is applied to different user groups, which can be divided by SSID or other attributes. The Access Policy Screen displays (see page 630) all configured UPAM Access Policies and is used to create (see page 621), edit (see page 628), and delete (see page 629) Access Policies.

To access the Access Strategy screen, click on **Network Access > UPAM-NAC > Access Policies** under the “Configure” section of the OmniVista Terra Menu (see page 45).



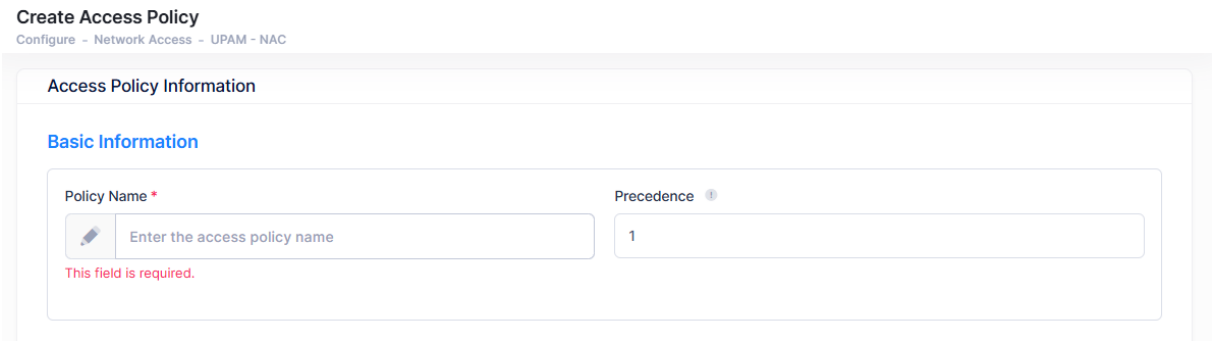
7.4.1.1 Creating an Access Policy

Click on **Create Access Policy** to bring up the Create Access Policy Screen. Use this screen to define the following attributes for an Access Policy configuration:

- Basic Information (see page 622)
- Mapping Condition (see page 622)
- Authentication Method (see page 623)
- Authentication Strategy (see page 624)
- Network Enforcement Policy
- MAC Check Enforcement Policy (see page 626)
- Web Redirection Enforcement Policy (see page 627)

When you are done configuring the attributes for the Access Policy, click on **Create Access Policy**.

7.4.1.1.1 Basic Information



- **Policy Name -** User-configured policy name.
- **Precedence -** Specify Access Policy Priority. A user requesting authentication may match several access policies and the one with highest priority will take effect after passing the authentication.
  (Range = 1-99, 1 is the highest priority and 99 is the lowest priority)

The Access Policy that you create or select defines the Authentication Strategy that UPAM applies when a client connects to the SSID. However, the Access Policy displayed for the SSID configuration is not always the policy used for authentication when the client is connecting to the SSID. This can occur if there are multiple Access Policies with the same precedence and overlapping rules configured through the Access Policies screen (Configure > Network Access > UPAM-NAC > Access Policies).

When a client connects to the SSID, UPAM selects the Access Policy with the highest precedence and evaluates whether its mapping rules align with the client's connection request. If a match is found, the associated authentication strategy is applied. If two Access Policies with the same precedence have identical mapping rules, UPAM defaults to the policy created first. This behavior may lead to unexpected results.

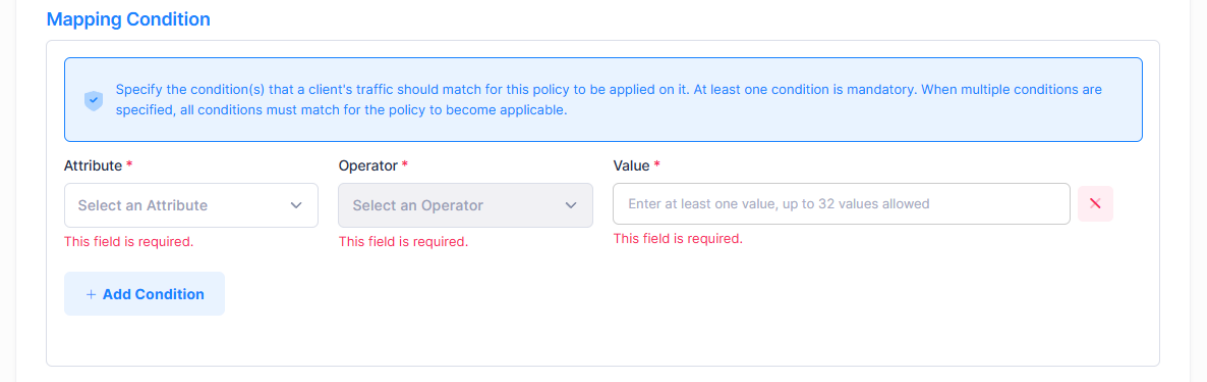
To prevent ambiguity, ensure that:

a) There are no Access Policies with overlapping rules, or

b) Access Policies with overlapping rules have different precedence. You can adjust the policy precedence configured for the Access Policies (Configure > Network Access > UPAM-NAC > Access Policies) to address these issues.

7.4.1.1.2 Mapping Condition

Mapping conditions specify the conditions that client traffic should match for this policy to be applied to the client. At least one condition is mandatory. When multiple conditions are specified, all conditions must match before the policy is applied.

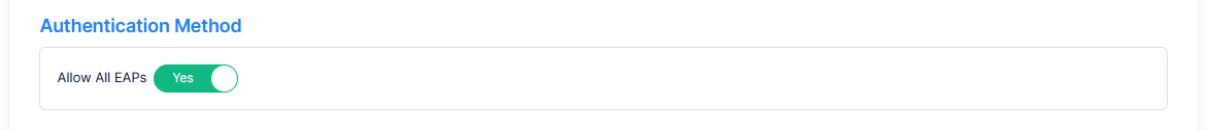


- **Attribute** - Select the Attribute (Basic or Advanced Attribute type) from the drop-down list.
  - **Basic Attributes** - Access Point Group, Authentication Type, NAS Device Location, NAS Device Name, NAS IP, NAS Port ID, NAS-Identifier, Network Type, Port Desc/WLAN Name, SSID.
  - **Advanced Attributes** - Alcatel-AP-Group, Alcatel-Device-Location, Alcatel-Device-Name, Alcatel-Port-Desc, Called-Station-Id, Calling-Station-Id, NAS-IP-Address, NAS-Identifier, NAS-Port-Id, NAS-Port-Type, Service-Type, User-Name.
- **Operator -** Select a condition operator.
- **Value -** Select a condition value. Enter at least one value. A maximum of 32 values are allowed.

> If you select “IMSI/IMEI Database” for the Authentication Source (see page 624), the Mapping Condition fields are automatically set to the following values and are no longer configurable:
>
> - **Attribute** = “Service-Type”
> - **Operator** = “Equals”
> - **Value** - “Authorize Only”

Click on **Add Condition** to add another mapping condition to the Access Policy.

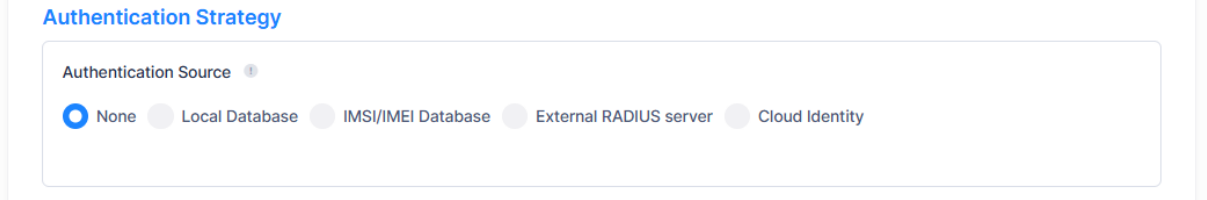
7.4.1.1.3 Authentication Method



- **Allow All EAPs** - Enables/Disables the use of all EAP methods supported by UPAM, Authenticator, and the client device. By default, this option is set to “Yes” (Enabled). When disabled, select the allowed EAP methods:
  - **EAP-TLS** - Restricts authentication to EAP-TLS Protocol.
  - **EAP-PEAP** - Restricts authentication to EAP-PEAP Protocol.
  - **EAP-TTLS** - Restricts authentication to EAP-TTLS Protocol.

If you select “IMSI/IMEI Database” for the Authentication Source (see page 624), the Authentication Method is not configurable.

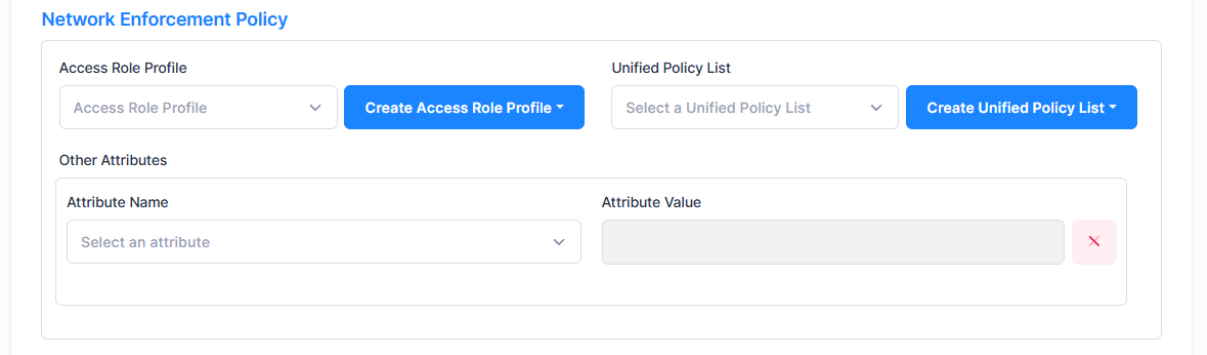
7.4.1.1.4 Authentication Strategy



- **Authentication Source -** Specify the source of the user profile (Account/Password). The user profile can reside on different servers and is required to be specified so that UPAM is able to obtain the user profile for authentication.
  - **None -** Authenticate against “None”. This is only supported for MAC authentication, which requires captive portal authentication. 802.1x Authentication is not supported. In this case, a user needs to pass captive portal authentication first (authentication method could be by Account + Password/Access Code/Terms of Use/etc.), the MAC address of the user will be stored and the user will complete the MAC authentication. Guest user devices are displayed in the Guest Devices - Guest Remembered Device (see page 894) list. Employee user devices are displayed in the BYOD Devices - Remember Devices (see page 900) list.
  - **Local Database -** Authenticate against the user profile in the local UPAM database. An Employee or Guest user must be created before authentication. An Employee Guest User is created on the Employee Accounts (see page 708) screen. A Guest User is created on the Guest Accounts Screen (see page 727).
  - **IMSI/IMEI Database** - Authenticate against the user profile in the UPAM IMSI/IMEI database (see page 761). Select this database when configuring UPAM integration with Celona devices.
    Note: When you select the IMSI/IMEI database, the following Access Policy attributes are no longer configurable:
    - Authentication Method (see page 623) (Allow All EAPs)
    - MAC Check Enforcement Policy (see page 626)
    - Web Redirection Enforcement Policy (see page 627)
  - **External Radius -** Authenticate against the user profile in an external RADIUS Server. Select a server from the **External Radius** drop-down. If necessary, you can click on **Create External RADIUS Server** to go to the Create External Radius Server screen to create a server.
  - **Cloud Identity -** Authenticate against the user profile with Azure Active Directory via the Certificate Connector for Microsoft. Azure AD has the ability to synchronize with on-premise Active Directory, providing authentication access to OmniVista Terra.

In this release of UPAM, cloud identity is only available for devices that use 802.1X authentication. Cloud identity cannot be used with BYOD or Guest Captive Portal at this time.

7.4.1.1.5 Network Enforcement Policy

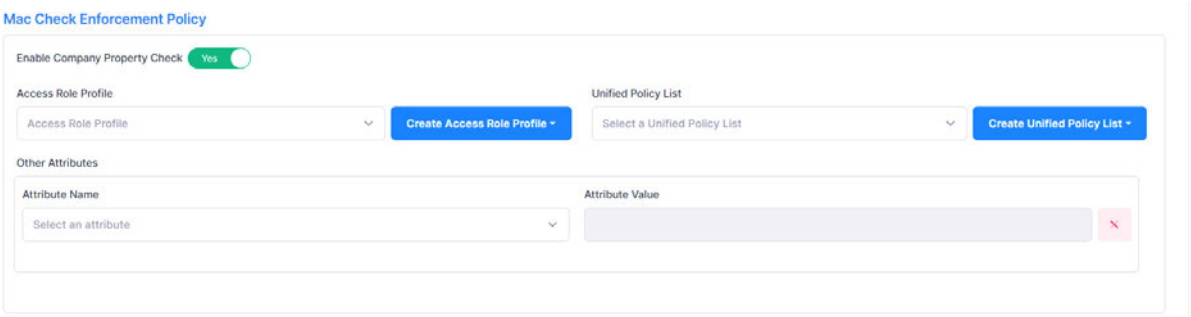


- **Access Role Profile** - Select the Access Role Profile from the drop-down list. If necessary, you can click on **Create Access Role Profile** to go to the Create Access Role Profile screen to create a profile. Note that this field is not available when the Authentication Source (see page 624) is set to the IMSI/IMEI database.
- **Unified Policy List** - Select a Unified Policy List from the drop-down list. If necessary, you can click on **Create Unified Policy List** to go to the Create Unified Policy List screen to create a policy list. Note that this field is not available when the Authentication Source (see page 624) is set to the IMSI/IMEI database.
- **Other Attributes** - Select the required attributes and provide values.
  - **Acct-Interim-Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600).
  - **Session-Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200).
  - **Tunnel-Private -Group-ID** - The Tunnel Private Group ID is used to determine the UNP for the device, if applicable. Tunnel Private Group ID is a RADIUS attribute that indicates the group ID for a particular tunnel session. It may be included in the Access-Request packet if the tunnel initiator can pre-determine the group resulting from a particular connection, and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. In most cases, L2 VLAN domain is a private group, and the Tunnel Group ID is pointing to the VLAN ID. (Range = 1 - 4094)
  - **WISPr-Bandwidth-Max-Down -** The user downstream bandwidth, in kbit/s. Value must be in range [0 - 2147483]. By default or set it to 0, it is not limited.
  - **WISPr-Bandwidth-Max-Up -** The user upstream bandwidth, in kbit/s. Value must be in range [0 - 2147483]. By default or set it to 0, it is not limited.

- **Reply-Message** - This attribute is automatically entered in the “Other Attributes” field when the IMSI/IMEI database is selected for the Authentication Source (see page 624). Enter the name of the Celona Access Role Profile.

7.4.1.1.6 Mac Check Enforcement Policy

Specifies whether or not to check to see if the device MAC address is in the Company Property (see page 716) database. By default MAC Check Enforcement Policy is disabled. When it is enabled, you have the option to specify an Access Role Profile, Policy List, or other attributes for when the check is successful (MAC address is in the database) and for when the check fails (MAC address is not in the Company Property database).



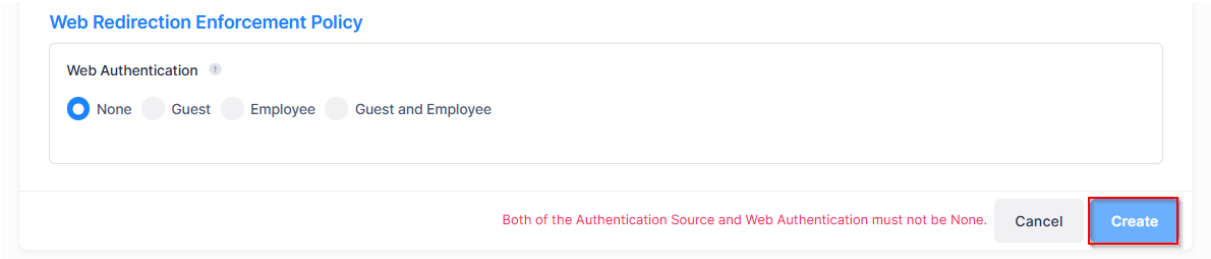
- **Enable Company Property Check** - Enables/Disables checking to see if the device MAC address is in the Company Property database. The Company Property Check is disabled (“No”) be default. When enabled, configure the following:
  - **Access Role Profile** - Select the Access Role Profile from the drop-down list. If necessary, you can click on **Create Access Role Profile** to go to the Create Access Role Profile screen to create a profile.
  - **Unified Policy List** - Select a Unified Policy List from the drop-down list. If necessary, you can click on **Create Unified Policy List** to go to the Create Unified Policy List screen to create a policy list.
  - **Other Attributes** - Select the required attributes and provide values.
    - **Acct-Interim-Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600).
    - **Session-Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200).
    - **Tunnel-Private -Group-ID** - The Tunnel Private Group ID is used to determine the UNP for the device, if applicable. Tunnel Private Group ID is a RADIUS attribute that indicates the group ID for a particular tunnel session. It may be included in the Access-Request packet if the tunnel initiator can pre-determine the group resulting from a particular connection, and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. In most cases, L2 VLAN domain is a private group, and the Tunnel Group ID is pointing to the VLAN ID. (Range = 1 - 4094)

- **WISPr-Bandwidth-Max-Down -** The user downstream bandwidth, in kbit/s. Value must be in range [0 - 2147483]. By default or set it to 0, it is not limited.
- **WISPr-Bandwidth-Max-Up -** The user upstream bandwidth, in kbit/s. Value must be in range [0 - 2147483]. By default or set it to 0, it is not limited.

Consider the following when an Access Policy with Company Property Check enabled is applied:

- If the device MAC address is found in the Company Property database (MAC check is successful), UPAM applies the Access Role Profile or Unified Policy List associated with the matching Company Property entry to the device. If the matching Company Property entry does not specify an Access Role Profile or Unified Policy List, then the profile and list specified in the MAC Check Enforcement Policy for the Access Policy is applied.
- If the device MAC address is not found in the Company Property database (MAC check fails), the following occurs:
  - For Portal Authentication, UPAM checks the following (in order) to obtain an Access Role Profile or Unified Policy List to apply to the device:
    - The Access Role Profile or Unified Policy List for the Account (LDAP Role mapping/ Guest/BYOD).
    - The Access Role Profile or Unified Policy List under “Post Portal Authentication Enforcement” for BYOD/Guest Strategy.
    - The Access Role Profile or Unified Policy List specified in “Network Enforcement Policy” of the Access Policy.
- If you select “IMSI/IMEI Database” for the Authentication Source (see page 624), enabling Company Property Check is not available.

7.4.1.1.7 Web Redirection Enforcement Policy



- **Web Authentication**
  Specify if web redirection is required and identify the web login page to use for authentication.
  - **Guest** - Specifies an access strategy for guest users. The user is redirected to the guest login page for the Guest Access Strategy.
    - **Guest Access Strategy** - Select the access strategy from the drop-down list. If necessary, you can click on **Create Guest Access Strategy** to go to the Create Guest Access Strategy (see page 633) screen to create a guest access strategy.
  - **Employee** - Specifies an access strategy for employee users with BYOD devices. The user is redirected to the employee login page for the BYOD Access Strategy.

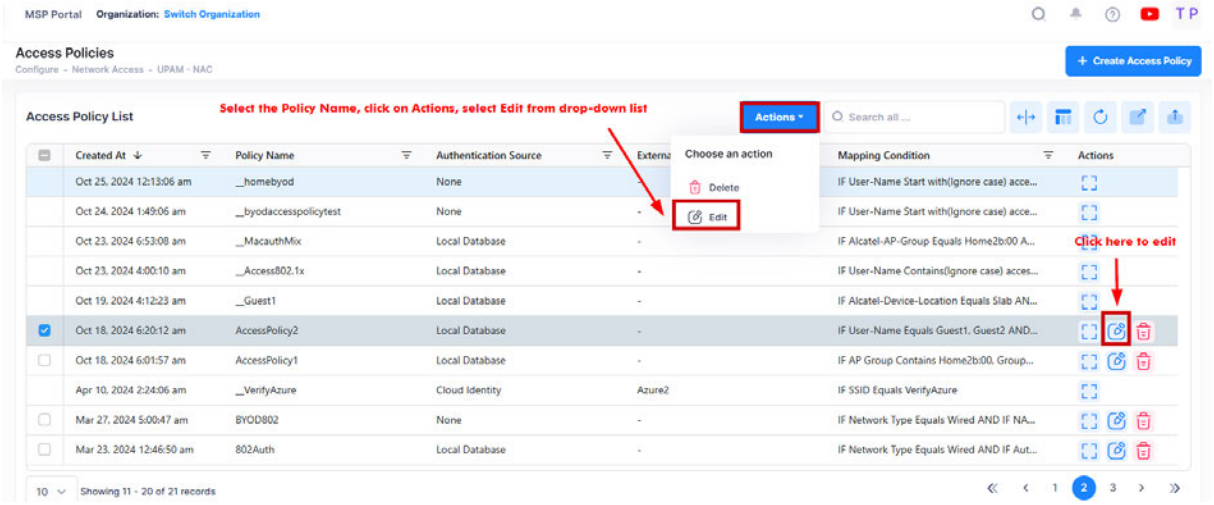
- **BYOD Access Strategy** - Select the access strategy from the drop-down list. If necessary, you can click on **Create BYOD Access Strategy** to go to the Create New BYOD Access Strategy (see page 658) screen to create a BYOD access strategy.

- **Guest and Employee** - Specify both a Guest and Employee access strategy. The user is redirected to a login page with the following two options:
  - **Register as Guest** (Guest configuration) - Click on this option to open the guest login page for the Guest Access Strategy.
  - **Network Account Login** (BYOD configuration) - Click on this option to open the employee login page for the BYOD Access Strategy.

- Both the Authentication Source and Web Authentication must not be set to “None”.
- If you select “IMSI/IMEI Database” for the Authentication Source (see page 624), configuring Web Authentication is not available.

7.4.1.2 Editing an Access policy

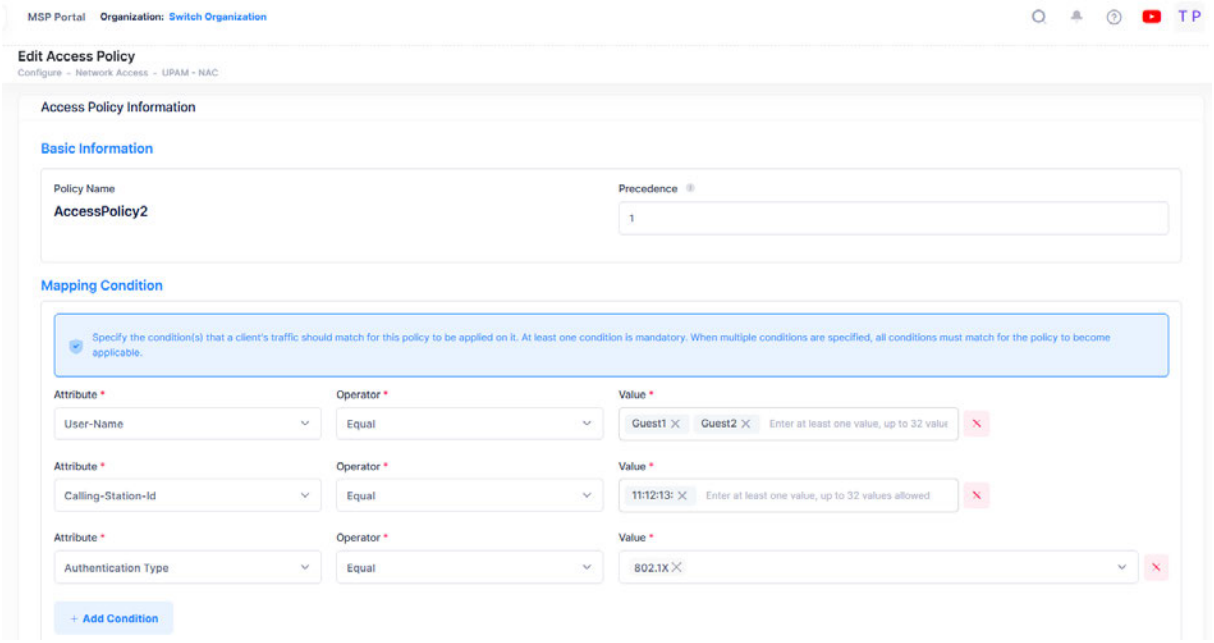
You can edit the parameter values for an existing Access Policy by accessing the Edit Access Policy screen.



Use one of the following methods to access the Edit Access Policy screen (as shown above):

- Select the policy to edit by clicking on the checkbox next to the policy name, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the policy name that you want to edit.

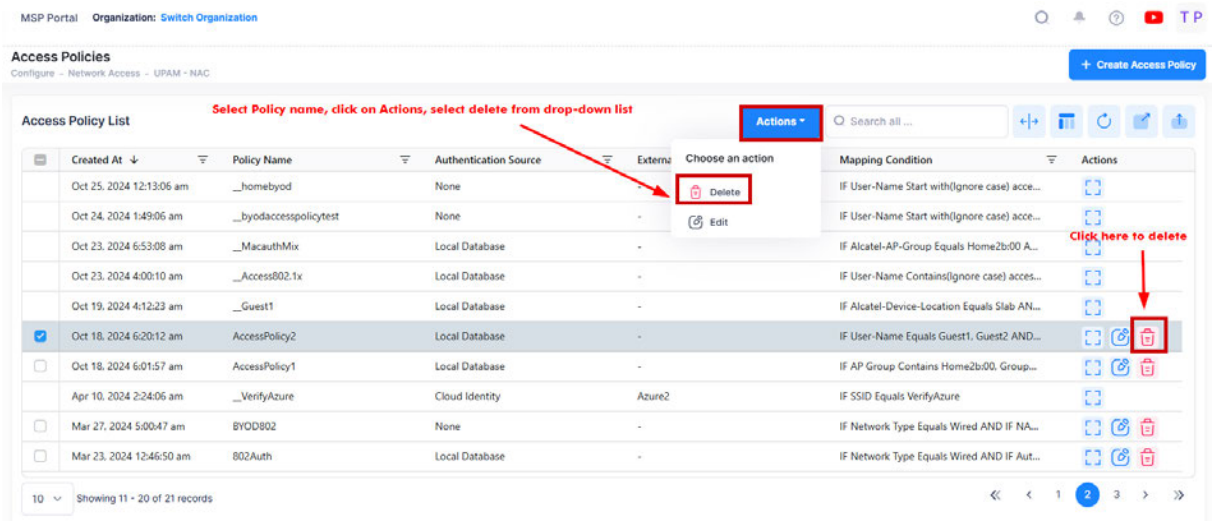
The following Edit Access Policy screen displays. Edit the fields as described above, then click on **Save**.



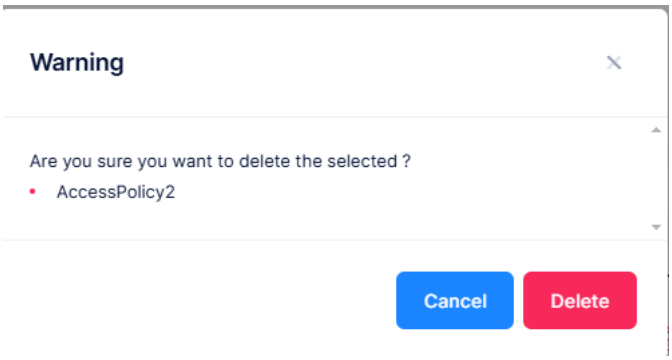
7.4.1.3 Delete an Access Policy

To delete an Access Policy, use one of the following methods to select the policy you want to delete:

- Select the policy to delete by clicking on the checkbox next to the policy name, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the policy name that you want to delete.



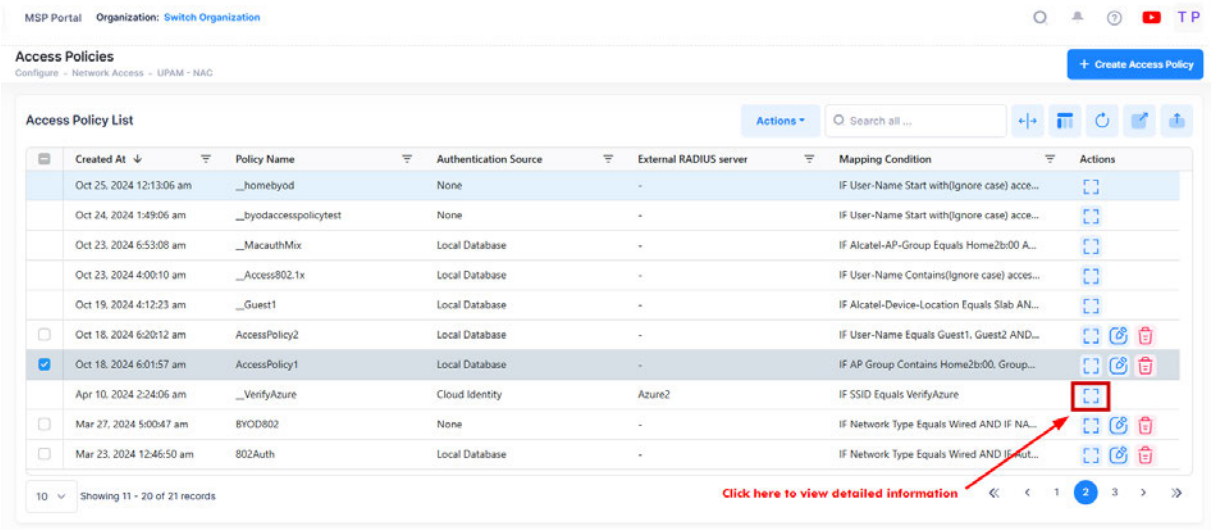
When you select the policy you want to delete, the following confirmation prompt appears:



Click on **Delete** to confirm that you want to delete the Access Policy.

7.4.1.4 Display Access Policy List

The Access Policy list displays information for the configured Access Policies. To display detailed information about a specific policy, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



The following information is displayed for each Access Policy:

- **Created At** - The date and time the policy was created.
- **Policy Name** - User configured policy name.
- **Authentication Source** - The source of the user profile (Account/Password). The user profile can reside on different servers and is required so that UPAM is able to obtain the user profile for authentication.
- **External RADIUS Server** - Authenticate against the user profile in an external RADIUS Server. You can select a server from the **External Radius** drop-down menu while creating the profile.
- **Mapping Condition** - Specifies the conditions that client traffic should match for this policy to be applied to the client. At least one condition is mandatory.
- **Priority** - The priority set for the Access Policy. The policy with the highest priority take effect after passing the authentication.
- **Access Role Profile** - The name of the Access Role Profile applied for Network Enforcement.
- **Unified Policy List** - The name of the Unified Policy List applied for Network Enforcement.
- **Guest Access Strategy** - The name of the Guest Access Strategy to use for Web redirection.
- **BYOD Access Strategy** - The name of the BYOD Access Strategy to use for Web redirection.
- **Web Authentication** - Specifies whether or not Web redirection is required.
- **Session Timeout** - The maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt.
- **Accounting Interim Interval** - Interval for RADIUS accounting, in seconds.
- **Upstream Bandwidth** - The user upstream bandwidth, in kbit/s.
- **Downstream Bandwidth** - The user downstream bandwidth, in kbit/s.
- **Allow All EAPs** - Indicates if all of the EAP methods supported by UPAM, Authenticator, and the client device are used.

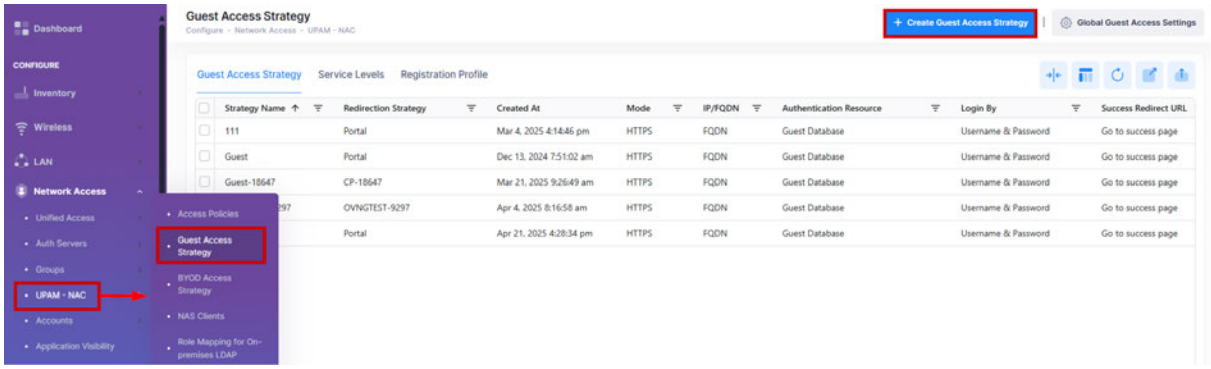
- **Allowed Methods** - Indicates which EAP methods are used (applies only when “Allow All EAPs” is set to “No”).
- **Enable Company Property Check** - Indicates if the Company Property database is checked to see if it contains the device MAC address.
- **MAC Check Access Role Profile** - The name of the Access Role Profile applied for Company Property Check.
- **MAC Check Unified Policy List** - The name of the Unified Policy List applied for Company Property Check.
- **MAC Check Other Attributes** - The attribute values applied for Company Property Check.

21 Oct 2025

7.4.2 Guest Access Strategy

The Guest Access Strategy screen displays information about configured Guest Access Strategies and is used to configure access attributes for guest users. The screen can be used to create (see page 633), edit (see page 638), and delete (see page 639)Guest Access Strategies.

To access the Guest Access Strategy screen, click on **Network Access > UPAM-NAC > Guest Access Strategy** under the “Configure” section of the OmniVista Terra Menu (see page 45).

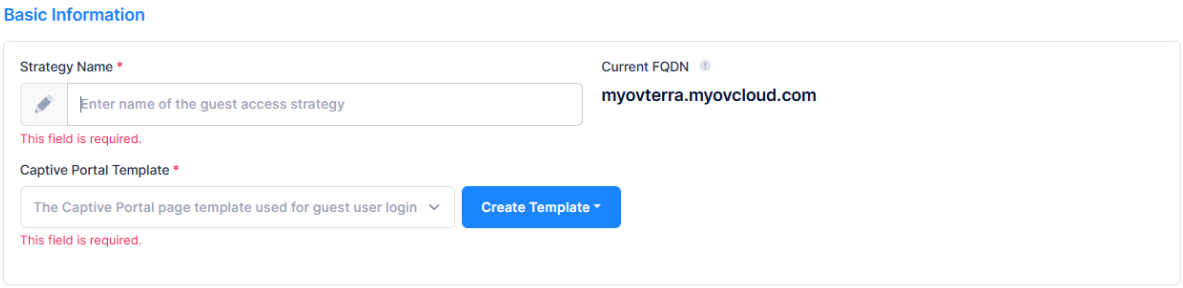


7.4.2.1 Creating a Guest Access Strategy

To add a Guest Access Strategy, click on **Create Guest Access Strategy** to open the Create Guest Access Strategy form. Complete the following sections of the form, then click **Create Guest Access Strategy** when you are finished.

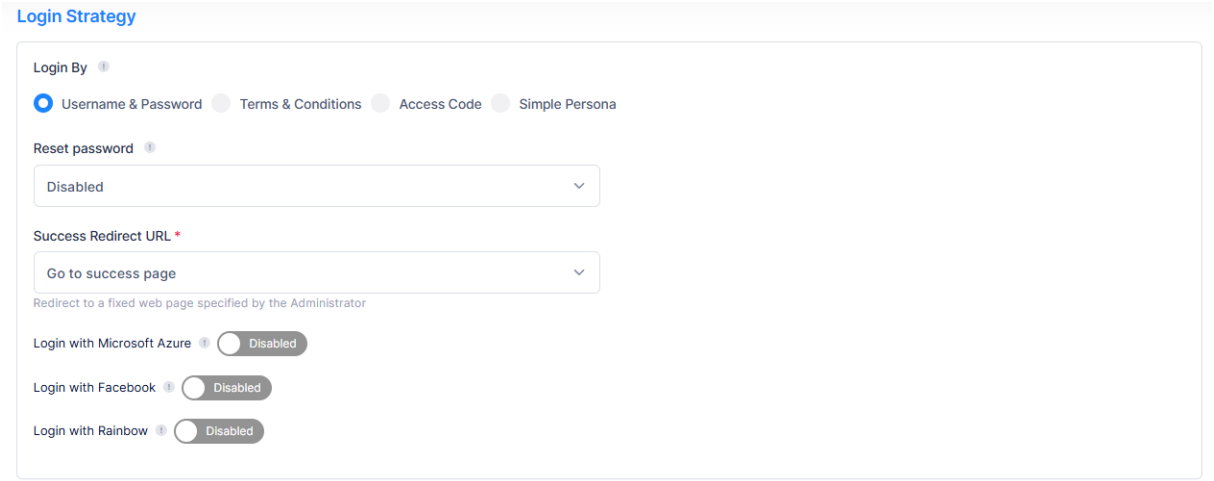
- Basic Information (see page 634) - Configure the Guest Access Strategy name and authentication attributes (Captive Portal Template, current FQDN).
- Login Strategy (see page 634) - Configure the guest user login strategy (for example, login by Username/Password, Terms & Conditions, Access Code, or Email address) and specify the success redirect URL.
- Post Portal Authentication Enforcement (see page 635) - Configure post-authentication enforcement for guest users.
- Self-Registration Strategy (see page 636) - Configure the self-registration attributes for guest user login when the guest user is required to perform self-registration and approval before accessing the network. In this case, the guest user account is automatically created and sent to the guest user through e-mail by UPAM. The self-registration strategy is only applicable when the login strategy (see page 634) is set to login by Username and Password.

7.4.2.1.1 Basic Information



- **Strategy Name** - Enter the name to assign to the Guest Access Strategy.
- **Captive Portal Template** - Select an existing Captive Portal page template to use for guest user login from the drop-down menu or click on **Create Template** to create a new template to use (see the Captive Portal Templates (see page 675) online help).
- **Current FQDN** - The Fully Qualified Domain Name to use for the Captive Portal page redirection.

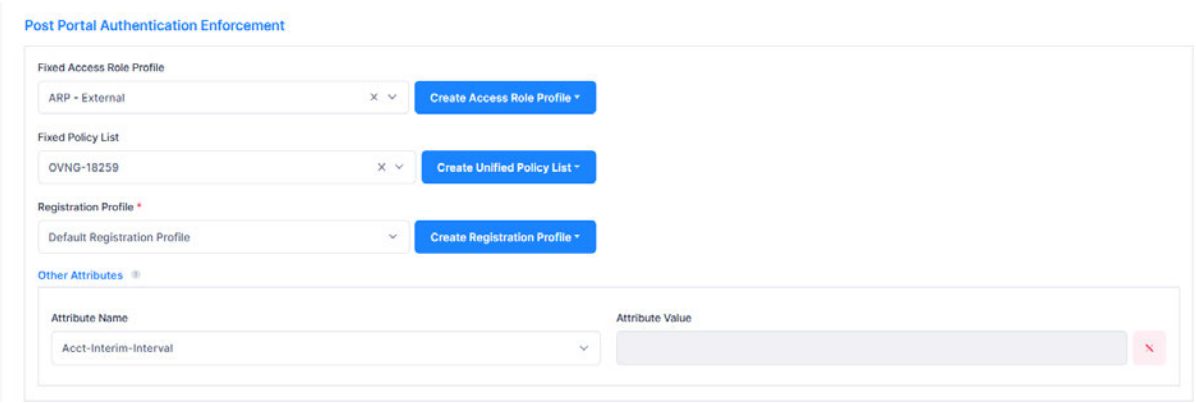
7.4.2.1.2 Login Strategy



- **Login By -** Specify the login method:
  - **Username & Password -** Guest user login by their credential (Username and Password). When this login method is selected, you can then enable and configure the following social media login options:
    - **Login with Microsoft Azure** (see page 640) - Use Microsoft Azure account for guest user login.
    - **Login with Facebook** (see page 640) - Use Facebook account for guest user login.
    - **Login with Rainbow** (see page 640) - Use Rainbow account for guest user login.
  - **Terms & Condition -** Guest user login by accepting the Terms and Conditions.
  - **Access Code -** Guest user login by a unified access code.
  - **Simple Persona** - Guest user login by email address. When this login method is selected, you can then set Custom Attributes (see page 635) and Registration Profile (see page 635) information for Simple Persona Captive Portal login.

- **Reset Password** - This option allows a guest user to change their login password without Administrator operation. When one of the following options is selected from the drop-down menu, the guest user will be able to click on the “Forget Password?” link on their account login screen to request a Verification Code to change their password:
  - **By E-mail** - The guest user receives the code through e-mail.
  - **By E-mail/SMS** - The guest user receives the code through e-mail and SMS.
  - **By SMS** - The guest user receives the code through SMS.
- **Success Redirect URL** - Specify the redirect URL for the browser after the guest user passes captive portal authentication:
  - **Go to fixed URL** - Redirect to a fixed web page. When you select this option, a “Fixed URL” field is displayed in which you enter the URL to use.
  - **Go to initial URL** - Redirect to the guest-user-input URL after passing authentication.
  - **Go to success page** - No redirect URL. Remain on the “Success” login page configured by the Administrator.
- **Custom Attributes** - Allow the Administrator to customize the attributes for guest user login to collect the guest user information. The Administrator can configure up to 20 attributes (max length 32 characters each). The configured attributes will be displayed on the Captive Portal page where the guest user can input 1 - 255 character(s) for each attribute. Note that this option is only visible for configuration when the selected login method is Terms & Conditions or Simple Persona. You can view the attribute values the user specifies during login on the Captive Portal Records (see page 889) screen after authentication.

7.4.2.1.3 Post Portal Authentication Enforcement

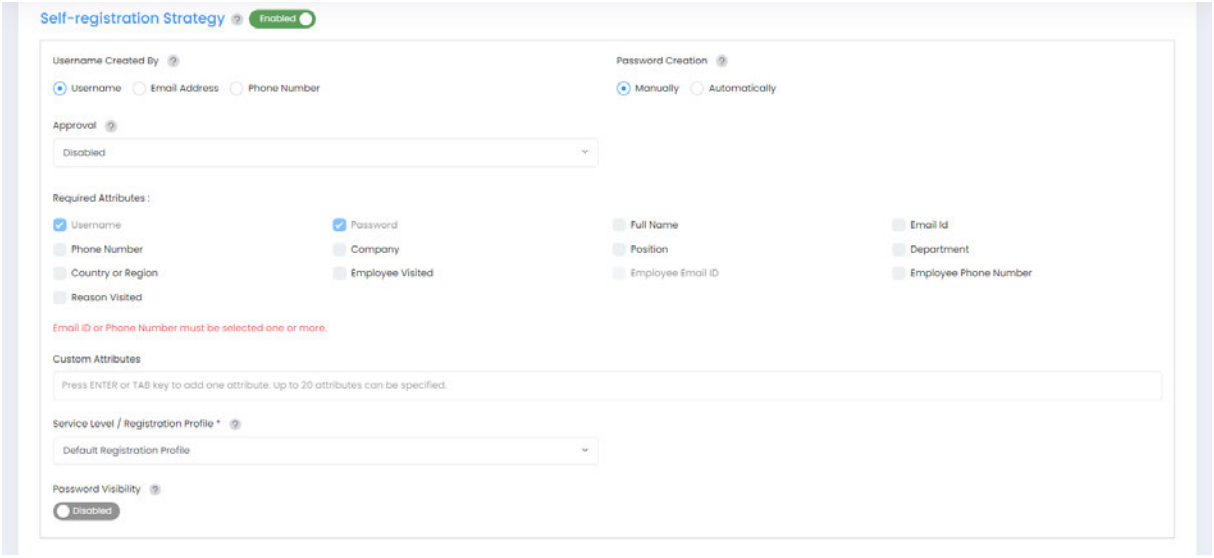


- **Fixed Access Role Profile** - The Access Role Profile assigned to the guest user after passing authentication. Select a profile from the drop-down menu or click on **Create Access Role Profile** to add a new profile to use (see the Access Role Profile (see page 514) online help).
- **Fixed Unified Policy List** - The Policy List assigned to the guest user after passing authentication. Select a list from the drop-down menu or click on **Create Unified Policy List** to add a new list to use (see the Unified Policies List (see page 551) online help).
- **Registration Profile** - The Registration Profile assigned to the guest user after passing authentication. Select a list from the drop-down menu or click on **Create Registration Profile** to add a new list to use (see the Registration Profile (see page 651) online help).

- **Other Attributes** - Select an attribute from the drop-down and enter a value. To add additional attributes, click on **Add Attribute**.
  - **Session-Timeout** - The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
  - **Acct-Interim-Interval** - The Accounting Interim Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
  - **WISPr-Bandwidth-Max-Up** - The user upstream bandwidth, in kbit/s. By default, it is not limited.
  - **WISPr-Bandwidth-Max-Down** - The user downstream bandwidth, in kbit/s. By default, it is not limited.

7.4.2.1.4 Self-Registration Strategy

The self-registration strategy is only available if the login method (see page 634) is set to Username & Password.



- **Self-Registration Strategy** - Enable or disable the self-registration feature. When enabled:
  - **Username Created By** - The field from which the guest user account is retrieved, the information is entered by the guest user in the self-registration login page:
    - **Username** - Login account for the guest user.
    - **Email Address** – Email address of the guest user.
    - **Phone Number** - Phone number of the guest user.
- **Password Creation** - The method for creating a password:
  - **Manually -** Password for guest user account is set by guest user in the self-registration web page.

    - **Automatically -** Password for guest user account is automatically generated by UPAM and sent to guest user through E-mail.
- **Approval -** Specify whether the guest registration request is required to be approved by a sponsor in the company or a guest operator. The employee sponsor could be an Administrator or employee the guest is going to visit.
    - **Disabled -** Approval by an employee or guest operator in not required.
    - **Approved by Employee Sponsor -** Approval by the employee specified in the Self-Registration Request Screen is required.
        - **Email Restriction** - Select **Suffix** or **Full Email**.
            - **Suffix -** Enter the employee sponsor e-mail suffix(es). This is the e-mail suffix used by the company employee, which will be combined with a specific employee e- mail ID to form a full e-mail address. The registration request will be sent to this e-mail address.
            - **Full Email -** Enter the full employee e-mail address.
    - **Approved by Guest Operator -** Approval by a guest operator specified on the Guest Operator screen is required.
        - **Location-Based Notification -** Enables/Disables location-based notification. When enabled, send the guest request to guest operators for the specific location. When disabled, send the guest request to all operators.
- **Required Attributes -** Customize the information fields that the guest user is required to input during self-registration. Certain fields are required and pre-configured for employee sponsor or guest operator approval.
    - **Username -** Login user name for the guest user.
    - **Password -** Login password for the guest user. If the password creation method is set to “Automatically”, the guest user does not have to enter this field.
    - **Full Name -** Full name of the guest user.
    - **Email ID-** Email address of the guest user.
    - **Phone Number -** Phone number of the guest user.
    - **Company -** Name of the company the guest user is representing.
    - **Position -** Position of the guest user in their company.
    - **Department –** Department of the guest user in their company.
    - **Country or Region -** Country or region of the guest user’s company.
    - **Employee Visited -** The employee being visited by the guest user.
    - **Employee Email ID -** Email address of the employee being visited.
    - **Employee Phone Number -** Phone number of the employee being visited.
    - **Reason Visited -** The purpose of the guest user’s visit.
- **Custom Attributes -** Allow the Administrator to customize the attributes for guest self-registration to collect the guest user information. The Administrator can configure up to 20 attributes (max length 32 characters each). The configured attributes will be displayed in the self-registration page where the guest user can input 1 - 255 character(s) for each attribute.

- **Service Level/Registration Profile** - Select a Service Level or Registration Profile from the drop-down menu. A “Default Registration Profile” is selected by default. To display, create, edit, or delete a Service Level or Registration Profile, click Settings (see page 641)at the top-right of the Guest Access Strategy screen.
- **Authorize by Verification Code -** If the e-mail or phone number is required, Enables/Disables whether to send a verification code to specified address to ensure the e-mail or phone number is correct.
- **Password Visibility -** Enables/Disables whether to display account information such as name and password on the Registration Result Page.

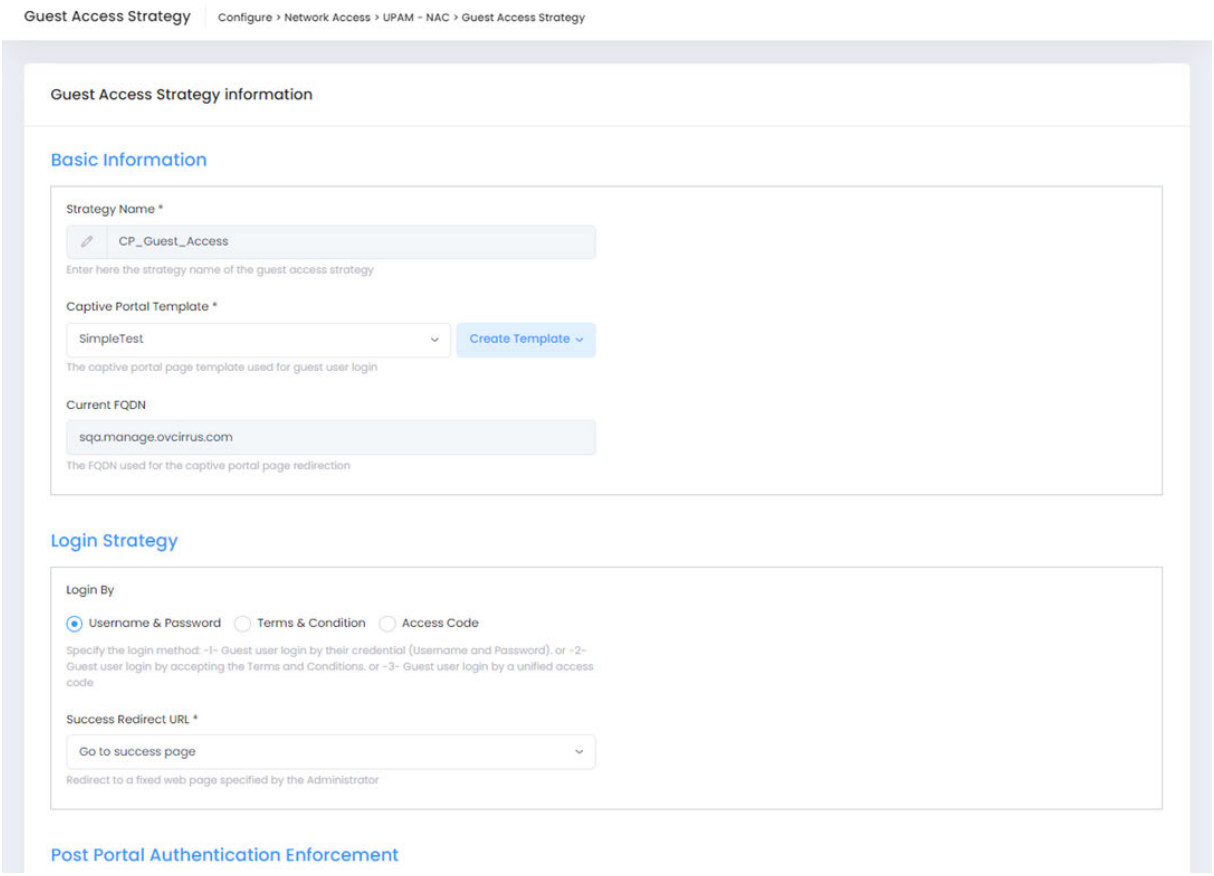
7.4.2.1.5 WiFi4EU

WiFi4EU provides free access to public Wi-Fi in parks, schools, public buildings, and health centers throughout the Country.

- **WiFi4EU -** Enables/Disables WiFi4EU. To use the WiFi4EU feature, the “Redirect Strategy“ must use the specified WiFi4EU template for the Captive Portal page. In addition, the validity period for Captive Portal authentication must be no more than 24 hours per the WiFi4EU requirement. This value can be changed in Registration Strategy from the Global Configuration (see page 642) screen.
- **Network Identifier -** The Network Identifier received from the WiFi4EU portal as part of the Installation report.
- **Self Test Modus -** The WiFi4EU portal self-test mode. (Default = Disabled).

7.4.2.2 Editing a Guest Access Strategy

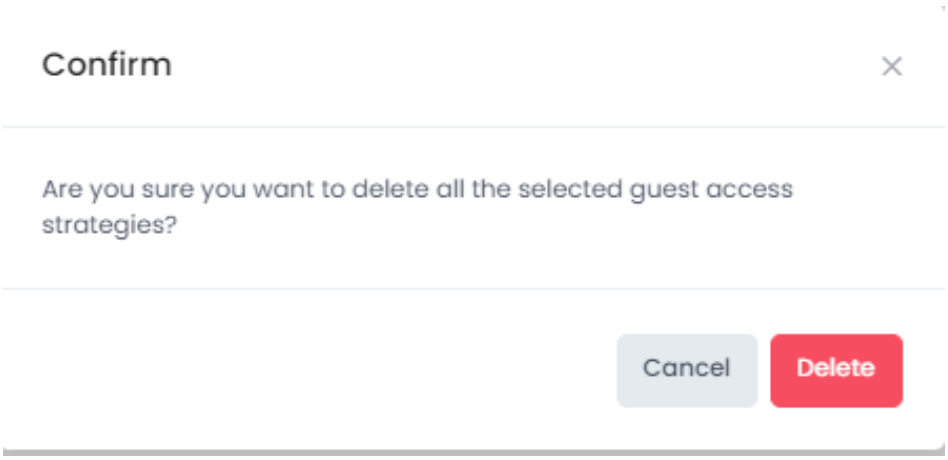
Select a Guest Access Strategy in the Guest Access Strategy List and click on the Edit icon under the “Actions” column or click on the **Actions** button and select Edit from the drop-down menu. The Guest Access Strategy Information screen opens on which you can edit any of the strategy attributes, as described above (see page 633). Note that you cannot change the Strategy Name.



After you have edited the Guest Access Strategy, click **Save**.

7.4.2.3 Deleting a Guest Access Strategy

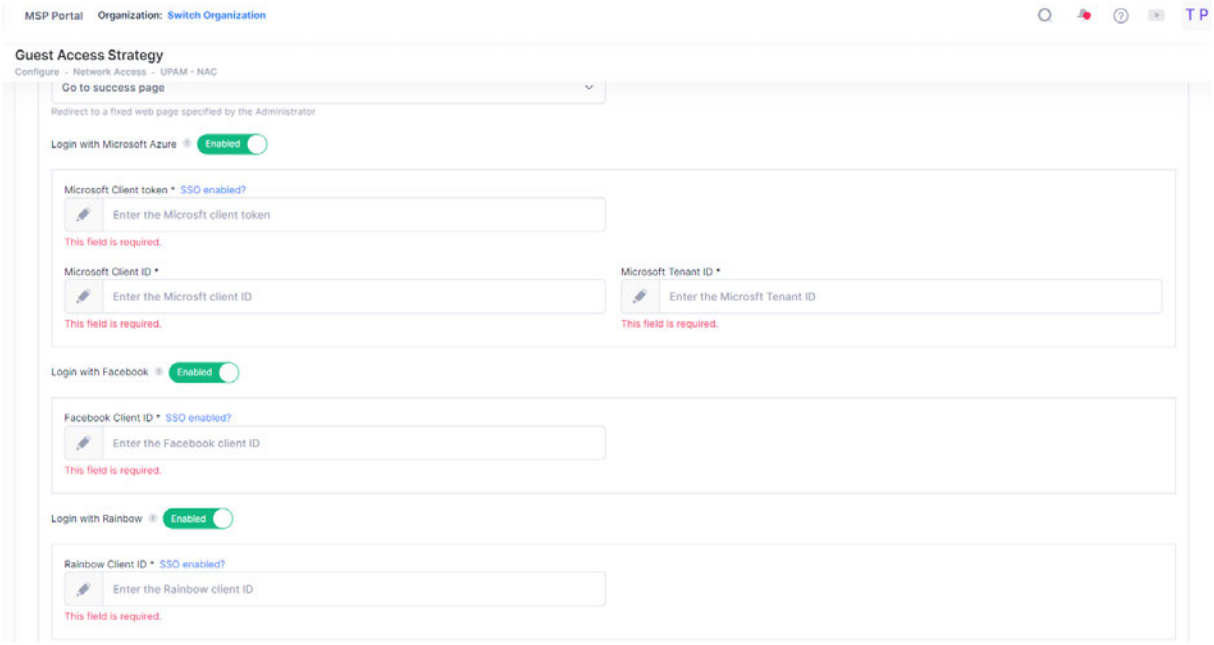
Select a Guest Access Strategy in the Guest Access Strategy List and click on the Delete icon under the “Actions” column or click on the **Actions** button and select Delete from the drop-down menu. When the following confirmation prompt appears, click on **Delete** to delete the profile.



7.4.2.4 Social Media Login Options

When you select the Username & Password login method, you can enable or disable (the default) using a Microsoft Azure, Facebook, and Rainbow accounts for guest user login. When you enable one or more of the social media login options, you are prompted to enter login information, as shown below.

Complete the fields below for social media login. Note that you must also configure the Wireless Client Social Login Vendor in an Access Role Profile (see page 514) for the applicable Social Media account (Microsoft Azure, Facebook, Rainbow).

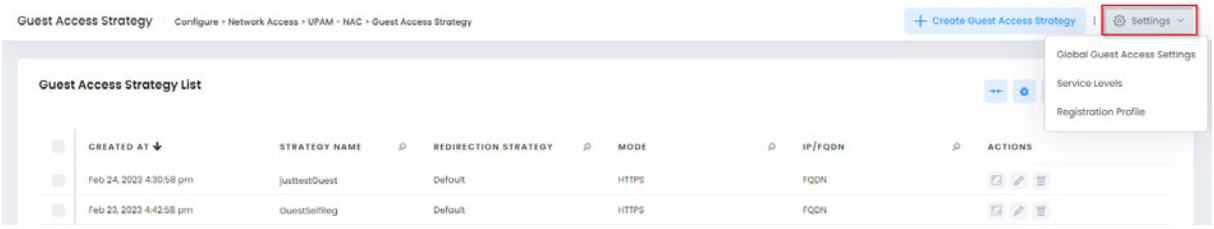


- **Login with Microsoft Azure** - Click to enable/disable this social media login option. When enabled, enter the following information for Microsoft OpenID Connect:
  - **Microsoft Client Token** - Enter the Microsoft Azure AD token.
  - **Microsoft Client ID** - Enter the Microsoft Azure AD client ID.
  - **Microsoft Tenant ID** - Enter the Microsoft Azure AD tenant ID.
- **Login with Facebook** - Click to enable/disable this social media login option. When enabled, enter the following information for Facebook OICD login:
  - **Facebook Client ID** - Enter the OAuth Client ID provided by Facebook.
- **Login with Rainbow** - Click to enable/disable this social media login option. When enabled, enter the following information for Rainbow login:
  - **Rainbow Client ID** - Enter the OAuth Client ID provided by Rainbow.

Note: If SSO integration is enabled, then add the SSO Provider Domain in the Allow List Domains of the Access Role Profile for the user.

7.4.2.5 Guest Access Strategy Settings

To display and configure global Guest Access settings, click **Settings** at the top-right corner of the Guest Access Strategy screen (as shown below).



When yo click on **Settings**, a drop-down menu displays the following options:

- **Global Guest Access Settings** (see page 642) - Select this option to enable the Batch Creation feature on the Guest Accounts (see page 727) screen and configure the required Registration Strategy fields that are required when "Terms & Condition" is selected as the guest user login method (see page 634).
- **Service Levels** (see page 645) - Configure the different service levels for a guest account by binding various levels of Access Roles and Policies. You can configure a Service Level for different guests when creating an account on the Guest Accounts (see page 727) screen.
- **Registration Profile** (see page 651) - Configure Data and Time Quota limits for user access, Device and Account Validity attributes, and Exhaustion Handling options (when Quota limits are reached). You can configure a Registration Profile for different guests when creating an account on the Guest Accounts (see page 727) screen.

> The global Settings options are used to set global configurations for Guest Access Strategy and Guest Accounts. Note that any global configuration changes you make will only be applied to Guest Accounts created after the changes are made. The configurations of existing accounts will not change.

21 Oct 2025

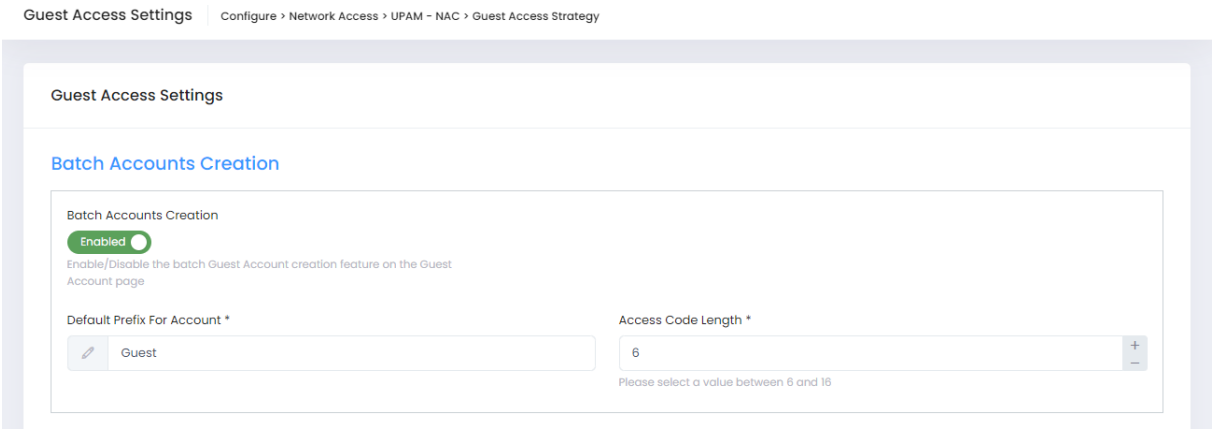
7.4.2.6 Global Guest Access Settings

When you click **Settings** on the Guest Access Strategy (see page 633) screen and select the **Global Guest Access Settings** option, the Guest Access Settings screen opens. This screen is used to set the Batch Account Creation (see page 642) and Registration Strategy (see page 642) settings for Guest Access Strategy and Guest Accounts. Complete the fields as described below, then click **Save**.

> Note that any global configuration changes you make will only be applied to Guest Accounts created after the changes are made. The configurations of existing accounts will not change.

7.4.2.6.1 Batch Account Creation

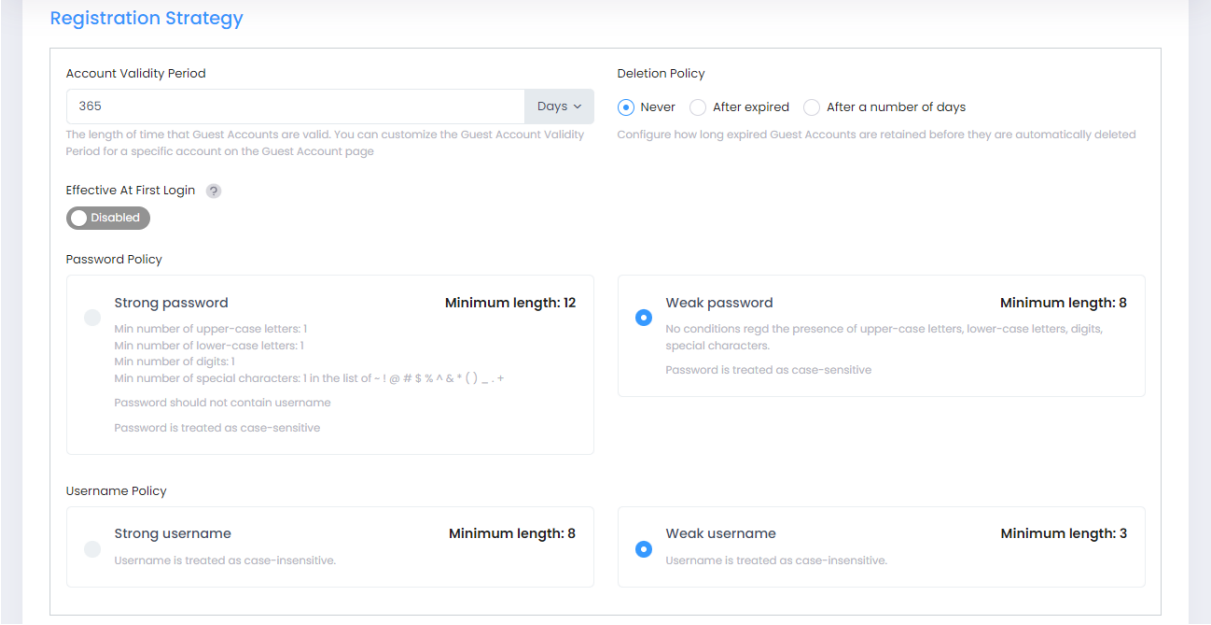
Batch Account creation enables you to quickly create batch accounts for Guest Users. Guest Accounts are configured on the Guest Account (see page 727) screen.



- **Batch Account Creation -** Enable/Disable the batch Guest Account creation function on the Guest Account page.
- **Default Prefix For Account -** Enter a default prefix used for batch Guest Account creation.
- **Access Code Length -** If Batch Account Creation is Enabled, you can set the Access Code Length for the created Guest Accounts (Range = 6 - 16, Default = 6).

7.4.2.6.2 Registration Strategy

Configures the basic Guest Account Registration strategy.



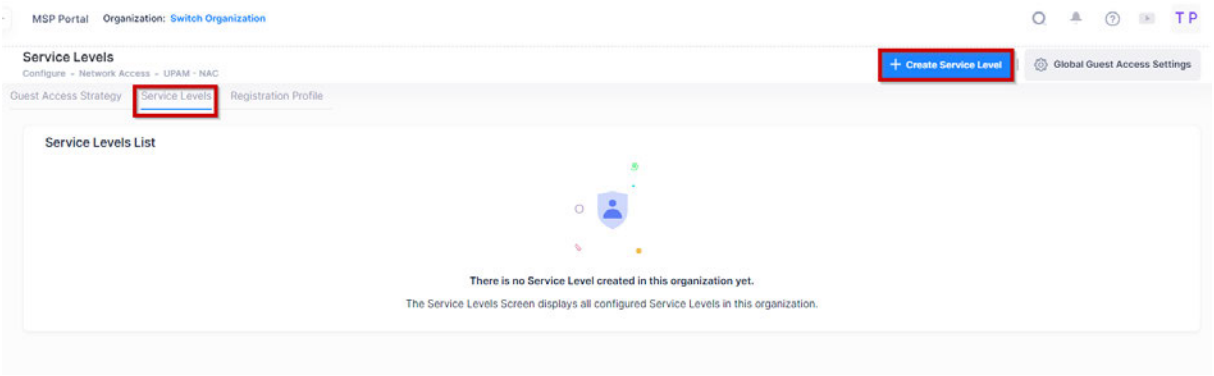
- **Account Validity Period** - Specify the length of time that Guest Accounts are valid. (Range = 1 – 365 Days, Default = 90 Days). You can customize the Guest Account Validity Period for a specific account on the Guest Accounts (see page 727) screen. However, the range you can set on the Guest Accounts page cannot be longer than the length set here. For example, if you set the global Account Validity Period to 180 days, the longest period you will be able to set on the Guest Account page will be up to 180 days.
- **Deletion Policy** - Configure how long expired Guest Accounts are retained before they are automatically deleted:
  - **Never -** Guest Accounts will **not** be deleted at the end of the Account Validity Period (Default).
  - **After Expired -** Guest Accounts will be automatically deleted at the end of the Account Validity Period.
  - **After Number of Days -** Guest Accounts will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).
- **Effective at First Login** - Specify when the Account Validity period begins. If enabled, the Guest Accounts created will begin their Account Validity Period the first time the user logs in. If disabled, the Validity Period begins when the Guest Account is created (Enabled/Disabled, Default = Disabled).
- **Password Policy** - Select the password policy to enforce when the user logins in.
  - **Strong Password** - Minimum password length is 12 with the following required guidelines:
    - Min number of upper-case letters: 1
    - Min number of lower-case letters: 1
    - Min number of digits: 1
    - Min number of special characters: 1 in the list of ~ ! @ # $ % ^ & * ( ) _ . +
    - Password should not contain username
    - Password is treated as case-sensitive

  - **Weak Password** (Default) - Minimum password length is 8 with no required guidelines. Password is case-sensitive.
- **Username Policy** - Select the username policy to enforce when the user logins in.
  - **Strong Username** - Minimum username length is 8 characters. Username is case insensitive.
  - **Weak Username** - Minimum username length is 3 characters. Username is case insensitive.

21 Oct 2025

7.4.2.7 Service Levels

When a Guest Account is created or edited, an optional Service Level from the global Service Levels List can be assigned to the account. To access the global Service Levels screen, click **Settings** on the Guest Access Strategy (see page 633) screen or the Guest Accounts (see page 727) screen and select **Service Levels** from the drop-down menu. The Service Levels screen displays a list of configured Service Levels.

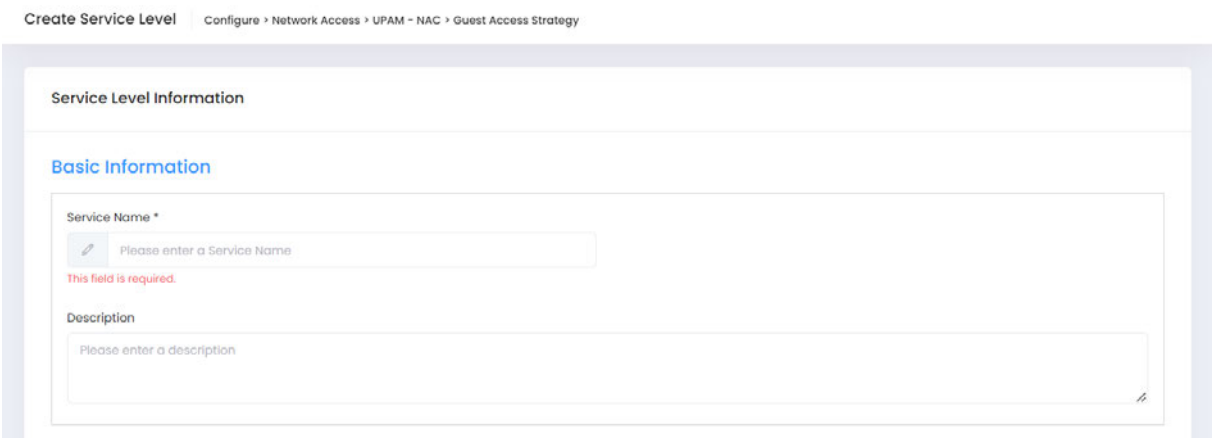


Use the Service Levels screen to display information (see page 649) about all configured Service Levels. This screen is also used to create (see page 645), edit (see page 647) , and delete (see page 648)Service Levels.

7.4.2.7.1 Creating a Global Service Level

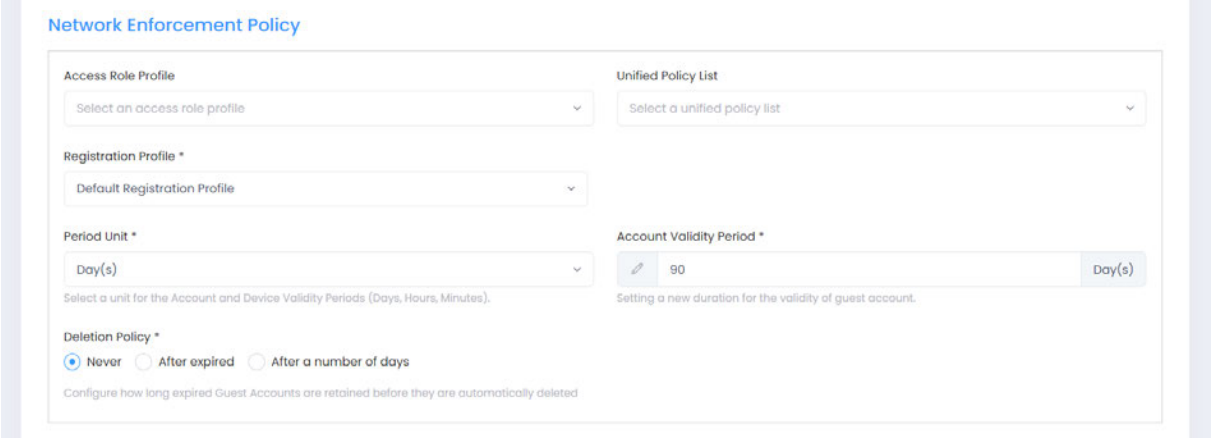
To create a new Service Level, click on **Create Service Level** to open the Create Service Level screen. Complete the following sections, as described below.

Basic Information



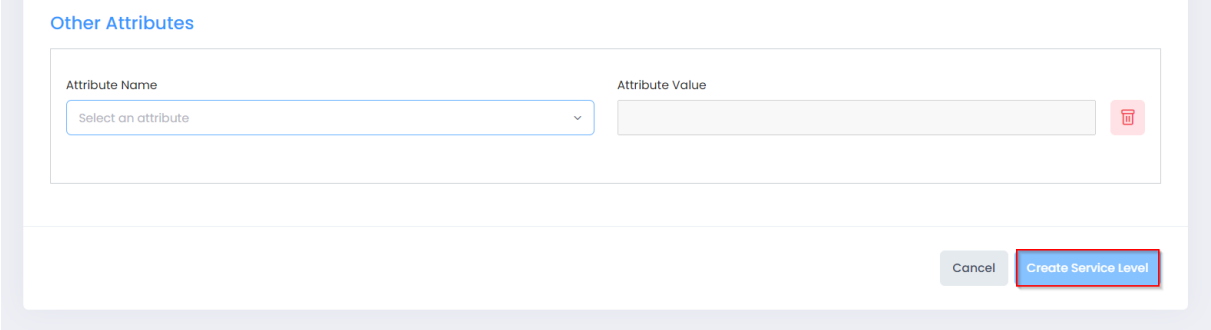
- **Service Name** - Enter a unique name to assign to the Service Level.
- **Description -** Optional description for the Service Level.

Network Enforcement Policy



- **Access Role Profile** - Select an Access Role Profile for the Service Level.
- **Unified Policy List** - Select a Unified Policy List for the Service Level.
- **Registration Profile** - Select a Registration Profile for the Service Level. By default, the "Default Registration Profile" is used.
- **Period Unit -** Specify the unit for the Account Validity Period attribute (Days, Hours, Minutes).
- **Account Validity Period** - Specify the length of time that Guest Accounts are valid. (Range = 1 – 365 Days, Default = 90 Days). This value is applied to Guest Accounts that are linked to this Service Level. If a Service Level is not linked to a Guest Account, then the default validity period configured on the Global Guest Access Settings (see page 642) screen is applied. You can also customize the Account Validity Period for a specific account on the Guest Accounts (see page 727) screen.
- **Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Accounts will **not** be deleted at the end of the Account Validity Period (Default).
  - **After Expired -** Guest Accounts will be automatically deleted at the end of the Account Validity Period.
  - **After Number of Days -** Guest Accounts will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).

Other Attributes



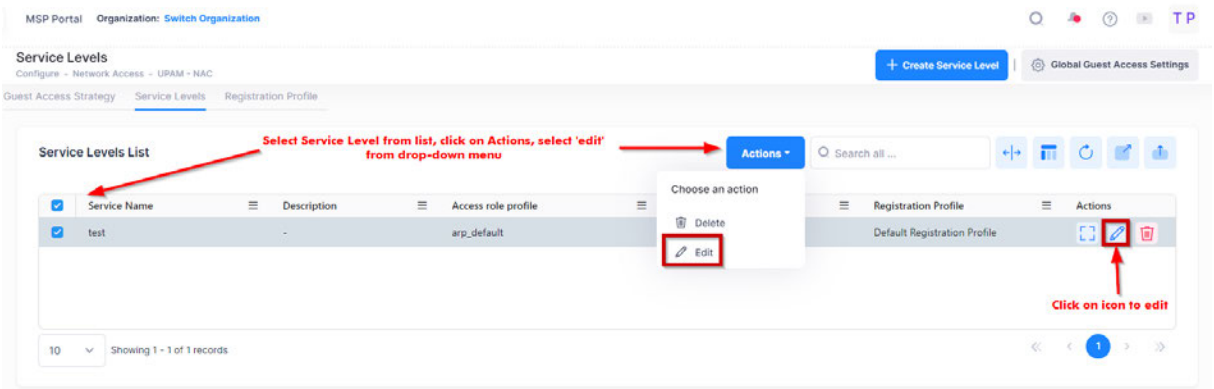
Select one of the following attributes from the drop-down, enter a value, and click on **Add Attribute**. Repeat this process to add more attributes to the Service Level.

- **Acct-Interim-Interval** - The Accounting Interim Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
- **Session-Timeout** - The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
- **WISPr-Bandwidth-Max-Up** - The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr-Bandwidth-Max-Down** - The user downstream bandwidth, in kbit/s. By default, it is not limited.

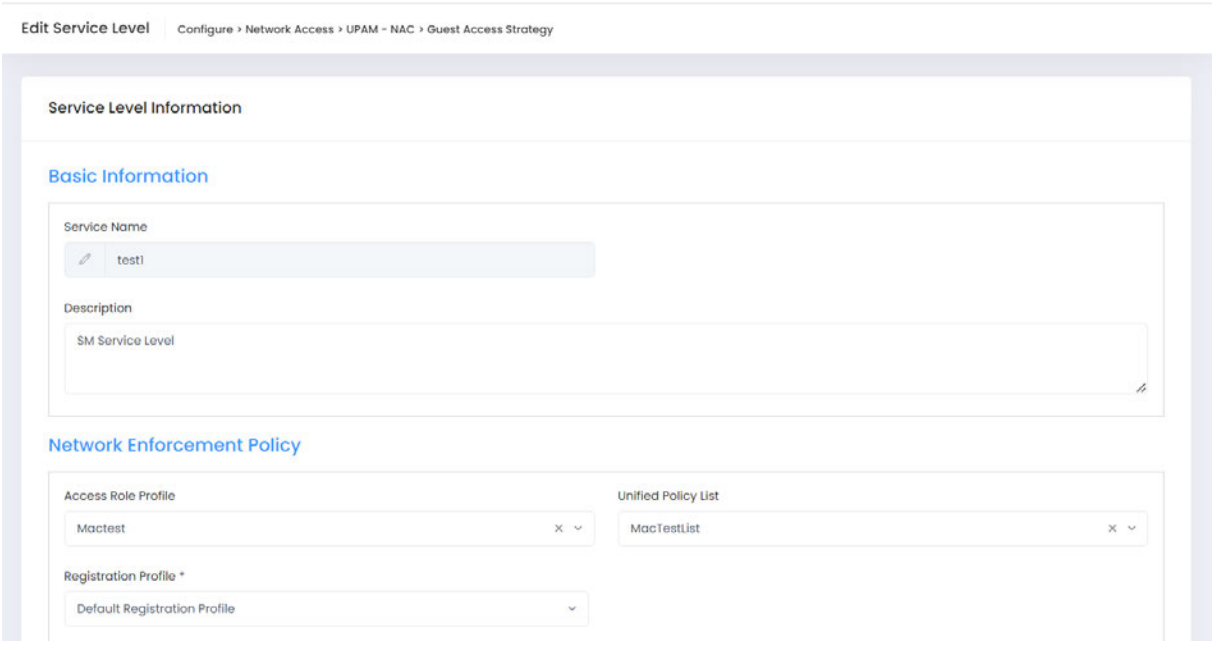
7.4.2.7.2 Editing a Global Service Level

You can edit the values for an existing Service Level by accessing the Edit Service Level screen. Use one of the following methods to access this screen:

- Select the Service Level entry to edit by clicking o the checkbox next to the entry, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the "Actions" column next to the Service Level entry that you want to edit.



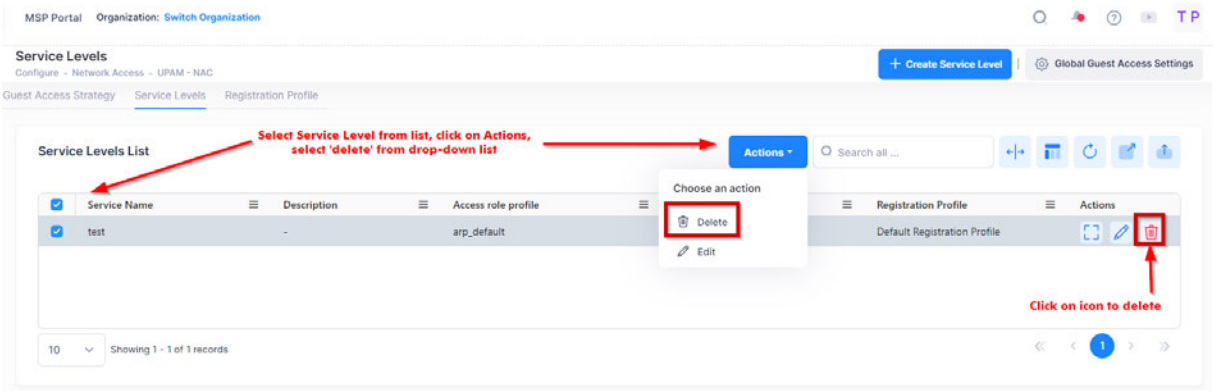
The following Edit Service Level screen displays. Edit the fields as described above (see page 645), then click on **Save**.



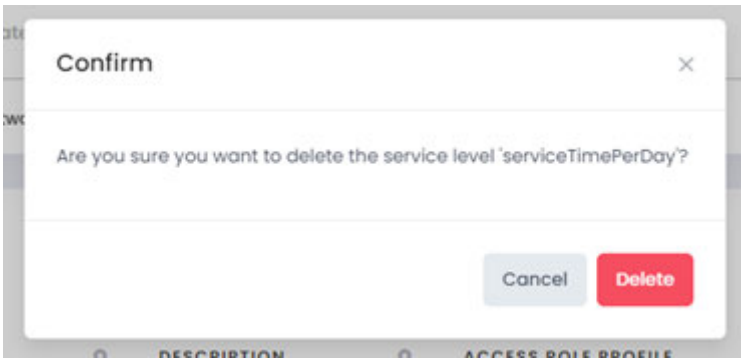
7.4.2.7.3 Deleting a Global Service Level

To delete a global Service Level, use one of the following methods to select the Service Level you want to delete:

- Select the Service Level entry to delete by clicking on the checkbox next to the entry, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the Service Level entry that you want to delete.

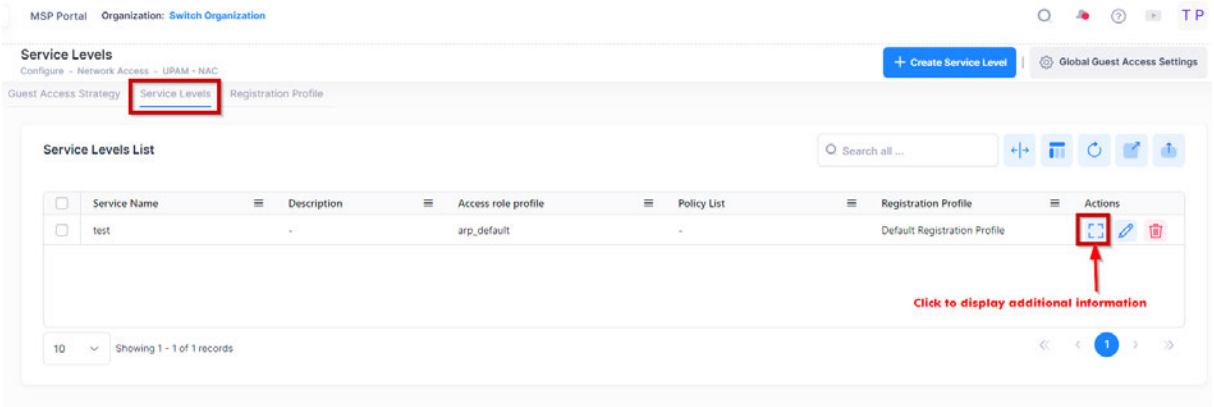


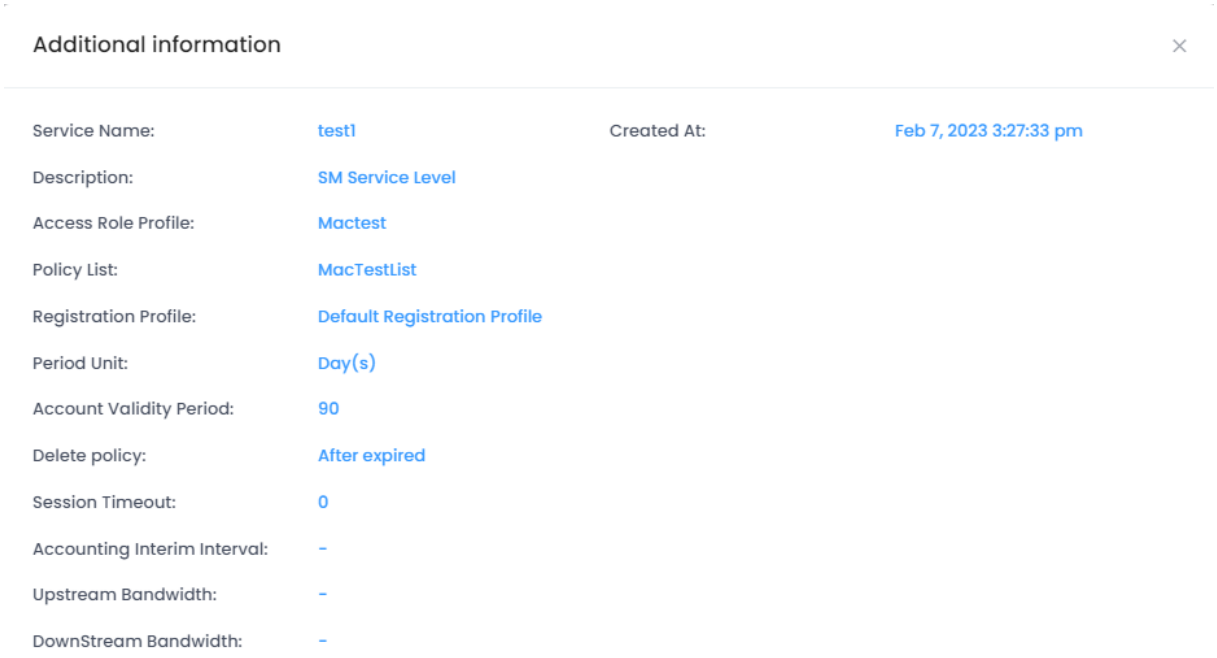
When the following confirmation prompt appears, click **Delete** to delete the profile.



7.4.2.7.4 Display Service Level Information

The Service Levels list displays information for the configured Service Levels. To display information about a specific Service Level, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is shown below.




Additional information
Service Name:
test1
Created At:
Feb 7, 2023 3:27:33 pm
Description:
SM Service Level
Access Role Profile:
Mactest
Policy List:
MacTestList
Registration Profile:
Default Registration Profile
Period Unit:
Day(s)
Account Validity Period:
90
Delete policy:
After expired
Session Timeout:
0
Accounting Interim Interval:
-
Upstream Bandwidth:
-
DownStream Bandwidth:
-

21 Oct 2025

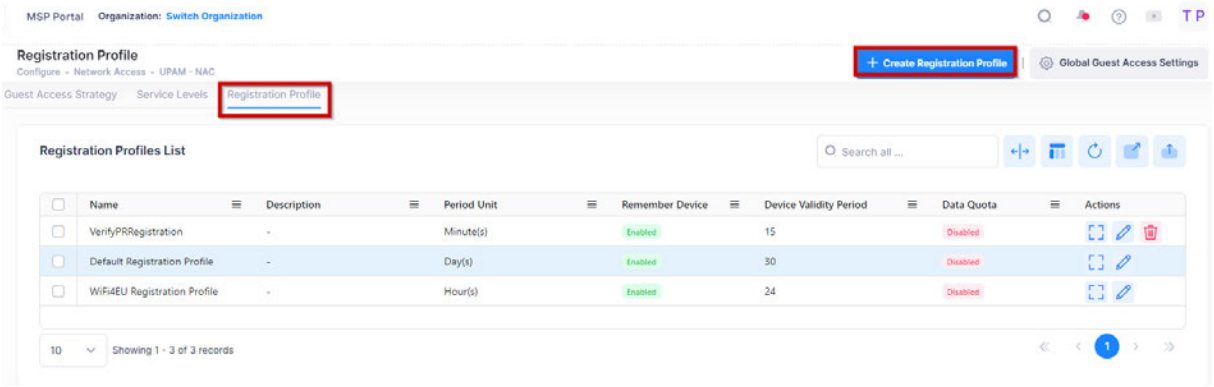
7.4.2.8 Registration Profiles

The Registration Profile determines Data and Time Quota limits for user access, Device and Account Validity attributes, and Exhaustion Handling (when Quota limits are reached).

A Registration Profile is specified during Guest Access Strategy configuration as follows:

- When the Username & Password login method is selected and Self-Registration is enabled, there is a Registration Profile/Service Level option for Self-Registration. By default, the “Default Registration Profile” is used (if a Service Level is not specified) or you can select another existing Registration Profile.
- If a Registration Profile is assigned to a Service Level and the Service Level is specified for Self-Registration, then the Service Level Registration Profile is used.
- When Terms & Conditions or Simple Persona is the selected login method. there is a Registration Profile option for Post Portal Authentication Enforcement. By default, the “Default Registration Profile” is used or you can select another existing Registration Profile.

When a Guest Account is created or edited, a Registration Profile (or optional Service Level linked to a Registration Profile) from the Registration Profiles List can be assigned to the account. To access the Registration Profiles screen, click **Settings** on the Guest Access Strategy (see page 633) or Guest Accounts (see page 727) screen and select **Registration Profile** from the drop-down menu. The Registration Profile screen displays a list of configured Registration Profiles.

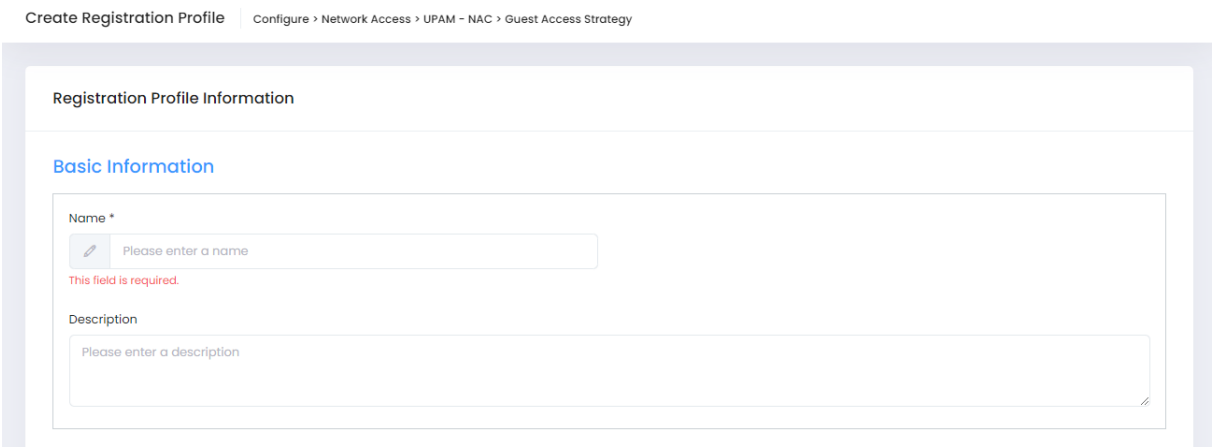


Use the Registration Profile screen to display information (see page 656) about configured Registration Profiles. This screen is also used to create (see page 652), edit (see page 655), and delete (see page 655)Registration Profiles.

7.4.2.8.1 Creating a Registration Profile

To create a new Registration profile, click on **Create Registration Profile** to open the Create Registration Profile screen. Complete the following sections, as described below.

Basic Information



- **Name** - Enter a unique name to identify the Registration Profile.
- **Description** - Enter an optional description for the Registration Profile.

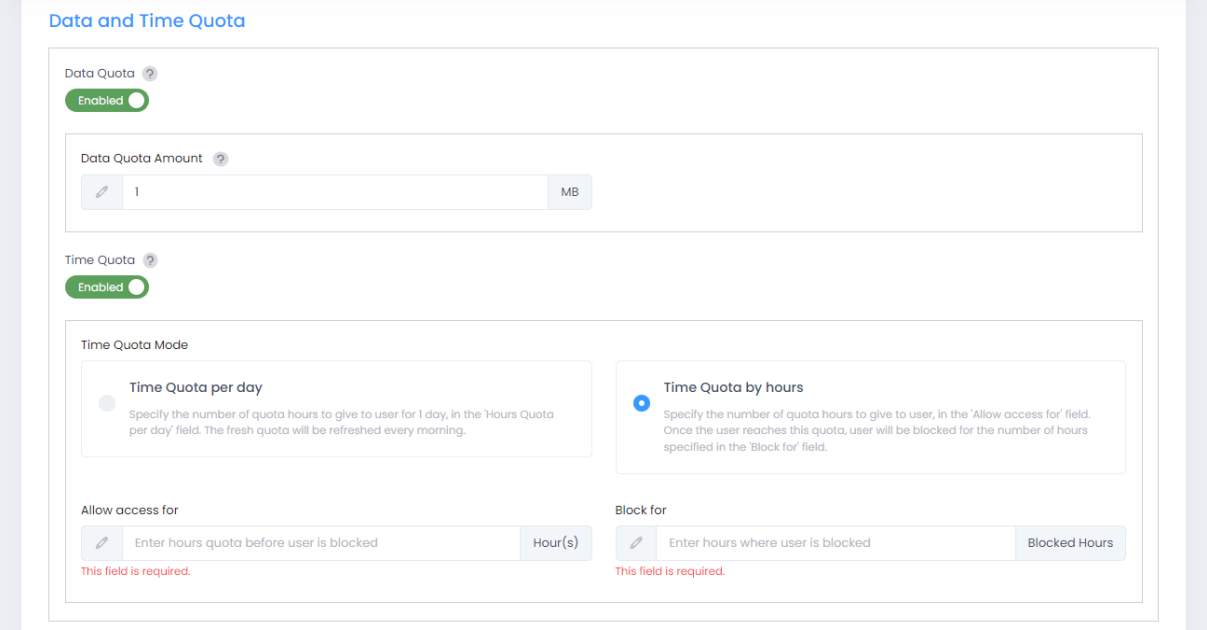
Data and Time Quota

Specify whether to control guest access based on user data quota and/or time quota. The Data Quota limit is applied only to a user who logs in with username and password credentials. It will not be applied to a user who logs in with an access code or a user who just accepts the terms and conditions.

You can have a data quota limit and a time quota limit enabled at the same time. If both limits are active, the data quota is reset whenever the time quota is reset. For example, When the Time Quota is set to 10 hours per-day and the Data Quota is specified as 5MB:

- If the user reaches the 5MB Data Quota before the Time Quota is reached, Exhaustion Handling (see page 654) is triggered for the user. The next day, the Time Quota of 10 hours and Data Quota of 5MB resets.
- If the user reaches the 10 hour Time Quota before the Data Quota is reached, Exhaustion Handling (see page 651) is triggered for the user. The next day, the Time Quota of 10 hours and Data Quota of 5MB resets.

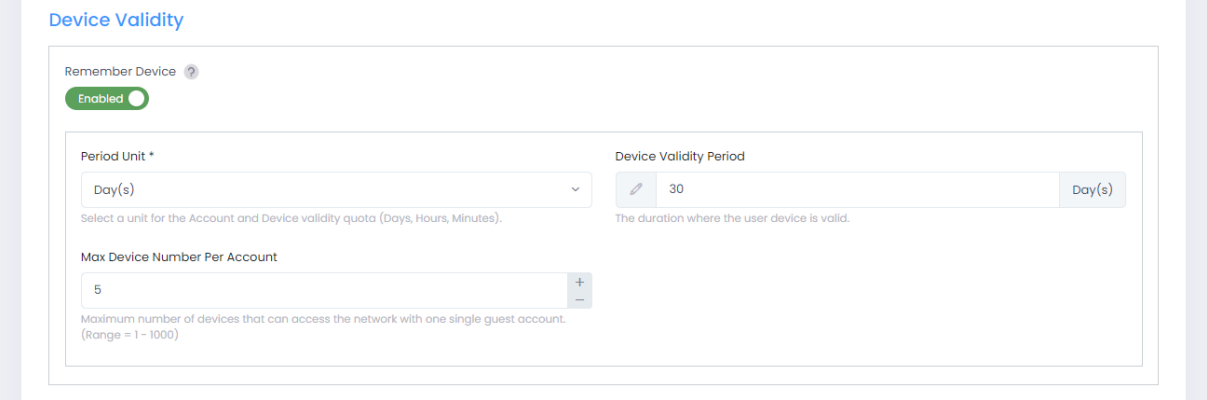
> The enforcement of Time and Data Quotas depends on the timing of when OmniVista Terra receives accounting packets from the Access Point. You can adjust the interval at which the Access Point sends the accounting packets by configuring the “Acct-Interim-Interval” attribute in the Guest Access Strategy (see page 635) for the user. The accounting interval attribute is set to 10 minutes by default.



- **Data Quota** - Enable or disable a data quota for guest traffic. When enabled:
  - **Data Quota Amount** - Specify the guest traffic quota, in MB, for the Guest Access Strategy.
- **Time Quota** - Enable or disable a time quota for guest traffic. When enabled:
  - **Time Quota Mode** - Select whether the time quota is applied on a per-day basis or for specific hours for the Guest Access Strategy.
    - **Time Quota per day** - When this mode is selected, specify the number of hours each day that the time quota is applied to guest traffic. The quota is reset at the beginning of each day.
    - **Time Quota by hours** - When this mode is selected:
      - **Allow access for** - Specify the number of hours that guest traffic is allowed.
      - **Block for** - Specify the number of hours to block guest traffic once the number of hours allowed is reached. After the number of hours to block is reached, the number of hours to allow guest traffic starts up again.

You can customize the data quota and/or time quota for different guests when creating accounts on the Guest Accounts (see page 727) screen.

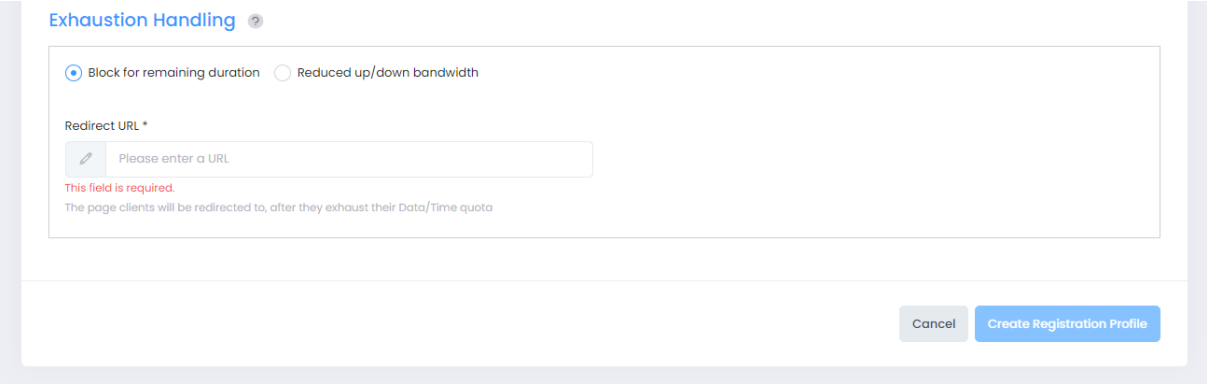
Device Validity



- **Remember Device** - Enable or disable whether to remember the device MAC address and make it valid after successful authentication. If the remembered device is valid, the MAC address check will be performed first and the device allowed access without re-authentication.
  - **Period Unit** - Select whether the validity period will be applied in days, hours, or minutes.
  - **Device Validity Period -** The length of time that the user device is valid. (Range = 1 – 365 Days, Default = 30 Days).
  - **Max Device Number Per Account -** The maximum number of devices that can access the network with one single account. (Range = 1 – 500,000, Default = 5).

Exhaustion Handling

Exhaustion Handling is active only if Data Quota and/or Time Quota is enabled.



Select one of the following options to specify the Exhaustion Handling method applied when a user reaches the Data Quota or Time Quota limit:

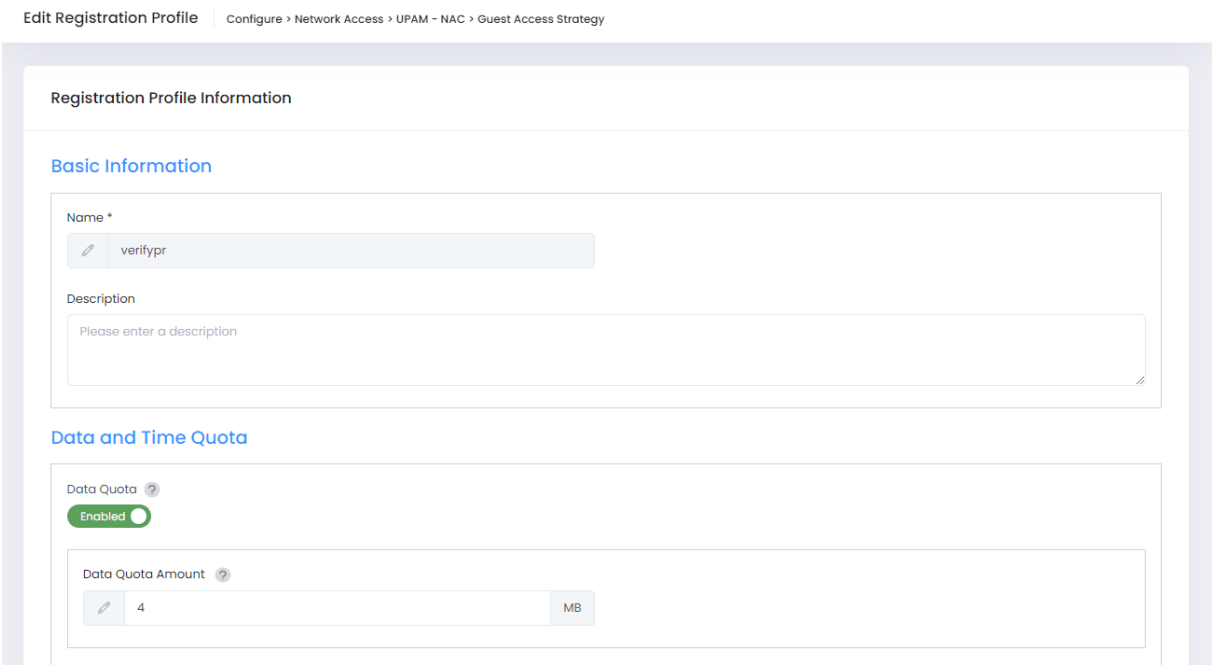
- **Block for remaining duration** - Block the user access for the remaining duration. If this option is selected, specify the following:

- **Redirect URL** - The URL of the page users are redirected to notifying them that they have exhausted the Data or Time Quota. Make sure that the specified URL is included as an allowed domain in the Access Role Profile (see page 520) associated with the SSID that the client has joined.

- **Reduced Up/Down Bandwidth** - Change the up/down bandwidth for the remaining duration.
  - **Up Bandwidth** - Reduce the AP-to-Client bandwidth. (Default = 100)
  - **Down Bandwidth** - Reduce the Client-to-AP bandwidth. (Default = 1000)

7.4.2.8.2 Editing a Registration Profile

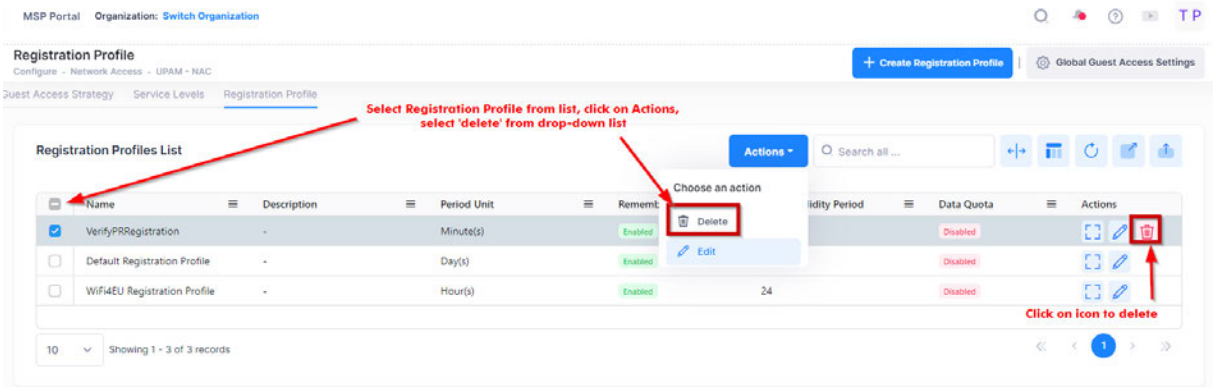
You can edit the values for an existing Registration Profile by accessing the Edit Registration Profile screen. Select the Registration Profile that you want to edit, then click on the pencil icon under the “Actions” column next to the profile entry. The following Edit Registration Profile screen displays. Edit the fields as described above (see page 652), then click on **Save**.



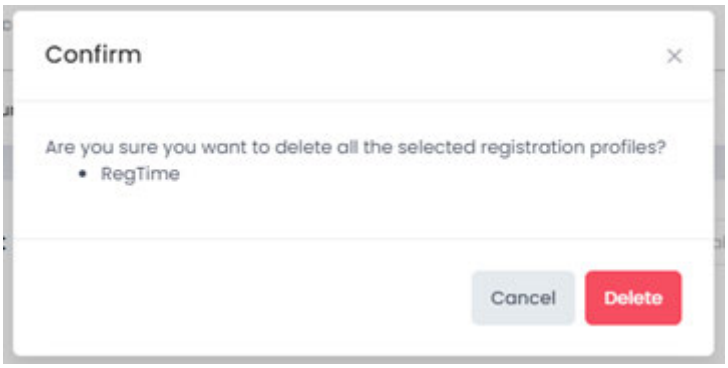
7.4.2.8.3 Deleting a Registration Profile

To delete a global Registration Profile, use one of the following methods to select the profile that you want to delete:

- Select the Registration Profile entry to delete by clicking on the checkbox next to the entry, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash can icon under the “Actions” column next to the Service Level entry that you want to delete.



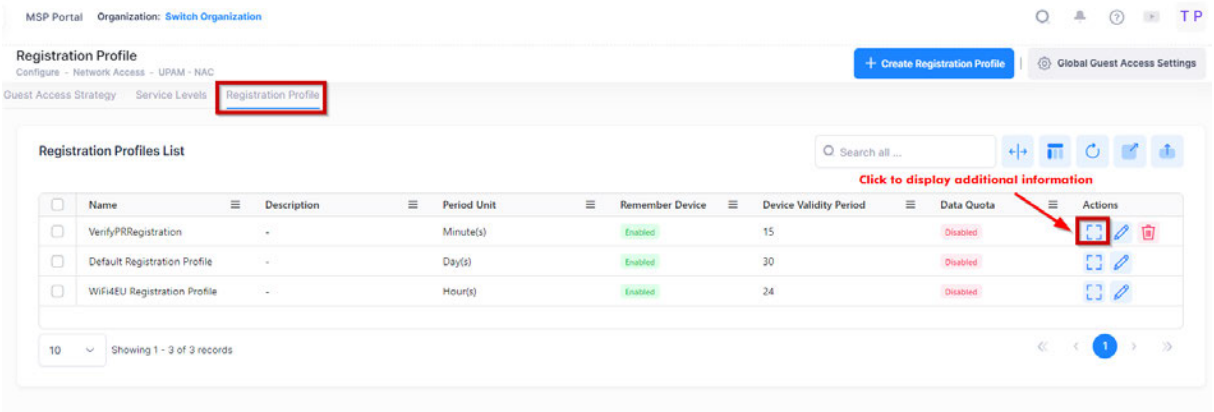
When you select the Registration Profile that you want to delete, the following confirmation prompt appears:

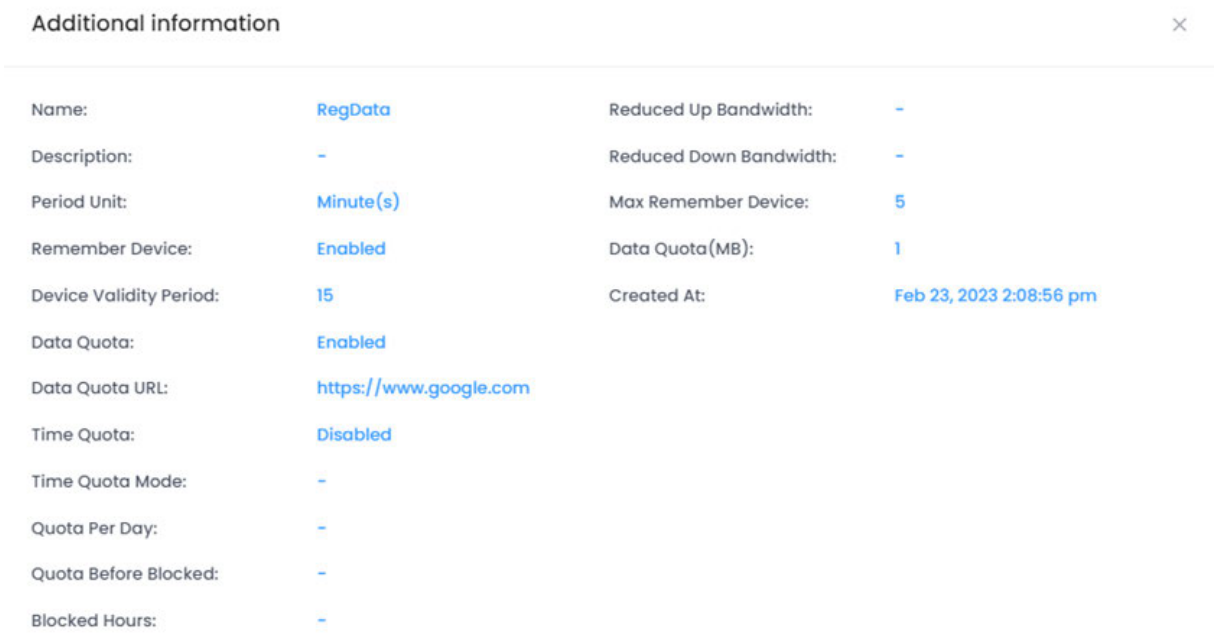


Click on **Delete** to confirm that you want to delete the selected profile.

7.4.2.8.4 Display Registration Profile Information

The Registration Profiles List displays information for the configured Registration Profiles. To display information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is shown below.



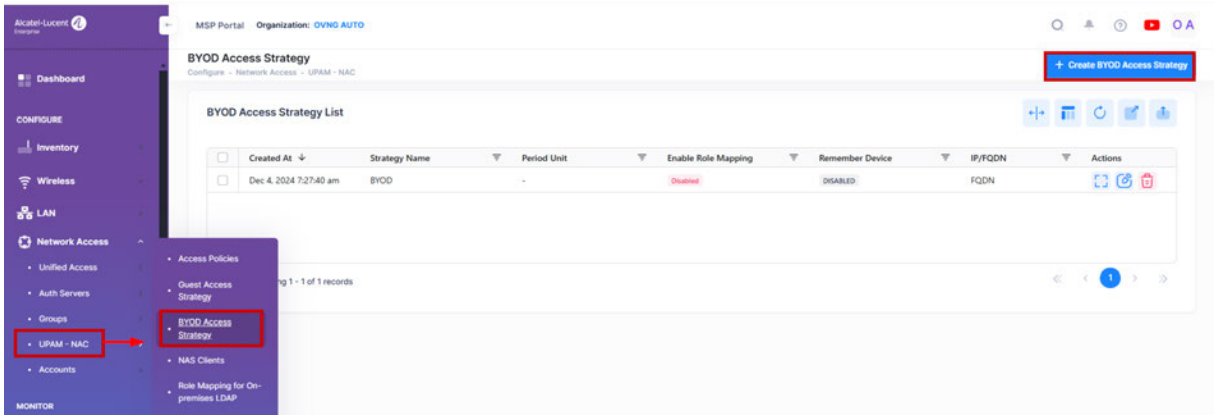

Additional information
Name: RegData
Description: -
Period Unit: Minute(s)
Remember Device: Enabled
Device Validity Period: 15
Data Quota: Enabled
Data Quota URL: https://www.google.com
Time Quota: Disabled
Time Quota Mode: -
Quota Per Day: -
Quota Before Blocked: -
Blocked Hours: -
Reduced Up Bandwidth: -
Reduced Down Bandwidth: -
Max Remember Device: 5
Data Quota(MB): 1
Created At: Feb 23, 2023 2:08:56 pm

8 21 Oct 2025

7.4.3 BYOD Access Strategy

The BYOD Access Strategy screen is used to configure access attributes for BYOD users. The screen displays information (see page 661) about configured strategies and can be used to create (see page 658), edit (see page 662), and delete (see page 662) BYOD Access Strategies. There is a pre-configured Default BYOD Access Strategy that you can edit, or you can create new BYOD Access Strategies (up to a maximum of 32).

To access the BYOD Access Strategy screen, click on **Network Access > UPAM-NAC > BYOD Access Strategy** under the “Configure” section of the OmniVista Terra Menu (see page 45).

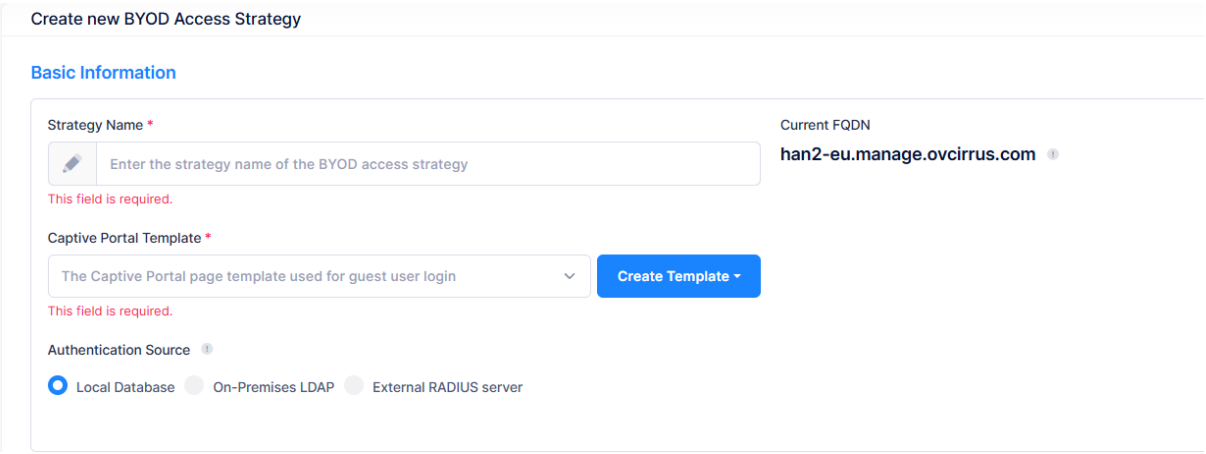


7.4.3.1 Creating a BYOD Access Strategy

To add a BYOD Access Strategy, click on **Create BYOD Access Strategy** to open the Create BYOD Access Strategy form. Complete the following sections of the form, then click on **Create** when you are finished.

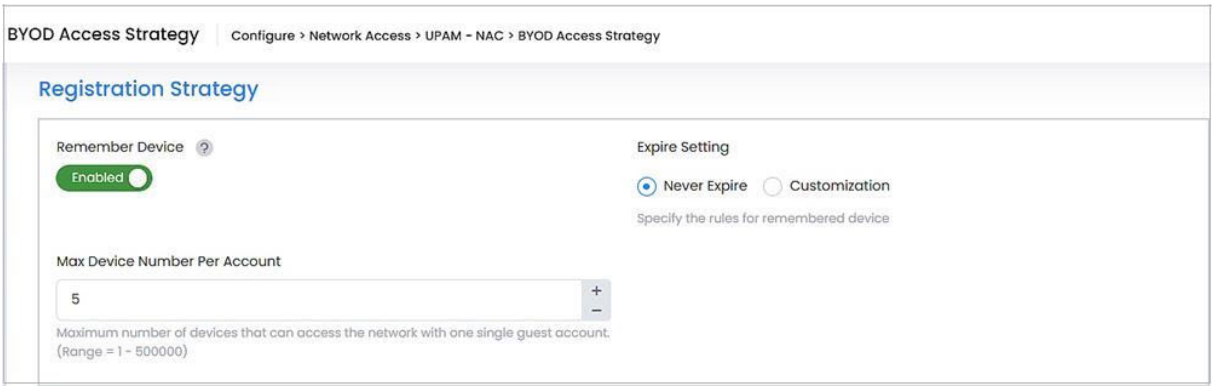
- **Basic Information** (see page 659) - Configure the BYOD Access Strategy name and authentication attributes (Captive Portal Template, current FQDN, Authentication Source).
- **Registration Strategy** (see page 659) - Specify whether to remember the device MAC address and make it valid after authentication success (Enabled/Disabled). If the remembered device is valid, the MAC address check will be performed first and the device is allowed access without re-authentication.
- **Login Strategy** (see page 660) - Specify the success redirect URL for the BYOD user login strategy.
- **Post Portal Authentication Enforcement** (see page 661)- Configure post-authentication enforcement for guest users.

7.4.3.1.1 Basic Information

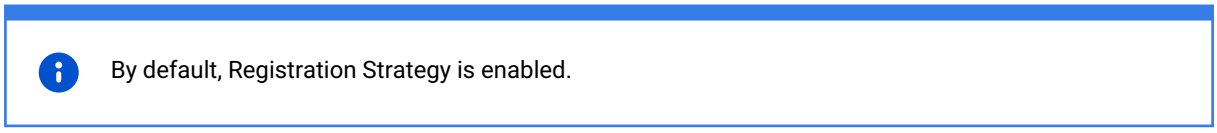


- **Strategy Name -** Enter the name to assign to the BYOD access strategy.
- **Captive Portal Template** - Select an existing Captive Portal page template to use for guest user login from the drop-down menu or click on **Create Template** to create a new template to use (see the Captive Portal Templates (see page 675) online help).
- **Current FQDN** - The Fully Qualified Domain Name to use for the Captive Portal page redirection.
- **Authentication Source** - Specify the source of the user profile (Account/Password).
  - **Local Database** - The employee account utilized for BYOD service is stored in the local database of UPAM.
  - **On-Premises LDAP** - The employee account utilized for BYOD service is stored in an on-premises LDAP Server (see page 597). If selected, a private LDAP Server is used instead of one in cloud for AP authentication. In this scenario, user authentication requests are communicated directly between an AP and the LADP Server, and are not exposed in the public network.
    Note: Certified LDAP Server versions: OpenLDAP Server version is 2.4 Standalone and Microsoft Window Server 2022.
  - **External Radius Server** - The employee account utilized for BYOD service is stored in the database of an external RADIUS Server (see page 692).

7.4.3.1.2 Registration Strategy

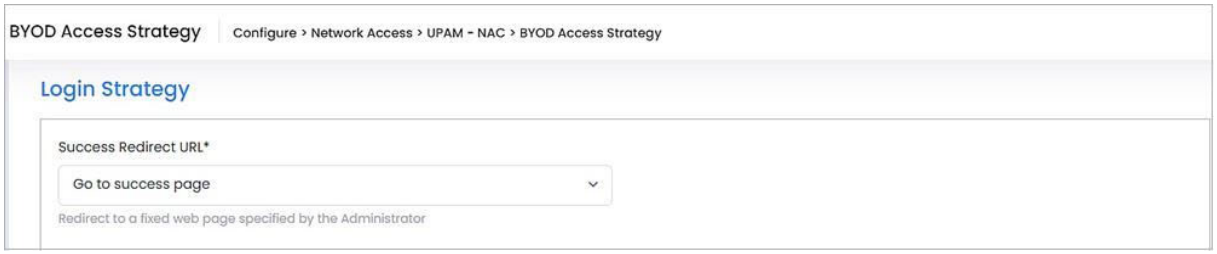


- **Enable Role Mapping** - When the **On-Premise LDAP** option is selected as the authentication source for the BYOD Strategy, an **Enable Role Mapping** option will appear in this section. Enable this option to apply Role Mapping for On-Premise LDAP (see page 669) (Default = Disabled). This option does not appear in this section for other authentication sources.
- **Remember Device** - Specify whether to remember the device MAC address and make it valid after authentication success (Enabled/Disabled). If the remembered device is valid, the MAC address check will be performed first and the device is allowed access without re-authentication.
- **Expire Setting** - Specify the rules for remembered device.
  - **Never Expire -** User remembered device will always be valid after authentication success.
  - **Customization -** Customize the valid period for the remembered devices.
    - **Period Unit** - Select whether the validity period will be applied in days, hours, or minutes.
    - **Device Validity Period -** Length of time that the guest user device is valid. Ranges and default values are shown below. (Range = 1 – 365, Default = 90, -1 = never expires)
- **Max Device Number Per Account -** Maximum number of devices that can access the network with one single guest account. (Range = 1 – 10, Default = 5)



By default, Registration Strategy is enabled.

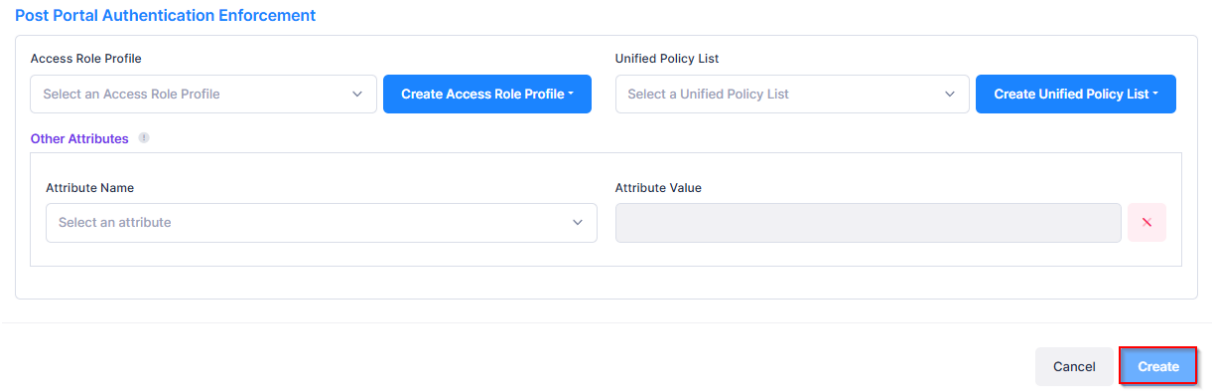
7.4.3.1.3 Login Strategy



Specify the URL to which a BYOD user is redirected after a successful login.

- **Success Redirect URL:**
  - **Go to Fixed URL -** Redirect the user to the specified fixed URL.
  - **Go to Initial URL -** Redirect to the guest-user-input URL after passing authentication
  - **Go to success page** - Redirect to a success webpage specified by the Administrator.

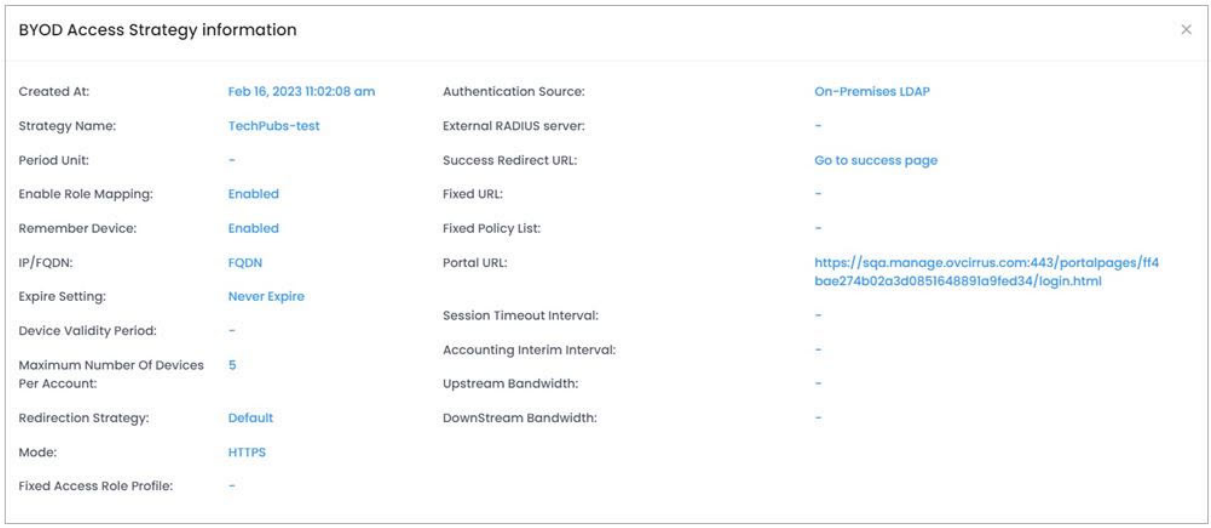
7.4.3.1.4 Post Portal Authentication



- **Access Role Profile** - The Access Role Profile assigned to the guest user after passing authentication. Select a profile from the drop-down menu or click on **Create Access Role Profile** to add a new profile to use (see the Access Role Profile (see page 481) online help).
- **Unified Policy List** - The Policy List assigned to the guest user after passing authentication. Select a list from the drop-down menu or click on **Create Unified Policy List** to add a new list to use (see the Unified Policies List (see page 481) online help).
- **Other Attributes** - Select an attribute from the drop-down menu and enter a value. To add additional attributes, click on **Add Attribute**.
  - **Session-Timeout** - The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
  - **Acct-Interim-Interval** - The Accounting Interim Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
  - **WISPr-Bandwidth-Max-Up** - The user upstream bandwidth, in kbit/s. By default, it is not limited.
  - **WISPr-Bandwidth-Max-Down** - The user downstream bandwidth, in kbit/s. By default, it is not limited.

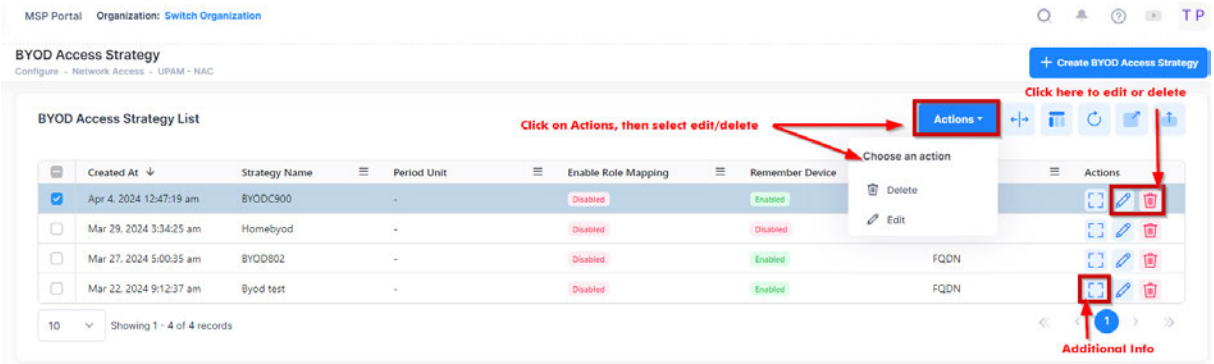
7.4.3.2 View Additional Information

Select the BYOD Access Strategy name in the list and click on the Additional Information icon to view additional information about the BYOD Access Strategy.



7.4.3.3 Editing a BYOD Access Strategy List

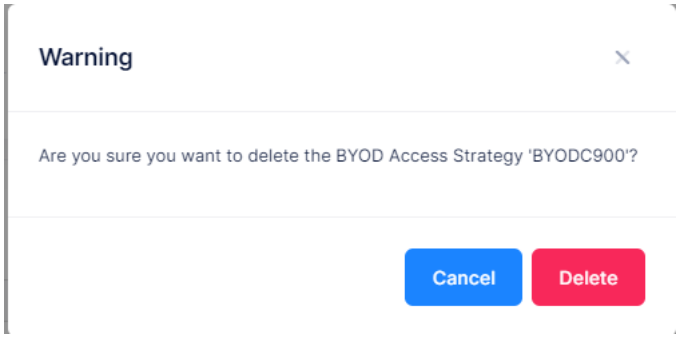
Select a BYOD Access Strategy name, then click on **Actions** and select **Edit**, or you can click on the Edit icon under the “Actions” column.



Edit the field(s) as described above (see page 658), then click on **Save**.

7.4.3.4 Deleting a BYOD Access Strategy List

Select a BYOD Access Strategy name, then click on **Actions** and select **Delete**, or you can click on the Delete icon under the “Actions” column. Click **Delete** at the Confirmation Prompt.

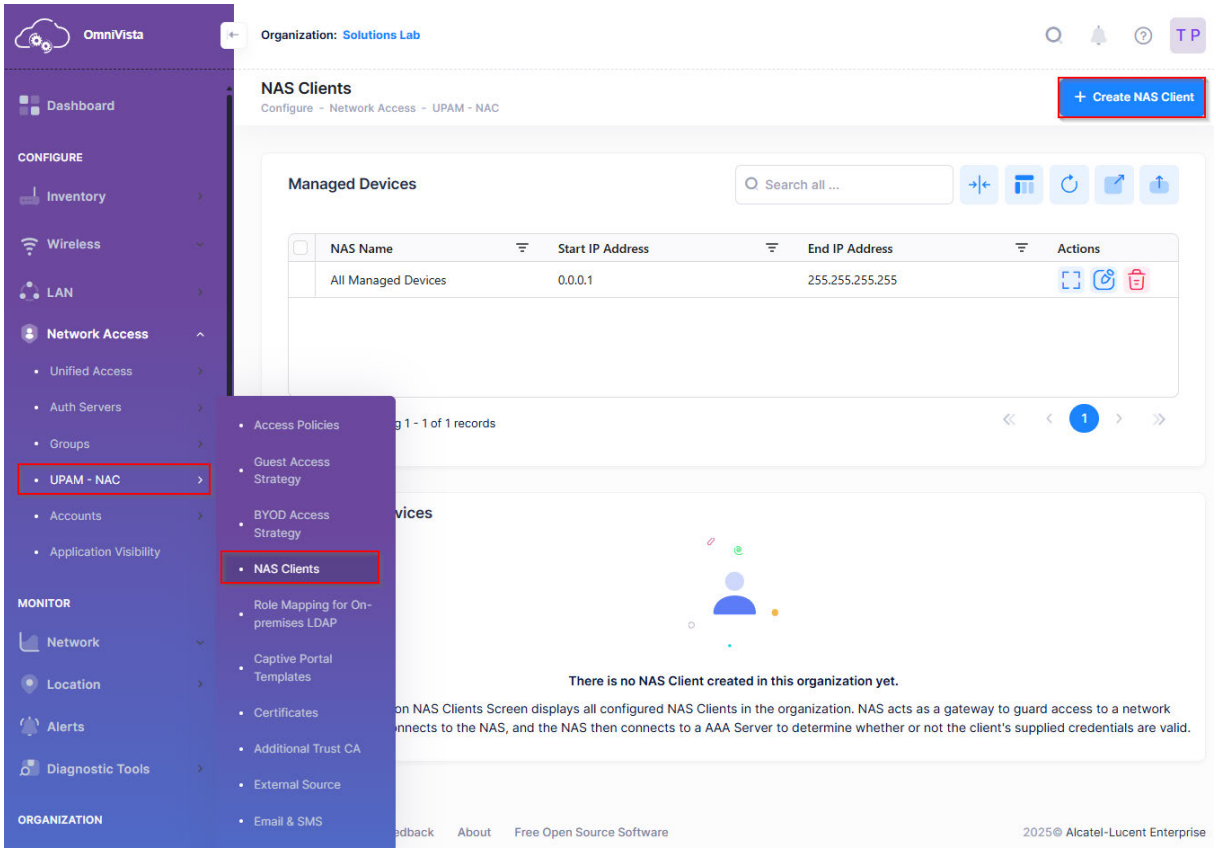


21 Oct 2025

7.4.4 NAS Clients

The NAS Clients screen displays all configured NAS Clients, including third-party devices, and is used to create (see page 663), edit (see page 666), and delete (see page 667) NAS Clients. NAS serves as a protective gateway, regulating access to network resources. A client connects to the NAS, which then communicates to an Authentication Server to verify the validity of the credentials provided by the client. The NAS then allows or denies access to the network resource. The network device within the infrastructure attaching with wired or wireless clients will act as a NAS client, communicating to UPAM which acts as an Authentication Server.

To access the NAS Clients screen, click on **Network Access > UPAM-NAC > NAS Clients** under the "Configure" section of the OmniVista Terra Menu (see page 45).



7.4.4.1 Creating a NAS Client

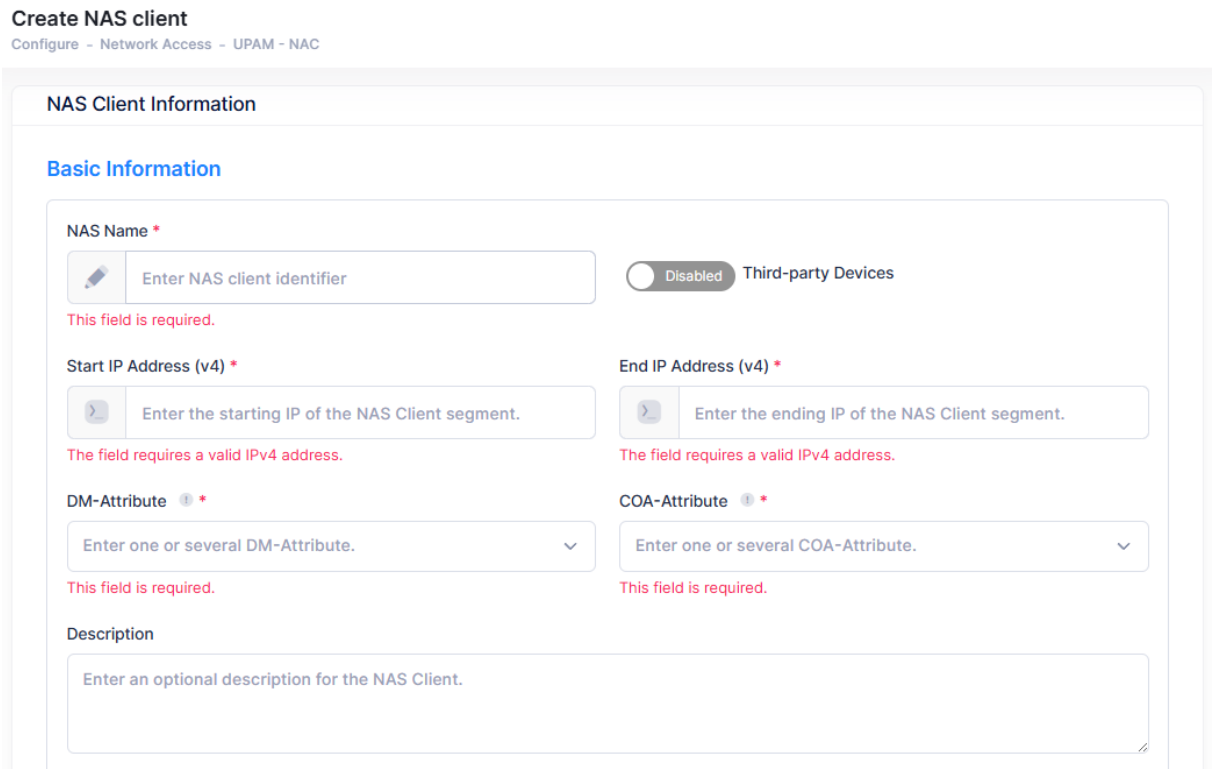
There is a pre-configured default NAS Client profile ("All Managed Devices") designated for each Organization. You can edit the default NAS Client profile or create a new one.

To add a NAS Client, click on **Create NAS Client** to open the Create NAS Client form. Complete the following sections of the form, then click **Create** when you are finished.

- **Basic Information** (see page 664) - Configure the NAS name, IP Addresses, DM-Attribute, COA-Attribute, description, and whether the NAS client is a third-party device.

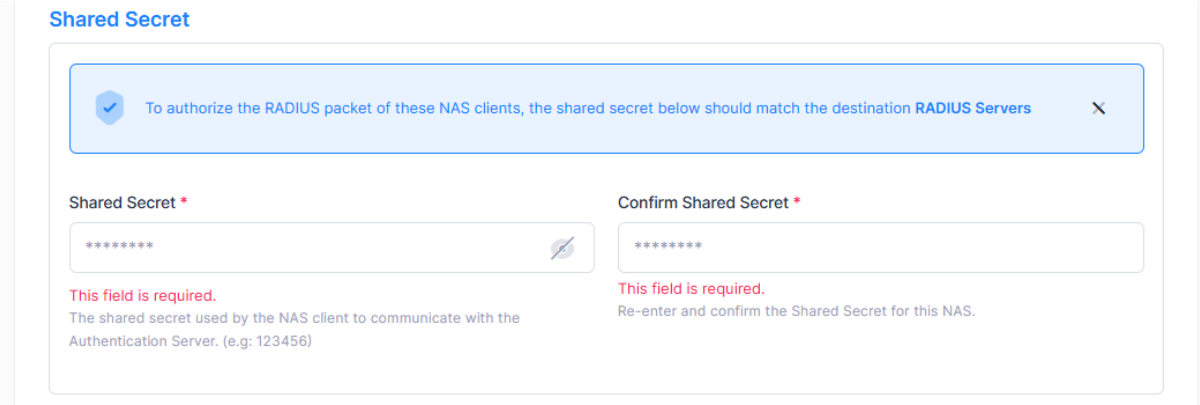
- **Shared Secret** (see page 665) - Configure the shared secret used by the NAS client to communicate with the Authentication Server. It is highly recommended that you change the default shared secret for NAS clients.
- **Require Message Authenticator** (see page 665) - Configure whether UPAM checks for the Message-Authenticator attribute in RADIUS request packets coming from NAS clients.

7.4.4.1.1 Basic Information



- **NAS Name -** The name of the NAS Client.
- **Third-party Devices** - Enable this option to indicate the NAS client is a third-party device. (Default = Disabled).
- **Start IP Address (v4) -** The starting IP of the NAS Client segment.
- **End IP Address (v4) -** The ending IP of the NAS Client segment.
- **DM-Attribute -** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes (User Name/ Calling Station ID) to identify the subscriber session.
  - **User Name -** The value should exactly match the subscriber name of the session.
  - **Calling Station ID -** The value should match the subscriber ID.
- **COA-Attribute -** The COA message is used to Change of Authentication (COA) in the system from the Radius Server. The COA request message should contain necessary attributes (Username/Calling Station ID) to identify the changes.

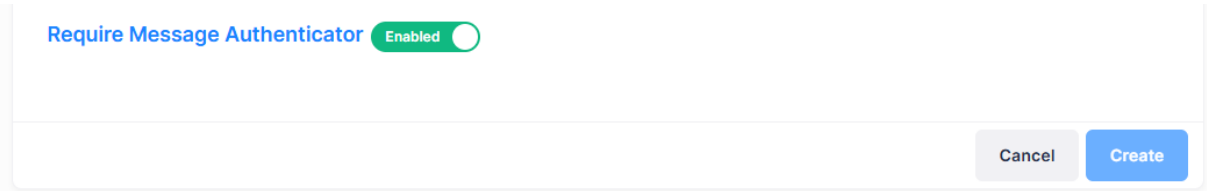
7.4.4.1.2 Shared Secret



- **Shared Secret** - Configure the shared secret used by the NAS client to communicate with the Authentication Server.
- **Confirm Shared Secret** - Enter the Shared Secret again to confirm.

If you change the shared secret used by the NAS client, then you must also update the shared secret of the UPAM RADIUS Server (see page 589). The NAS client and UPAM RADIUS Server must use the same shared secret to ensure that RADIUS traffic from the NAS client is authorized.

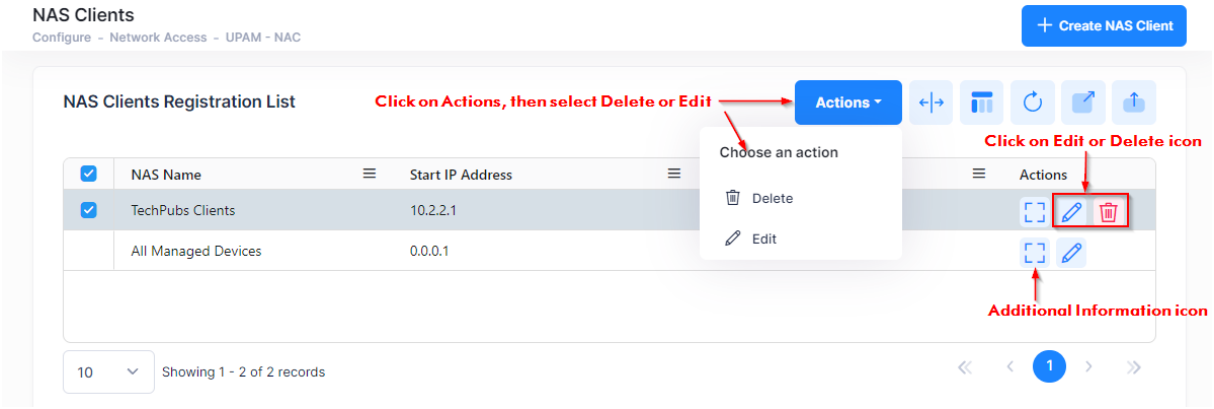
7.4.4.1.3 Require Message Authenticator

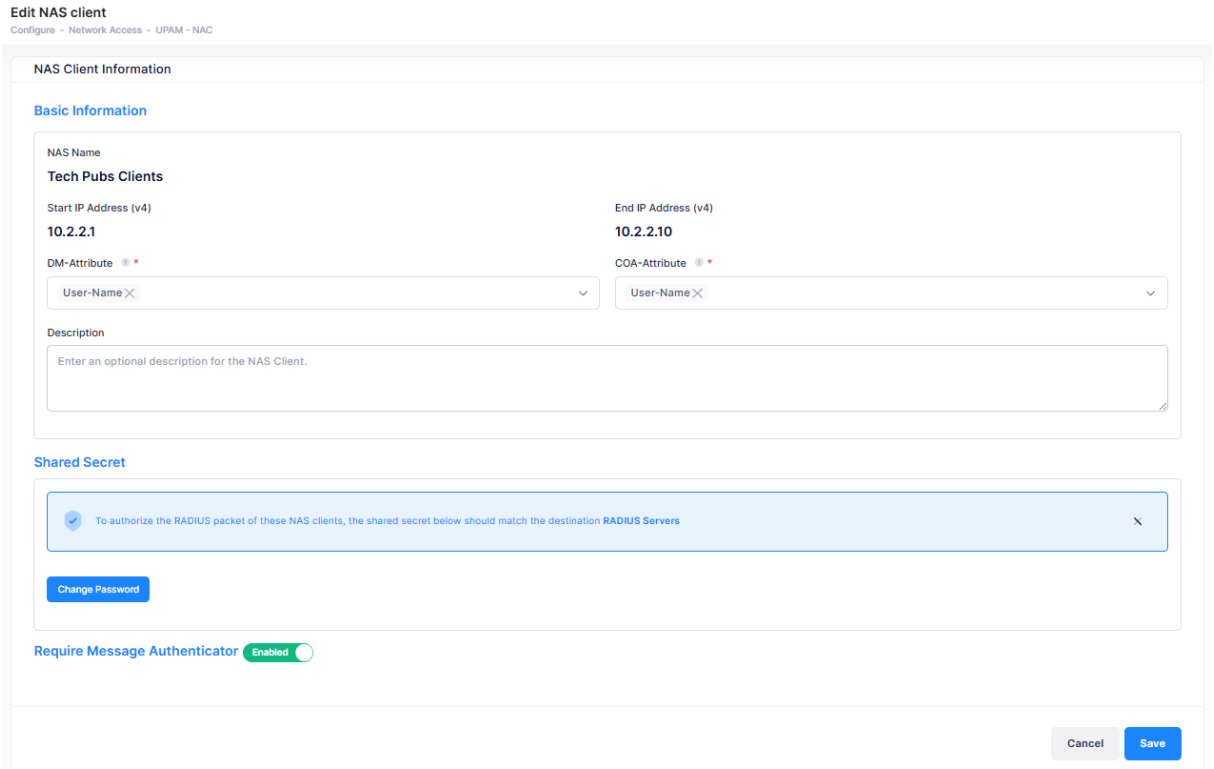


- **Require Message Authenticator** - Enables/Disables UPAM checking for the Message-Authenticator attribute in RADIUS request packets coming from NAS clients within the specified IP address range. Access Points always include the Message-Authenticator attribute; however, you must use the **aaa radius message-authenticator** CLI command to enable an OmniSwitch to include this attribute in request packets. Checking for this attribute is also configurable when defining a UPAM External RADIUS server and a RADIUS Authentication server. Refer to the Require Message Authenticator Use Cases (see page 704) for more information.
  - **Enabled** - UPAM will drop request packets that do not contain the Message-Authenticator attribute. Enabling the Require Message Authenticator flag is highly recommended to prevent attempts to forge authentication responses by spoofing UDP-based RADIUS response packets.
  - **Disabled** - UPAM does not check if request packets contain the Message-Authenticator attribute.

7.4.4.2 Editing a NAS Client

Select a NAS Client entry, then click on **Actions** and select **Edit** from the drop-down menu or click on the Edit icon under the “Actions” column next to the NAS Client entry.





Edit the field(s) as described above (see page 663), then click on **Save**.

Modifying the default “All Managed Devices” NAS Client will affect all managed devices.

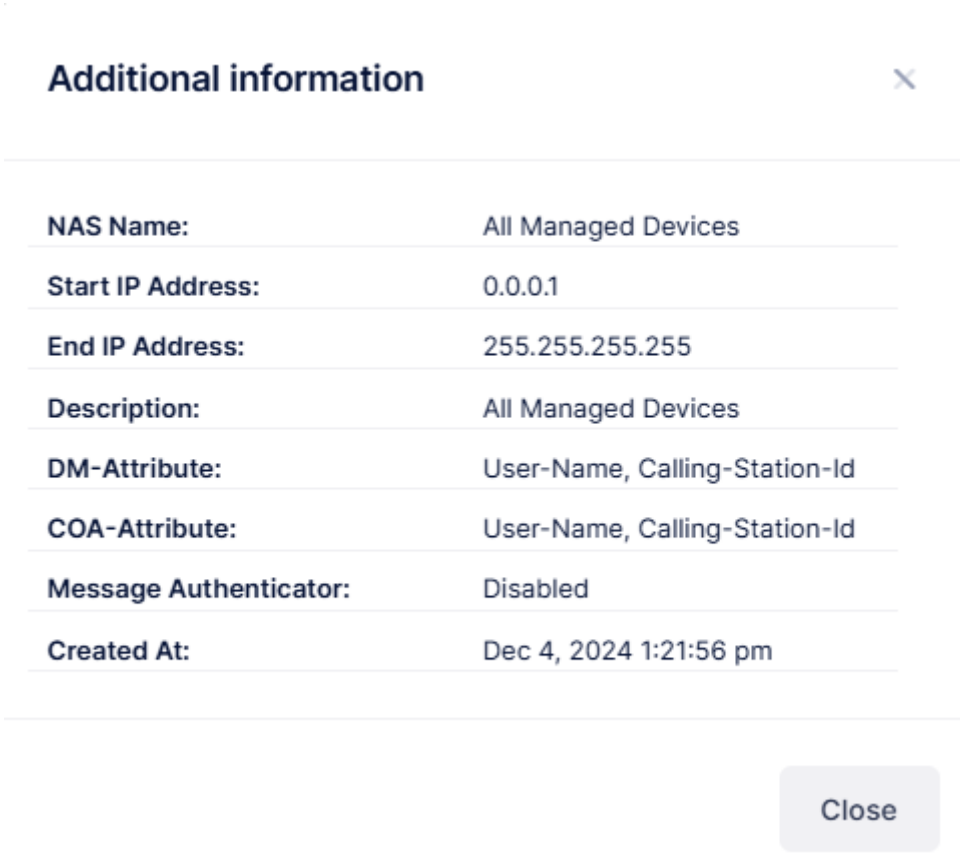
7.4.4.3 Deleting a NAS Client

Select a NAS Client entry, then click on **Actions** and select **Delete** from the drop-down menu or click on the Delete icon under the “Actions” column next to the NAS Client entry. Click **Delete** at the Confirmation Prompt.

> Note that you cannot delete the default “All Managed Devices” NAS Client profile entry.

7.4.4.4 View Additional NAS Client Information

Select the NAS Client name in the list and click on the Additional Information icon under the “Actions” column next to the NAS Client entry.



- **NAS Name -** The name of the NAS Client.
- **Start IP Address (v4)** - The starting IP of the NAS Client segment.
- **End IP Address (v4)** - The ending IP of the NAS Client segment.
- **Description** - The optional description for the NAS Client. (Default = NAS Name)
- **DM-Attribute -** The DM message used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes (User Name/ Calling Station ID) to identify the subscriber session.

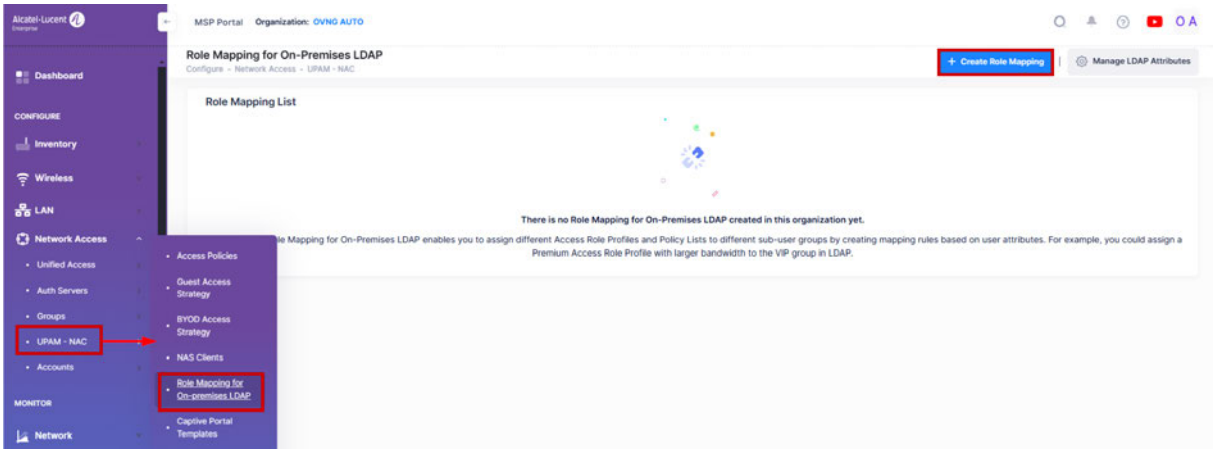
- **COA-Attribute -** The COA message used to Change of Authentication (COA) in the system from the Radius Server. The COA request message should contain necessary attributes (Username/ Calling Station ID) to identify the changes.
- **Message Authenticator** - Indicates whether UPAM checks for the Message-Authenticator attribute in RADIUS request packets coming from NAS clients within the specified IP address range. (Default = Enabled)
- **Created At** - The date and time the NAS Client was created.

21 Oct 2025

7.4.5 Role Mapping for On-premises LDAP

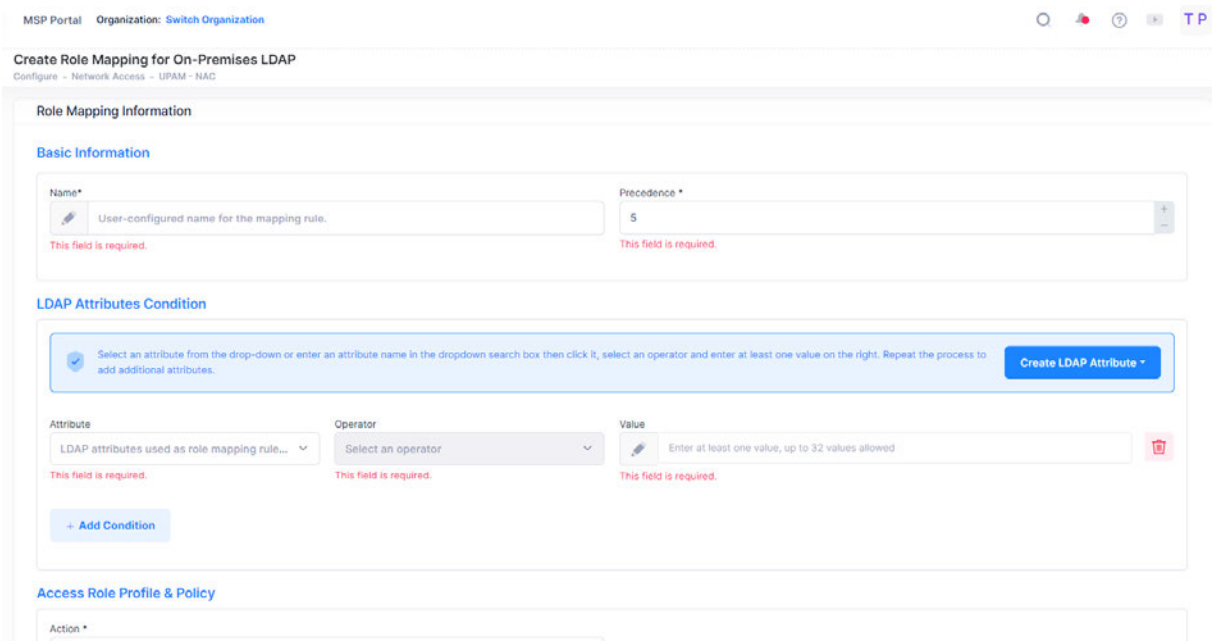
Authentication Role Mapping for On-Premises LDAP enables you to assign different Access Role Profiles and Policy Lists to different sub-user groups by creating mapping rules (see page 669) based on user attributes. For example, you could assign a Premium Access Role Profile with larger bandwidth to the VIP group in LDAP. The Role Mapping for On-Premises LDAP Screen displays information (see page 671) about all configured mappings and is used to create (see page 669), edit (see page 672), and delete (see page 673) mappings.

To access the Role Mapping for On-premises LDAP screen, click on **Network Access > UPAM-NAC > Role Mapping for On-premises LDAP/AD** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.4.5.1 Creating a Mapping

Click on the **Create Role Mapping** icon to bring up the Create Role Mapping for On-Premises LDAP screen. Complete the fields as described below, then click on the **Create Role Mapping** button.



Basic Information

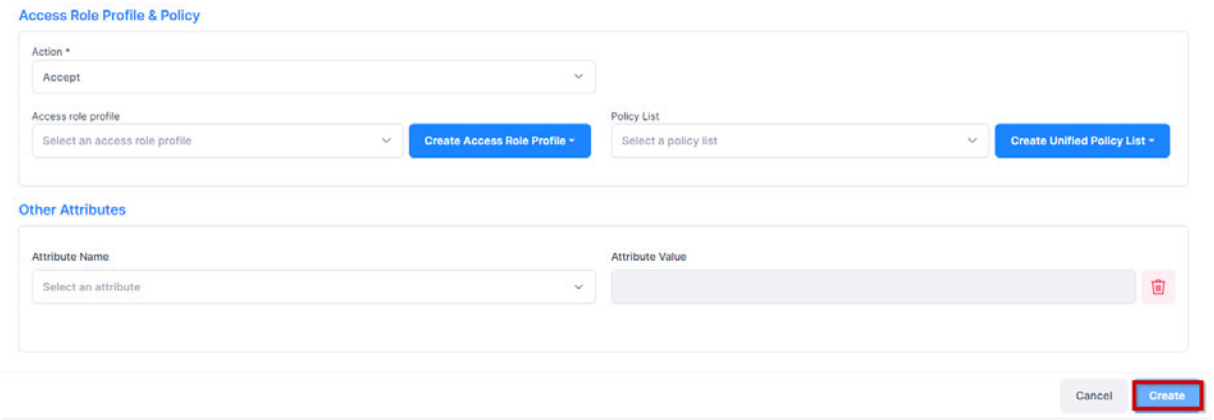
- **Name** - Enter user-configured name for the mapping rule.
- **Precedence -** Priority of the role mapping rule. A user requesting LDAP authentication may match several role mapping rules; the one with highest priority will take effect after passing authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest).

LDAP/AD Attributes Condition

Select an attribute from the drop-down or enter an attribute name in the dropdown search box then click it, select an operator and enter at least one value on the right. Repeat the process to add additional attributes.

- **Attribute -** LDAP attributes used as role mapping rule key.
  - **Operator -** Select an operator for the attribute's value from the drop down list.
  - **Value -** Attribute's value on the LDAP Server.

Access Role Profile & Policy



- **Action -** Accept or Reject user authentication with 802.1X matching with Access Policy.
- **Access Role Profile -** Access Role Profile applied to the user after matching the role mapping rule.
- **Policy List -** Policy List applied to the user after matching the role mapping rule.

Other Attributes

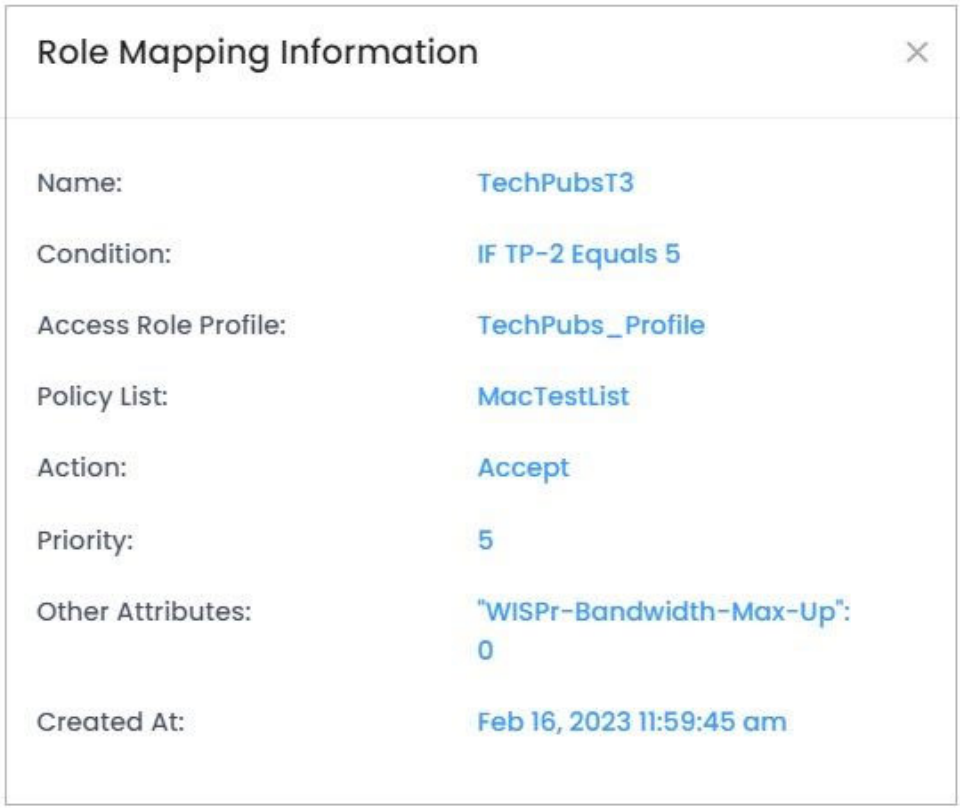
Select an attribute from the drop-down menu and enter a value. To add additional attributes, click on **Add Attribute**.

- **Acct-Interim-Interval** - The Accounting Interim Interval for RADIUS accounting, in seconds. If not configured, the device's default accounting policy will take effect. (Range = 60 - 1200, Default = 600)
- **Session-Timeout** - The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device's default session timeout policy will take effect. (Range = 12000 - 86400, Default = 43200)
- **WISPr-Bandwidth-Max-Up** - The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr-Bandwidth-Max-Down** - The user downstream bandwidth, in kbit/s. By default, it is not limited.

After entering the required parameters, click on the **Create** button to complete.

7.4.5.2 View Additional Role Mapping List Information

Select the Role Mapping name in the list and click on the Additional Information icon to view additional information for the mapping rule.

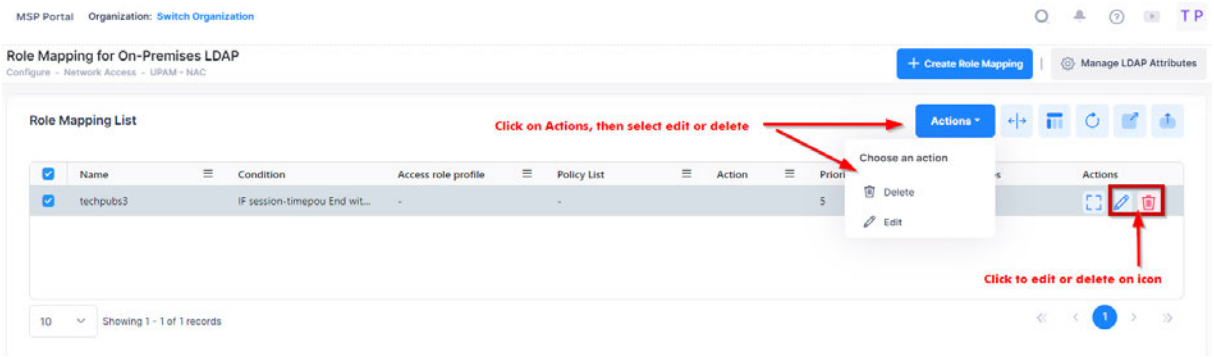


The Role Mapping List displays information about all configured mappings.

- **Name -** User-configured name for the mapping rule.
- **Condition -** The mapping condition.
- **Access Role Profile -** Access Role Profile applied to the user after matching the role mapping rule.
- **Policy List -** Policy List applied to the user after matching the role mapping rule.
- **Action -** When you choose On-Premise LDAP, for authentication, A new option is introduced to enable or disable Role-Mapping in Registration Strategy. By default, Role-Mapping is disabled.
- **Priority -** Priority of the role mapping rule. A user requesting LDAP authentication may match several role mapping rules; the one with highest priority will take effect after passing authentication. (Range = 1 - 99, 1 is the highest priority and 99 is the lowest).

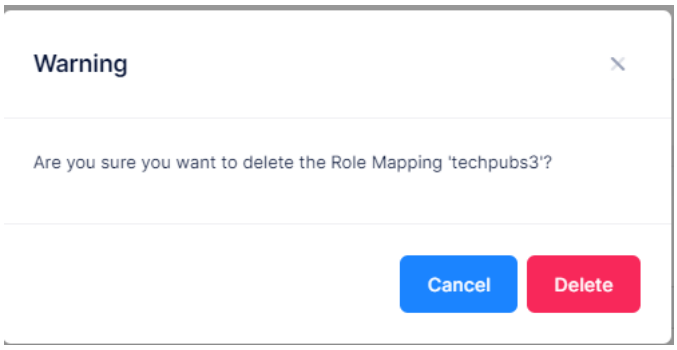
7.4.5.3 Editing a Mapping

Select a mapping in the Role Mapping List and click on the Edit icon. Edit the field(s) as described above (see page 669), and click on the **Save** button. Note that you cannot edit a Mapping Name.



7.4.5.4 Deleting a Mapping

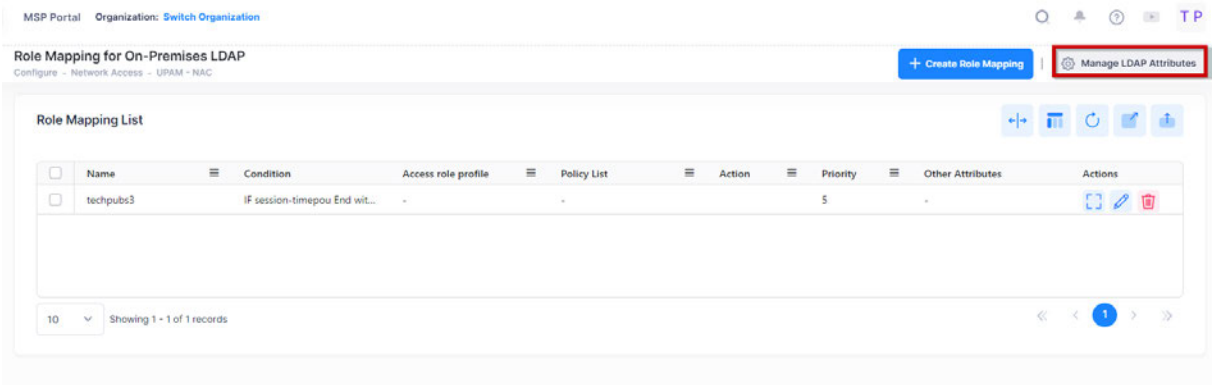
Select a mapping in the Role Mapping List and click on the Delete icon. Click **Delete** at the Confirmation Prompt.



7.4.5.5 Attribute for On-Premises LDAP

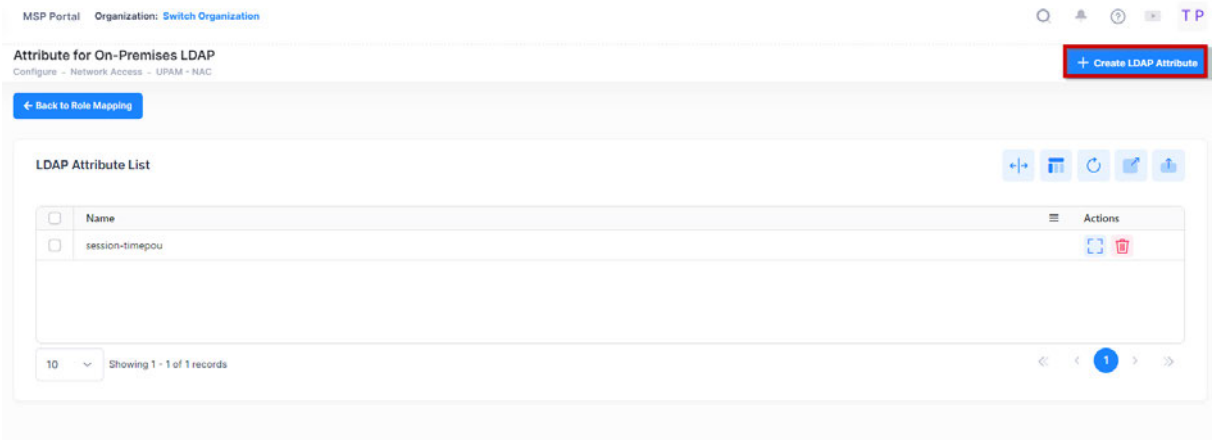
The Attribute for On-Premises LDAP screen is used to manage the LDAP attributes for AP authentication through an external on-premises LDAP Server. The attributes can be used as mapping conditions for assigning Role/Access Role Profiles. You can create attributes for the LDAP Server. Attributes in the list can be selected as mapping conditions on the Role Mapping for On-Premises LDAP screen.

To access the Manage LDAP Attributes screen, click on **Manage LDAP Attributes** at the top right corner of the screen.

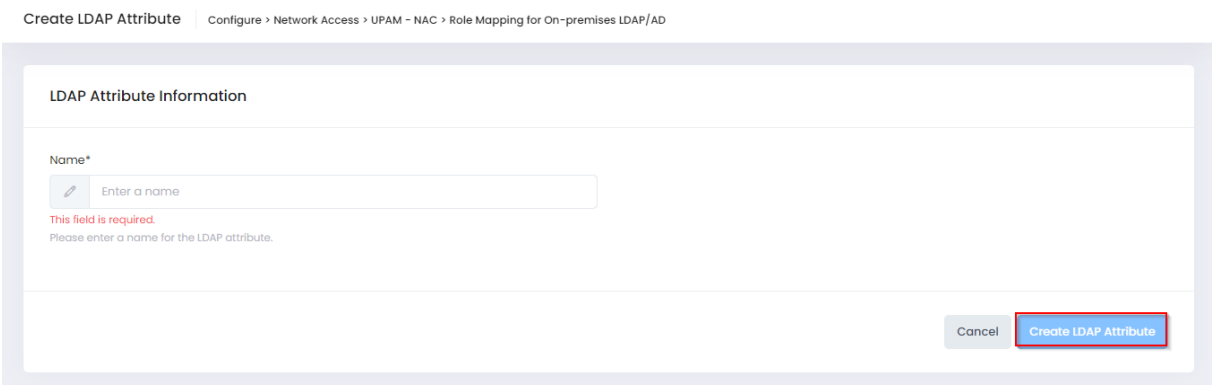


7.4.5.5.1 Creating LDAP Attributes

Click on **Create LDAP Attribute** to open the Create LDAP Attribute screen.



Enter the attribute in the Name field and click on the **Create LDAP Attribute**.



On the LDAP Attributes List screen, you can click on **Back To Role Mapping** to go back to the Role Mapping for On-premises LDAP screen (see page 669).

7.4.5.5.2 Deleting LDAP Attributes

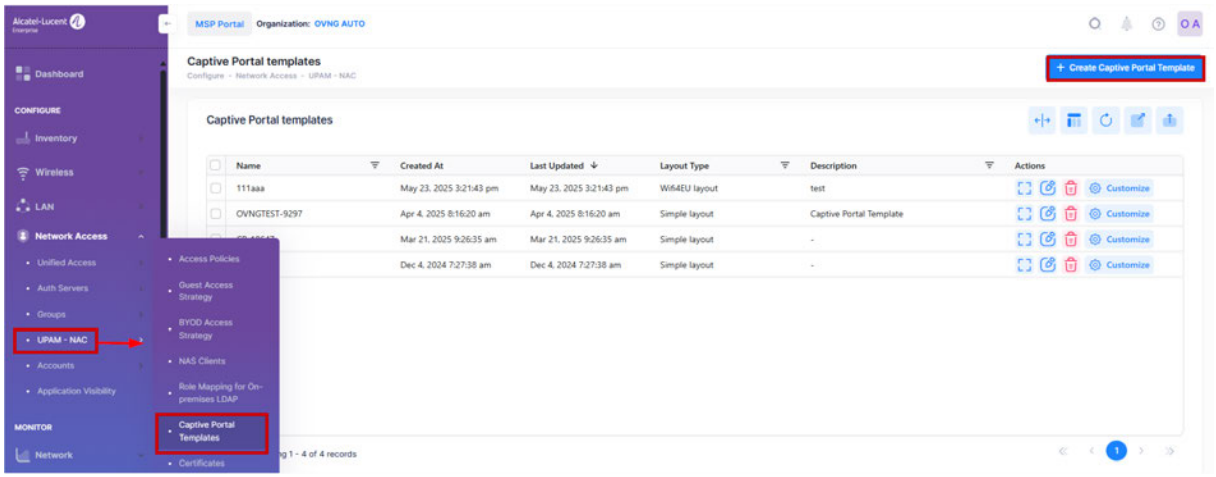
Select the attribute(s) in the LDAP Attribute List and click on the Delete icon. Click **Confirm** at the Confirmation Prompt.

21 Oct 2025

7.4.6 Captive Portal Templates

A Captive Portal template defines the login page that is presented to the user for Guest and BYOD login. The Captive Portal Templates screen displays all configured Captive Portal templates and is used to create (see page 675), edit (see page 676), delete (see page 677), and customize (see page 678)Captive Portal templates.

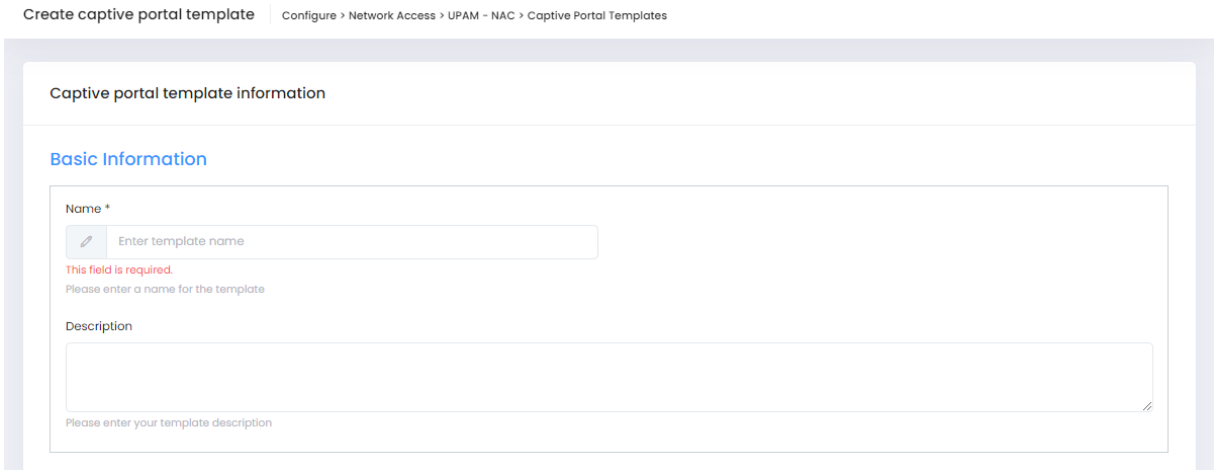
To access the Captive Portal Templates screen, click on **Network Access > UPAM-NAC > Captive Portal Templates** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.4.6.1 Creating a Captive Portal Template

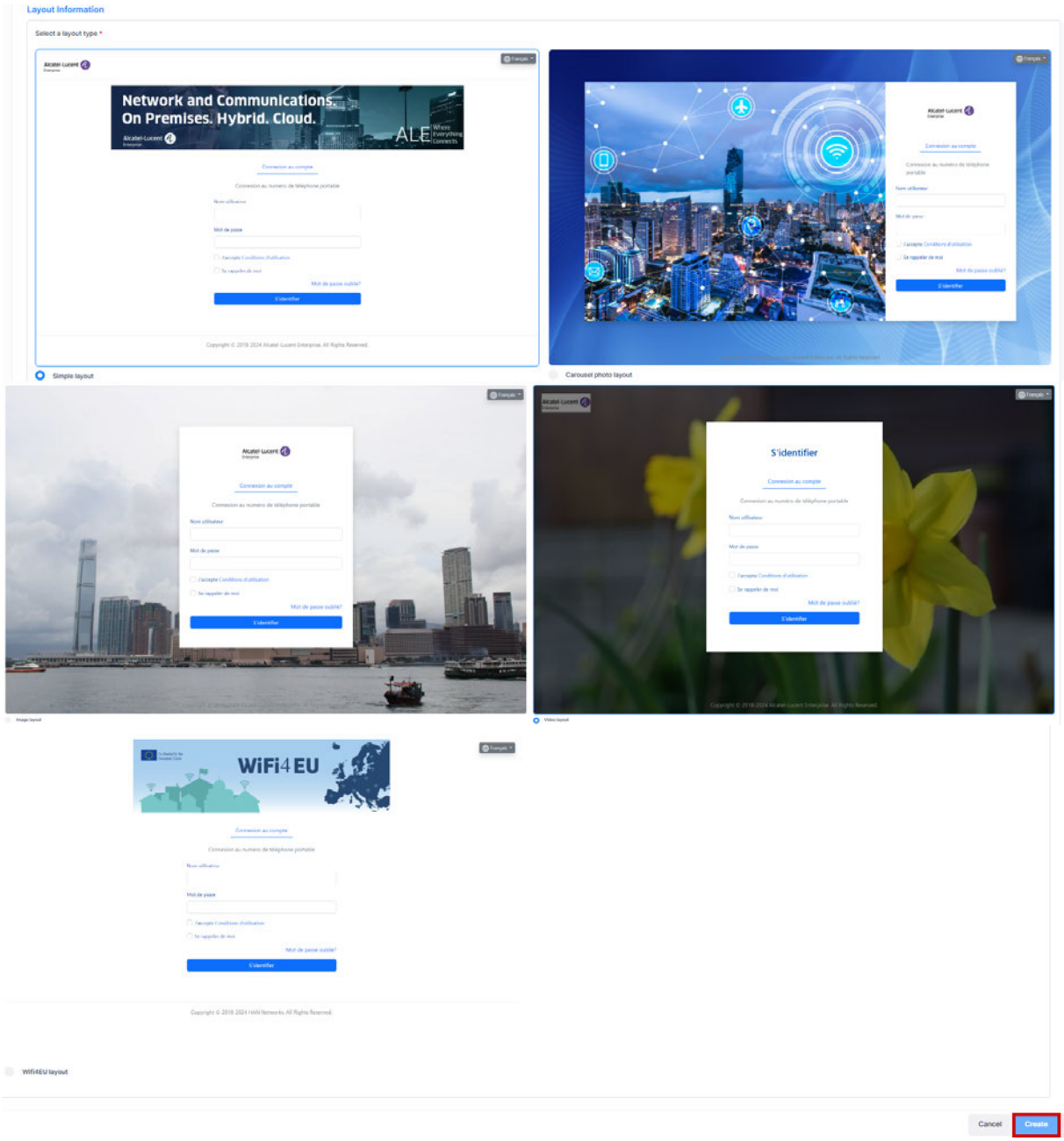
To create a Captive Portal Template, click on **Create Captive Portal Template** to open the Captive Portal Template Information form. Complete the Basic Information (see page 675) and Layout Information (see page 676) sections, as described below.

7.4.6.1.1 Basic Information



- **Name** - Enter the name to assign to the template.
- **Description** - Enter an optional description.

7.4.6.1.2 Layout Information

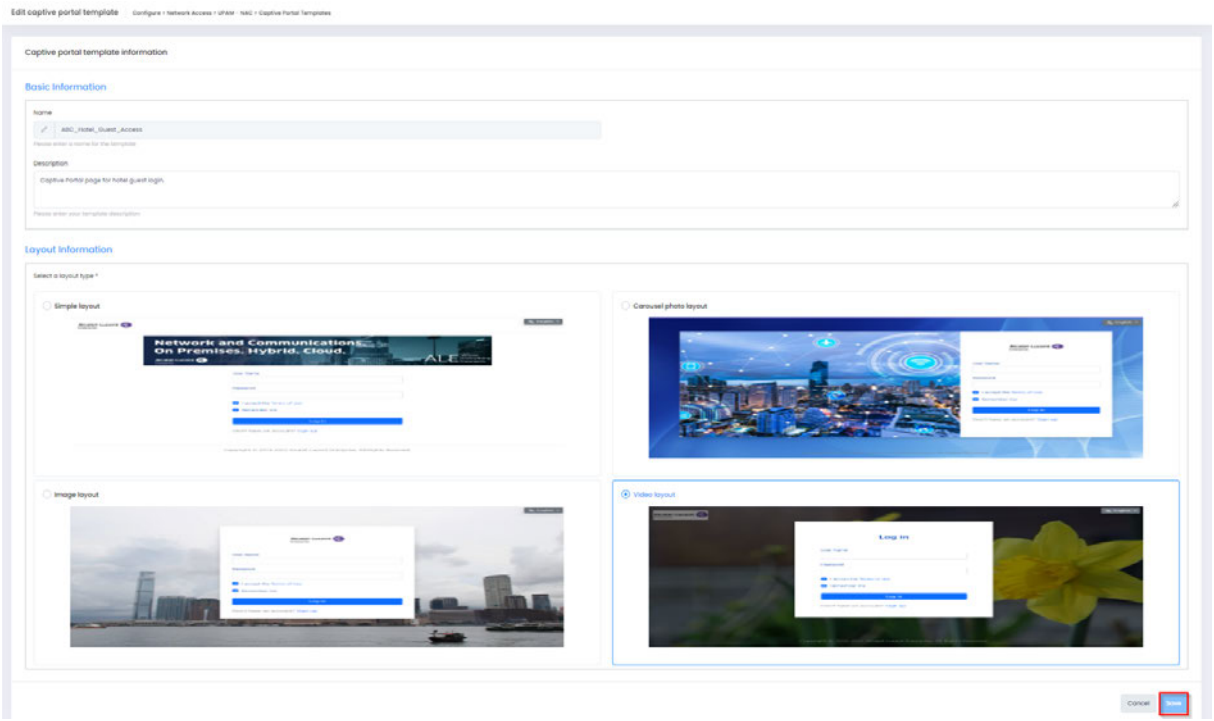


Select one of the five template layouts to use, then click on **Create** button to create the template. Once you have created the basic template, you can customize (see page 678)the page with different images and welcome message.

7.4.6.2 Editing a Captive Portal Template

Select a template from the Captive Portal Templates list and click on the Edit icon under the “Actions” column or click on the **Actions** button and select Edit from the drop-down menu. The Edit Captive Portal Template screen opens on which you can edit the basic information and select a different

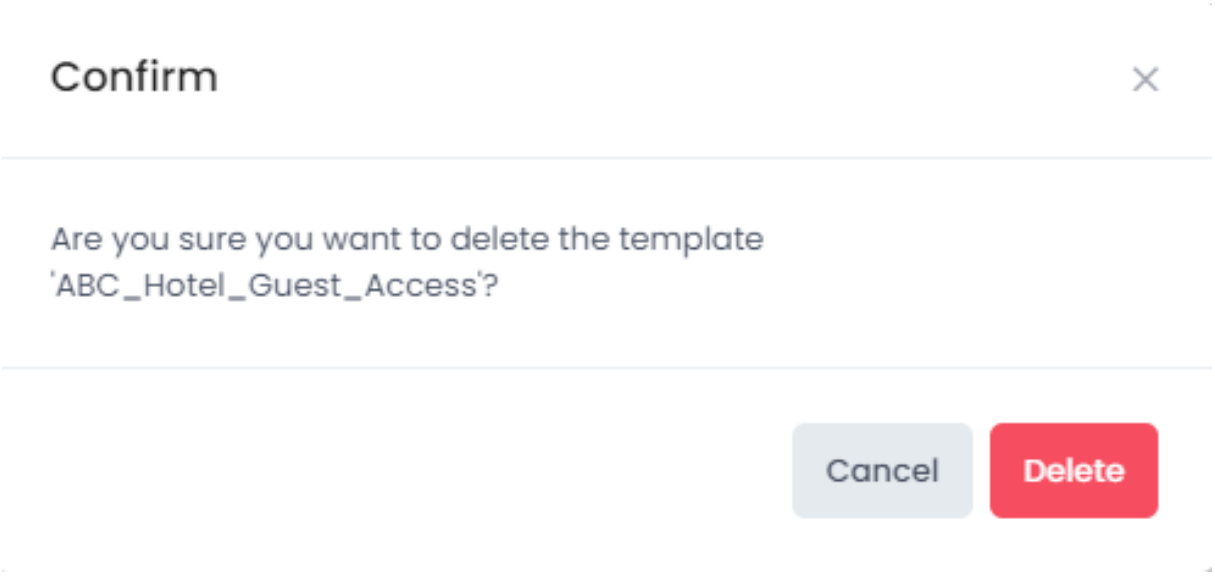
layout, as described above (see page 675). Note that you cannot change the name of the template that you specified when the template was created.



After you have edited the Captive Portal template, click on **Save**. You can also customize (see page 678)the template layout.

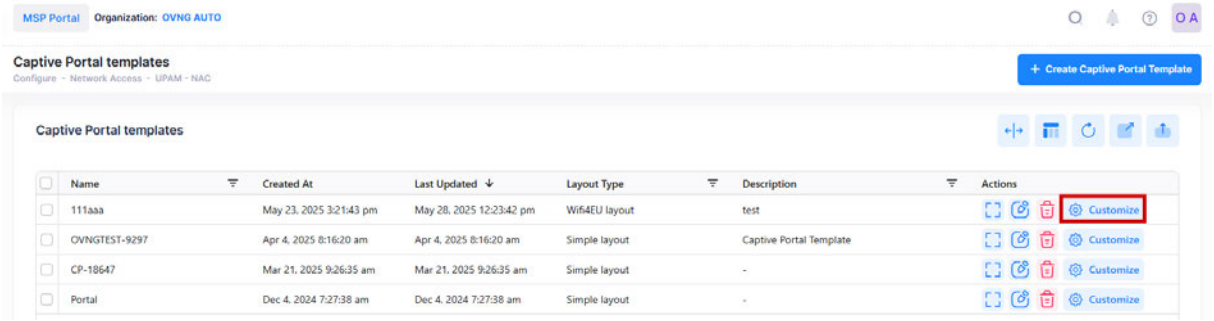
7.4.6.3 Deleting a Captive Portal Template

Select a template from the Captive Portal Templates list and click on the Delete icon under the “Actions” column or click on the **Actions** button and select Delete from the drop-down menu. When the following confirmation prompt appears, click on **Delete** to delete the profile.

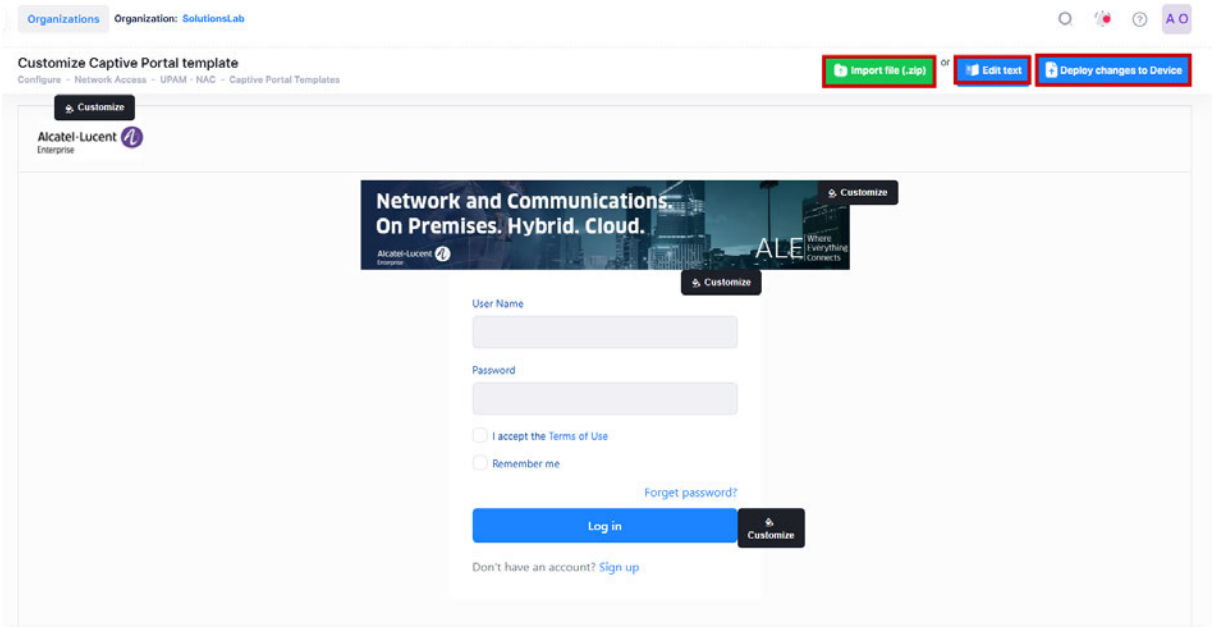


7.4.6.4 Customizing the Captive Portal Template

To customize an existing Captive Portal Template, select the template from the Captive Portal Templates list and click on **Customize** under the “Actions” column.



The Customize Captive Portal Template screen opens with the selected template displayed. The **Customize** buttons on this screen indicate the page objects that you can customize. For example, if you selected the video format for the template layout, the following screen would appear:

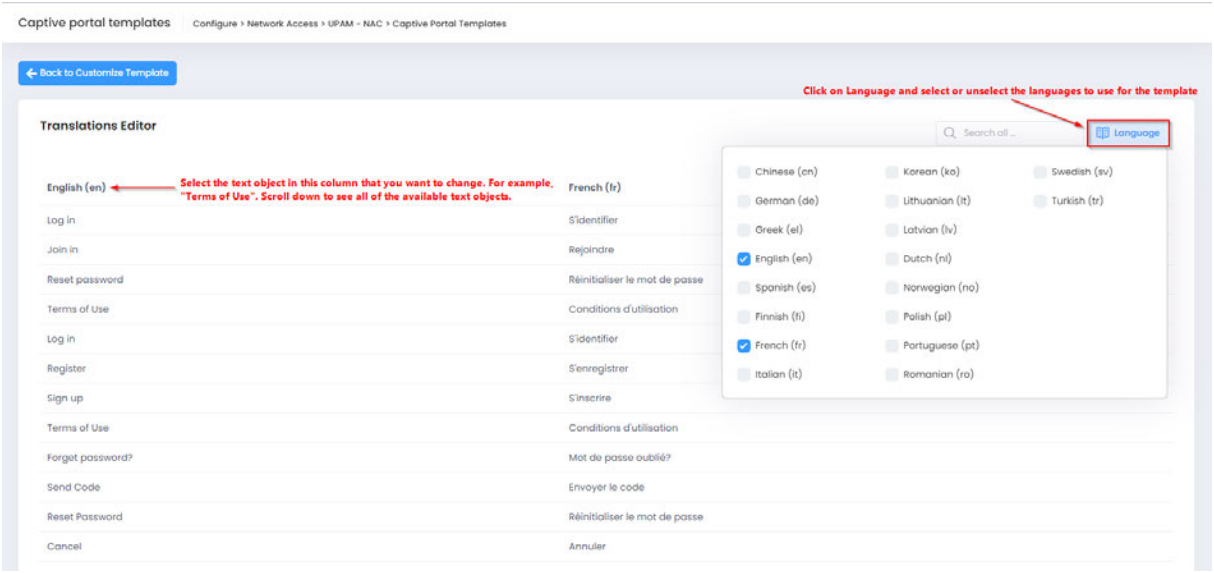


When you click on any one of the **Customize** buttons, you will then be prompted to modify attributes or upload image/video files, depending on the object you selected to customize.

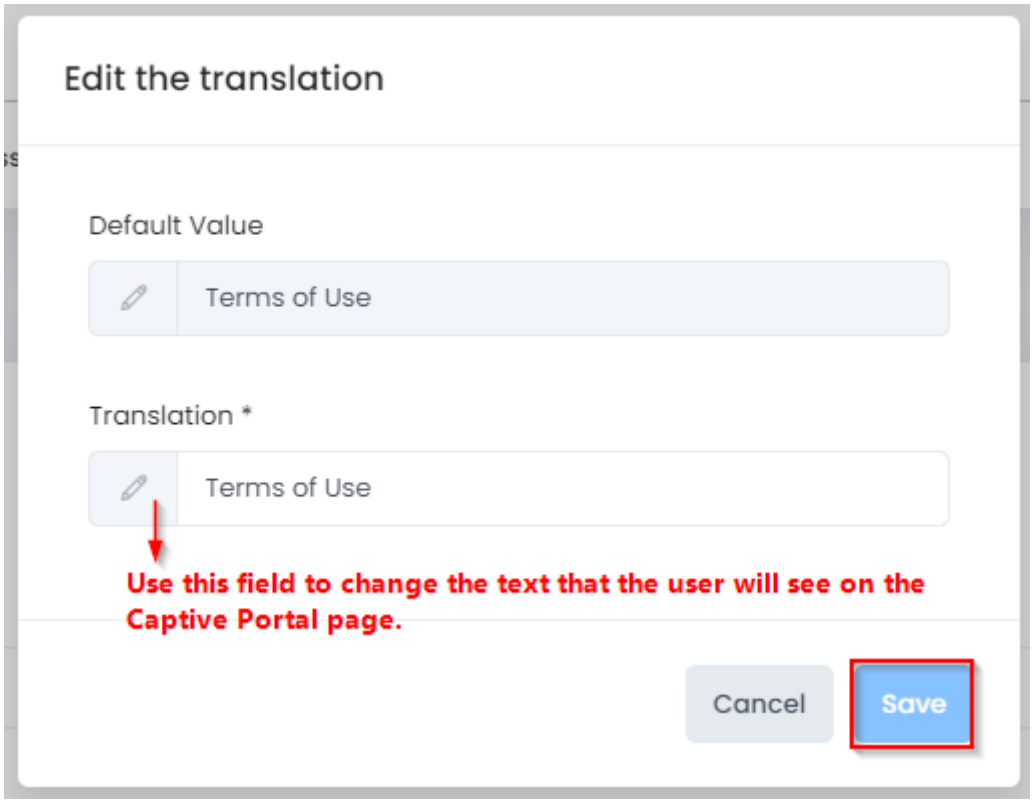
- To restore the original settings the template was created with, click on **Reset to default**.
- To save the changes you have made, click on **Save**.
- To cancel all changes you have made and return to the Captive Portal Templates screen, click on **Cancel**.

7.4.6.4.1 Using the Translation Editor

Click on **Translation Editor** on the Customize Captive Portal Template screen to edit the text for field labels and messages to the user. The following Translation Editor screen opens:



Select the text that you want to change to open the Edit Translation modal.

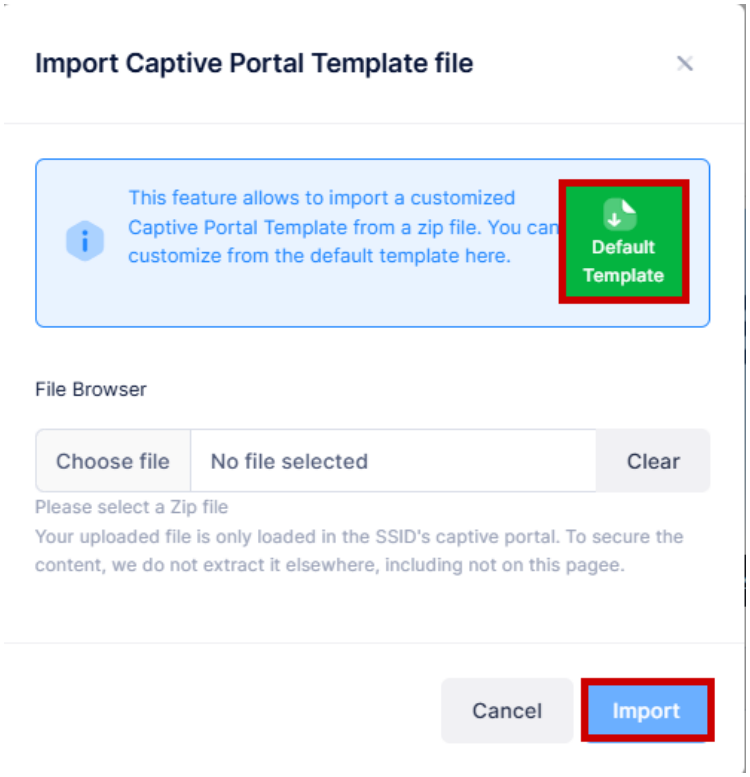


Change the text in the Translation field, as necessary. For example, if you selected the “Terms of Use” text object and changed the text in the Translation field to “Terms and Conditions”, the user would see “Terms and Conditions”. When you are done, click on **Save** to make the translation change for the selected text object.

You can edit the text objects for any of the selected languages. Click on **Languages** and select which languages to add or remove from the Translation Editor screen.

7.4.6.4.2 Import Default zip File for Customizing Captive portal Template

Click on **Import file (.zip)** on the Customize Captive Portal Template screen to replace the Captive portal template content with the zip file default template content. The following screen opens:



Select the **Default Template** button to download a default Captive Portal Template in zip file format. It is recommended that the customization is modified from the code base of this zip. Then re-zip it and select **Import** button to replace the existing Template with a new one.

After importing the zip file, there is no need to click on the 'Deploy changes to Device' button, as the deployment will occur automatically.

Note: Your uploaded file is only loaded in the SSID's captive portal. To secure the content, do no extract it elsewhere, including not on this page. Once a customized zip is uploaded, the traditional customization is disabled. If you want to deploy the traditional customization, the zip content is overwritten.

7.4.6.4.3 Deploying the Custom Captive Portal Template

When you are done customizing the Captive Portal Template, click on **Deploy changes to Access Point** to apply the updated template to the Access Points in the network. The next time users are presented with this Captive Portal page, they will see the updated, custom version of the page.

If the customized Captive Portal page does not display correctly on the guest device, click on **Deploy changes to Access Point** again.

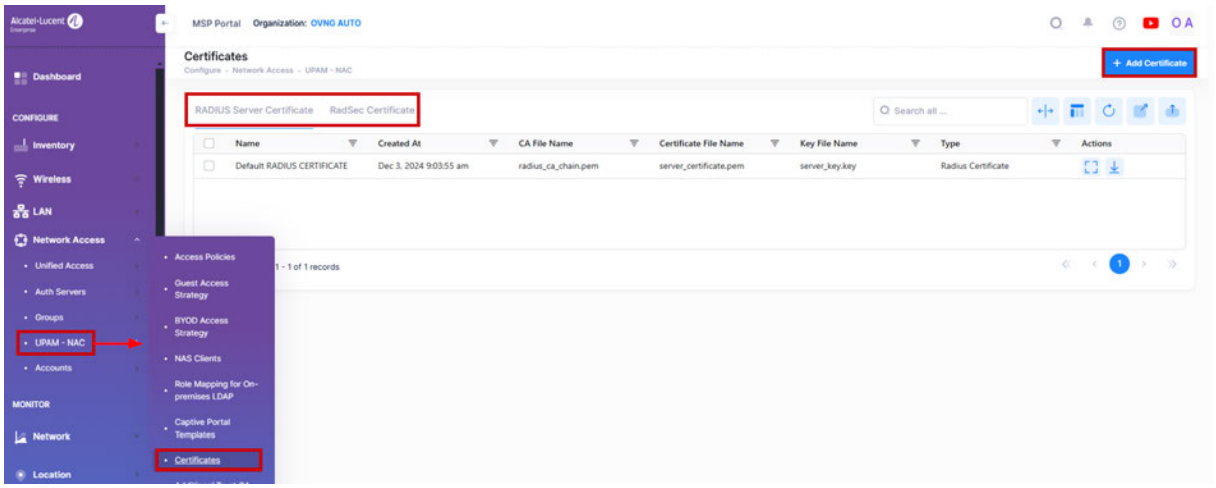
21 Oct 2025

7.4.7 Certificates - UPAM

The RADIUS Certificates screen displays information (see page 686) about all RADIUS Server and RadSec Certificates. Use this screen to add (see page 682), download (see page 684), and delete (see page 685)the following UPAM RADIUS Server certificates:

- **RADIUS Server Certificate** - Used to establish a secure connection with a network device for 802.1X or TLS authentication.
- **RadSec Cretificate** - Used to establish a secure connection between UPAM and an external RADIUS server that uses RadSec (RADIUS-over-TLS). UPAM acts as a RadSec client when communicating with the RadSec server (see the External RADIUS Server (see page 692) online help for more information).

To manage RADIUS certificates, click on **Network Access > UPAM-NAC > Certificates** under the "Configure" section of the OmniVista Terra Menu (see page 45).



The Certificates screen provides a separate tab for each of the two types of certificates. Click on the desired tab to view existing certificates and/or add new ones.

7.4.7.1 Adding a Certificate

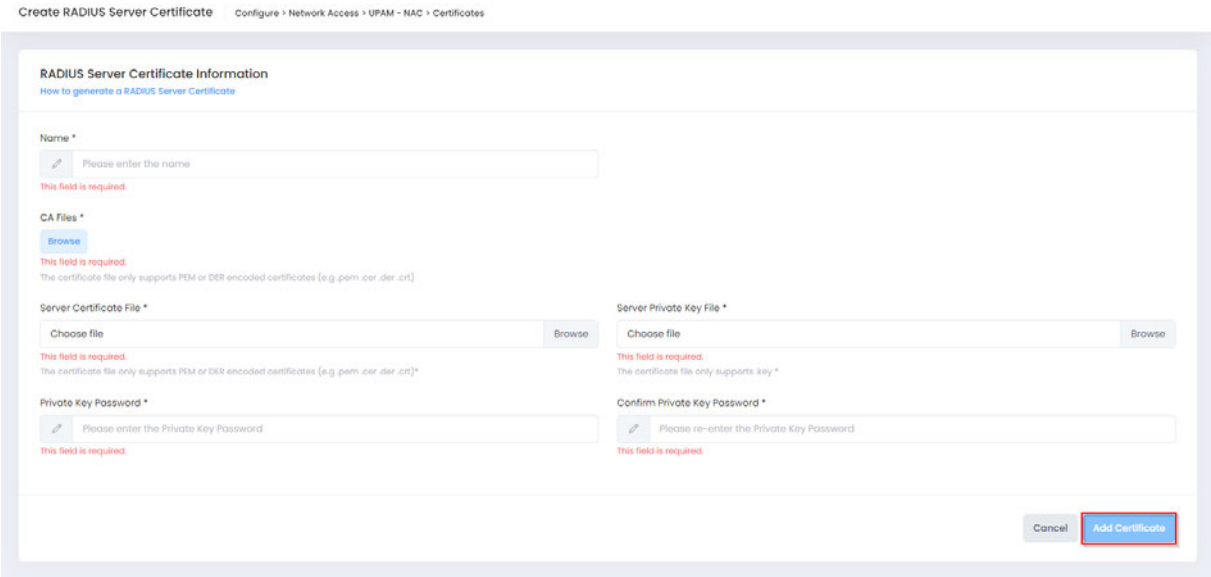
Click on one of the two tabs shown to select which certificate you want to create and upload.

- RADIUS Server Certificate (see page 682)
- RadSec Certificate (see page 683)

7.4.7.1.1 Adding a RADIUS Server Certificate

A default certificate ("Default RADIUS Certificate") is made available at the time the Organization is created. However, it is strongly recommended that you install custom certificates.

To add a custom certificate, select the RADIUS Server Certificate tab on the Certificates screen, then click on **Add Certificate** to open the following screen to define the certificate information:



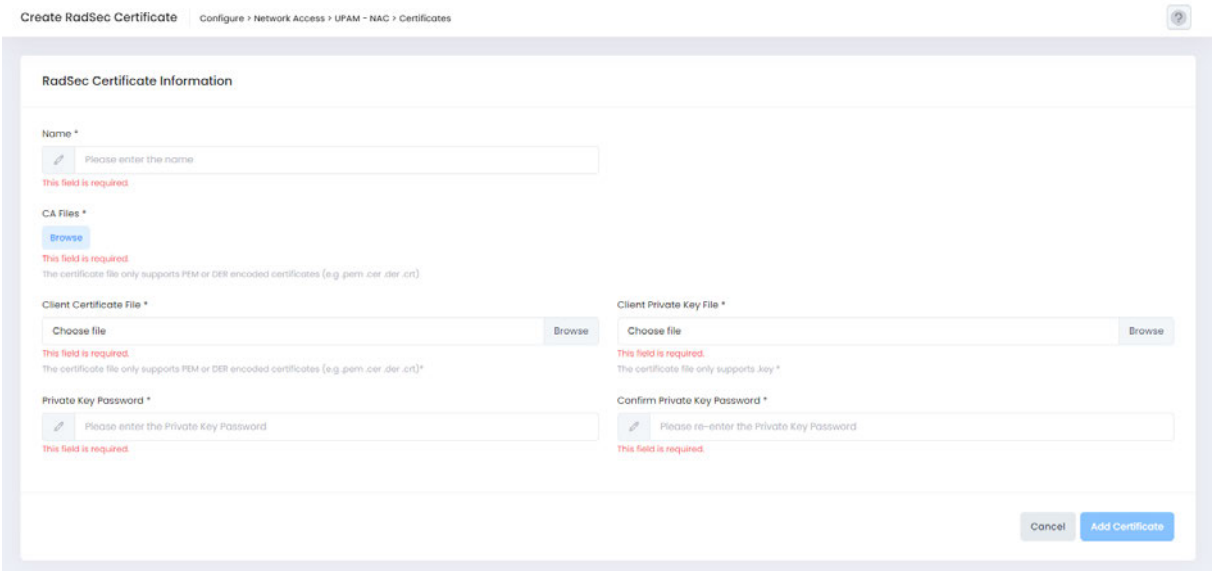
Complete the fields as described below, then click on **Add Certificate**.

- **Name** - Enter a name to identify the certificate.
- **CA Files -** Click on **Browse** to locate and import the RADIUS Server's CA Certificate (PEM or DER encoded certificates only).
- **Server Certificate File -** Click on **Browse** to locate and import the Certificate File (PEM or DER encoded certificates only).
- **Server Private Key File -** Click on **Browse** to locate and import the Certificate Private Key File.
- **Private Key Password -** Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Confirm Private Key Password** - Re-enter the Private Key password.

If necessary, you can generate a new RADIUS Server Certificate (see page 685).

7.4.7.1.2 Adding a RadSec Certificate

Select the RadSec Certificate tab on the Certificates screen, then click on **Add Certificate** to open the following screen to define the certificate information:

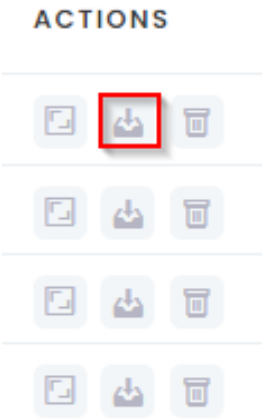


Complete the fields as described below, then click on **Add Certificate**.

- **Name** - Enter a name to identify the certificate.
- **CA Files -** Click on **Browse** to locate and import the RADIUS Server's CA Certificate (PEM or DER encoded certificates only).
- **Client Certificate File -** Click on **Browse** to locate and import the Certificate File (PEM or DER encoded certificates only).
- **Client Private Key File -** Click on **Browse** to locate and import the Certificate Private Key File.
- **Private Key Password -** Enter a Private Key Password to encrypt the key file when generating the CA File.
- **Confirm Private Key Password** - Re-enter the Private Key password.

7.4.7.2 Downloading a Certificate

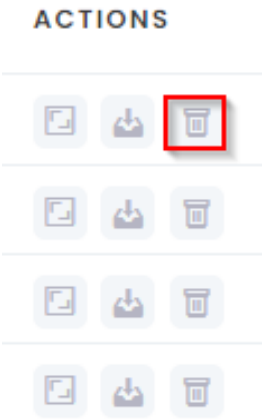
You can download a certificate from the RADIUS Server Certificates List or from the RadSec Certificates List to your machine. Select the certificate in the list and click on the download icon under the “Actions” column.



The certificate will be downloaded to your designated Download folder.

7.4.7.3 Deleting a Certificate

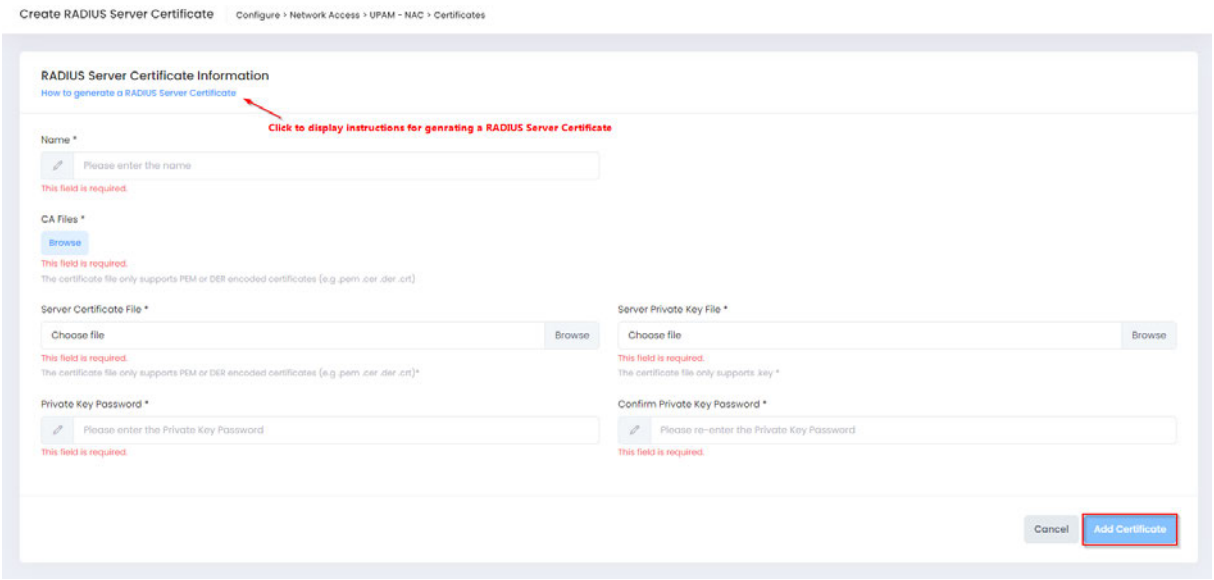
Select a certificate in the RADIUS Server Certificates List or in the RadSec Certificates List and click on the Delete icon under the “Actions” column.



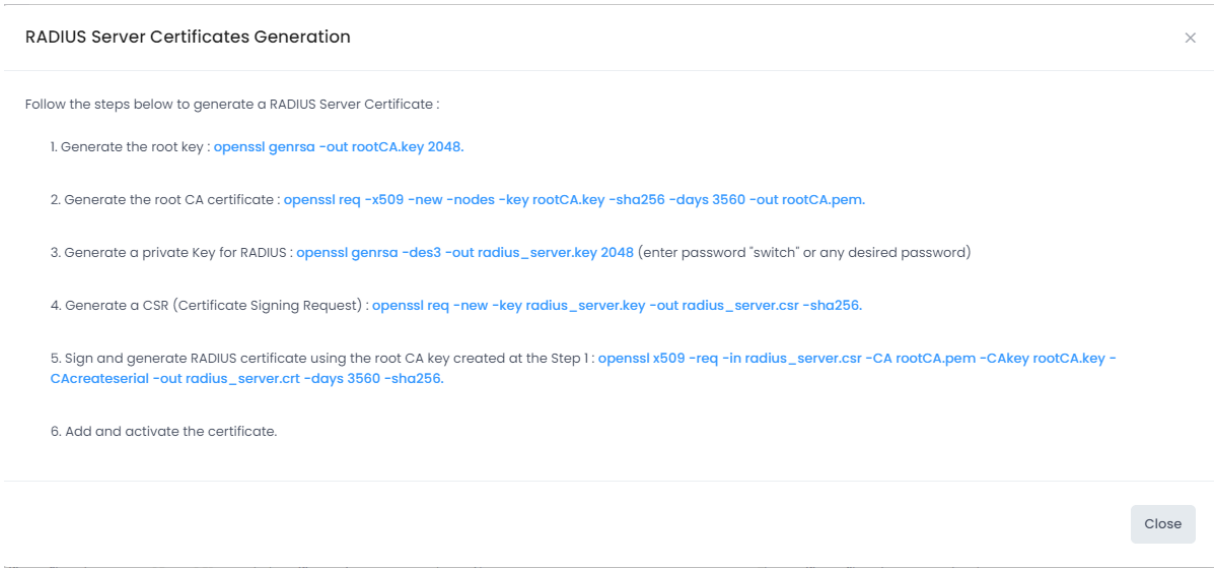
Click **Delete** at the Confirmation Prompt. Note that you cannot delete an active (“being used”) certificate. You must first activate a different certificate before you can delete it.

7.4.7.4 Generating a RADIUS Server Certificate

To display instructions on how to create a RADIUS Server Certificate, click on the **How to generate a RADIUS Server Certificate** link on the RADIUS Server Certificate Information screen.



The following instructions are displayed:



Follow these instructions to generate a RADIUS Server Certificate.

7.4.7.5 Certificate List

The RADIUS Server Certificate List displays the following information for each certificate:

- **Name -** Identifier for the certificate in UPAM.
- **Created At** - The date and time the certificate was added.
- **CA File Name -** The name of the uploaded CA Certificate file.
- **Server Certificate File -** The name of certificate file in the RADIUS server. The Server File contains the contents of the Sever Certificate file and the Server Key file.
- **Server Private Key File** - The name of the Server Key file.
- **Type -** The type of certificate file stored in the RADIUS server (RADIUS certificate or RadSec Client).
- **Usage Status -** Indicates whether the certificate is “Being Used” or “Not Used” in the RADIUS server.
- **Validity Start Time -** The start date and time when the certificate is valid.
- **Validity End Time -** The date and time after which the certificate is no longer valid.
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.

The RadSec Certificate List displays the following information for each certificate:

- **Name -** Identifier for the certificate in UPAM.
- **Created At** - The date and time the certificate was added.
- **Validity Start Time -** The start date and time when the certificate is valid.
- **Validity End Time -** The date and time after which the certificate is no longer valid.
- **Usage Status -** Indicates whether the certificate is “Being Used” or “Not Used” in the RADIUS server.

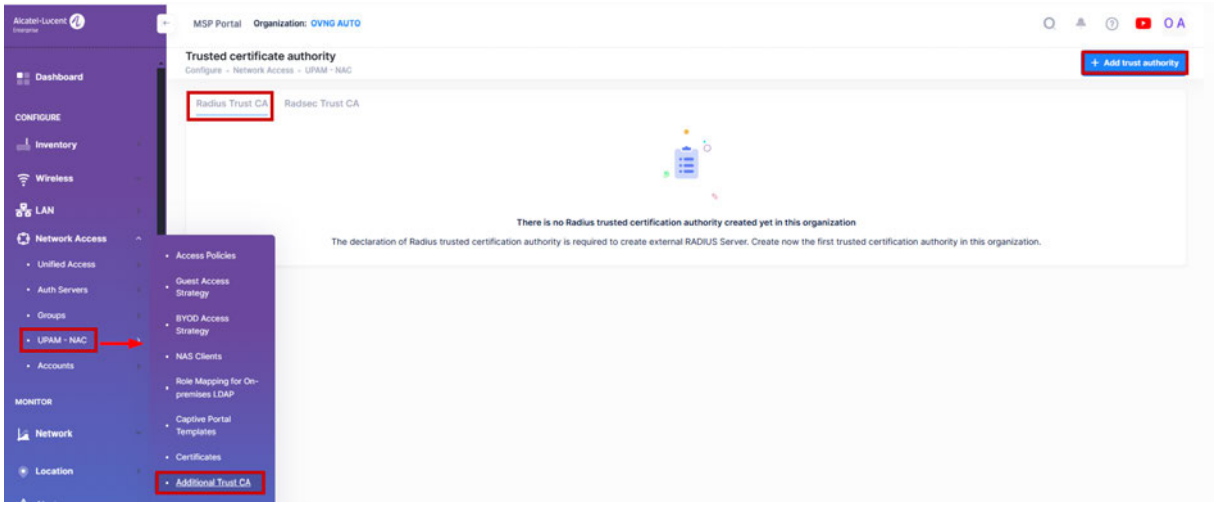
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.
- **CA File Name -** The name of the uploaded CA Certificate file.
- **Client Certificate File -** The name of certificate file in the RADIUS server. The Server File contains the contents of the Sever Certificate file and the Server Key file.
- **Client Private Key File** - The name of the Server Key file.
- **Type -** The type of certificate file stored in the RADIUS server (RADIUS certificate or RadSec Client).

21 Oct 2025

7.4.8 Additional Trust CA

The Trusted Certificate Authority screen displays information (see page 690) about all RADIUS Trust CAs and RadSec Trust CAs in the UPAM Trust RADIUS Store. Use this screen to add (see page 688), download (see page 690), and delete (see page 690)a certificate in the UPAM RADIUS server for client authentication.

To manage Trusted Certificate Authorities, click on **Network Access > UPAM-NAC > Additional Trust CA** under the “Configure” section of the OmniVista Terra Menu (see page 45).

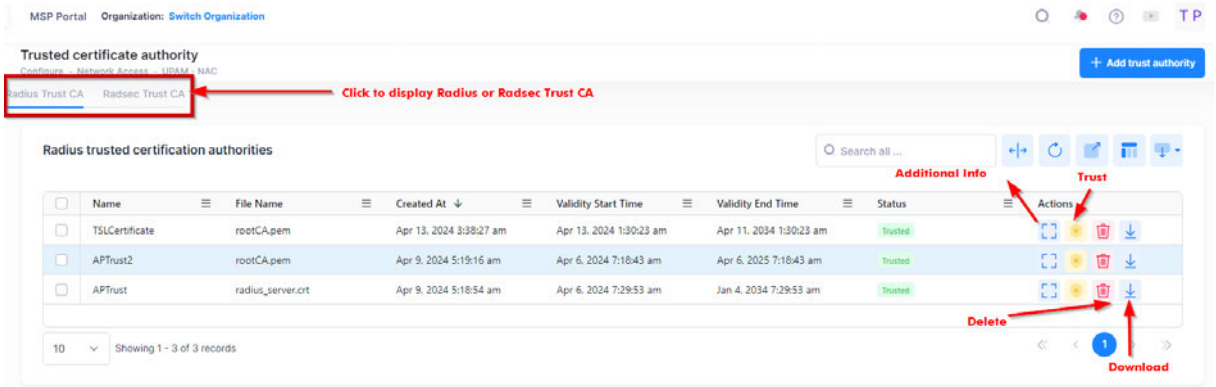


7.4.8.1 Adding a Certificate to the Trust RADIUS Store

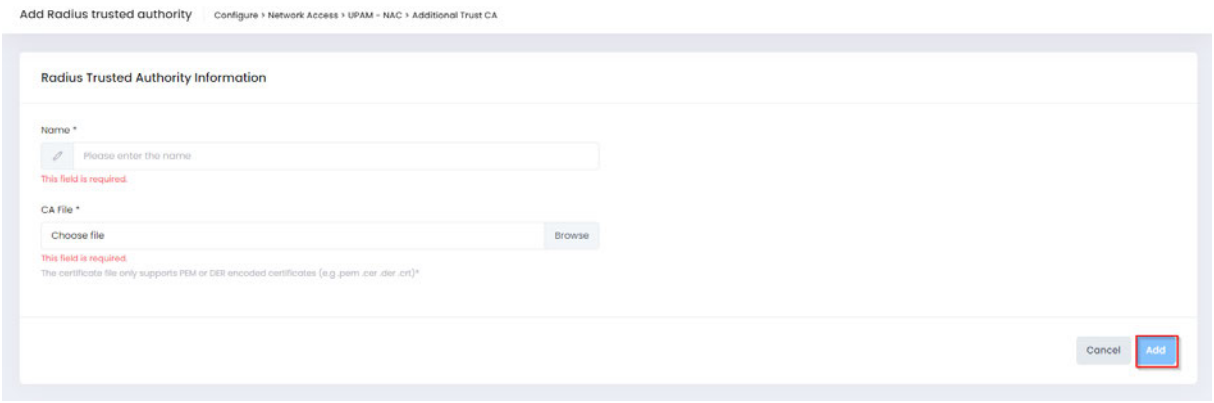
Click on one of the two tabs shown on the Trusted Certificate Authority screen to select which certificate you want to create and upload.

- RADIUS Trust CA (see page 688)
- RadSec Trust CA (see page 689)

7.4.8.1.1 Adding a RADIUS Trust CA



To add a RADIUS Trust CA to the UPAM RADIUS server for client authentication, select the RADIUS Trust CA tab on the Trusted Certificate Authority screen, then click on **Add Trust Authority**. The following RADIUS Trusted Authority Information screen opens:



Complete the fields as described below, then click on **Add**.

- **Name** - Enter a name to identify the certificate.
- **CA File** - Click on **Browse** to locate and import the CA Certificate (PEM or DER encoded certificates only).

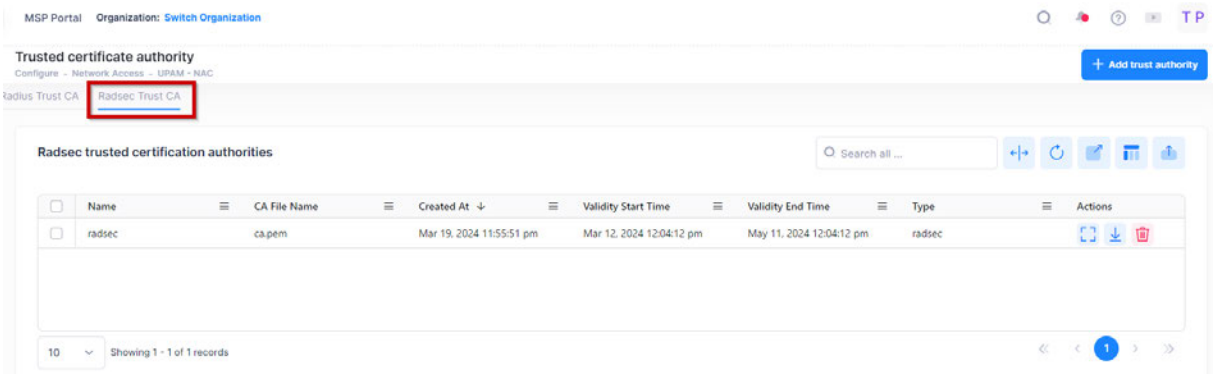
The certificate is now available and appears in the list of certificates on the RADIUS Trust CA screen.

7.4.8.1.1.1 Trust a RADIUS Certificate Authority

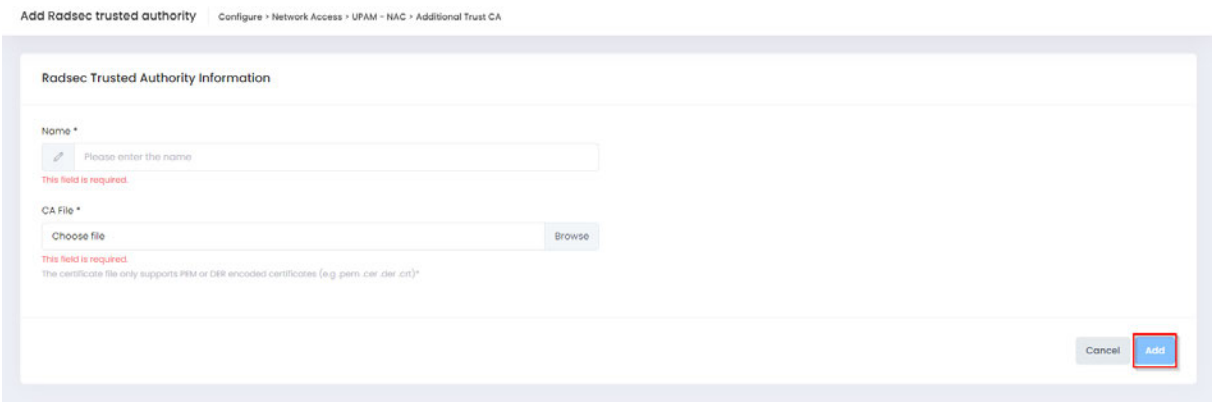
When a RADIUS Trust CA is added, it is untrusted by default. To trust a certificate, select the certificate from the RADIUS Trusted Certification Authorities List and click on the Trust Certification icon under the “Actions” column. The “Status” column for the selected certificate will change from Untrusted to Trusted if the trust certificate operation was successful.

Note: The Trust Certificate option will only appear under the Actions column when there is at least one RADIUS Server Certificate in use under **Network Access > UPAM-NAC > Certificates > Radius Server Certificate** (see page 682).

7.4.8.1.2 Adding a RadSec Trust CA



To add a RadSec Trust CA to the UPAM RADIUS server for client authentication, select the RadSec Trust CA tab on the Trusted Certificate Authority screen, then click on **Add Trust Authority**. The following RADIUS Trusted Authority Information screen opens:



Complete the fields as described below, then click on **Add**.

- **Name** - Enter a name to identify the certificate.
- **CA File** - Click on **Browse** to locate and import the CA file (PEM or DER encoded certificates only).

The certificate is now available and appears in the list of certificates on the RadSec Trust CA screen.

7.4.8.2 Downloading a Certificate

You can download a certificate from the RADIUS Trusted Authority Information List or from the RadSec Trusted Authority Information List to your machine. Select the certificate in the list and click on the download icon under the “Actions” column. The certificate will be downloaded to your designated Download folder.

7.4.8.3 Deleting a Certificate

Select a certificate in the RADIUS Trusted Authority Information List or from the RadSec Trusted Authority Information List and click on the Delete icon. Click **Delete** at the Confirmation Prompt.

7.4.8.4 Trusted Certificate Authority List

The RADIUS Trusted Authority Information List and the RadSec Trusted Authority Information List displays the following information for each certificate:

- **Name -** Identifier for the certificate in UPAM.
- **CA File Name** - The name of the uploaded CA Certificate file.
- **Created At** - The date and time the certificate was added.
- **Validity Start Time -** The start date and time when the certificate is valid.
- **Validity End Time -** The end date and time when the certificate is valid.
- **Status -** Indicates the trust status for the certificate (Trusted or UnTrusted).
- **Type -** The type of Trust CA file stored in the RADIUS server (RADIUS or RadSec).
- **Issued By -** The certification authority (CA) that issued the certificate.
- **Issued To -** The entity to which the certificate is assigned.

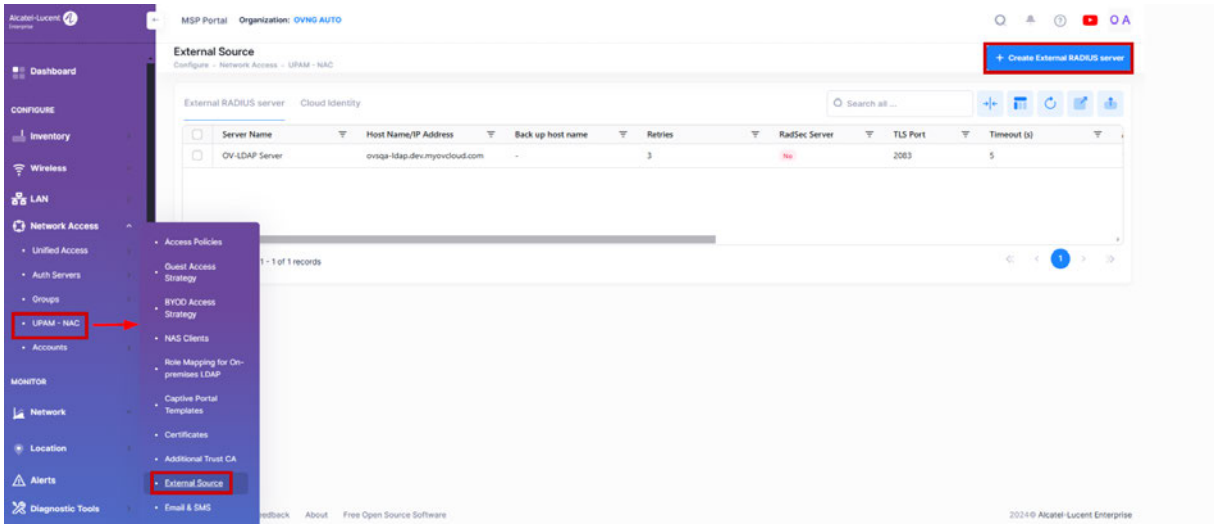
21 Oct 2025

7.4.9 External RADIUS Server

The External RADIUS Server screen displays information (see page 696) about External RADIUS Servers that are configured for UPAM to use for authentication. This screen is also used to create (see page 692), edit (see page 695), and delete (see page 696)an external server.

To access the External RADIUS Server screen, click on **Network Access > UPAM NAC > External Source** under the “Configure” section of the OmniVista Terra Menu (see page 45).

Click on the External RADIUS Server tab shown on the External Source screen to access the External RADIUS Server List.

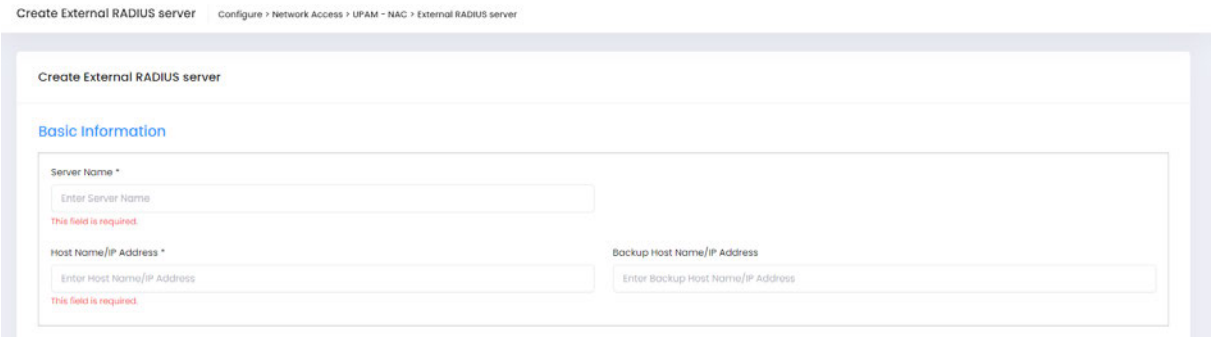


7.4.9.1 Creating an External RADIUS Server

To add an External RADIUS Server to UPAM, click on **Create External RADIUS Server** to open the Create External RADIUS Server screen. Complete the following sections of the form, then click **Create RADIUS Server** when you are finished.

- Basic Information (see page 693) - Configure an External RADIUS Server name and related attributes to identify the server.
- Is this a RadSec Server? (see page 693) - Enables/disables UPAM to act as a RadSec client if the External RADIUS Server is a RadSec server.
- Advanced Information (see page 694) - Configure the timeout and retry values that UPAM will use to determine if a server is unreachable.
- Shared Secret (see page 694) - Configure a shared key that UPAM will use to communicate with the External RADIUS Server.
- Pre-emption (see page 694) - Enables/disables whether UPAM will switch back to a primary External RADIUS Server at the end of a specified countdown timer value.
- Require Message Authenticator (see page 695) - Enables/disables whether UPAM checks for the Message-Authenticator attribute in RADIUS response packets coming from the external RADIUS Server.

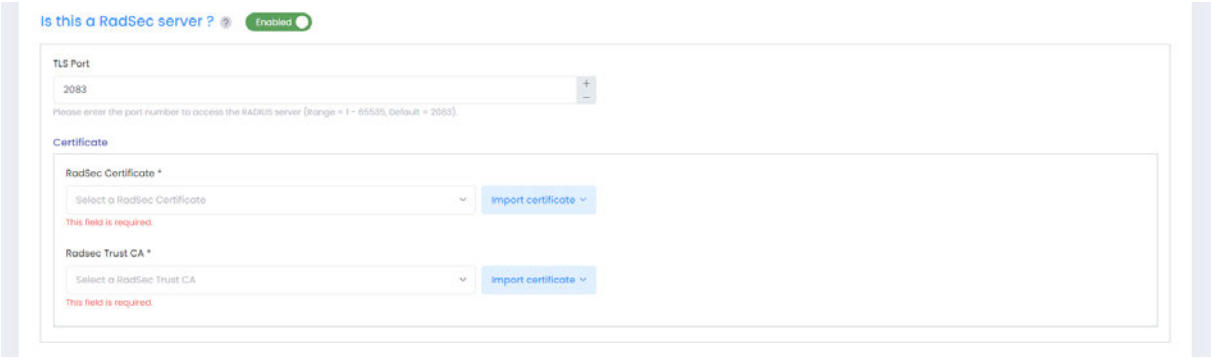
7.4.9.1.1 Basic Information



- **Server Name** - Enter a name to identify the External RADIUS Server configuration.
- **Hostname/IP Address** - Enter the hostname or IP address of the primary External RADIUS Server.
- **Backup Hostname/IP Address** - Enter the hostname or IP address of a backup External RADIUS Server, if applicable. UPAM will attempt to use the backup server when the primary server is deemed unreachable.

If the External RADIUS Server uses RadSec to provide client authentication, make sure the IP address for the External RADIUS Server is a public IP address.

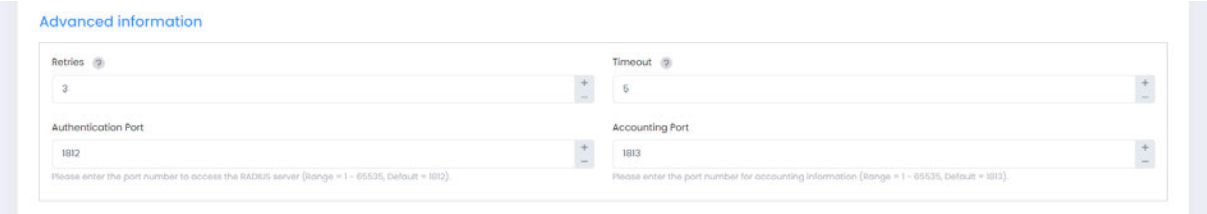
7.4.9.1.2 Is this a RadSec Server?



If the external RADIUS server uses RadSec (RADIUS-over-TLS), you can enable this option to allow UPAM to act as a RadSec client when communicating with the external RadSec server. By default, this option is disabled. When enabled, complete the following fields as described:

- **TLS Port** - Enter the port number for the Transport Layer Security tunnel that will be used to pass RADIUS packets between the UPAM RadSec client and the external RadSec server. (Range = 1 - 65535, Default = 2083)
- **RadSec Certificate** - Select an existing RadSec client certificate or click on **Import Certificate** to open the Create RadSec Certificate screen to import a new RadSec client certificate to use.
- **RadSec Trust CA** - Select an existing RadSec Trust CA or click on **Import Certificate** to open the Add RadSec Trusted Authority screen and import a new RadSec Trust CA.

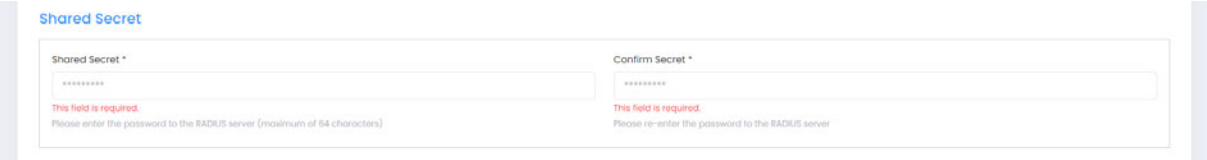
7.4.9.1.3 Advanced Information



- **Retries** - Specify the number of times UPAM will attempt to reconnect to the External Radius Server when the connection timeout occurs before concluding that the External Radius Server is unreachable. (range = 1 – 3, Default = 3)
- **Timeout** - Specify the amount of time, in seconds, that UPAM will attempt a connection to the External Radius Server before timing out. (Range = 1 – 30, Default = 5)
- **Authentication Port** - Enter the TCP/UDP port used to perform authentication. (Range – 1 – 65535, Default = 1812)
- **Accounting Port** - Enter the TCP/UDP port used to perform accounting. (Range – 1 – 65535, Default = 1813)

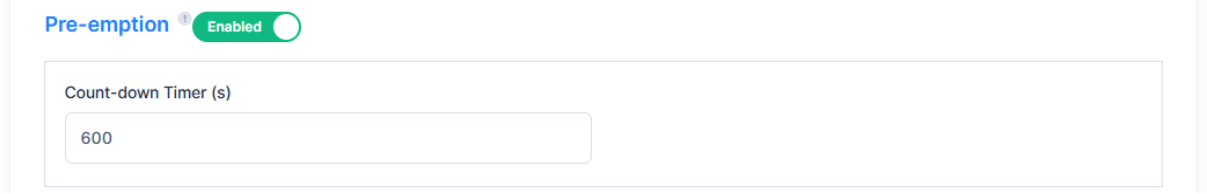
Note that the “Authentication Port” and “Accounting Port” options are not available if UPAM is acting as a RadSec client (see page 693).

7.4.9.1.4 Shared Secret



- **Shared Secret** - Specify the shared key that UPAM uses to communicate with the External Radius Server. (4 - 64 characters)
- **Confirm Secret -** Re-enter to confirm the shared secret key. (4 - 64 characters)

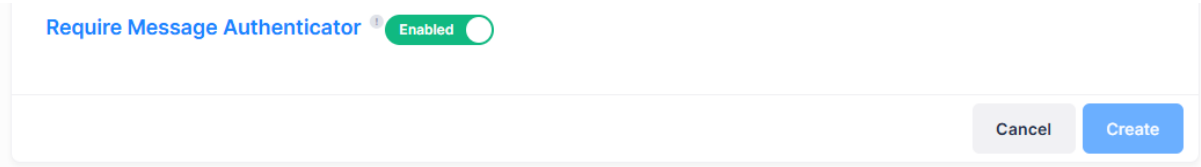
7.4.9.1.5 Pre-emption



- **Pre-emption** - Enables/Disables whether to go back to the primary External RADIUS Server. (Default = Disabled). When enabled:
  - **Count-down Timer** - Specify the amount of time to wait, in seconds, after a failover to the backup External RADIUS Server before attempting to go back to the primary External

RADIUS Server. The countdown timer restarts on every switchover to the backup server. (Default = 600 seconds)

7.4.9.1.6 Require Message Authenticator

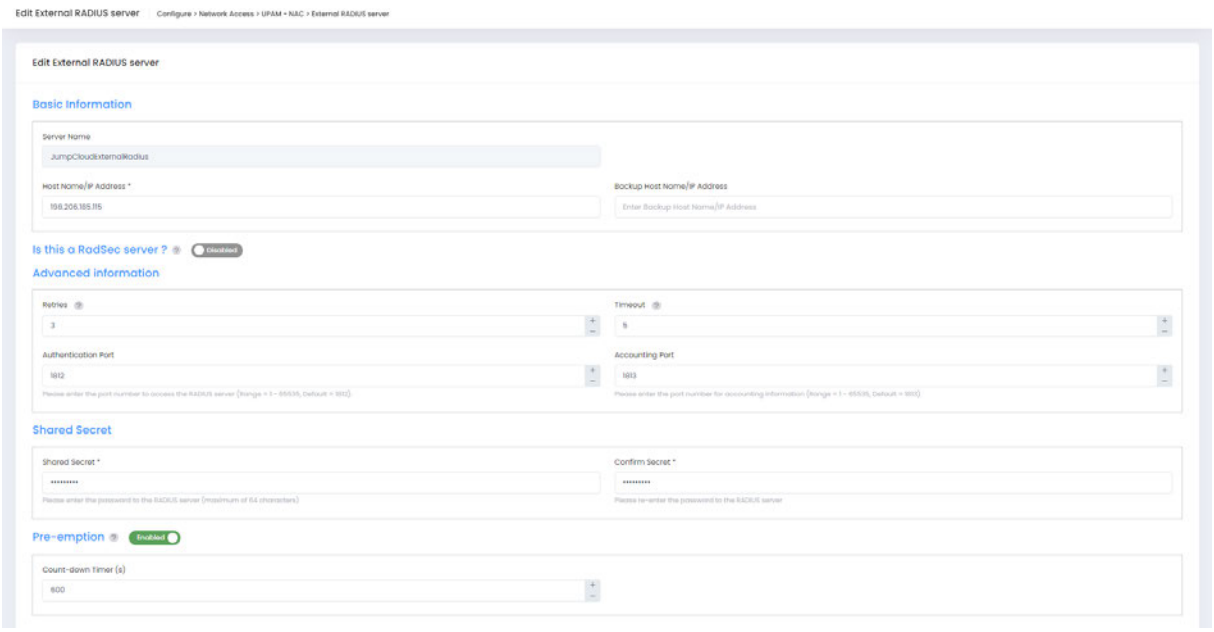


- **Require Message Authenticator** - Enables/Disables UPAM checking for the Message-Authenticator attribute in RADIUS response packets coming from the external RADIUS Server. Enabling the Require Message Authenticator check is the recommended setting to prevent attempts to forge authentication responses by spoofing UDP-based RADIUS response packets. Checking for this attribute is also configurable when defining a RADIUS Authentication server (see page 589). Refer to Require Message Authenticator Use Cases (see page 704) for more information.
  - **Enabled** - Checks for the Message-Authenticator attribute and drops any response packets that do not contain this attribute.
  - **Disabled** - Does not check for the Message-Authenticator attribute in RADIUS response packets.

- If the option to configure UPAM to act as a RadSec client (see page 693) is enabled, the Require Message Authenticator option is not available.
- Require Message Authenticator is enabled by default when you are creating an External RADIUS Server; however, this option is disabled by default for existing servers that were created in OVC 10.4.3. This ensures that devices managed in OVC 10.4.3 can still pass RADIUS authentication after an upgrade to OVT 10.5.1.

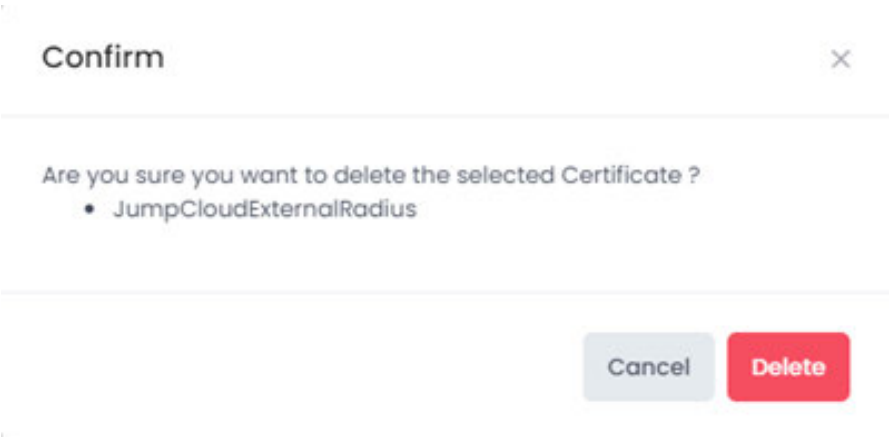
7.4.9.2 Editing an External RADIUS Server

Select a server in the External RADUIS Server List and click on the Edit icon. The Edit External RADIUS Server screen opens on which you can edit the fields as described above (see page 692), When you are done making changes to the Server attributes, click on **Save** to return to the External RADIUS Server List.



7.4.9.3 Deleting an External RADIUS Server

Select a server in the External RADIUS Server List and click on the Delete icon under the “Actions” column or click on the **Actions** button and select Delete from the drop-down menu. When the following confirmation prompt appears, click on **Delete** to delete the profile.



7.4.9.4 External RADIUS Server List

The following information is displayed for each Server in the External RADIUS Server List:

- **Server Name** - The name assigned to the Server configuration.
- **Hostname/IP Address** - The hostname or IP address of the primary External RADIUS Server.
- **Backup Hostname/IP Address** - The hostname or IP address of a backup External RADIUS Server, if applicable. UPAM will attempt to use the backup server when the primary server is deemed unreachable.

- **Retries** - The number of times UPAM will attempt to reconnect to the External Radius Server when the connection timeout occurs before concluding that the External Radius Server is unreachable
- **Timeout(s)** - The amount of time, in seconds, that UPAM will attempt a connection to the External Radius Server before timing out
- **Authentication Port** - The TCP/UDP port used to perform authentication.
- **Accounting Port** - The TCP/UDP port used to perform accounting.
- **RadSec Server** - Whether the external server is a RadSec server (Yes or No). If Yes, UPAM communicates with the external server as a RadSec client.
- **TLS Port** - The port number for the Transport Layer Security tunnel that will be used to pass RADIUS packets between the UPAM RadSec client and the external RadSec server.
- **Pre-emption** - Whether or not UPAM should go back to the primary External RADIUS Server at the end of a count-down timer. (Enabled = go back after count-down timer ends; Disabled = go back only when backup server times out).
- **Message Authenticator** - Whether the check for the Message-Authenticator attribute in RADIUS response packets is enabled or disabled.
- **Count-down Timer** - When pre-emption is enabled, this value is the amount of time UPAM will wait, in seconds, after a failover to the backup External RADIUS Server before attempting to go back to the primary External RADIUS Server. The countdown timer restarts on every switchover to the backup server.
- **Created At** - The date and time the External RADIUS Server configuration was created.

21 Oct 2025

7.4.10 Cloud Identity

The UPAM-NAC Cloud Identity integrates with Microsoft Entra ID Connect via the Certificate Connector for Microsoft, enabling support for Employee 802.1x clients using EAP-TTLS. Microsoft Entra ID Connect is a standard protocol that ensures secure authentication and authorization between identity providers (like Entra ID) and relying party applications. Implementing Entra ID Connect allows organizations to establish trust between their identity provider and third-party applications, facilitating seamless and secure access to resources. Additionally, Microsoft Entra ID can synchronize with on-premises Active Directory, providing authentication access to OmniVista Terra.

Before you begin, you must create an identity in Microsoft Entra ID (formerly Azure Active Directory). For more details, refer to Microsoft Help.

In this release of UPAM, cloud identity is only available for devices that use 802.1X authentication. Cloud identity cannot be used with BYOD or Guest Captive Portal at this time.

To apply a Cloud Identity to AP's SSID, Assign the Cloud Identity to an Access Policy in Authentication Strategy section. You can then assign this Access Policy to a SSID Authentication Strategy and choose the Access Policy.

7.4.10.1 Microsoft Entra ID Overview

Microsoft provides an overview of Microsoft Entra Domain Services (part of Microsoft Entra ID) to help customers continue using their legacy applications. Legacy domain services, such as domain join, group policy, LDAP, and Kerberos/NTLM authentication, are still supported, with the key difference being that these services now run in the cloud.

Additionally, Microsoft Entra can serve as the backend account database to support 802.1X clients using EAP-TTLS with PAP as the inner authentication protocol.

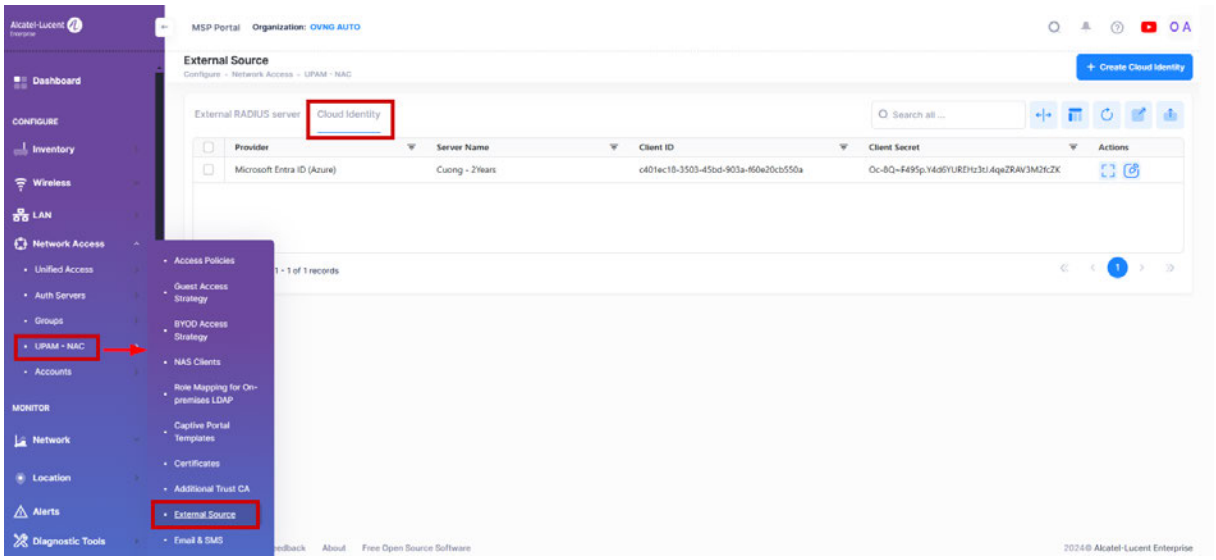
Implementing Microsoft Entra ID provides organizations with several advantages.

- **Identity Management:** Allows organizations to create, manage, and authenticate user identities across multiple platforms and services.
- **Access Control:** Enables the definition and enforcement of access policies based on user roles, groups, and permissions to protect sensitive data and resources.
- **Single Sign-On (SSO):** Provides users with the convenience of accessing multiple applications and services using a single set of credentials, boosting productivity.
- **Multi-Factor Authentication (MFA):** Enhances security by requiring users to verify their identity through multiple authentication factors, such as passwords, biometrics, or one-time codes.

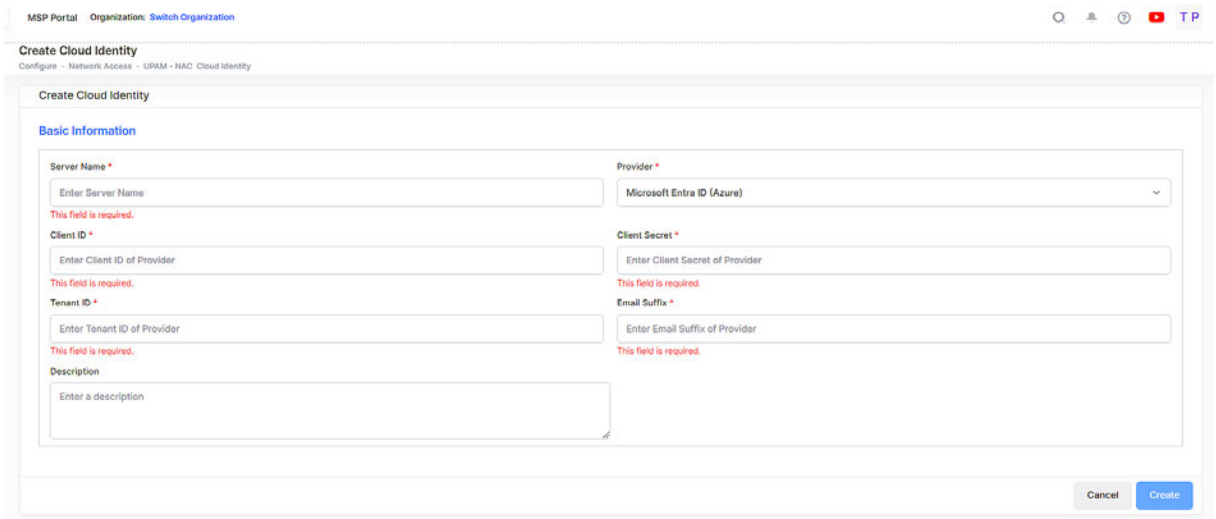
7.4.10.2 Creating a Cloud Identity

To create a Cloud Identity, click on **Network Access > UPAM-NAC > External Source** under the “Configure” section of the OmniVista Terra Menu (see page 45).

Click on Cloud Identity tab shown on the External Source screen to create a Cloud Identity.



Complete the fields as described below, then click on **Create**.

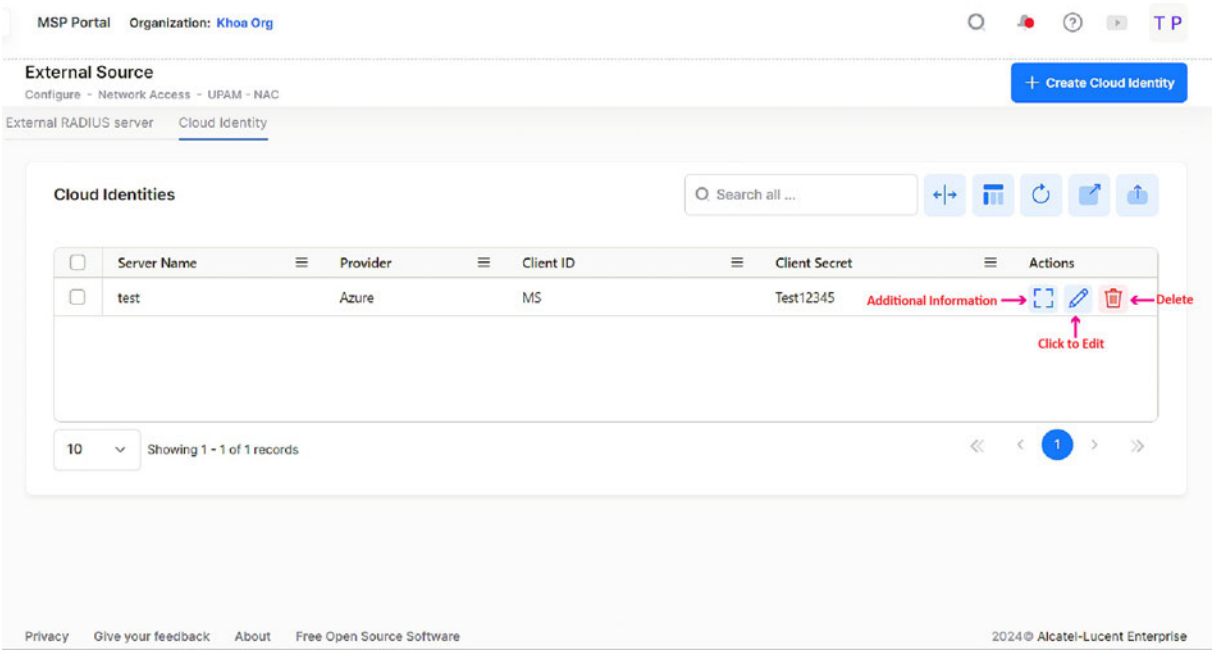


- **Server Name** - Enter a name to identify the Cloud Identity Server configuration..
- **Provider-** Select the name of the Cloud service provider. (Microsoft Entra ID)
- **Client ID -** Enter the Client ID Provider
- **Client Secret** - Enter the Client Secret of the Provider.
- **Tenant ID-** .Enter the Tenant ID of the Provider.
- **Email Suffix-** Enter the email suffix of the Provider.
- **Description-** Enter a description for the Cloud Identity.

Click **Create** to create a Cloud Identity.

7.4.10.3 Editing a Cloud Identity

Select a server name in the Cloud Identity List and click on the Edit icon. The Edit Cloud Identity screen opens on which you can edit the fields as described above, When you are done making changes to the Server attributes, click on **Save** to return to the External RADIUS Server List.

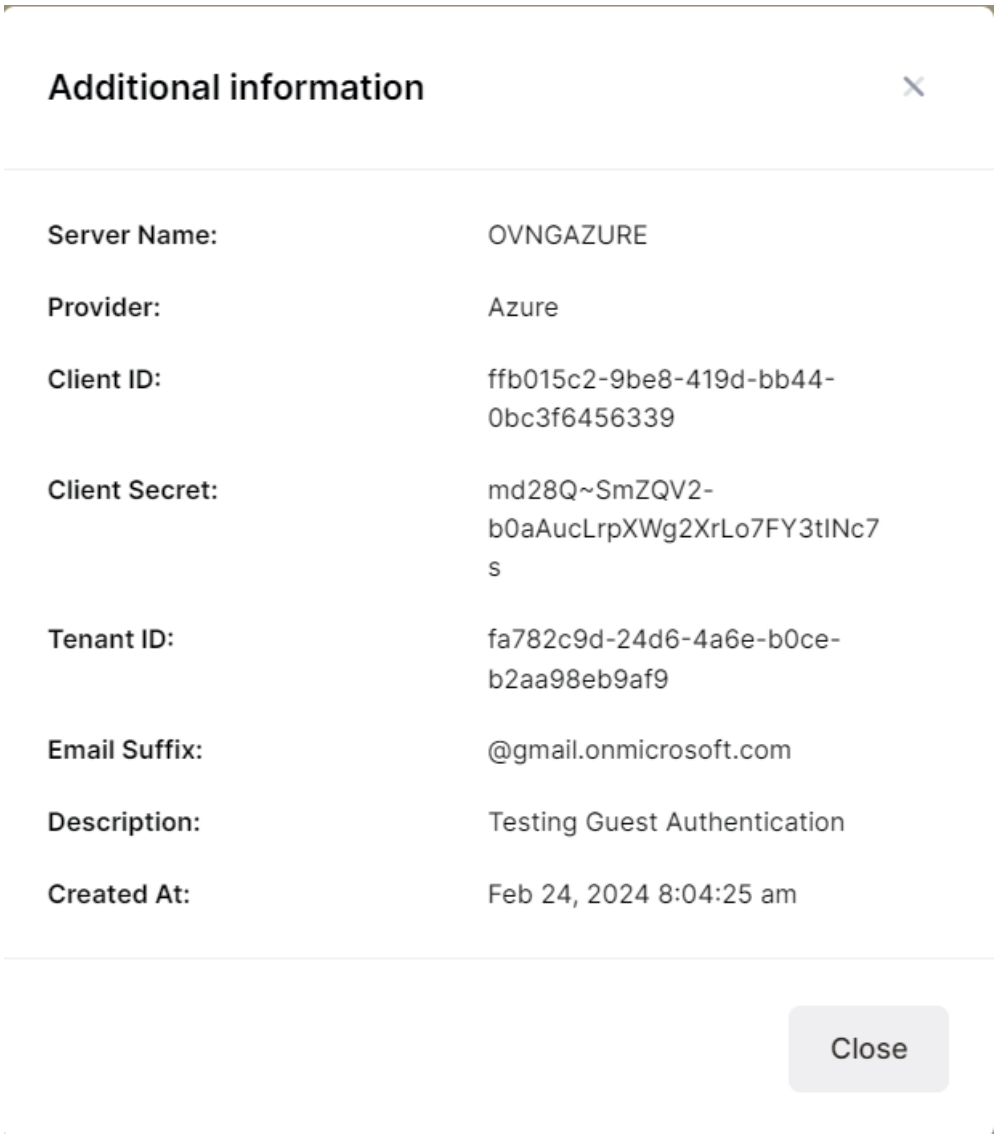


7.4.10.4 Deleting a Cloud Identity

Select a server name in the Cloud Identity List and click on the Delete icon. Click on **Delete** to confirm deleting the External RADIUS Server List.

7.4.10.5 View Information about a Cloud Identity

Select a server name in the Cloud Identity List and click on the **Additional Information** icon. The Additional Information Cloud Identity screen opens on which you can view the fields of the selected server.

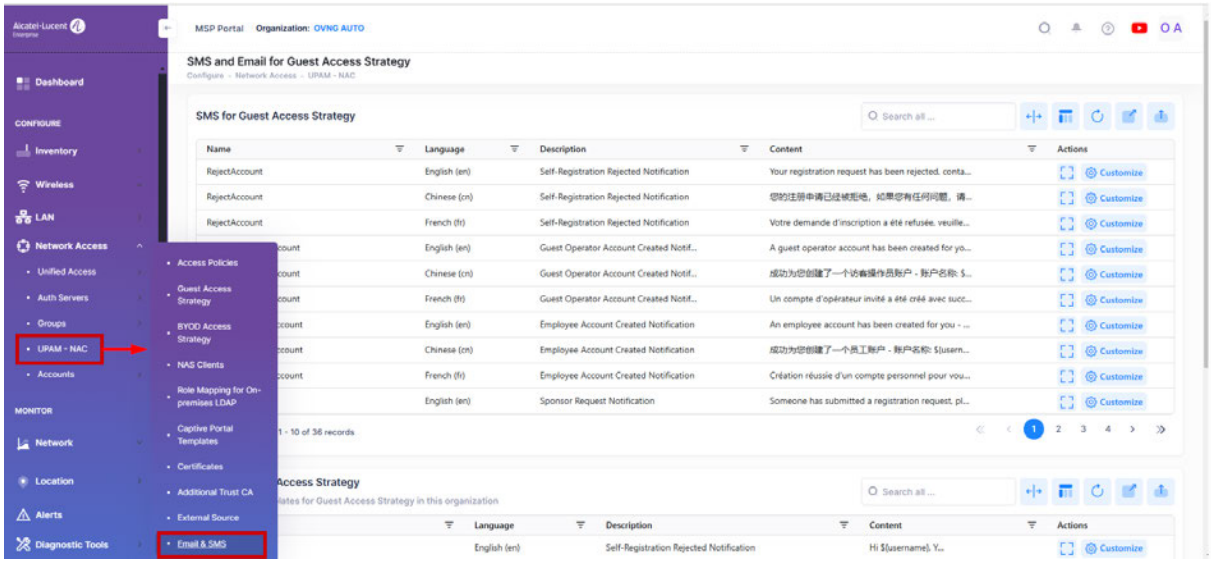

Additional information
Server Name:
OVNGAZURE
Provider:
Azure
Client ID:
ffb015c2-9be8-419d-bb44-0bc3f6456339
Client Secret:
md28Q~SmZQV2-b0aAucLrpXWg2XrLo7FY3tINc7s
Tenant ID:
fa782c9d-24d6-4a6e-b0ce-b2aa98eb9af9
Email Suffix:
@gmail.onmicrosoft.com
Description:
Testing Guest Authentication
Created At:
Feb 24, 2024 8:04:25 am
Close

21 Oct 2025

7.4.11 Email & SMS

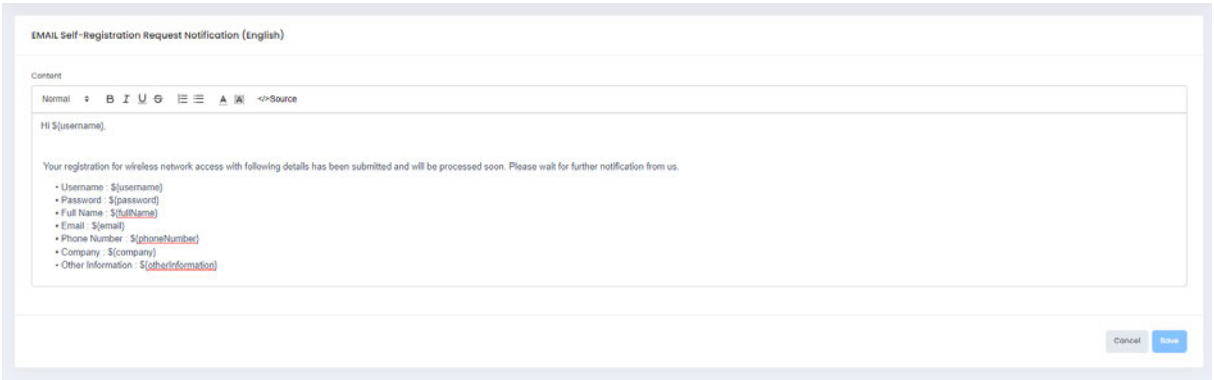
The SMS and Email for Guest Access Strategy screen lists the pre-defined content templates used for SMS text messages and Emails sent from OmniVista Terra. Emails/messages are sent during certain user-interactions, such as self-registration or the user forgot their password.

To access the SMS and Email for Guest Access Strategy screen, click on **Network Access > UPAM-NAC > Email & SMS** under the “Configure” section of OmniVista Terra Menu (see page 45). You can use this screen to display the contents and customize the content of the templates.



7.4.11.1 Customizing the Template Contents

To customize the contents of an SMS message or Email template, click on **Customize** under the “Actions” column next to the template that you want to modify. The template contents is displayed. For example, if you selected the “Self-Registration Request Notification (English)” Email template, the following screen would appear:



Edit the contents of this template and click on **Save**. The next time OmniVista Terra sends this Email. the updated contents is included in the Email.

Note that the content templates for Emails define the text that is included in Organization Emails sent to users. The template for the Email is also customizable. See the online help for Email Templates (see page 131) for more information.

7.4.11.2 Viewing the Contents of SMS and Email Templates

The following information is provided for each template in the SMS and Email templates list:

- **Name** - The name of the template.
- **Language** - The language of the template contents. The language used in a message/Email is based on the language used by the guest user.
- **Description** - A description of what the message/Email will send to the user. For example, “Self-Registration Approved Notification”.
- **Content** - The customizable contents that the user will see in the message/Email.

To view the full contents of a template, click on the Additional Information icon under the “Actions” column next to the template.

21 Oct 2025

7.4.12 Use Cases - Require Message Authenticator

The following scenarios document the use cases for configuring the Request Message Authenticator flag to check for the Message-Authenticator attribute in RADIUS packets. This flag is configurable when defining the following:

- UPAM as RADIUS Server for AP/OmniSwitch (see page 704)
- External Radius server for AP/OmniSwitch (No UPAM) (see page 705)
- UPAM as Proxy between AP/OmniSwitch and External Radius (see page 706)

7.4.12.1 UPAM as RADIUS Server for AP/OmniSwitch

The Require Message Authenticator flag influences the behavior of the UPAM RADIUS server when accepting RADIUS requests from clients within a specified IP range. When enabled, UPAM requires that each RADIUS request packet contains the Message-Authenticator attribute; otherwise, it will drop the packet. When disabled, UPAM does not check for the presence of the Message-Authenticator attribute.

UPAM always includes the Message-Authenticator attribute in its RADIUS response packets, and the Require Message Authenticator setting (enabled or disabled) does not affect that behavior. It is up to the RADIUS client (AP or OmniSwitch) whether to check for the Message-Authenticator attribute in response packets received from UPAM.

Access Point RADIUS Packets:

- Access Points always include the Message-Authenticator attribute in RADIUS request packets.
- You can configure Access Points to check for the Message-Authenticator attribute in RADIUS responses received from a given Radius server. Refer to the External RADIUS online help (see page 692) for information about how to configure the Request Message Authenticator check.

OmniSwitch RADIUS Packets:

By default,

- The OmniSwitch does not send the Message-Authenticator attribute in RADIUS requests.
- The OmniSwitch does not check for the Message-Authenticator attribute in RADIUS responses.

To ensure that the OmniSwitch includes the Message-Authenticator in all RADIUS packets sent and also enforces validation of the Message-Authenticator attribute in all responses received from any RADIUS server, use the **aaa radius message-authenticator** CLI command on the switch. This CLI command is a global command supported on AOS 8.10R2 or higher. Note that you can also issue this command using the OmniVista CLI Scripting application.

Notes:

- If you enable the Require Message Authenticator flag for NAS Clients, UPAM will drop all RADIUS packets received from OmniSwitches running AOS 8.10R1 (or lower), or if the **aaa radius message-authenticator** CLI command is not configured.
- If some APs and switches in your network include the Message-Authenticator attribute in RADIUS requests while others do not, create multiple NAS Client instances with different IP ranges and configure the flag accordingly for each group.

- Default settings for the Require Message Authenticator flag in NAS Clients:
  - Enabled when a new NAS Client is created.
  - Enabled for the "All Managed Devices" NAS Client on a fresh OmniVista installation.
  - Disabled for a NAS Client that already existed when OmniVista was upgraded from release 10.4.3 to 10.5.1. If the flag is then enabled on 10.5.1, the status is retained on subsequent OmniVista release upgrades.
- Enabling the Require Message Authenticator flag is highly recommended to prevent attempts to forge authentication responses by spoofing UDP-based RADIUS response packets.

7.4.12.2 External Radius Server for AP/OmniSwitch (No UPAM)

An Access Point or OmniSwitch sends RADIUS AAA requests directly to a RADIUS server (on-premises or hosted elsewhere); UPAM is not involved in this scenario.

Access Point RADIUS Packets:

- OmniVista configures the AAA RADIUS settings on the AP or OmniSwitch through the AAA Server Profile.
- The Require Message Authenticator flag in the AAA Server configuration on an Access Point influences the behavior of APs running AWOS >= 5.0.2 when accepting RADIUS response packets from the specified RADIUS server.
  - When enabled, the AP enforces that the RADIUS response packet from the RADIUS server includes the Message-Authenticator attribute; otherwise, it drops the response packet.
  - When disabled—or for APs running AWOS < 5.0.2—the AP does not verify the Message-Authenticator attribute in RADIUS responses from any RADIUS server.
- Access Points always send the Message-Authenticator attribute in RADIUS requests, regardless of the AWOS version or the Require Message Authenticator setting (enabled or disabled). It is up to the RADIUS server whether to check for the Message-Authenticator attribute in the RADIUS request packets received from the AP.

OmniSwitch RADIUS Packets:

By default,

- The OmniSwitch does not send the Message-Authenticator attribute in RADIUS requests.
- The OmniSwitch does not check for the Message-Authenticator attribute in RADIUS responses.

To ensure that the OmniSwitch includes the Message-Authenticator in all RADIUS packets sent and also enforces validation of the Message-Authenticator attribute in all responses received from any RADIUS server, use the **aaa radius message-authenticator** CLI command on the switch. This CLI command is a global command supported on AOS 8.10R2 or higher. Note that you can also issue this command using the OmniVista CLI Scripting application.

Notes:

- The Require Message Authenticator flag is not supported on TLS-enabled RADIUS servers; therefore, not configurable when TLS is enabled.
- Default settings for the Require Message Authenticator flag:

    - Enabled when a new RADIUS server is created (TLS is disabled).
    - Enabled for the "UPAMRadiusServer" on a fresh OmniVista installation.
    - Disabled for a RADIUS server that already existed when OmniVista was upgraded from release 10.4.3 to 10.5.1. If the flag is then enabled on 10.5.1, the status is retained on subsequent OmniVista release upgrades.
    - Disabled for a TLS-enabled RADIUS server (Require Message Authenticator flag not available).
- Enabling the Require Message Authenticator flag is highly recommended to prevent attempts to forge authentication responses by spoofing UDP-based RADIUS response packets.

7.4.12.3 UPAM as Proxy between AP/OmniSwitch and External Radius

UPAM proxies incoming RADIUS requests from an Access Point or OmniSwitch to an external RADIUS server.

- When the Require Message Authenticator flag is enabled for the external RADIUS server, UPAM checks for the Message-Authenticator attribute in response packets received from the external RADIUS server. UPAM will then drop any response packets that do not contain the Message-Authenticator attribute but will continue to send RADIUS request packets to the external RADIUS Server for the specified number of Retries.
- When the Require Message Authenticator flag is disabled for the external RADIUS server, UPAM does not check for the Message-Authenticator attribute in RADIUS response packets.

Note that UPAM always includes the Message-Authenticator attribute in RADIUS request packets sent to the external server, regardless of the Require Message Authenticator setting (enabled or disabled). It is up to the external RADIUS Server whether to check for the Message-Authenticator attribute in RADIUS request packets received from UPAM.

The default settings for the Require Message Authenticator flag for external RADIUS servers are as follows:

- Enabled when a new external RADIUS server is created.
- Disabled for an external RADIUS server that already existed when OmniVista was upgraded from release 10.4.3 to 10.5.1. If the flag is then enabled on 10.5.1, the status is retained on subsequent OmniVista release upgrades.

Enabling the Require Message Authenticator flag is highly recommended to prevent attempts to forge authentication responses by spoofing UDP-based RADIUS response packets.

21 Oct 2025

7.5 Accounts

Configuring user login accounts is done as part of a UPAM authentication strategy. Login accounts are created in the UPAM database and are used to define network access control for users attempting to access network resources. The following group of applications are used to configure Employee and Guest accounts and are accessible by clicking on **Network Access > Accounts** under the “Configure” section of the OmniVista Terra Menu (see page 45):

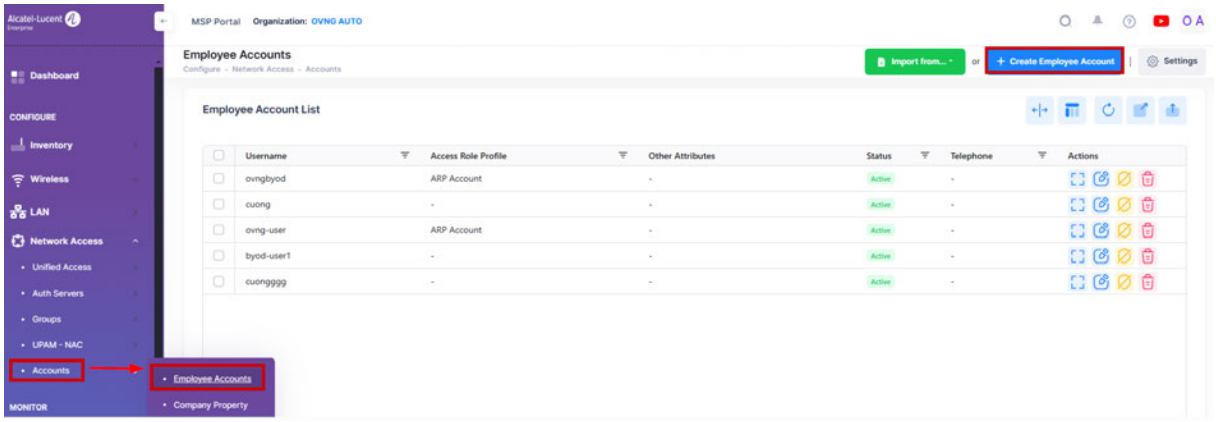
- **Employee Accounts** (see page 708) - Displays information about configured employee accounts and is used to create, edit, and delete employee accounts.
- **Company Property** (see page 716) - Displays information about devices owned by a company that can be assigned to an employee for daily use (for example, printers, IP phones, laptops, tablets), and is used to create, edit, and delete property information.
- **Guest Accounts** (see page 727) - Displays all configured Guest Accounts and is used to create, edit, and delete Guest Accounts.
- **Guest Operator** (see page 745) - Displays all configured Guest Operators and is used to create, edit, and delete a Guest Operator. A Guest Operator is a network operator who manages the guest user network access, which includes creating guest user accounts and approving guest user self-registration requests.
- **Dynamic PGPSK Configuration** (see page 750) - Displays a list of Private Group PSK profiles and a list of devices connected through PSK authentication. This application is also used to create, edit, and delete Private Group PSK profiles.
- **IMSI/IMEI Accounts** (see page 761) - Displays information about configured IMSI/IMEI accounts that are used for UPAM authentication/authorization of Celona devices.

21 Oct 2025

7.5.1 Employee Accounts

The Authentication Employee Accounts screen is used to create the login accounts for the employee users in the UPAM network. The employee accounts screen will display all configured employee accounts under the UPAM network.

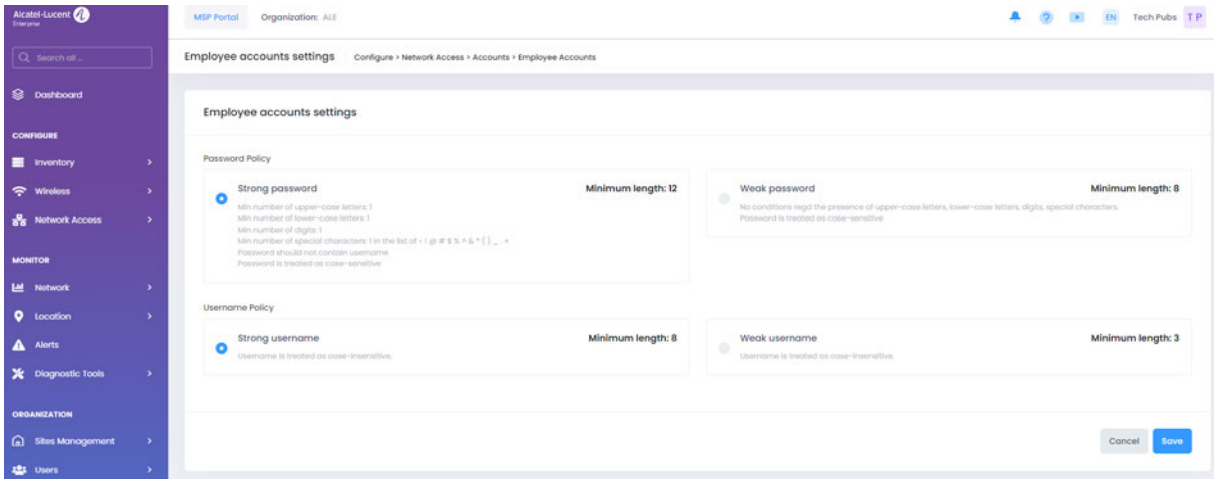
Use the Employee Account list screen to display information (see page 714) about all of the configured employee accounts in the UPAM database. This screen also allows you to create (see page 709), edit (see page 713), and delete (see page 714) accounts. To access the Employee Accounts screen, click on **Network Access > Accounts > Employee Accounts** under the “Configure” section of the OmniVista Terra Menu (see page 45).



Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.

7.5.1.1 Employee Accounts Settings

To create Employee Accounts username and password , go to **Settings** to access the Employee Account Settings screen as shown below.



9 **Employee Accounts Settings**

- **Password Policy** - Select the password policy to enforce when the user logins in.
  - **Strong Password** - Minimum password length is 12 with the following required guidelines:

- Min number of upper-case letters: 1
- Min number of lower-case letters: 1
- Min number of digits: 1
- Min number of special characters: 1 in the list of ~ ! @ # $ % ^ & * ( ) _ . +
- Password should not contain username
- Password is treated as case-sensitive

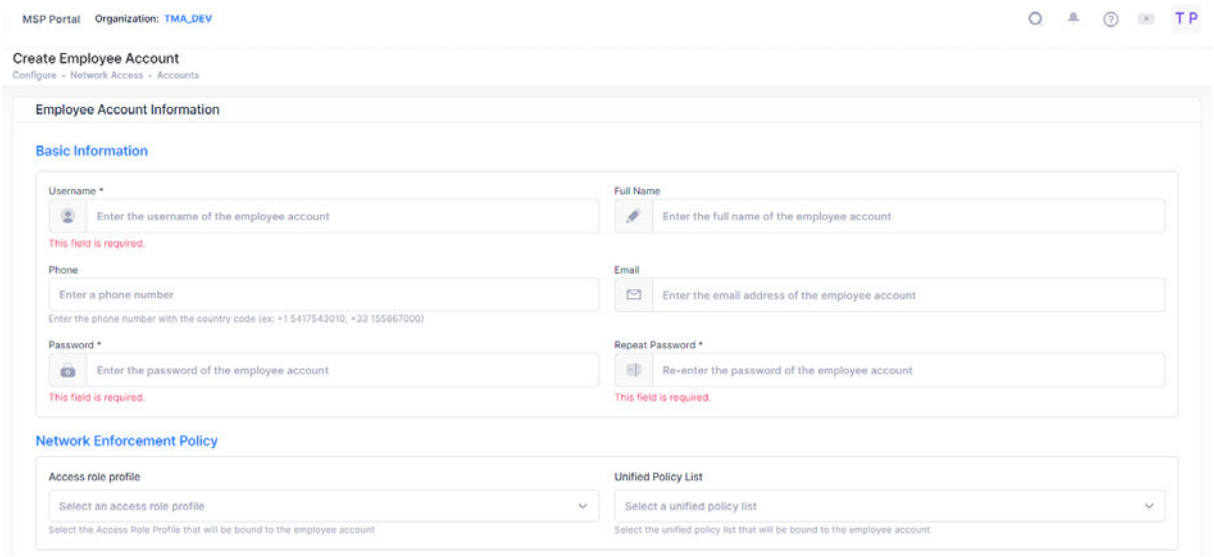
- **Weak Password** - Minimum password length is 8 with no required guidelines. Password is case-sensitive.

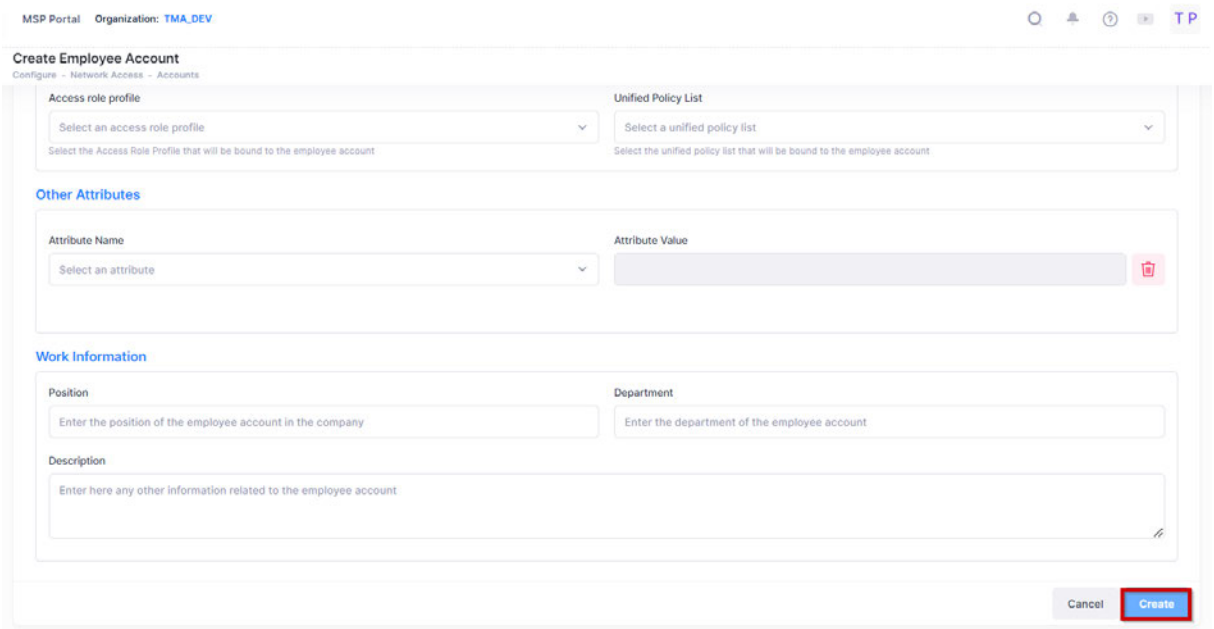
- **Username Policy** - Select the username policy to enforce when the user logins in.
  - **Strong Username** - Minimum username length is 8 characters. Username is case insensitive.
  - **Weak Username** - Minimum username length is 3 characters. Username is case insensitive.

7.5.1.2 Creating an Employee Account

There are three methods for creating an Employee Account for an UPAM Network: Import an Excel XLSX file (see page 711), Import a CSV file (see page 712) or manually create an Employee Account.

To create a new employee account, click on the add icon to display the **Create Employee Account** screen. The Create Employee Account screen opens as shown below.





Complete the following fields as described:

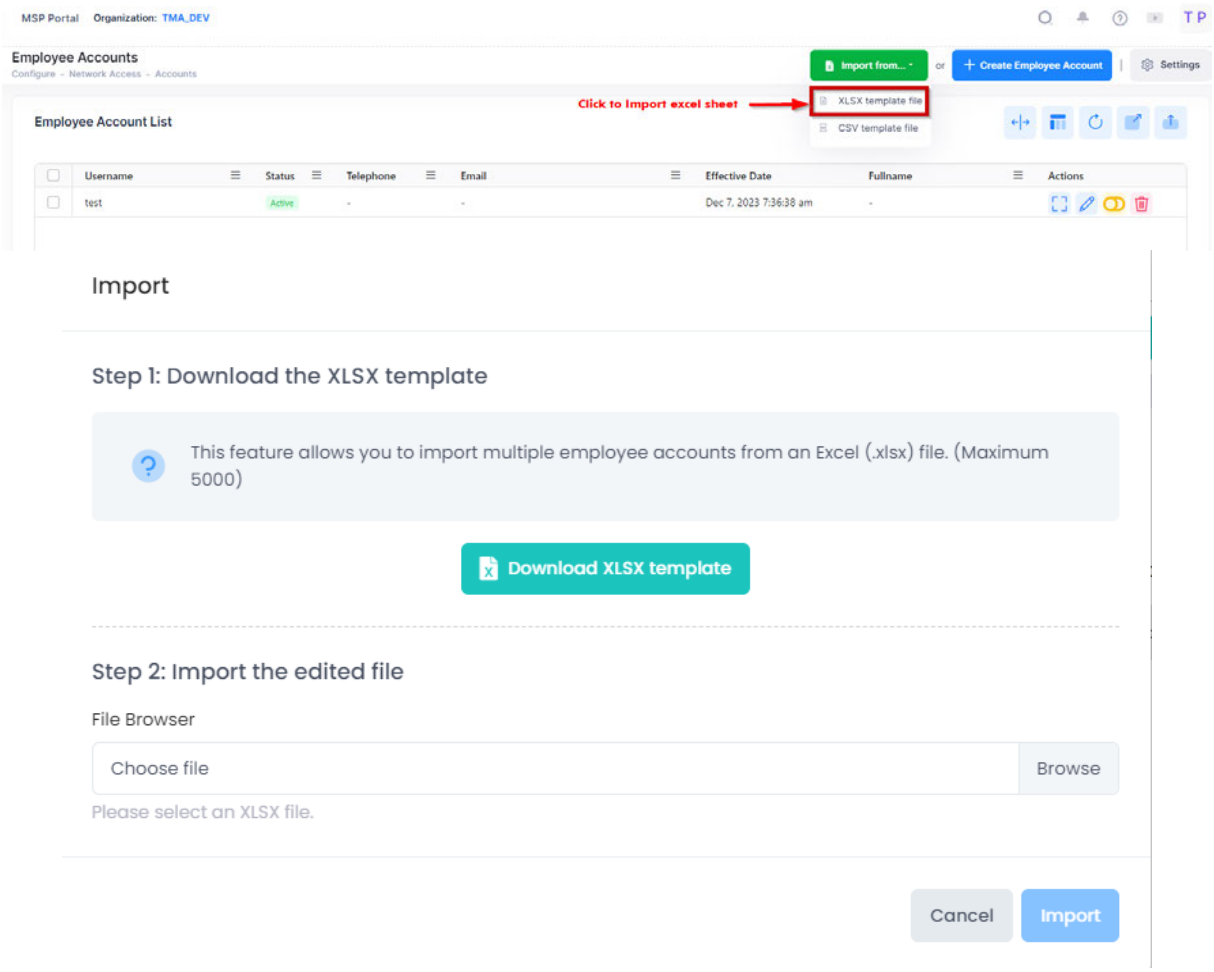
- **Username**: Username for the employee account.
- **Full Name**: Full Name of the employee.
- **Password**: Password for the employee account.
- **Repeat Password**: Re-enter to confirm the employee password.
- **Telephone**: Telephone number of the employee. (optional).
- **E-mail**: E-mail address of the employee. (optional).
- **Access Role Profile**: Access Role Profile that is bound to the employee account.
- **Unified Policy List**: Policy List that is bound to employee account.
- **Attribute Name**: Select an attribute from the drop-down list, enter a value and click on the Add icon to add the attribute. Repeat the process to add the additional attributes.
  - **Session Timeout**: The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt.
  - **Accounting Interim Interval**: Interval for RADIUS accounting, in seconds.
  - **WISPr Bandwidth Max Up**: The user upstream bandwidth in Kbit/s.
  - **WISPr Bandwidth Max Down**: The user downstream bandwidth in Kbit/s.
  - **Tunnel Private Group ID** - The Tunnel Private Group ID is used to determine the UNP for the device, if applicable. It is a RADIUS attribute that indicates the group ID for a particular tunnel session. It may be included in the Access-request packet if the tunnel initiator can pre-determine the group resulting from a particular connection, and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. In most cases, L2 VLAN domain is a private group, and the Tunnel Group ID is pointing to the VLAN ID. (Range= 1-4094).
- **Attribute Value:** The user downstream bandwidth in kbit/s. By default, it is set to 0.
- **Department**: Department of the employee.

- **Position**: Employee Position in the organization.
- **Description**: Description of employee account.

After you have finished with the field values, click on the **Create** button to create the account.

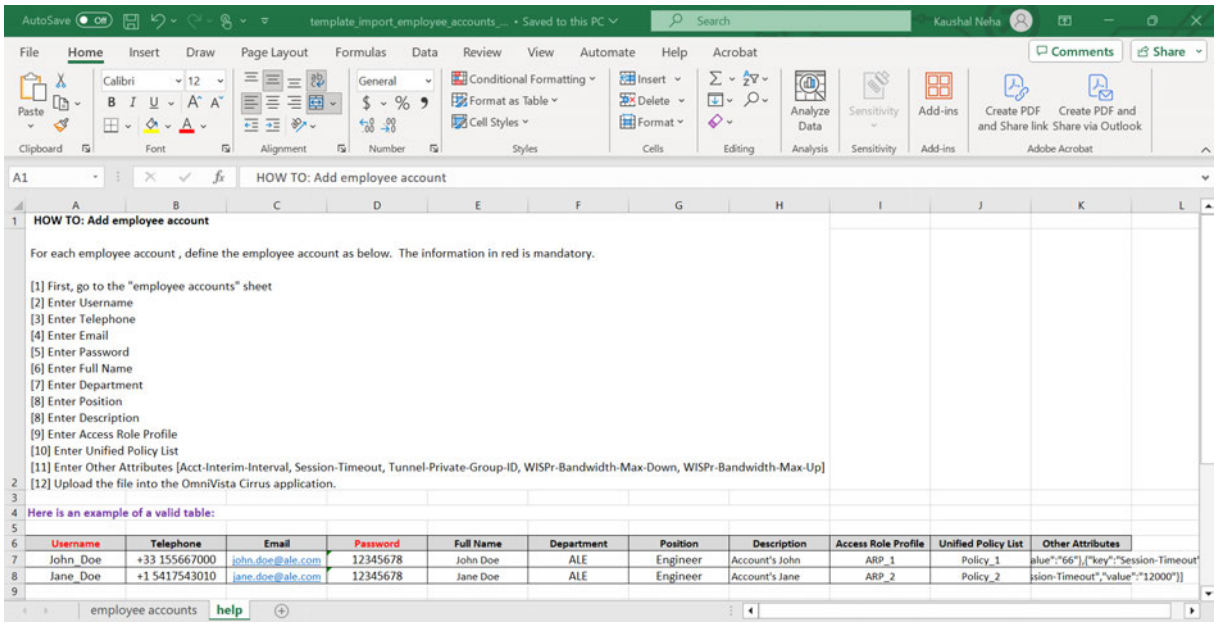
7.5.1.3 Import the Employee Accounts from an Excel Sheet

To import multiple employee accounts from an existing Excel sheet (.xlxs), click on **Import from…** and select **XLSX template file**. You will then be prompted to download an XLSX template file that contains steps on how to define the employee account in the Excel file to create multiple accounts.



Step 1: Click on **Download XLSX template** and specify where you would like to save the template file. When you open the template file, instructions are provided about how to define the employee account to be added.

The following sample template file is an example of the template provided for add employee account.



Fill out the template with information for each employee account that is to be imported.

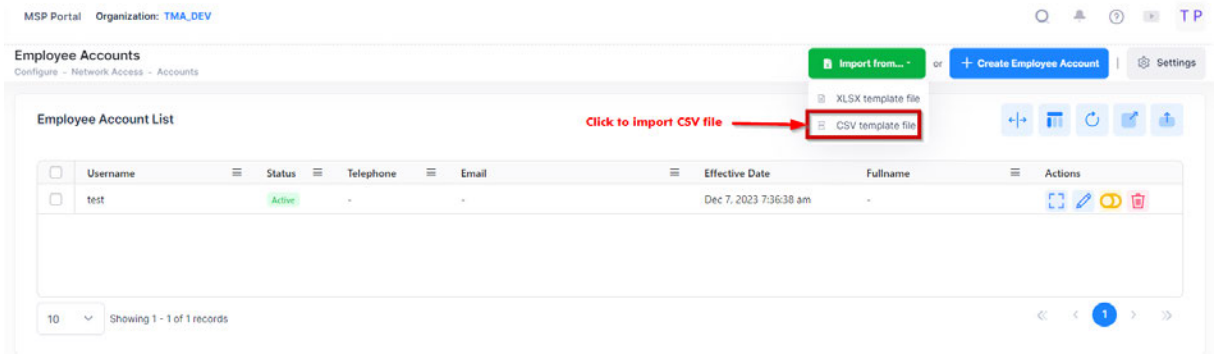
Step 2: Import the edited file and select the site of attachment

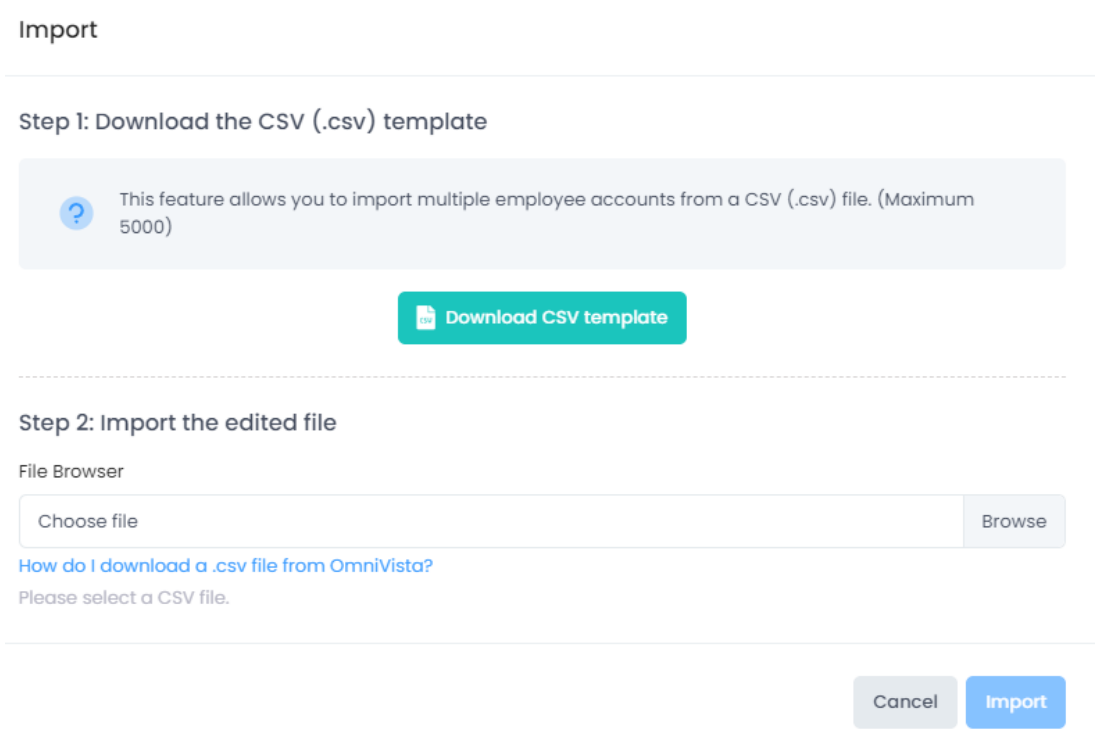
- **File Browser** - Click in this field to find and select the existing template file to import.

Once the Import form is complete, click on **Import**. The Employee Account list is populated with the imported Employee Accounts.

7.5.1.4 Import the Employee Accounts from CSV File

To import multiple employee accounts from an existing .csv file, click on **Import from…** and select **CSV template file**. You will then be prompted to download the CSV template file that contains steps on how to define the employee account from a csv file to create multiple accounts.





Step 1: Download the CSV template file and add employee account information based on the template instructions.

Step 2: Import the edited file and select the site of attachment

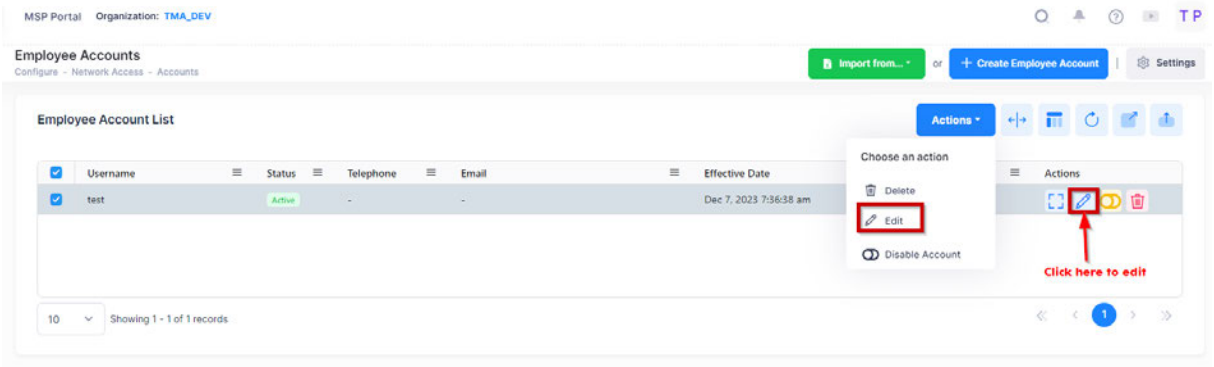
Complete the following fields as described to select and upload the CSV file.

- **File Browser** - Click in this field to find and select the existing CSV file to import.

Click on **Import**. The employee account list is populated with the imported employee accounts.

7.5.1.5 Editing an Employee Account

The Employee account can be edited by using the Actions menu from the Employee Account List home page.
Select an Employee from the Employee Account List and click on **Actions** to open the Actions menu.
Select “Edit” option to edit the account.

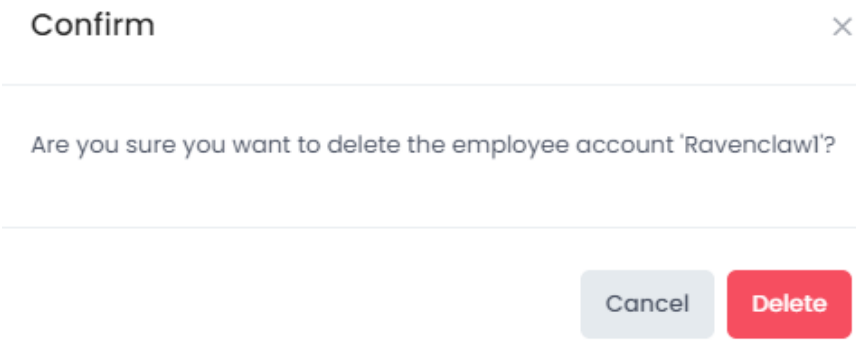


10 **Edit the Employee Account**

The edit Employee Account screen appears and edit the fields as described above to make any changes. Then click on the **Save** button to save the changes. Note that you cannot edit an username.

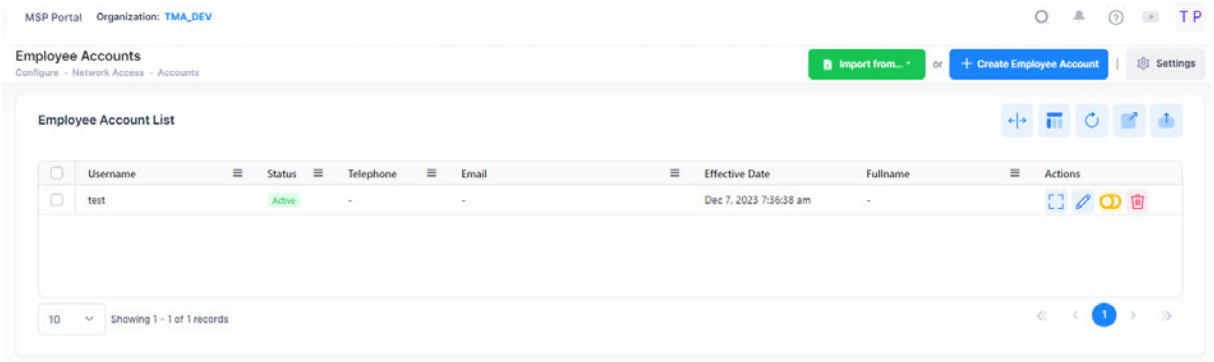
7.5.1.6 Deleting an Employee Account

Select an Employee from the Employee Account list and click on the Delete icon under the “Actions” column or click on the **Actions** button and select Delete from the drop-down menu. When the following confirmation prompt appears, click on **Delete** to delete the Employee Account.



7.5.1.7 Display Employee Account

The Employee Account list displays information for the all configured Employee Accounts. To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



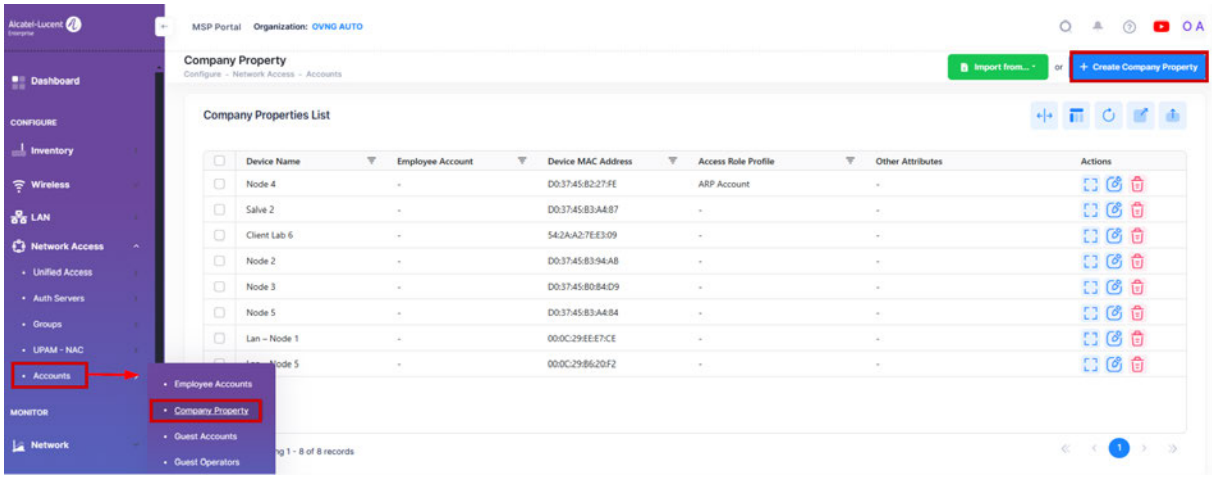
- **Username -** User name for the employee account.
- **Telephone -** Optional telephone number of the employee.
- **Email -** Optional Email address of the employee.
- **Effective Date -** The date and time the account was created.
- **Full Name -** Full name of the employee.
- **Department -** Department of the employee.
- **Position -** Employee position in the company.
- **Description -** Description of the employee account.
- **Access Role Profile -** Access Role Profile that is bound to the employee account. It is prior to the Access Role Profile configured in Authentication Strategy.
- **Policy List -** Policy List that is bound to the employee account. It is prior to the Policy List configured in an Authentication Strategy.
- **Status -** The administrative status of the account (Enable/Disable).

21 Oct 2025

7.5.2 Company Property

The Authentication Company Property Screen displays (see page 725) information about devices owned by a company that can be assigned to an employee for daily use (for example, printers, IP phones, laptops, tablets), and is used to create (see page 716), edit (see page 722), and delete (see page 723) property information.

To access the Company Property screen, click on **Network Access > Accounts > Company Property** under the “Configure” section of the OmniVista Terra Menu (see page 45).



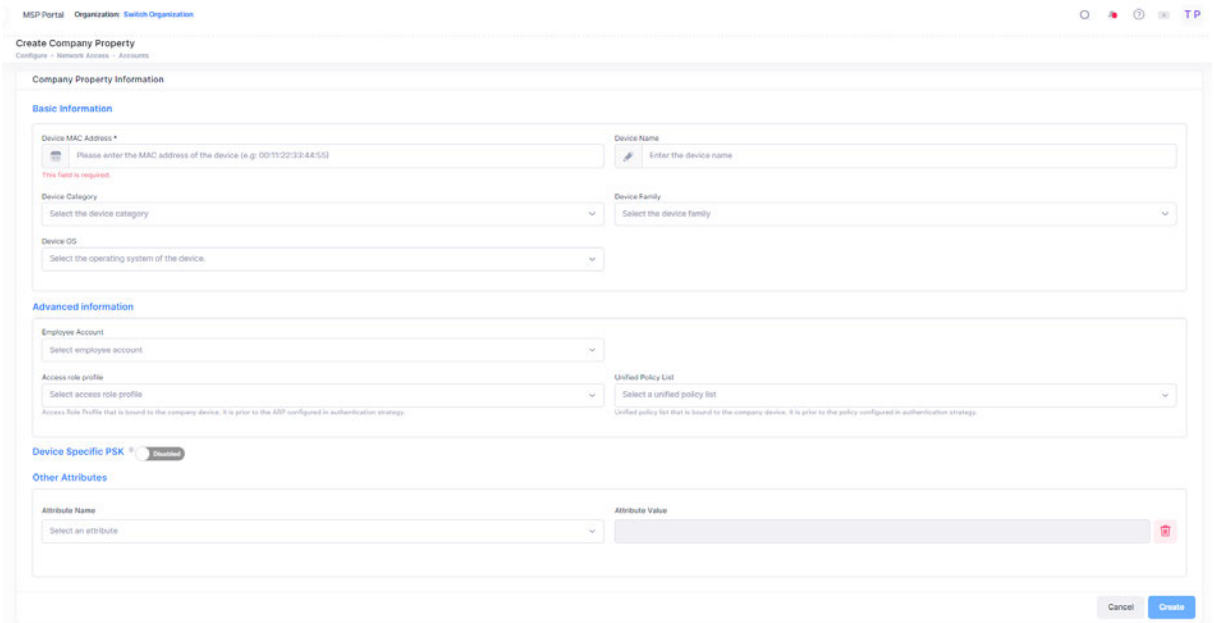
Data displayed in the Company Properties List can be exported into a CSV, PDF or Excel sheet format. You can also display the list in full-screen mode for a better display.

7.5.2.1 Creating a Company Property List Entry

There are three methods for creating a Company Property List entry for a UPAM network: Import an Excel XLSX file (see page 719), Import a CSV file (see page 721) or manually add (see page 716) a Company Property.

7.5.2.1.1 Manually Add Company Property

To manually add a new Company Property List entry, click on **Create Company Property** to display the Create Company Property screen.



Complete the following fields as described:

Basic Information

- **Device MAC Address -** MAC address of the company device.
- **Device Name -** System name of the company device.
- **Device Category -** Category of the company device:
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver
  - Others
- **Device Family -** Production vendor of the company device:
  - Alcatel-Lucent Enterprise
  - Apple
  - Samsung
  - Huawei
  - Microsoft
  - LG
  - Lenovo
  - HP
  - IBM
  - Nokia
  - MI
  - HTC

  - Sony
  - Blackberry
  - Others
- **Device OS -** Operating system of the company device:
  - Linux
  - Windows
  - MacOS
  - Android
  - IOS
  - Others

Advanced Information

- **Employee Account -** The employee account to which the company device is associated.
- **Access Role Profile -** Access Role Profile that is bound to the company device. It is prior to the ARP configured in authentication strategy.
- **Unified Policy List -** Policy List that is bound to the company device.

Device Specific PSK

- **Device Specific PSK -** Enables/Disables Device Specific PSK. Device Specific PSK provides more security than traditional PSK. If Device Specific PSK is enabled on a wireless network and Device Specific PSK is enabled for the device, when the AAA Server sends the RADIUS Access-Accept for MAC Authentication for the device, it will also send the specific pre-shared key for that device, differentiated by the device's MAC Address. This means that each device will have a different key. When Device Specific PSK is enabled for the company property device, complete the following fields:
  - **Passphrase -** The Device Specific Passphrase.
  - **Passphrase Retype-** Re-enter the Passphrase.
  - **Generate Random Passphrase** - Click on this option to automatically generate a passphrase for the device. The passphrase will be entered in the Device Specific Passphrase fields.
  - **Passphrase Validity Period -** Select the duration for the Device Specific Passphrase (**Always Valid** or **Custom** - configure a specific date and time for the validity period to expire).

Other Attributes

- **Attribute Name -** Select an attribute name from the drop-down menu list.
  - **Session Timeout -** The Session Timeout Interval is the maximum number of consecutive seconds of connection allowed to the user before termination of the session or prompt. If not configured, the device’s default session timeout policy will take effect. (Range = 12000 - 86400, Default =43200)
  - **Accounting Interim Interval -** Interval for RADIUS accounting, in seconds. If not configured, the device’s default accounting policy will take effect. (Range = 60 - 1200, Default = 600)

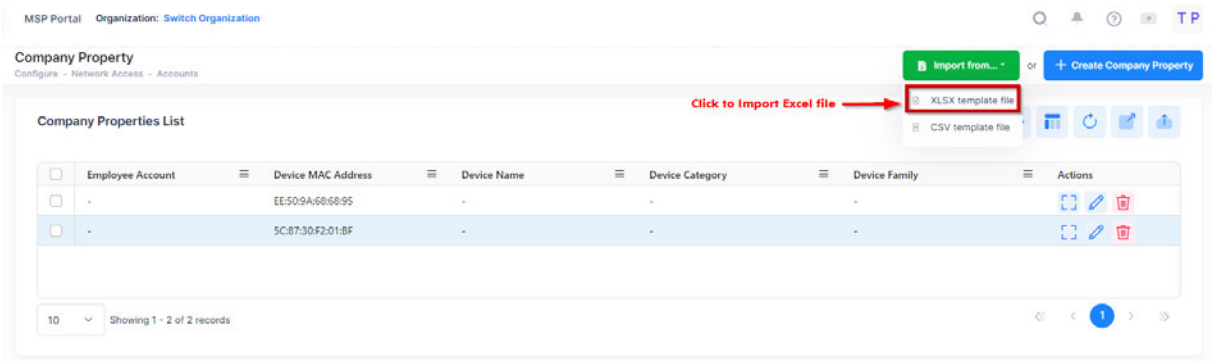
- **WISPr Bandwidth Max Up -** The user upstream bandwidth, in kbit/s. By default, it is not limited.
- **WISPr Bandwidth Max Down -** The user downstream bandwidth, in kbit/s. By default, it is not limited.
- **Tunnel Private Group ID** - The Tunnel Private Group ID is used to determine the UNP for the device, if applicable. It is a RADIUS attribute that indicates the group ID for a particular tunnel session. It may be included in the Access-request packet if the tunnel initiator can pre-determine the group resulting from a particular connection, and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. In most cases, L2 VLAN domain is a private group, and the Tunnel Group ID is pointing to the VLAN ID. (Range= 1-4094).

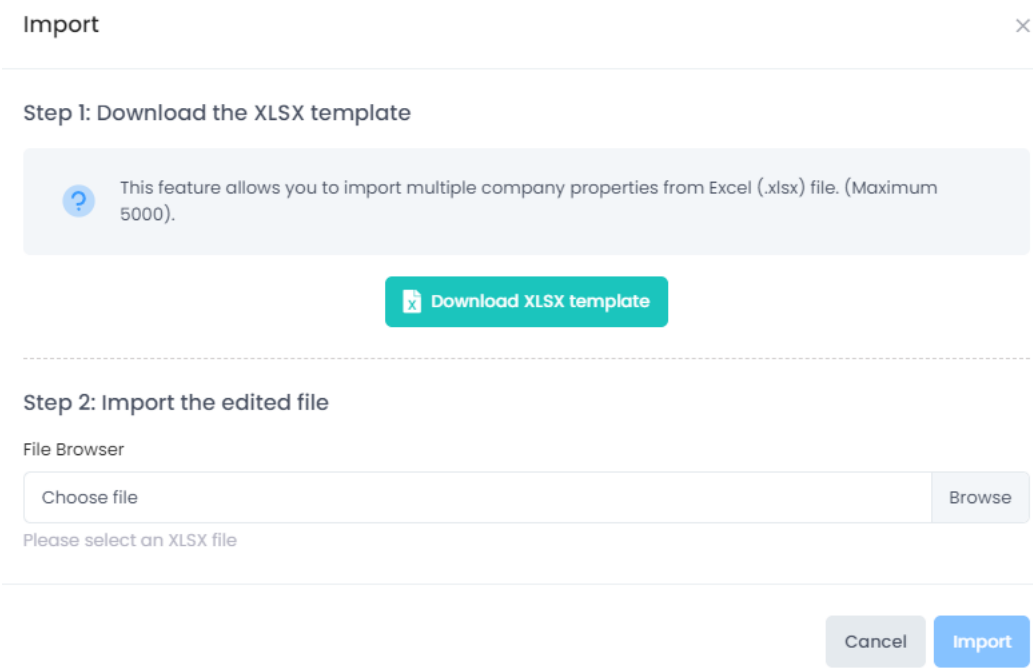
- **Attribute Value** - Enter the value required for the selected Attribute Name.

After you have finished completing the field values, click on **Create** to add a device.

7.5.2.1.2 Import Company Property from an Excel Sheet

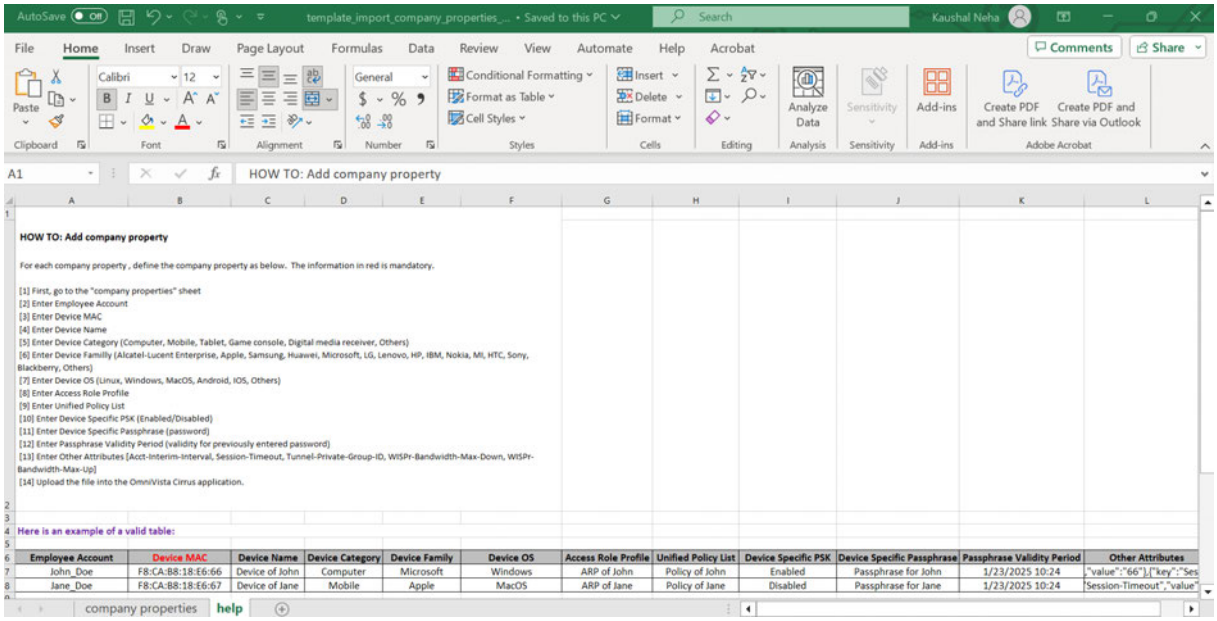
To import multiple company properties from an existing Excel sheet (.xlxs), click on **Import from…** and select **XLSX template file**. You will then be prompted to download an XLSX template file that contains steps on how to add the company property in the Excel file to create multiple company properties .





Step 1: Click on **Download XLSX template** and specify where you would like to save the template file. When you open the template file, instructions are provided about how to define the company property to be added.

The following sample template file is an example of the template provided for add company property.



Fill out the template with information for each company property that is to be imported.

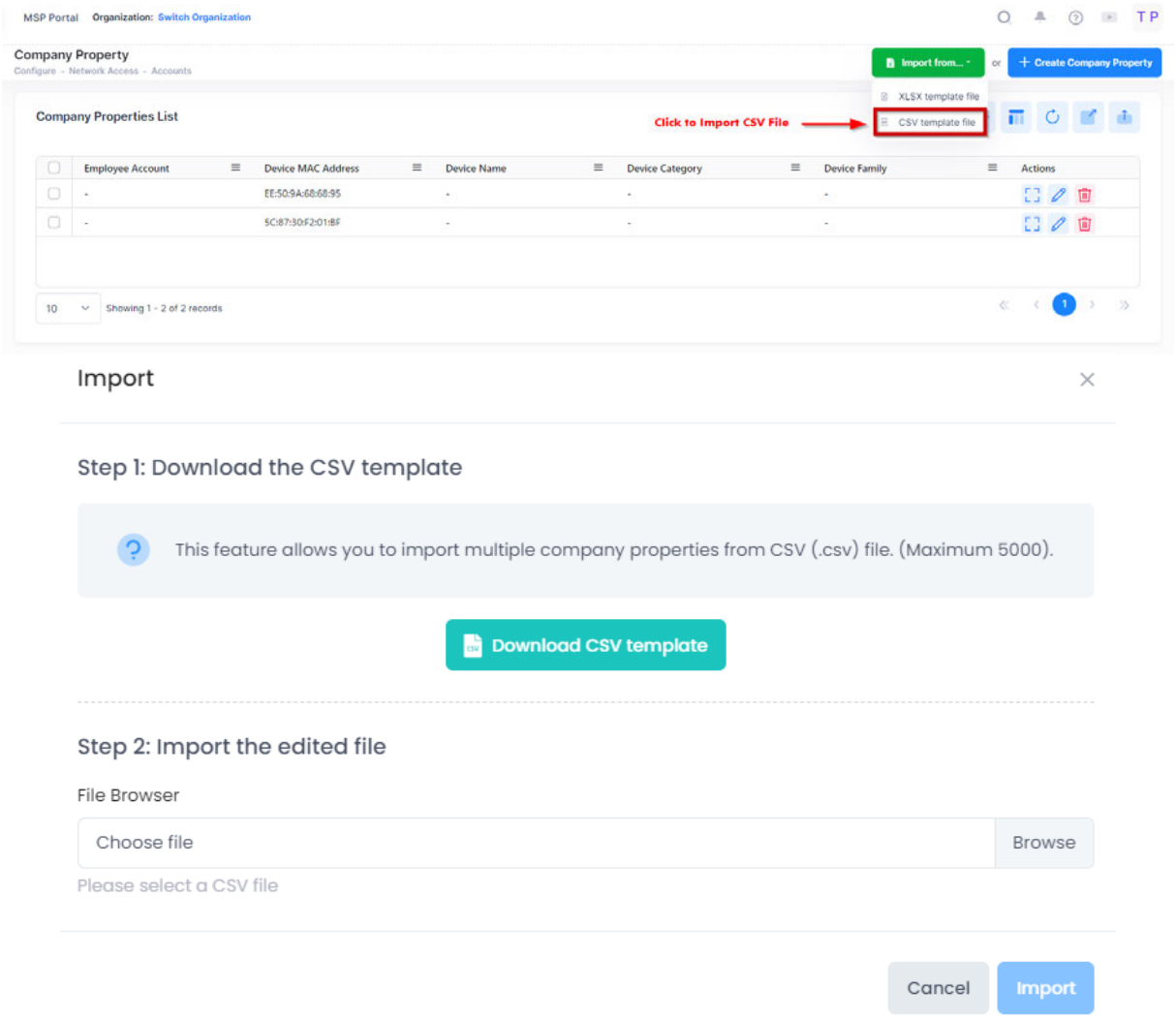
Step 2: Import the edited file and select the site of attachment

- **File Browser** - Click in this field to find and select the existing template file to import.

Once the Import form is complete, click on **Import**. The Company Property list is populated with the imported Company Properties.

7.5.2.1.3 Import the Company Property from CSV File

To import multiple company properties from an existing .csv file, click on **Import from…** and select **CSV template file**. You will then be prompted to download the CSV template file that contains steps on how to define the company property from a csv file to create multiple company properties.



Step 1: Download the CSV template file and add company property information based on the template instructions.

Step 2: Import the edited file and select the site of attachment

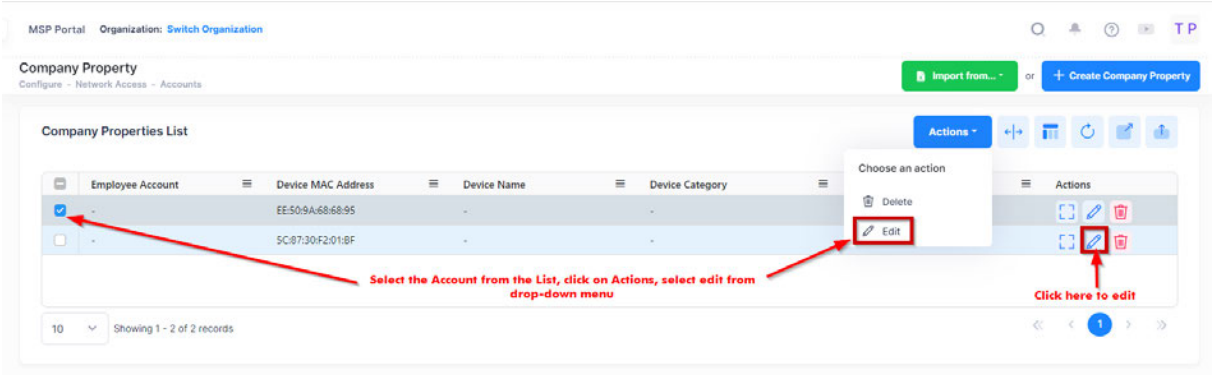
Complete the following fields as described to select and upload the CSV file.

- **File Browser** - Click in this field to find and select the existing CSV file to import.

Click on **Import**. The company property list is populated with the imported company properties.

7.5.2.2 Editing a Company Property Entry

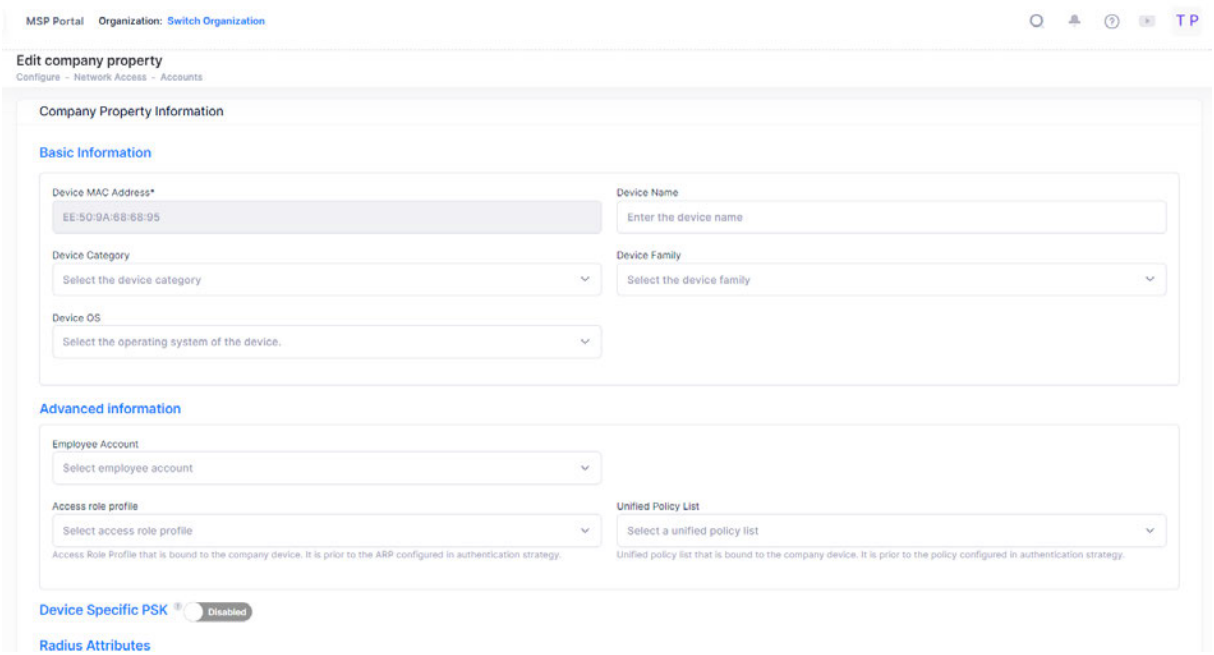
You can edit the parameter values for a Company Property entry by accessing the Edit Company Property screen.



Use one of the following methods to access the Edit Company Property screen (as shown above):

- Select the Company Property to edit by clicking on the checkbox next to the Employee Account, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the Company Property that you want to edit.

The following Edit Company Property screen displays. Edit the fields as described above (see page 483), then click on **Save**.

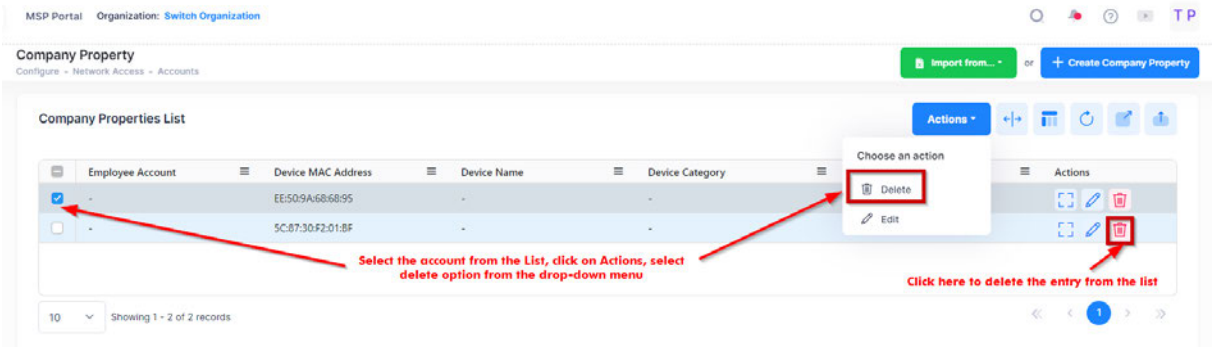


Note that you cannot edit the Device MAC address.

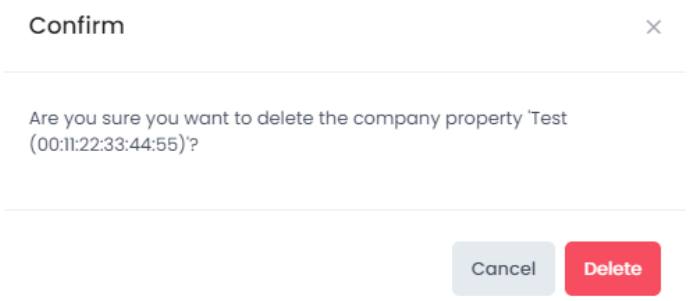
7.5.2.3 Deleting a Company Property Entry

To delete a Company Property Entry, use one of the following methods to select the Company Property you want to delete:

- Select a Company Property to delete by clicking on the checkbox next to the Employee Account, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash icon under the “Actions” column next to the Company Property Entry that you want to delete.



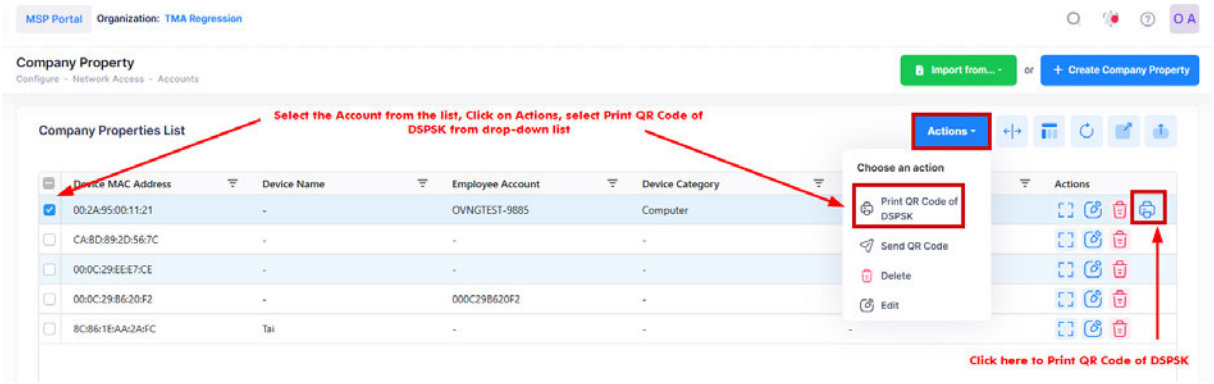
When you select the Company Property Entry you want to delete, the following confirmation prompt appears:



Click on **Delete** to confirm that you want to delete the Company Property Entry.

7.5.2.4 Print QR Code of DSPSK of a Company Property Entry

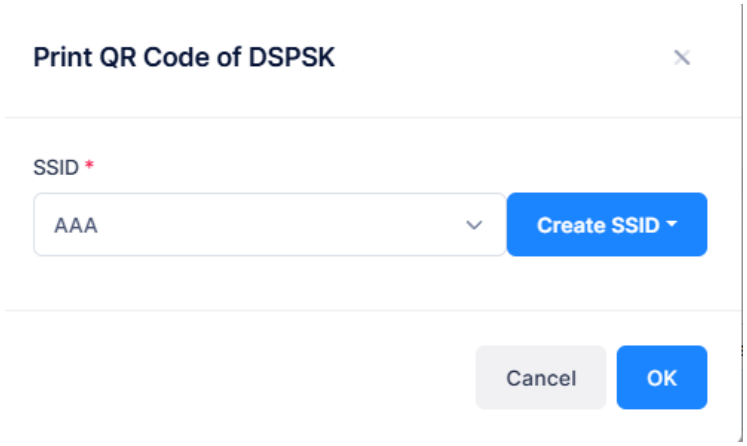
You can Print QR Code of DSPSK for a Company Property entry by accessing the Print QR Code of DSPSK screen.



Use one of the following methods to access the Print QR Code of DSPSK screen (as shown above):

- Select the Company Property by clicking on the checkbox next to the Device MAC Address, click on **Actions**, then select **Print QR Code of DSPSK** from the drop-down menu.
- Click on the print icon under the “Actions” column next to the Company Property that you want to Print QR Code of DSPSK.

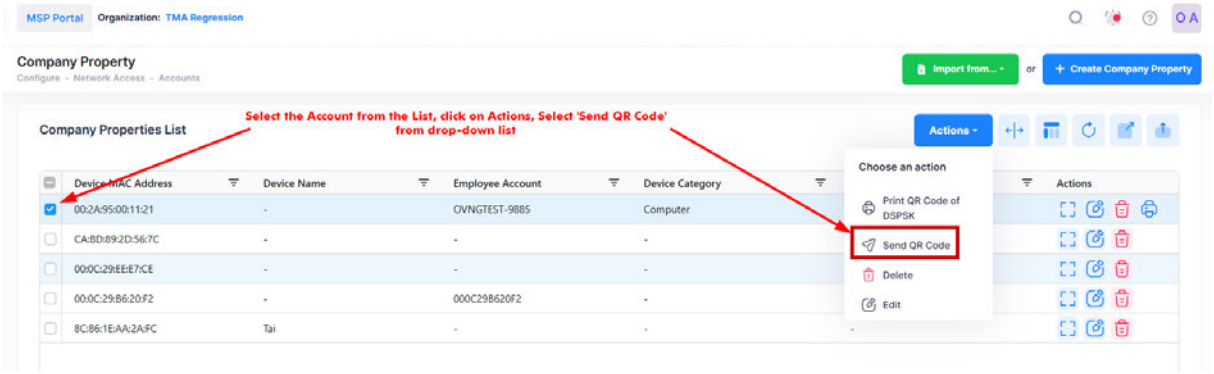
The following screen appears. Enter the SSID from the drop-down list or click on **Create SSID** button, which launch the Create SSID screen in a new tab and you can create a new SSID profile from that screen, then click on **OK** to save the changes.



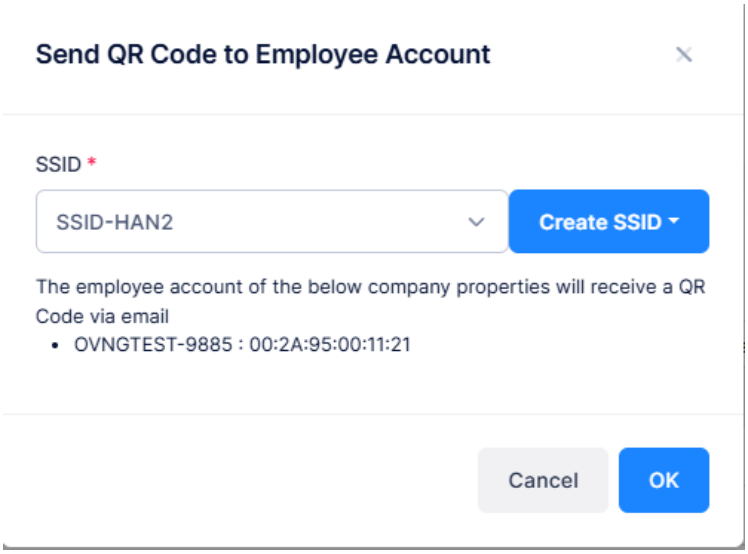
7.5.2.5 Send QR Code of a Company Property Entry to Employee Account

You can send the QR Code for a Company Property entry to an Employee Account by accessing the Send QR Code screen.

Select a Company Property entry from the List and click on **Actions** to open the Actions menu, Select “Send QR Code” option from the drop-down menu.

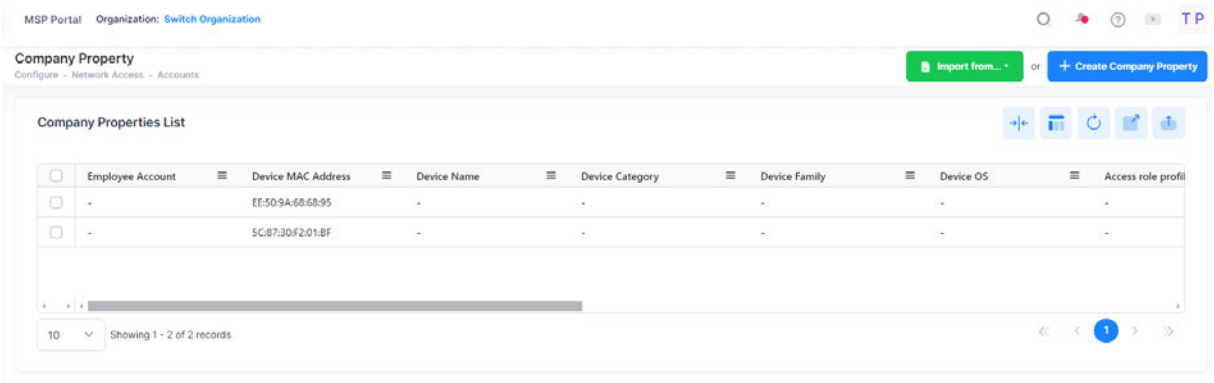


The following screen appears. Enter the SSID from the drop-down list or click on **Create SSID** button, which launch the Create SSID screen in a new tab and you can create a new SSID profile from that screen. The employee account of the selected company properties will receive a QR code by the email. You can click on **OK** to save the changes.



7.5.2.6 Display Company Property List

The Company Property List displays information about company property that can be assigned to employees. To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column.



For each of the configured Company Property entry for an employee, the following attributes values are displayed:

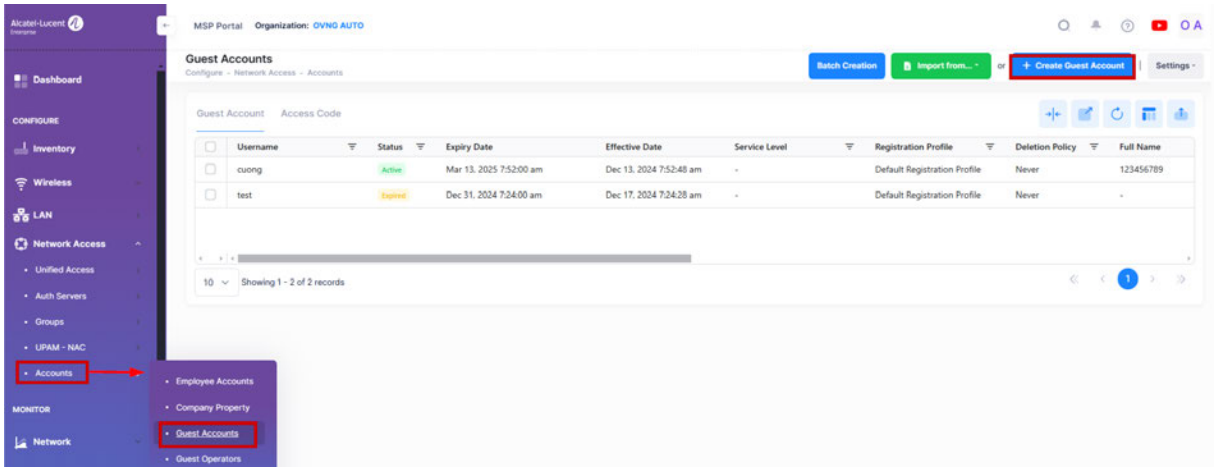
- **Employee Account -** The employee account to which the company device is associated.
- **Device MAC Address -** The MAC address of the company device.
- **Device Name -** The system name of the company device.
- **Device Category -** The category of the company device (e.g., Computer, Mobile Tablet).
- **Device Family -** The Production vendor of the company device (e.g., Alcatel Lucent Enterprise, Apple IBM).
- **Device OS -** The operating system of the company device (e.g., Linux, Windows, IOS).
- **Device Specific PSK -** The administrative status of Device Specific PSK for the device (Enabled/ Disabled).
- **Status -** The operational status of the device (Online/Offline).
- **Access Role Profile -** Access Role Profile that is bound to the company device. It is prior to the ARP configured in authentication strategy.
- **Policy Name -** Policy Name that is bound to the company device.
- **Passphrase Validity Period -** The duration for the Device Specific Passphrase (**Always Valid** or a specific date and time for the validity period to expire).
- **Created At -** The date and time of the creation of the company property account.
- **Other Attributes -** The attribute name (Session Timeout/ Accounting Interim Interval/WISPr Bandwidth Max Up/ WISPr Bandwidth Max Down) and attribute value in Kbit/s (default value is set to 0).

21 Oct 2025

7.5.3 Guest Accounts

The Guest Accounts screen is used to create the login accounts for the Guest users in the UPAM network. The Guest accounts screen will display all configured Guest accounts under the UPAM network. If self-registration is not enabled, you can manually create a login account for a Guest User and relay the information to the Guest User.

Use the Guest Account list screen to display information (see page 743) about all of the configured Guest accounts in the UPAM database. This screen also allows you to create (see page 727), edit (see page 739), delete (see page 740), extend (see page 740), enable (see page 741) and disable (see page 742) accounts. To access the Guest Accounts screen, click on **Network Access > Accounts > Guest Accounts** under the "Configure" section of the OmniVista Terra Menu (see page 45).



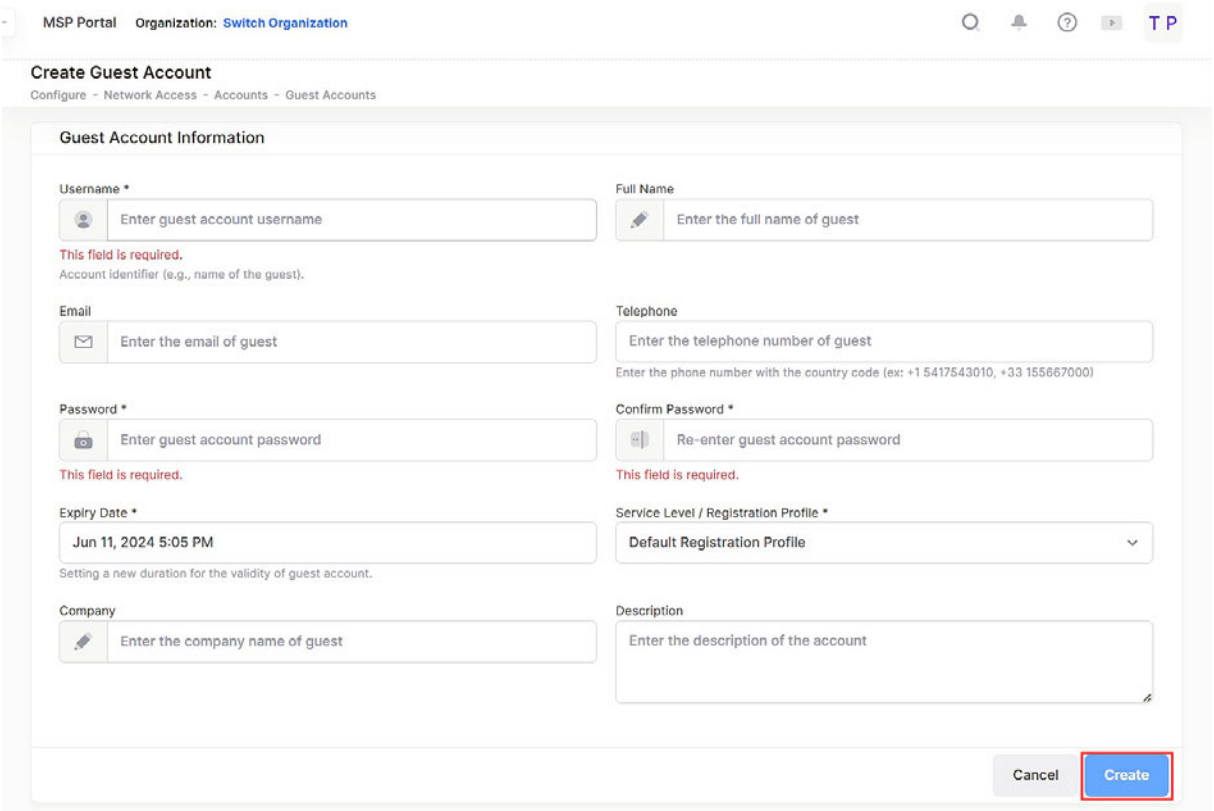
Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.

7.5.3.1 Creating a Guest Account

There are three methods for creating Guest Accounts for a UPAM Network: Import an Excel XLSX file (see page 728), Import a OmniVista CSV file (see page 730) or manually create (see page 727) a Guest Account.

7.5.3.1.1 Manually Create a Guest Account

To manually create a new Guest Account, click on **Create Guest Account** on the Guest Accounts List screen. The Create Guest Account screen opens as shown below.



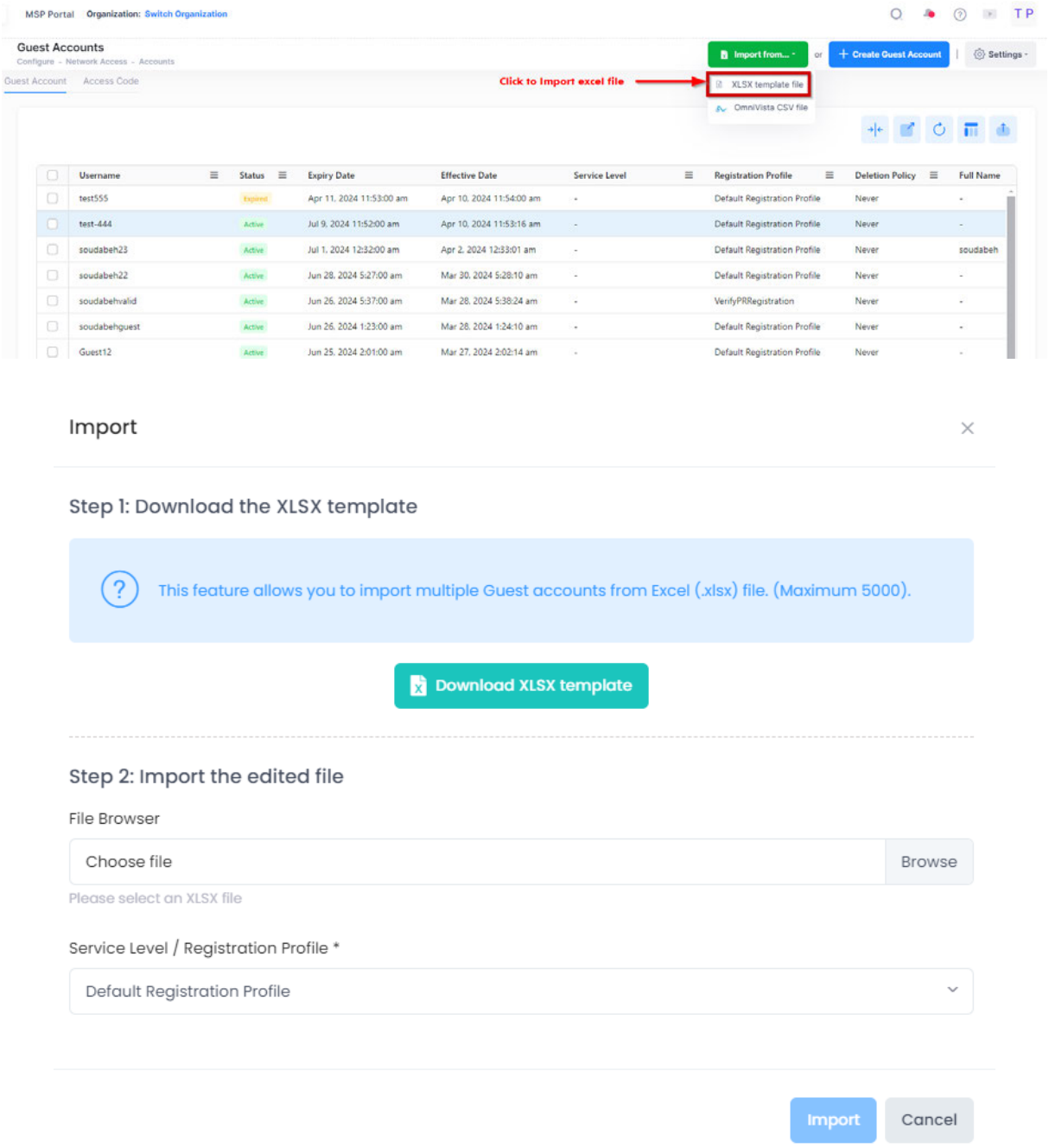
Complete the following fields as described:

- **User Name -** Account identifier (e.g., name of the guest).
- **Full Name -** Full name of the Guest User.
- **Password -** Password for the account.
- **Confirm Password -** Re-enter and confirm the Guest Account password.
- **Expiration Date -** The length of time that the Guest Account is valid.
- **Service Level/ Registration Profile -** Specify the service level or Registration Profile for the Guest Account.
- **Telephone -** Telephone number of the Guest User.
- **Email -** Email address of the Guest User.
- **Company -** Company name of the Guest User.
- **Description -** Optional description for the account.

After you have finished with the field values, click on the **Create** button to create the account.

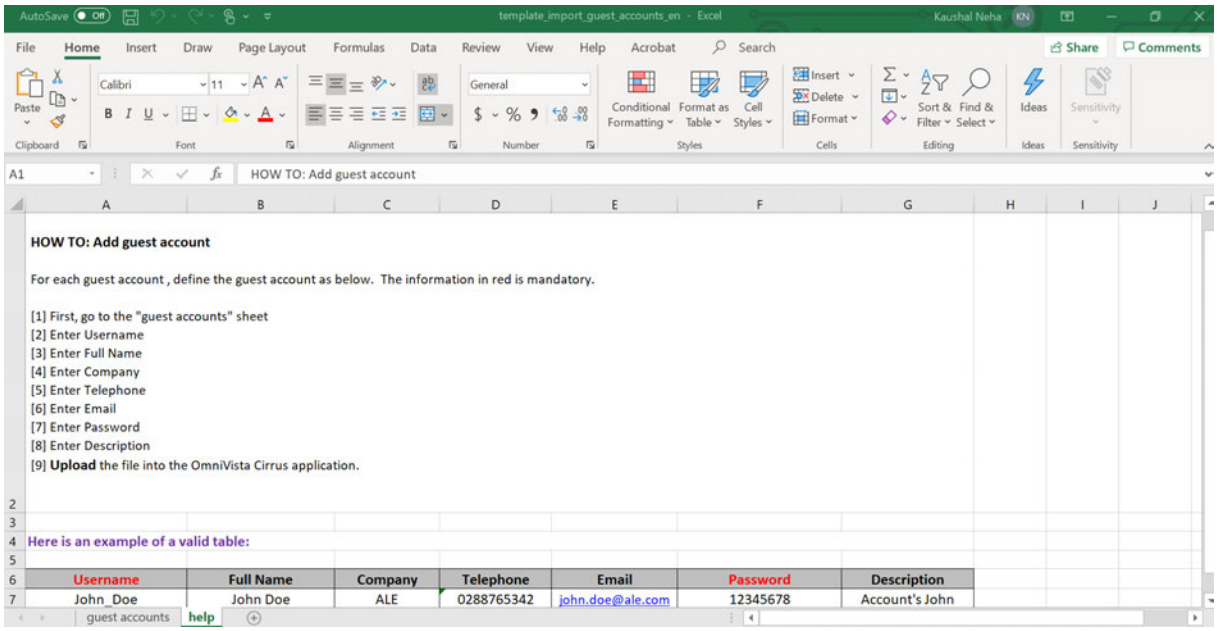
7.5.3.1.2 Import Multiple Guest Accounts from an Excel Sheet

To import multiple Guest Accounts from an existing Excel sheet (.xlxs), click on **Import from…** and select **XLSX template file**. You will then be prompted to download an XLSX template file that contains steps on how to define the Guest Accounts in the Excel file to create multiple accounts.



Step 1: Click on **Download XLSX template** and specify where you would like to save the template file. When you open the template file, instructions are provided about how to define the Guest Accounts to be added.

The following sample template file is an example of the template provided for adding Guest Accounts.



Fill out the template with information for each Guest Account that is to be imported.

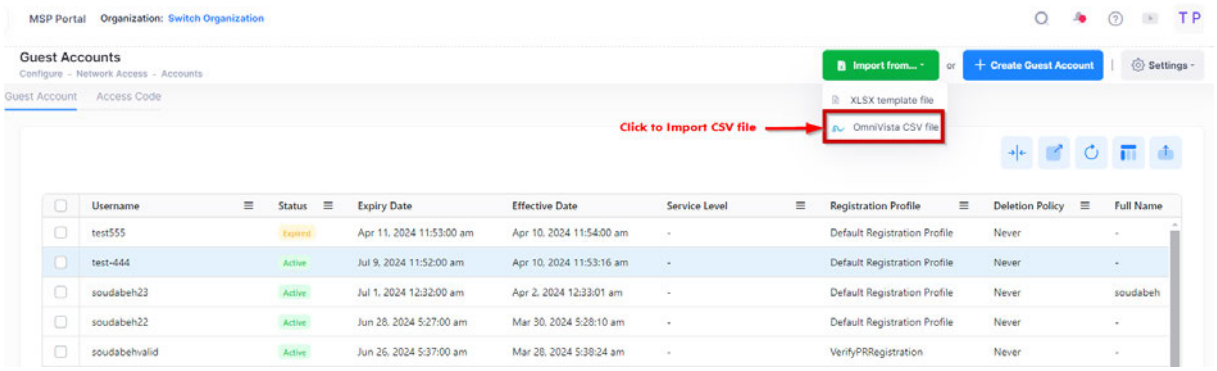
Step 2: Import the edited file and select the site of attachment

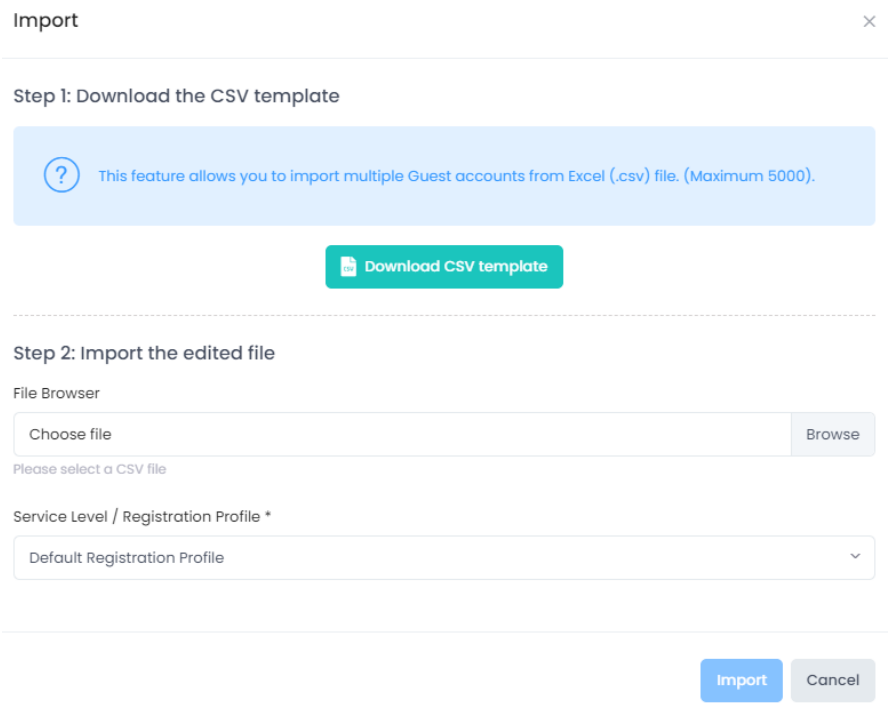
- **File Browser** - Click in this field to find and select the existing template file to import.
- **Service Level/ Registration Profile** - Select a Registration Profile or Service Level that is linked to a Registration Profile that will be assigned to each account. By default, the “Default Registration Profile” is used. See the online Service Levels help (see page 645) and the online Registration Profiles help (see page 651) for more information.

Once the Import form is complete, click on **Import**. The Guest Account List is populated with the imported Guest Accounts.

7.5.3.1.3 Import the Guest Accounts from OmniVista CSV File

To import multiple Guest Accounts from an existing .csv file, click on **Import from...** and select **OmniVista CSV file**. You will then be prompted to download the CSV template file that is used to define the Guest Account information to create multiple accounts.





Step 1: Download the CSV template

Download the CSV template file and add Guest Account information based on the template instructions.

Step 2: Import the edited file

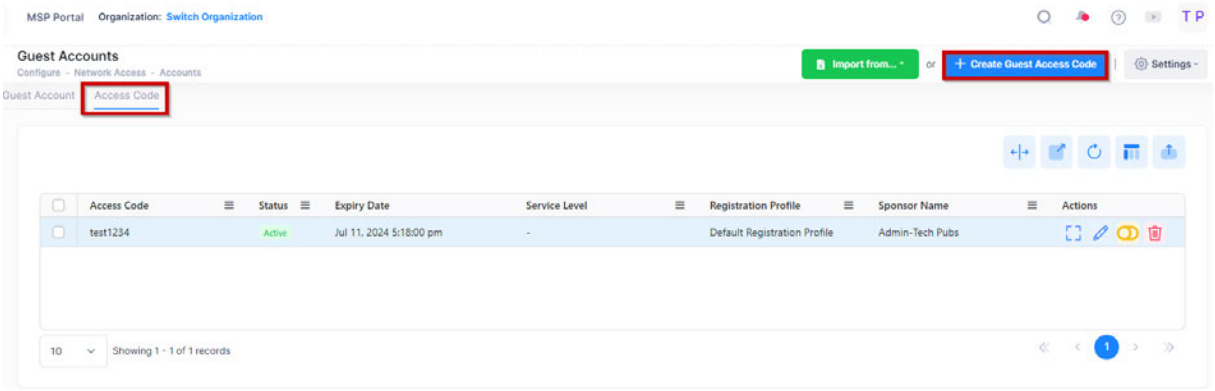
Complete the following fields as described to select and upload the CSV file.

- **File Browser** - Click in this field to find and select the existing CSV file to import.
- **Service Level/ Registration Profile** - Select a Registration Profile or Service Level that is linked to a Registration Profile that will be assigned to each account. By default, the "Default Registration Profile" is used. See the online Service Levels help (see page 645) and the online Registration Profiles help (see page 651) for more information.

Click on **Import**. The Guest Account List is populated with the imported Guest Accounts.

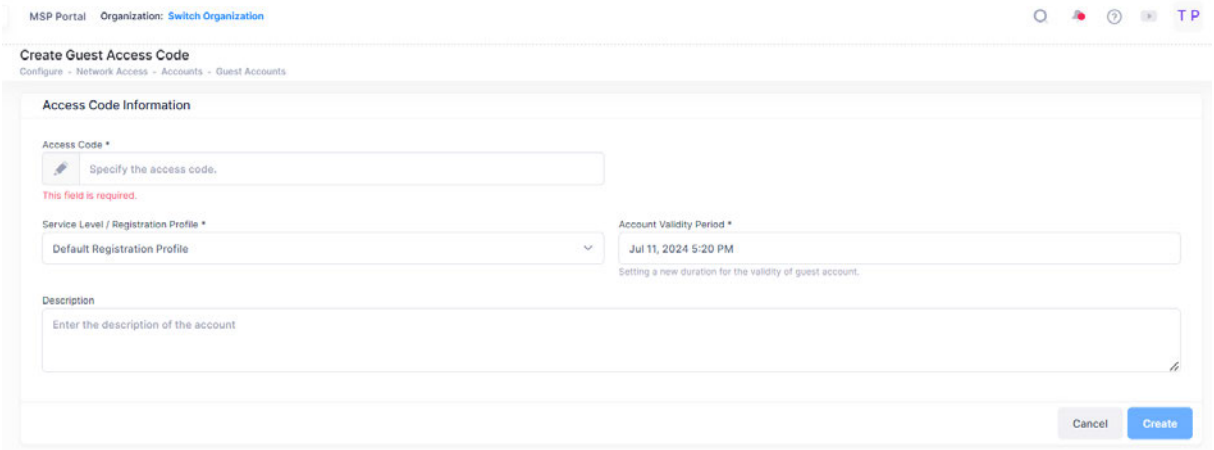
7.5.3.2 Creating a Guest Access Code Account

To create a new Guest Access Code Account, click on the "Access Code" tab on the Guest Accounts screen and click on **Create Guest Access Code** to access the Create Guest Access Code screen as shown below:



Complete the following fields as described below:

- **Access Code -** The Access Code of the Guest Account.
- **Service Level/ Registration Profile -** Specify the service level or Registration Profile for the Guest Account.
- **Account Validity Period -** Setting a new duration for the validity of Guest Account.
- **Description -** Optional description for the account.

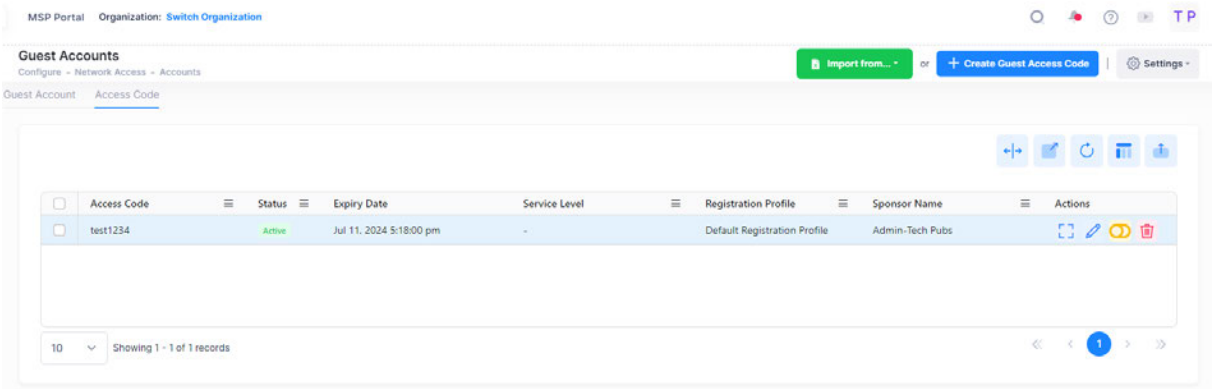


After you have finished with the field values, click on the **Create** button to create the Access Code for Guest Account.

7.5.3.3 Display Access Code List

The Guest Account Access Code list displays information for the all configured Access Code the Guest User is using to log in into the Network. To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.

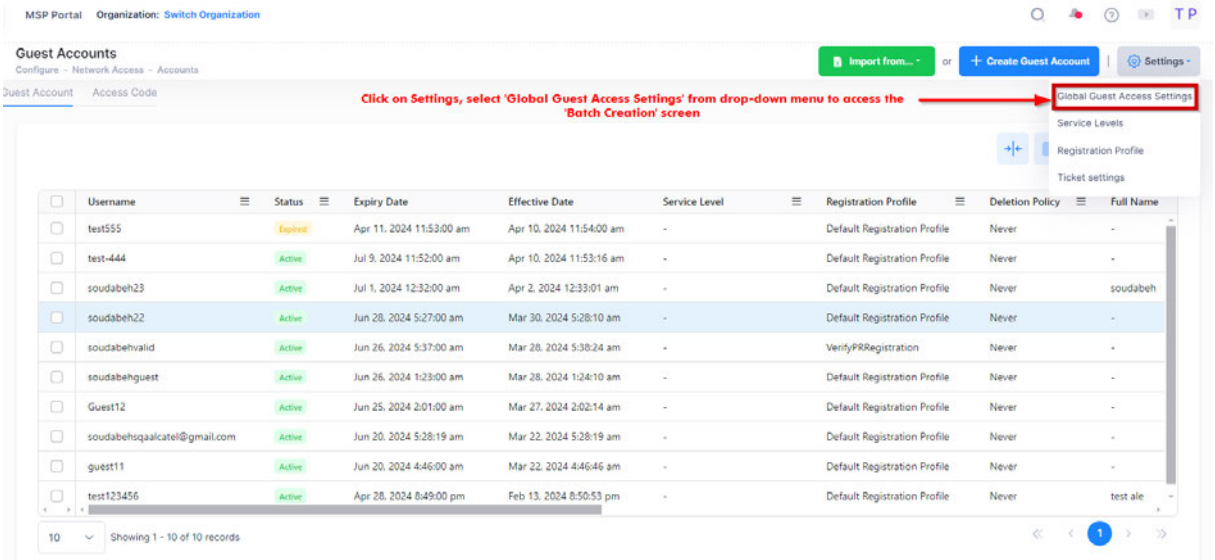


- **Access Code -** The Access Code of the Guest User.
- **Service Level -** The Service Level for the Guest Account, if configured.
- **Status -** The administrative status of the account (Enabled/Expired/Disabled).
- **Expiration Date -** The date and time the Guest Account expires.
- **Registration Profile** - The registration profile for the Guest Account.
- **Sponsor Name -** Sponsor who created the Guest Account or approved it for self-registration.
  - **Admin-XXX -** Indicates the sponsor belongs to the Administrator group; XXX indicates the account in the group.
  - **EmployeeSponsor-YYY -** Indicates the sponsor belongs to the Employee group; YYY indicates the employee account in the group.
  - **GuestSponsor-ZZZ -** Indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account in the group.
  - **SelfRegister-AAA -** Indicates no sponsor is involved and there is no need approval for the self-registration request; AAA indicates the login password is guest-user-defined (Manually) or UPAM-defined (Automatically).
- **Description -** Optional description for the account.
- **Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Account will **not** be deleted at the end of the Account Validity Period (Default).
  - **Immediately -** Guest Account will be automatically deleted at the end of the Account Validity Period.
  - **Number of Days -** Guest Account will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).
- **Effective Date -** The first time the user logs in into the Guest Account.
- **Created At -** The date and time the account was created.

7.5.3.4 Creating Multiple Guest Accounts

You can quickly create multiple Guest Accounts by clicking on the **Batch Creation** button at the top of the screen. If this button does not appear, the Batch Creation feature is not enabled. To enable this

feature, click on the **Settings** button and select **Global Guest Access Settings** from the drop-down menu.



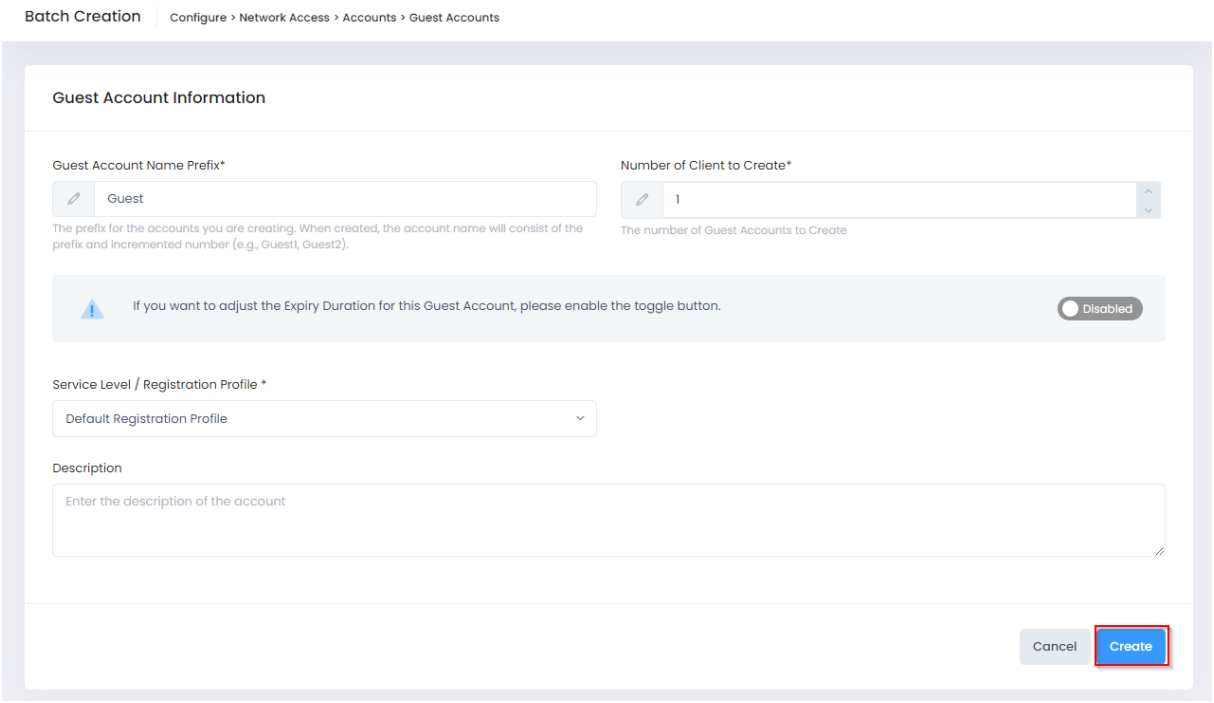
The Guest Access Settings screen opens. Refer to the Global Guest Access Settings (see page 642) online help for information about how to enable Batch Creation and configure the Registration Strategy for Guest Accounts.

Once you have enabled the Batch Creation feature, the **Batch Creation** button will appear at the top of the Guest Accounts screen.

Click on **Batch Creation** to open the Batch Account Creation screen. Based on whether the Guest Accounts List (“Account” tab) or the Access Code List (“Access Code” tab) is displayed, one of the following Batch Account Creation screens will open:

- Batch Creation for Guest Accounts (see page 734)
- Batch Creation for Access Code Guest Accounts (see page 735)

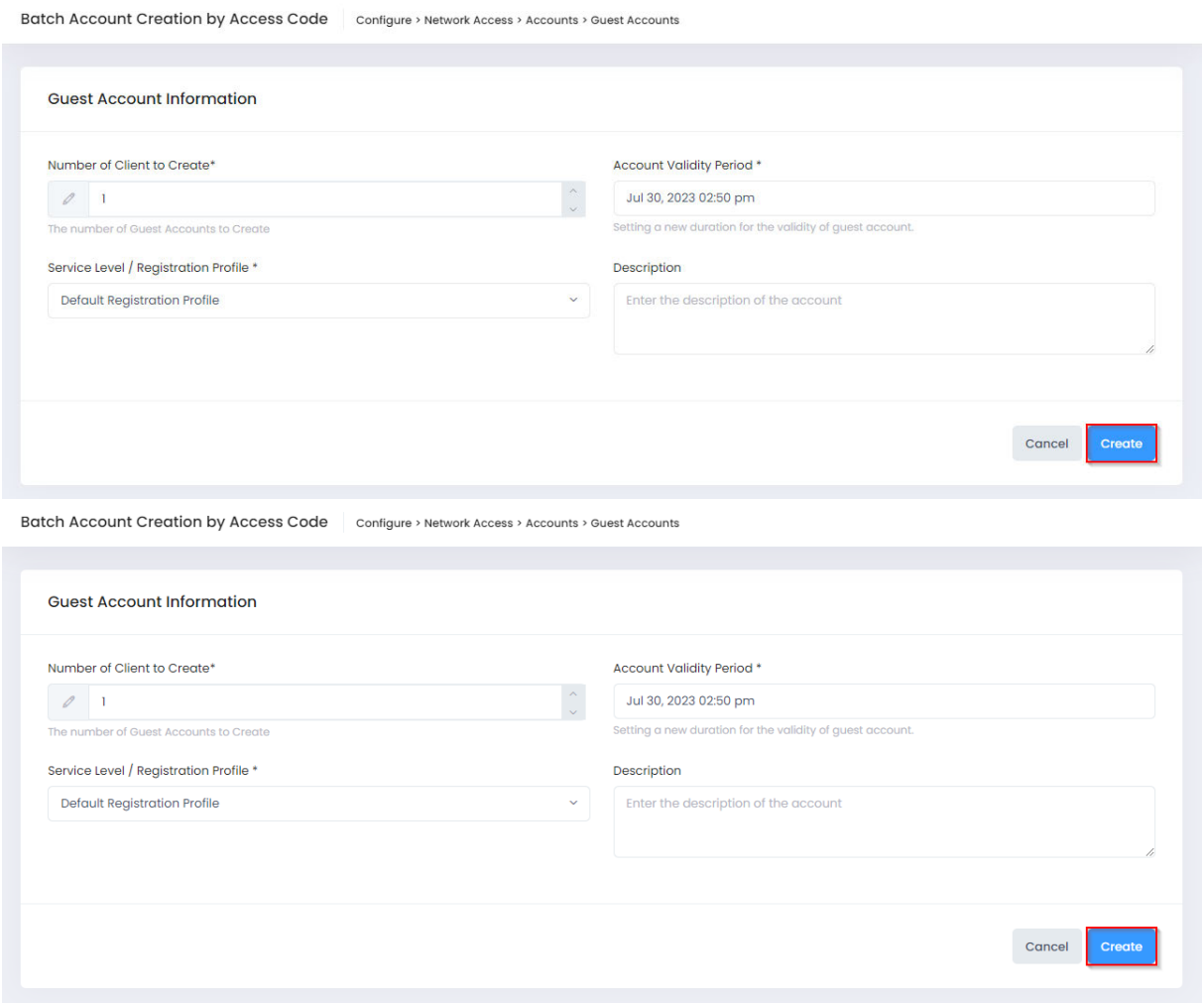
Batch Account Creation for Guest Accounts List



Complete the fields as described below, then click **Create**.

- **Guest Account Name Prefix -** Enter a prefix for the accounts you are creating. When created, the account name will consist of the prefix and incremented number (for example, Guest1, Guest2).
- **Number of Clients to Create** - Enter the number of Guest Accounts you want to create. (Range = 1 - 5000)
- **If you want to adjust the Expiry Duration for this Guest Account, please enable the toggle button** - Enable/disable whether you want to adjust the Account Validity Period for the specified number of Guest Accounts that will be created. Disabled by default. When enabled, the following setting appears:
  - **Account Validity Period** - Set a new length of time, in days, that the Guest Account is valid. Make sure the value specified here does not exceed the value defined in the Global Guest Access Settings (see page 642). For example, if you set the Global Account Validity Period to 180 days, the longest period you will be able to set here will be up to 180 days. (Range = 1 – 365, Default = 90).
- **Service Level / Registration Profile** - Specify if a Registration Profile or Service Level that is linked to a Registration Profile is assigned to each account created. By default, the “Default Registration Profile” is used. See the online Service Levels help (see page 645) and the online Registration Profiles help (see page 651) for more information.
- **Description** - Enter an optional description that will be used for each account created.

Batch Account Creation by Access Code



Complete the fields as described below, then click **Create**.

- **Number of Clients to Create** - Enter the number of Guest Accounts you want to create. (Range = 1 - 5000)
- **Account Validity Period** - Set a new length of time, in days, that the Guest Account is valid. Make sure the value specified here does not exceed the value defined in the Global Guest Access Settings. For example, if you set the Global Account Validity Period to 180 days, the longest period you will be able to set here will be up to 180 days. (Range = 1 – 365, Default = 90).
- **Service Level / Registration Profile** - Specify if a Registration Profile or Service Level that is linked to a Registration Profile is assigned to each account created. By default, the “Default Registration Profile” is used. See the online Service Levels help (see page 645) and the online Registration Profiles help (see page 651) for more information.
- **Description** - Enter an optional description that will be used for each account created.

7.5.3.5 Creating a Service Level

When a Guest Account is created or edited, an optional Service Level from the Service Levels List can be assigned to the account. The Service Level binds Access Roles and Policies to the Guest Account user.

To access the Service Levels screen, click **Settings** on the Guest Access Strategy (see page 633) screen or the “Guest Accounts” screen and select **Service Levels** from the drop-down menu. The Service Levels screen displays a list of configured Service Levels.

Use the Service Levels screen (see page 645) to display information about configured Service Levels that you can apply to different Guest users. This screen is also used to create, edit, and delete Service Levels.

7.5.3.6 Creating a Registration Profile

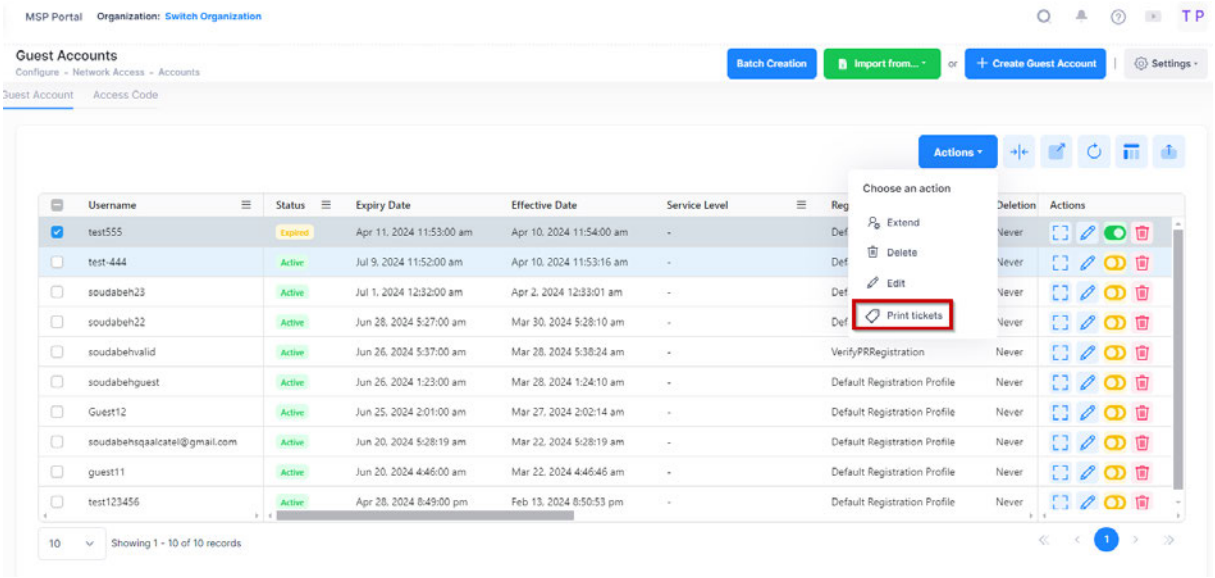
You can create a Registration Profile for Guest Accounts to customize the network access settings per the requirements of the Guest user. The Registration Profile determines Data and Time Quota limits for user access, Device and Account Validity attributes, and Exhaustion Handling (when Quota limits are reached).

When a Guest Account is created or edited, a Registration Profile (or optional Service Level linked to a Registration Profile) can be assigned to the account. To access the Registration Profile screen, click **Settings** on the Guest Access Strategy (see page 642) or “Guest Accounts” screen and select **Registration Profile** from the drop-down menu. The Registration Profile screen displays a list of configured Registration Profiles.

Use the Registration Profile screen (see page 651) to display information about configured Registration Profiles. This screen is also used to create, edit, and delete Registration Profiles.

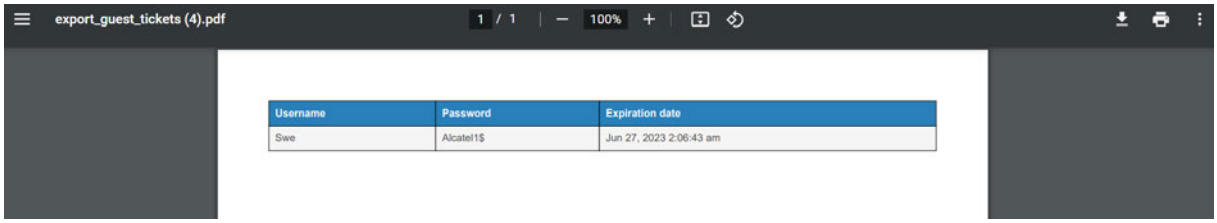
7.5.3.7 Print Tickets

You can print a ticket that contains Guest Account login information to send to the user. To print a login information ticket for a Guest Account, select the Guest Account(s) by clicking on the checkbox next to the Guest Accounts List entry, then click on **Actions** and select **Print tickets** from the drop-down menu list.

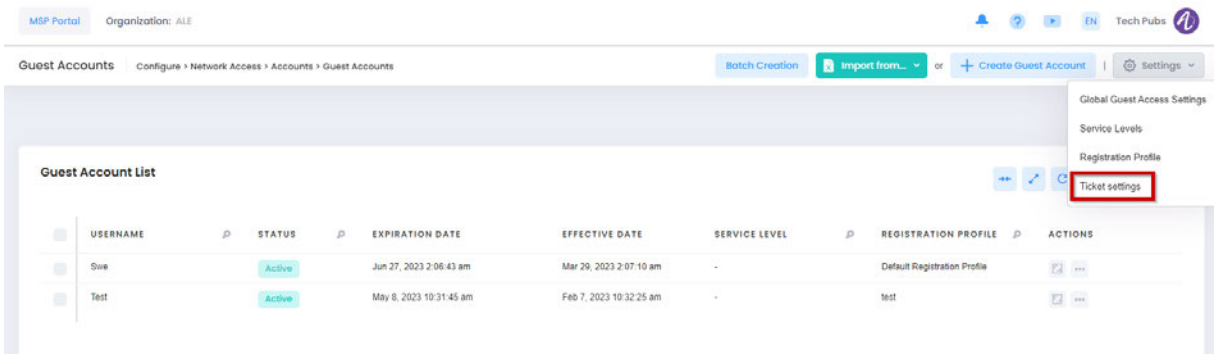


11 **Print Tickets**

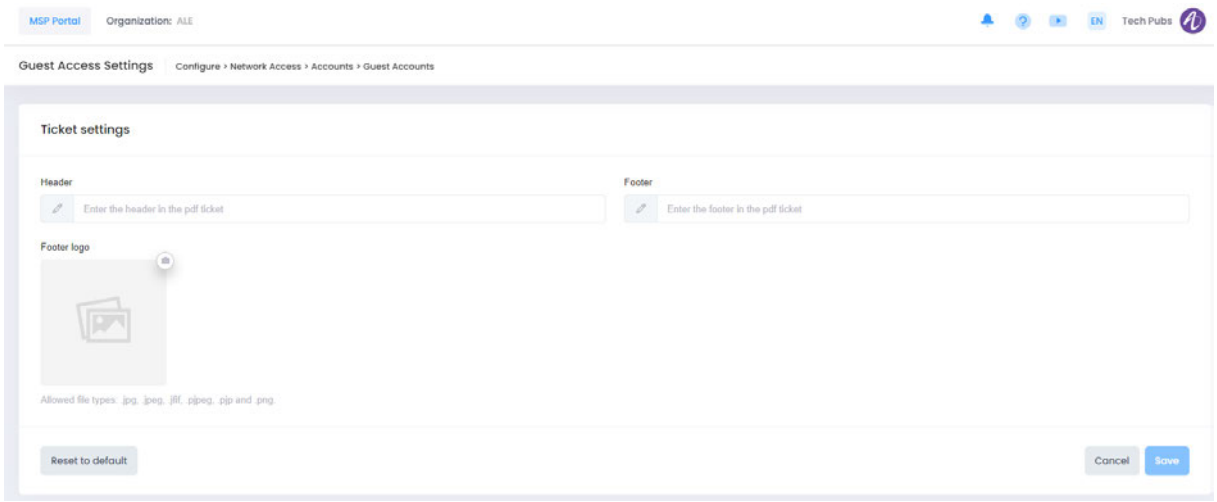
The following output will be generated in the form of PDF document containing the user login information for the Guest Account.



To customize the print tick PDF, click on **Settings** on the Guest Accounts screen and select **Ticket Settings** from the drop-down menu.



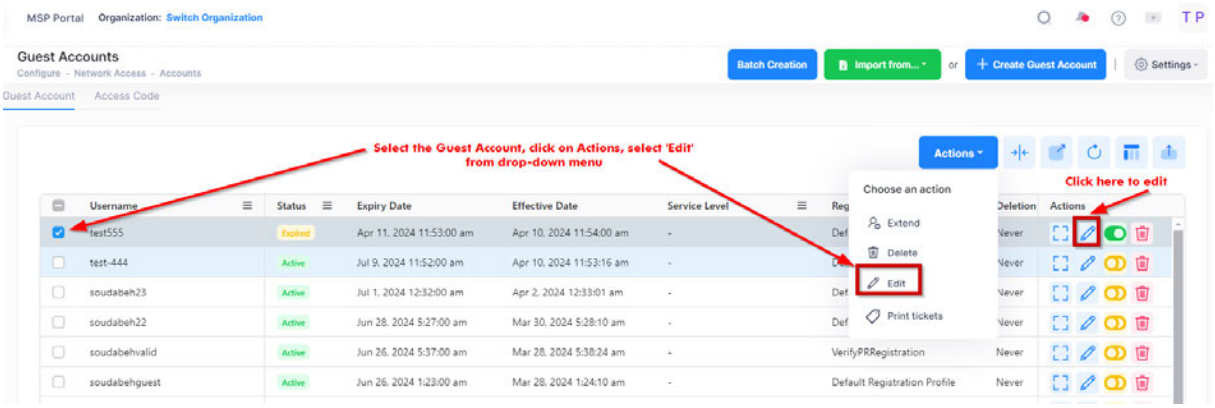
The following Ticket Settings screen appears. Enter the required fields and click on **Save** to save the settings.



- **Header -** Enter the header to use in the PDF ticket.
- **Footer -** Enter the footer to use in the PDF ticket.
- **Footer logo -** Upload the logo for the footer (the file type can be in jpg, jpeg, jfif, pjpeg, pjp and png format).
- **Reset to default -** Click on this button to automatically change all the custom ticket settings back to the default settings.

7.5.3.8 Editing a Guest Account

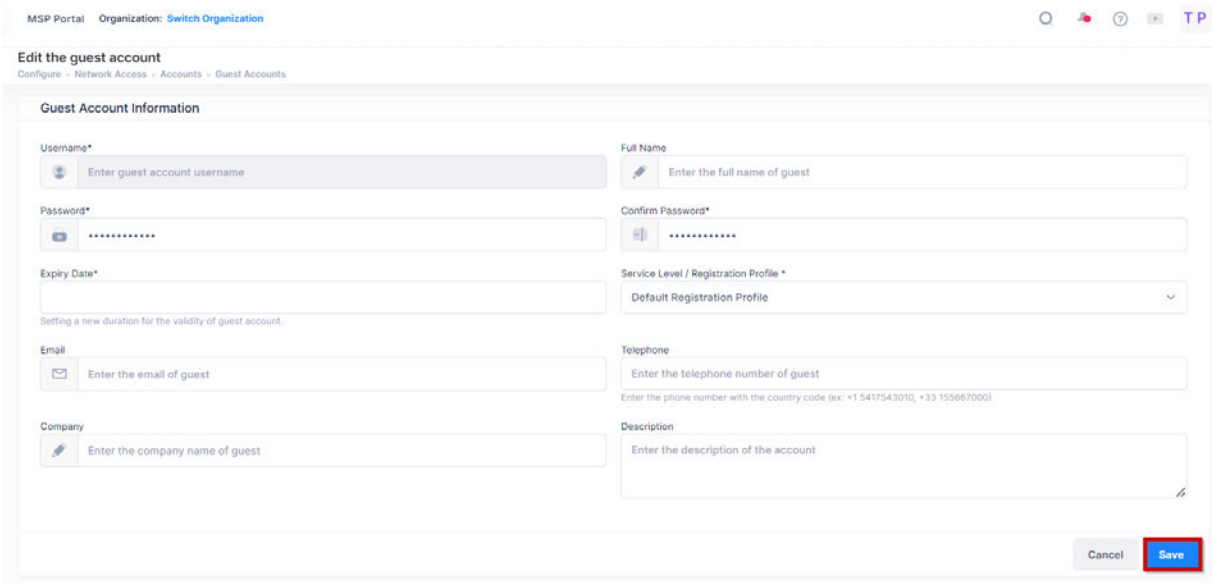
You can edit the parameter values for a guest account in the Guest Account List by accessing the Edit the Guest Account screen.



Use one of the following methods to access the Edit the Guest Account screen (as shown above):

- Select the Guest Account to edit by clicking on the checkbox next to the Guest Account List, click on edit icon under the **Actions** column.
- Select the Guest Account to edit and Click on the “Actions” button on the top of the screen and then select **Edit** from drop-down menu.

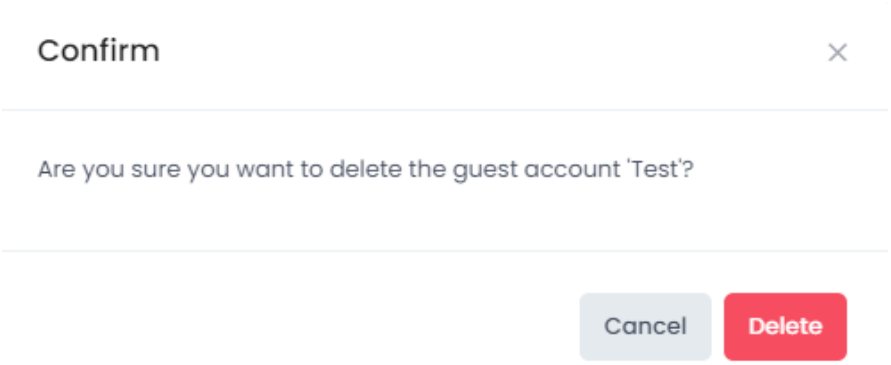
The following Edit the Guest Account screen displays. Edit the fields as described above, then click on **Save**.



Note that you cannot edit an Account Name.

7.5.3.9 Deleting a Guest Account

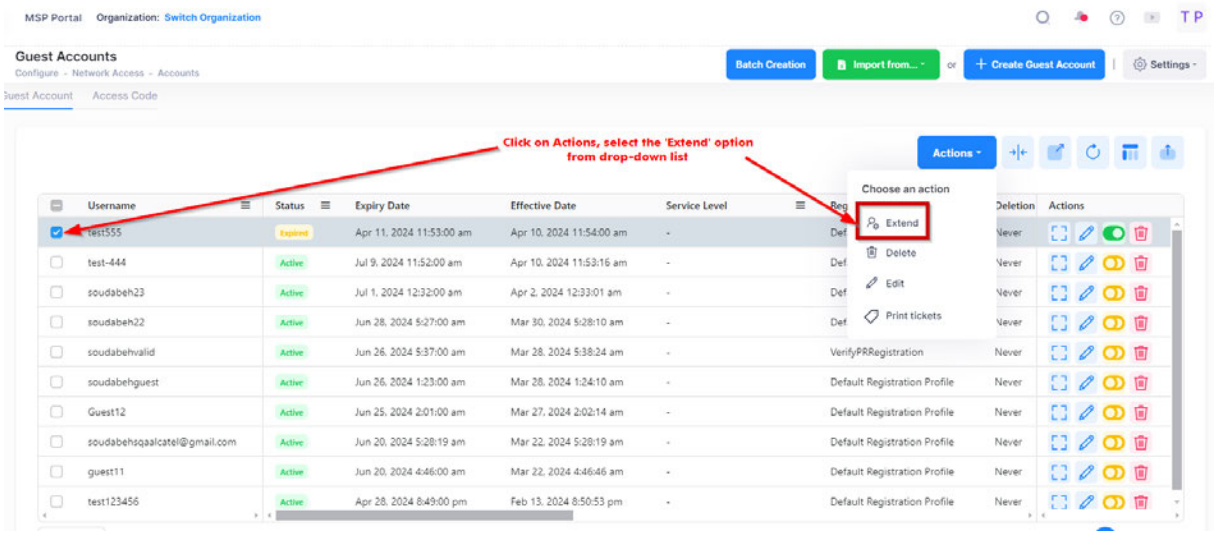
Select a Guest from the Guest Account list and click on the Delete icon under the “Actions” column or click on the **Actions** button and select Delete from the drop-down menu. When the following confirmation prompt appears, click on **Delete** to delete the Guest Account.



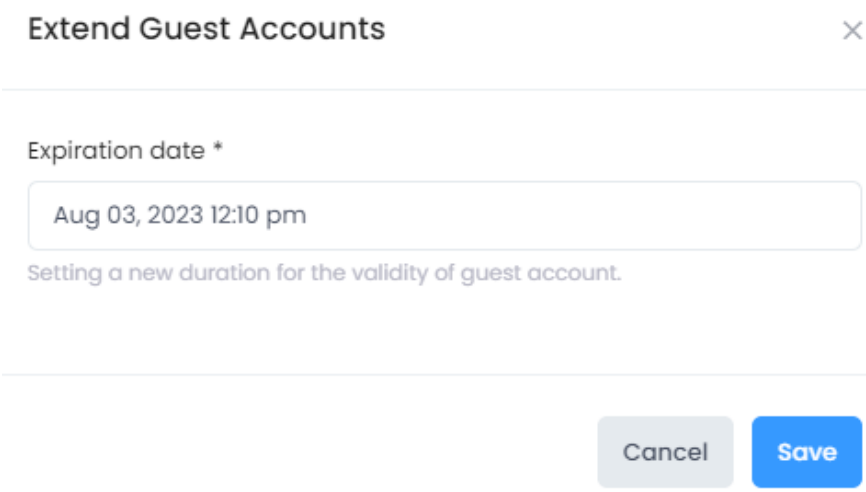
Click on **Delete** to confirm that you want to delete the Guest Account from the List .

7.5.3.10 Extend a Guest Account

You can extend the expiration date for a guest account or guest access code account in the Guest Account List by accessing the Extend Guest Accounts screen.



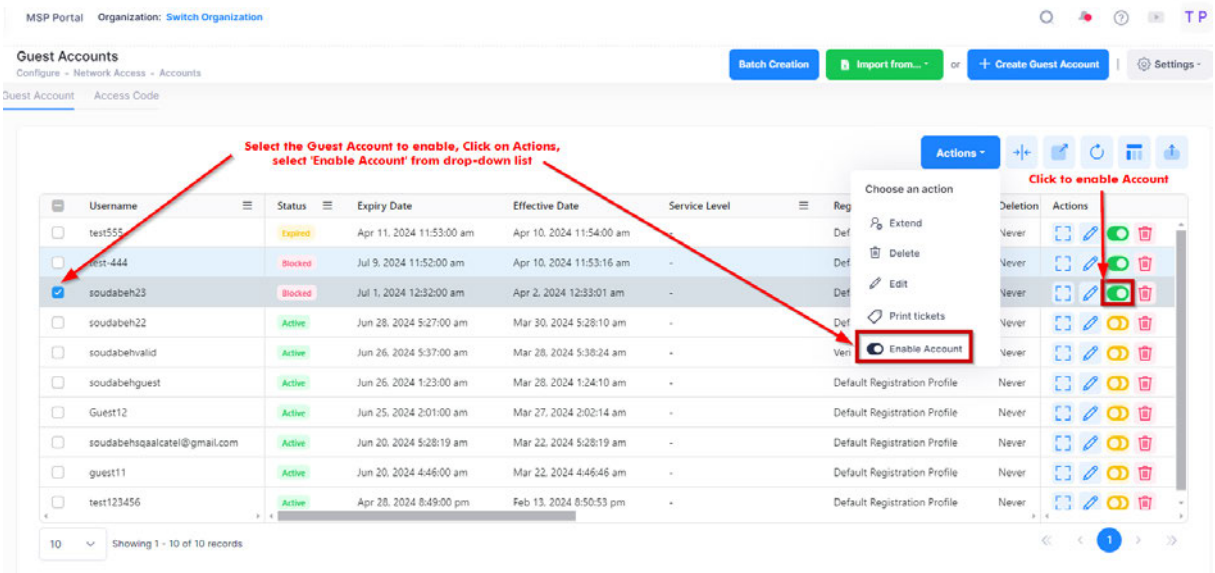
The following Extend the Guest Accounts screen displays. Select a new duration for the validity of the guest accounts or guest access code accounts ,then click on **Save**.



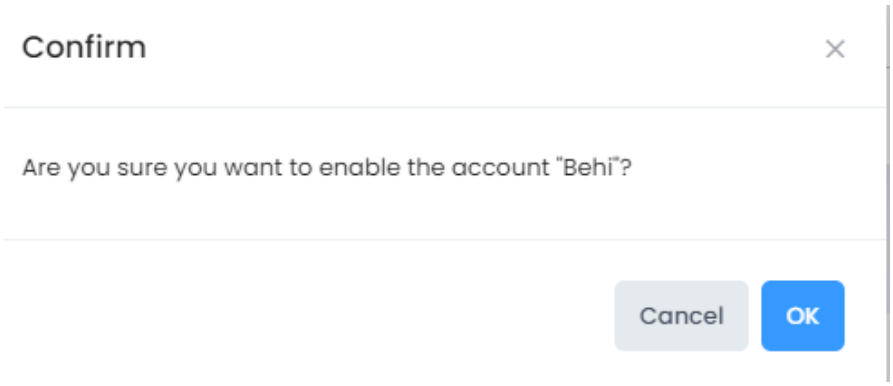
7.5.3.11 Enable a Guest Account

To enable a Guest Account, use one of the following methods for the guest accounts you want to activate:

- Select a Guest Account by clicking on the checkbox next to the Guest Account List, click on **Actions**, then select **Enable Account** from the drop-down menu.
- Click on the dot icon under the “Actions” column next to the Guest Account List, then select **Enable Account** from the drop-down menu.



When you select the Guest Account you want to enable, the following confirmation prompt appears:

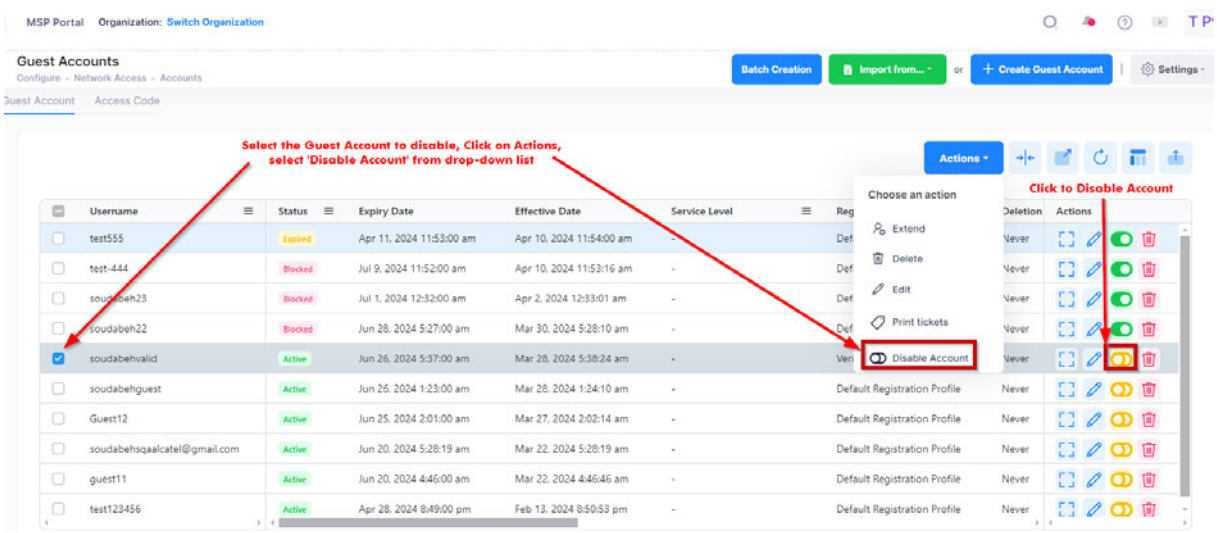


Click on **OK** to confirm that you want to enable the Guest Account(s) from the List .

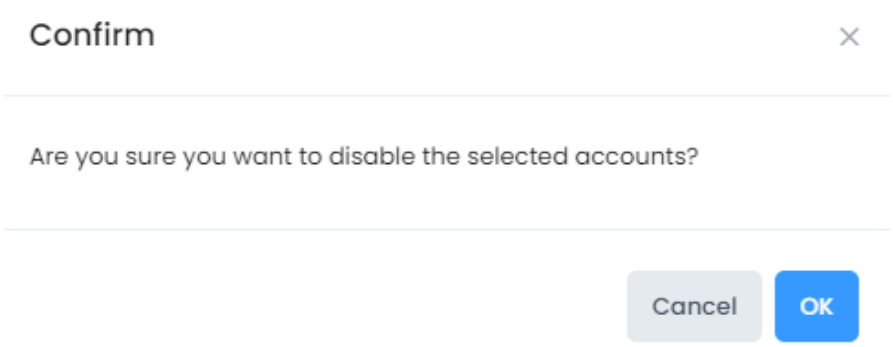
7.5.3.12 Disable a Guest Account

To disable a Guest Account, use one of the following methods for the guest accounts you want to block:

- Select a Guest Account by clicking on the checkbox next to the Guest Account List, click on **Actions**, then select **Disable Account** from the drop-down menu.
- Click on the dot icon under the “Actions” column next to the Guest Account List, then select **Disable Account** from the drop-down menu.



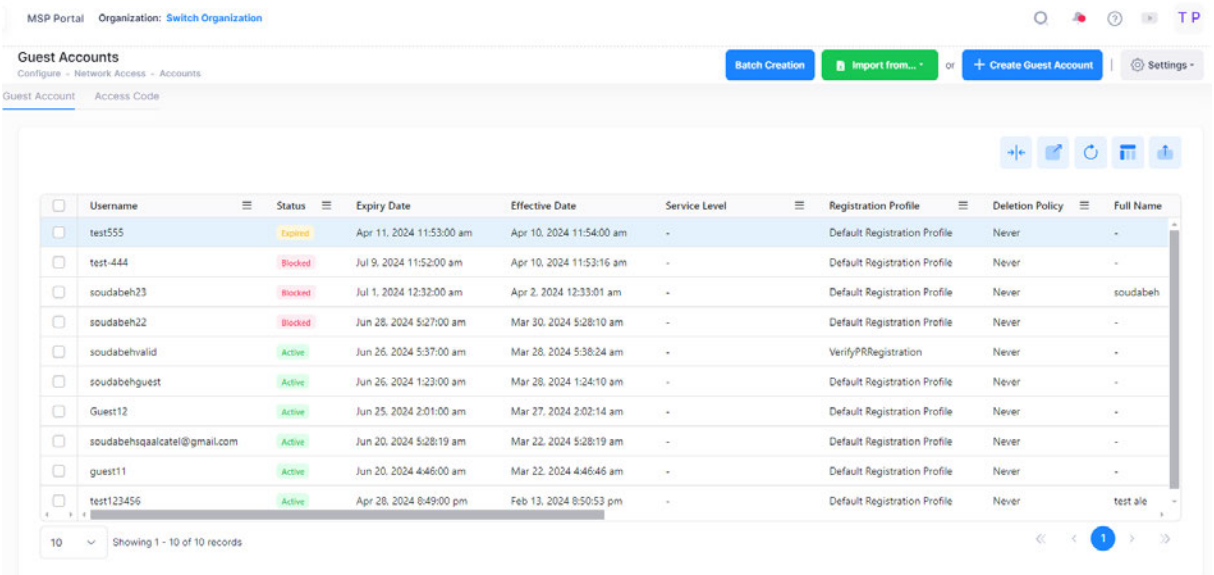
When you select the Guest Account you want to disable, the following confirmation prompt appears:



Click on **OK** to confirm that you want to disable the Guest Account(s) from the List .

7.5.3.13 Display Guest Account List

The Guest Account list displays information for the all configured Guest Accounts. To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



12 **Guest Accounts List**

- **User Name -** Account identifier (e.g., name of the guest).
- **Service Level -** The Service Level for the Guest Account, if configured.
- **Status -** The administrative status of the account (Enabled/Expired/Disabled).
- **Effective Date -** The date and time the account was created.
- **Expiration Date -** The date and time the Guest Account expires.
- **Registration Profile** - The registration profile for the Guest Account.

- **Full Name -** Full name of the Guest User.
- **Company -** Company name of the Guest User.
- **Telephone -** Telephone number of the Guest User.
- **Email -** Email address of the Guest User.
- **Sponsor Name -** Sponsor who created the Guest Account or approved it for self-registration.
  - **Admin-XXX -** Indicates the sponsor belongs to the Administrator group; XXX indicates the account in the group.
  - **EmployeeSponsor-YYY -** Indicates the sponsor belongs to the Employee group; YYY indicates the employee account in the group.
  - **GuestSponsor-ZZZ -** Indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account in the group.
  - **SelfRegister-AAA -** Indicates no sponsor is involved and there is no need approval for the self-registration request; AAA indicates the login password is guest-user-defined (Manually) or UPAM-defined (Automatically).
- **Description -** Optional description for the account.
- **Guest Account Deletion Policy -** The number of days after the Account Validity Period expires before Guest Accounts are automatically deleted:
  - **Never -** Guest Account will **not** be deleted at the end of the Account Validity Period (Default).
  - **Immediately -** Guest Account will be automatically deleted at the end of the Account Validity Period.
  - **Number of Days -** Guest Account will be automatically deleted on the configured number of days after the end of the Account Validity Period (Range = 1 - 90).

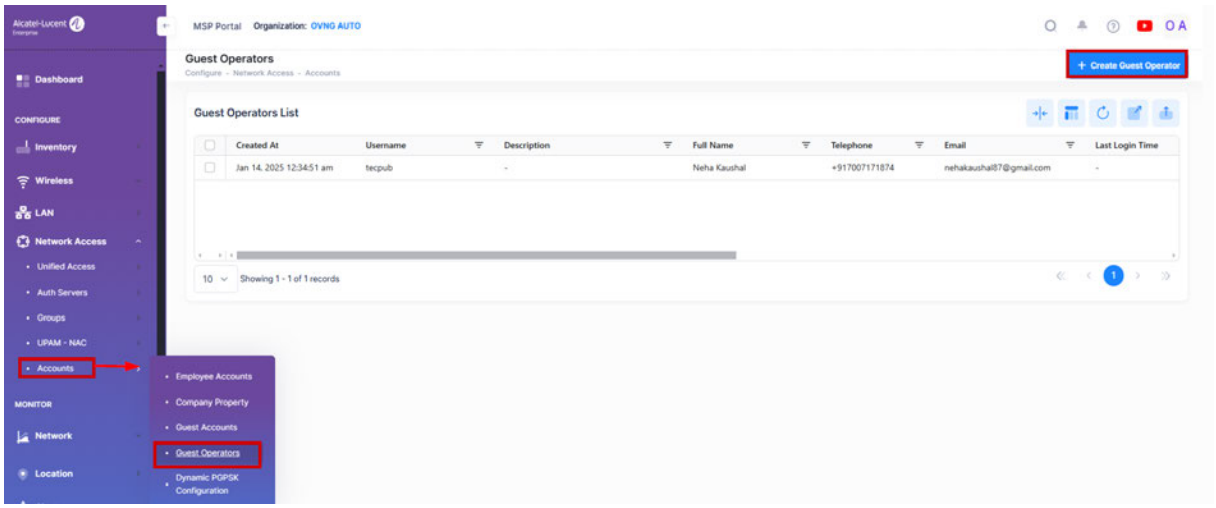
21 Oct 2025

7.5.4 Guest Operators

The Guest Access Guest Operators screen is used to create the Guest Operators in the UPAM network. A Guest Operator is a network operator who manages the guest user network access. A Guest Operator can create Guest user accounts and approve Guest user self-registration requests.

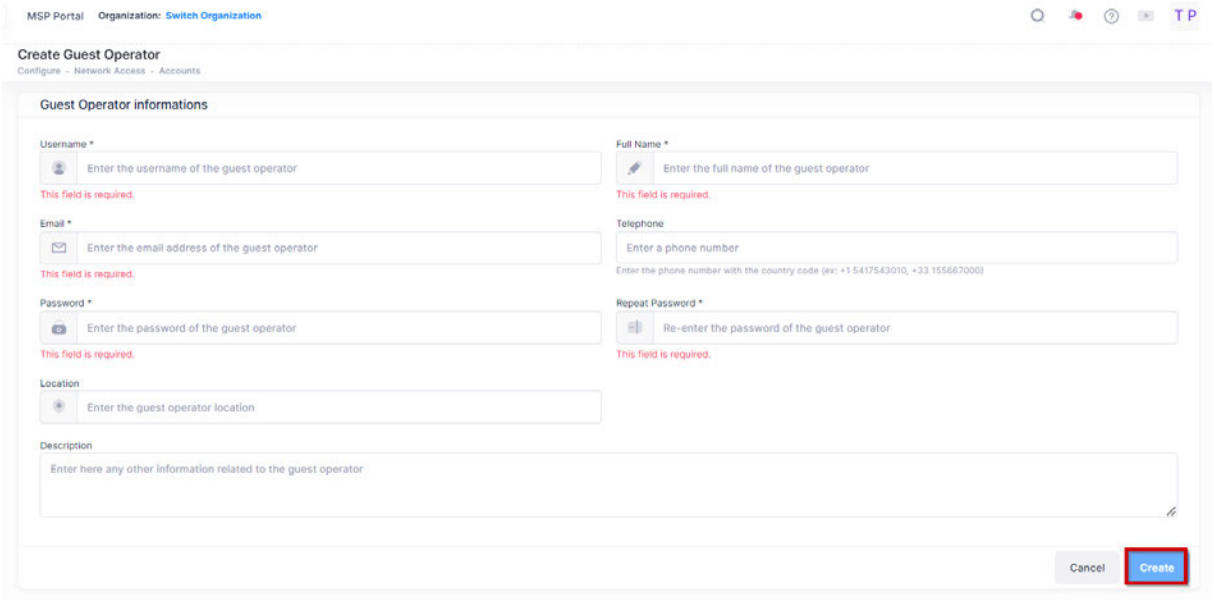
> The Guest Operator URL will not work in the same browser window that is used to access OmniVista Terra. Open a new browser window for Guest Operator login.

Use the Guest Operators list screen to display information (see page 748) about all of the configured Guest Operators in the UPAM database. This screen also allows you to create (see page 745), edit (see page 746), and delete (see page 747) accounts. To access the Guest Operators screen, click on **Network Access > Accounts > Guest Operators** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.5.4.1 Creating a Guest Operator

To create a new Guest Operator, click on the add icon to display the **Create Guest Operator** screen. The Create Guest Operator screen opens as shown below.



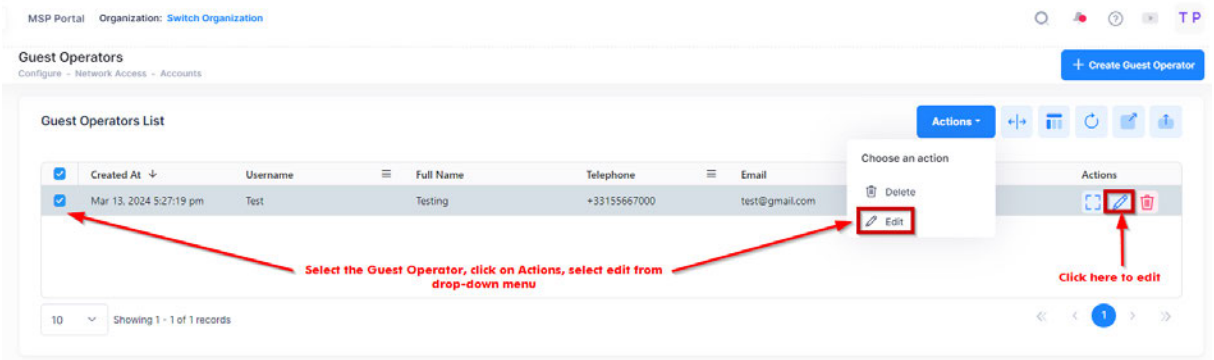
Complete the following fields as described:

- **Username -** User name of the Guest Operator account.
- **Full Name -** Full name of the Guest Operator.
- **Password -** Password of the Guest Operator account.
- **Repeat Password -** Re-enter to confirm the account password.
- **Telephone -** Telephone of the Guest Operator.
- **Email -** Email address of the Guest Operator.
- **Location -** Location/Site of the Guest Operator. Guest requests are sent to the operator for this location.
- **Description -** Optional description information for the Guest Operator account.

After you have finished with the field values, click on the **Create** button to create the operator.

7.5.4.2 Editing a Guest Operator

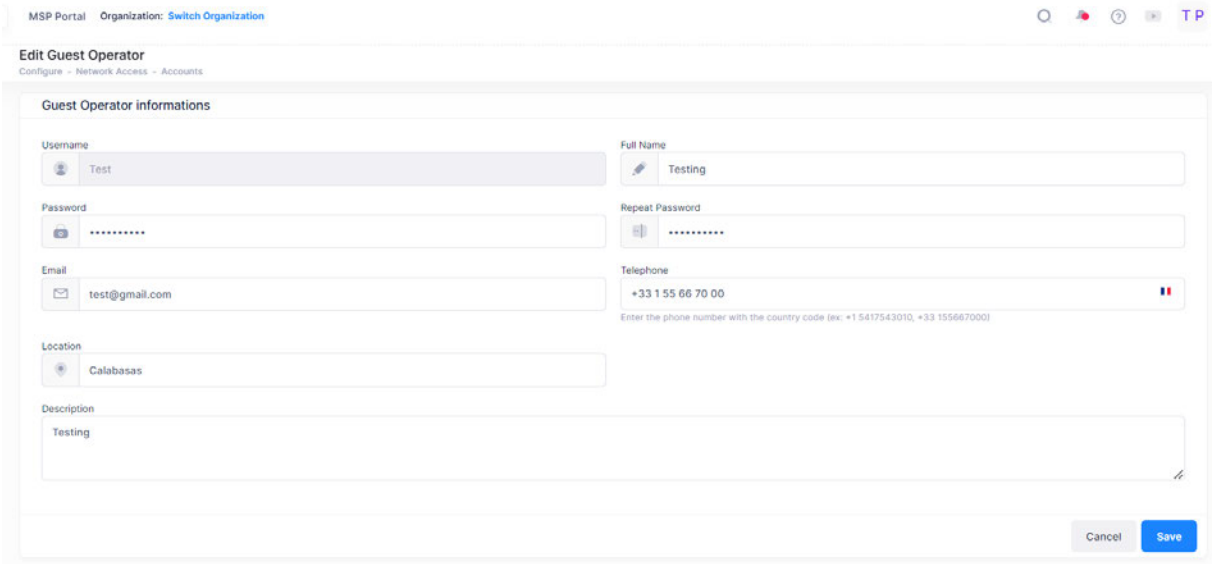
You can edit the parameter values for a Guest Operator in the Guest Operator List by accessing the Edit Guest Operator screen.



Use one of the following methods to access the Edit Guest Operator screen (as shown above):

- Select the Guest Operator to edit by clicking on the checkbox next to the Guest Operator List, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the Guest Operator that you want to edit.

The following Edit Guest Operator screen displays. Edit the fields as described above, then click on **Save**.

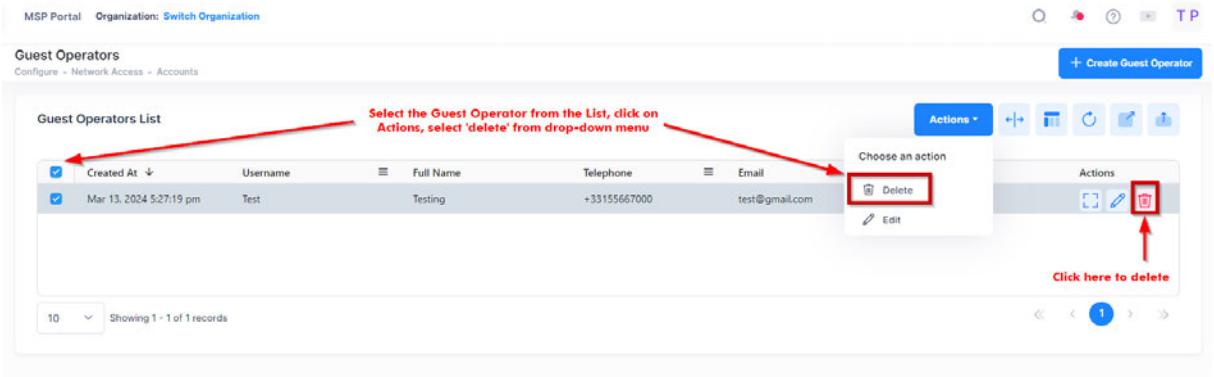


Note that you cannot edit a User Name.

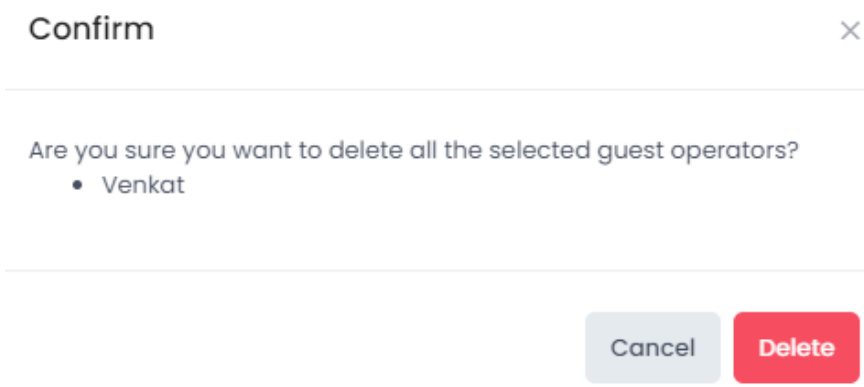
7.5.4.3 Deleting a Guest Operator

To delete a Guest Operator, use one of the following methods to select the Guest Operator you want to delete:

- Select the Guest Operator to delete by clicking on the checkbox next to the Operator, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the trash icon under the “Actions” column next to the Guest Operator that you want to delete. (as shown below).



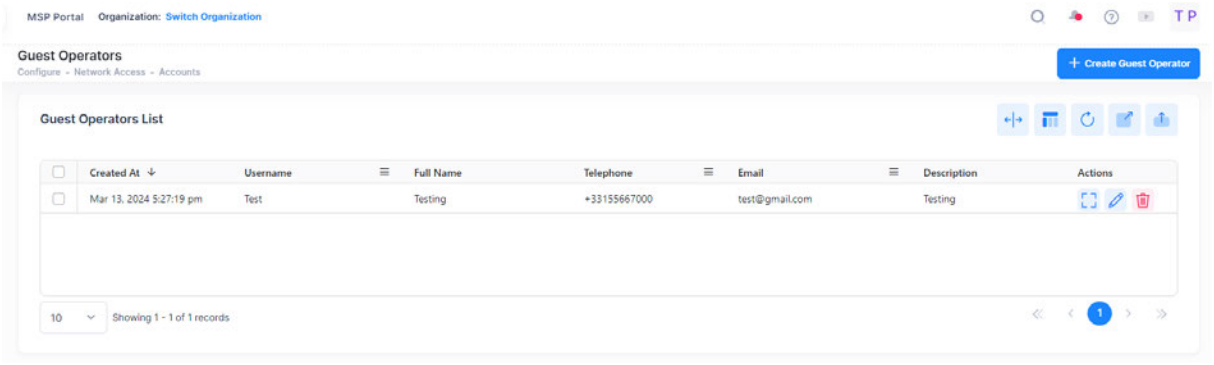
When you select the Guest Operator you want to delete, the following confirmation prompt appears:



Click on **Delete** to confirm that you want to delete the Guest Operator.

7.5.4.4 Display Guest Operator List

The Guest Operator list displays information for the all configured Operators. To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



13 **Guest Operators List**

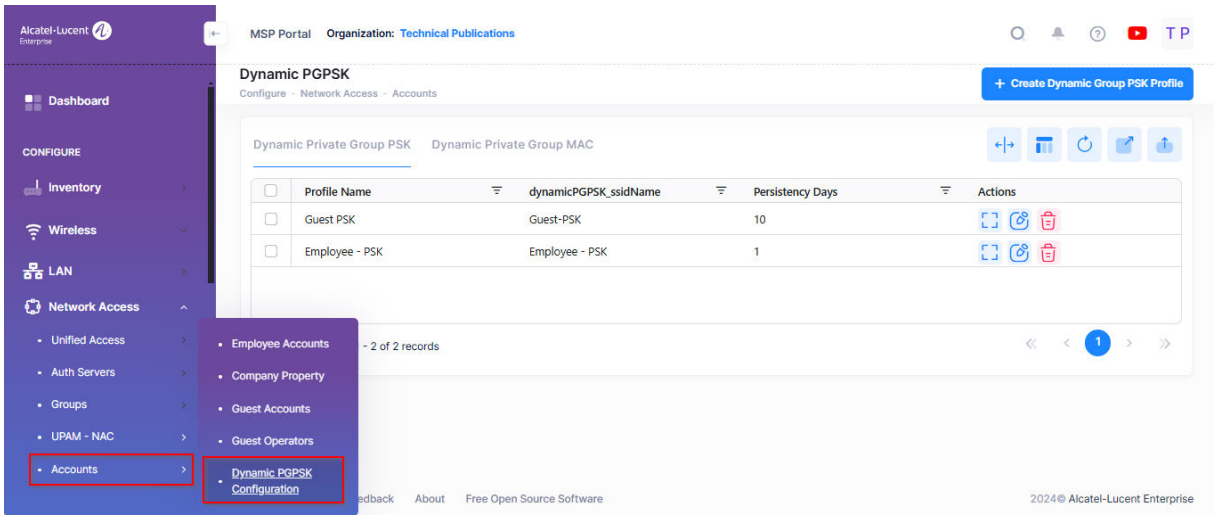
- **Username -** User name of the Guest Operator account.
- **Full Name -** Full name of the Guest Operator.
- **Telephone -** Telephone of the Guest Operator.
- **Email -** Email address of the Guest Operator.
- **Location -** Location/Site of the Guest Operator. Guest requests are sent to the operator for this location.
- **Description -** Optional description information for the Guest Operator account.
- **Last Login Time -** Latest login time for the Guest Operator account.
- **Login URL -** The management interface for Guest Operator. It uses the secondary IP address of OmniVista.

21 Oct 2025

7.5.5 Dynamic PGPSK Configuration

The Dynamic PGPSK Configuration screen is used to create Dynamic Private Group PSK (PGPSK) profiles in the UPAM database. The Dynamic PGPSK profiles are checked when Dynamic PGPSK is enabled for an SSID. If a PSK entry in one of the profiles matches a device authenticating through the SSID, the device is saved to the list of devices authenticated through UPAM PSK in the Dynamic Private Group PSK MAC tab (see page 759).

Use the Dynamic PGPSK Configuration screen to display information (see page 758) about all of the configured Dynamic PGPSK profiles in the UPAM database and view the devices connected through PSK authentication. This screen also allows you to create (see page 751), edit (see page 753), and delete (see page 757) profiles. To access the Dynamic PGPSK Configuration screen, click on **Network Access > Accounts > Dynamic PGPSK Configuration** under the “Configure” section of the OmniVista Terra Menu (see page 45).



There are two tabs available on the Dynamic PGPSK screen:

- Dynamic Private Group PSK (see page 750) - Displays configured PGPSK profiles.
- Dynamic Private Group MAC (see page 759) - Displays devices connected through UPAM PSK authentication.

7.5.5.1 Using the Dynamic Private Group PSK Tab

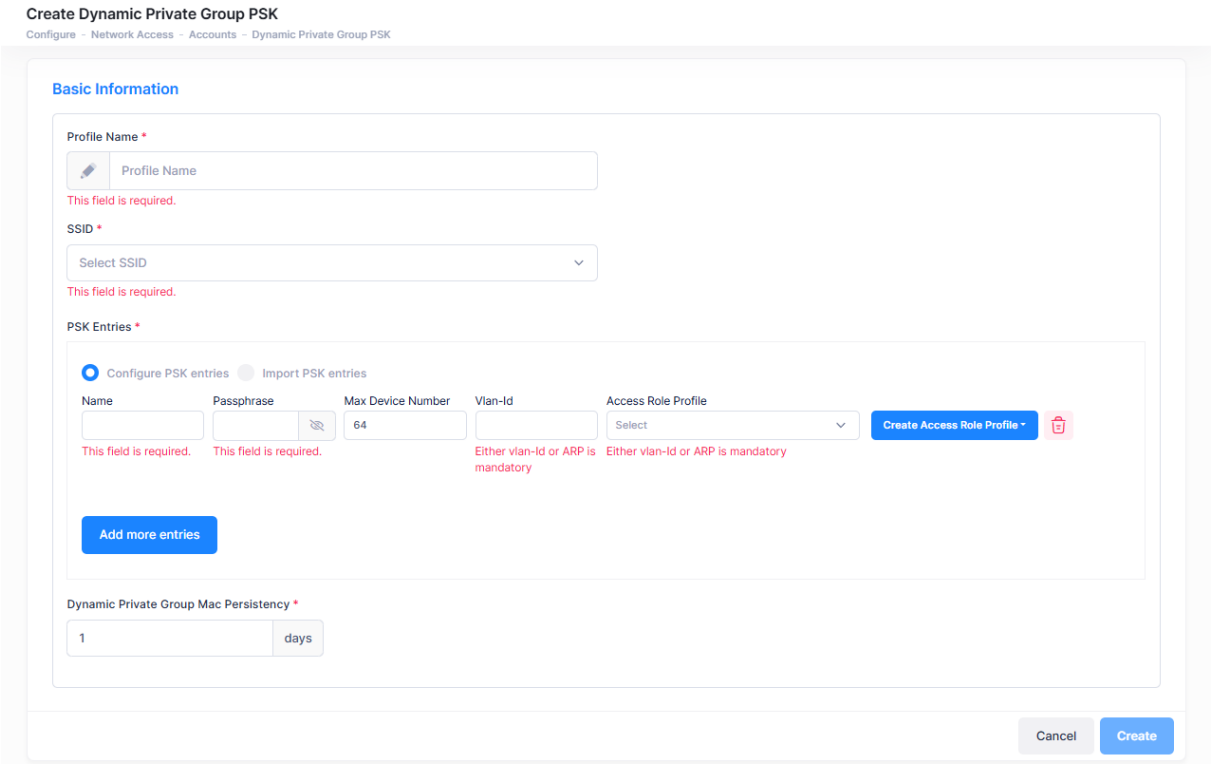
The Dynamic Private Group PSK tab provides a list of all configured Dynamic PGPSK profiles. Use this tab to create, edit, or delete Dynamic PGPSK profiles.

Each profile contains one or more PSK entries that are configured in the UPAM database. Each client device specifies a Passphrase when connecting to an SSID. If the passphrase matches any of the PSK entries in a Dynamic PGPSK profile, the client is placed in the specified VLAN ID or Access Role Profile.

Note that UPAM checks the Company Property list first to see if there’s a match for the device; if not, the list of entries in the Private Group PSK UPAM database are checked. When a device is authenticated through Dynamic Private Group PSK, the matched entry is added to the Dynamic Private Group PSK MAC tab (see page 759).

7.5.5.1.1 Creating a Dynamic Private Group PSK Profile

To create a PGPSK profile, click **Create Dynamic Private Group PSK Profile**. The Create Dynamic Private Group PSK Profile screen opens.



Complete the following fields as described below:

- **Profile Name** - Enter a unique name to identify the PGPSK profile.
- **SSID** - The name of the SSID that is configured for a Protected Network with Dynamic Group PSK (see page 354) enabled. Note that only SSIDs with this configuration are included for selection from the drop-down list.
- **PSK Entries** - There are two methods for creating a PSK Entry (see Guidelines for Configuring PSK Entries (see page 751)):
  - **Configure PSK Entries** - Manually configure (see page 752) each PSK entry.
  - **Import PSK Entries** - Import multiple PSK entries (see page 752) from an Excel sheet (.xlxs).
- **Dynamic Private Group Mac Persistency** - Enter the number of days for the MAC persistency duration that is applied to devices authenticated through the Dynamic PGPSK profile.

7.5.5.1.1.1 Guidelines for Configuring PSK Entries

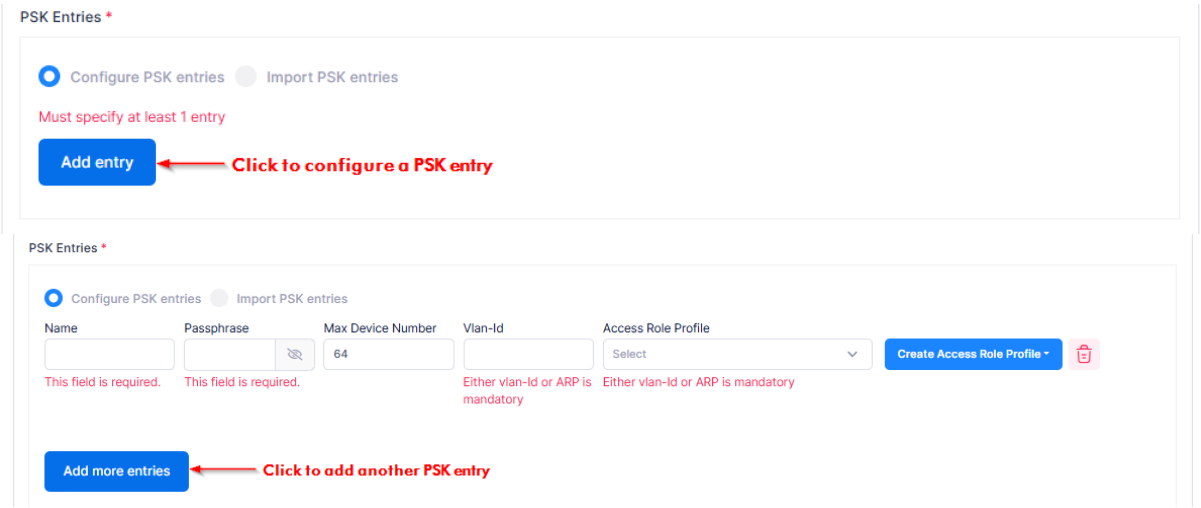
Consider the following guidelines when configuring PSK entries for Dynamic Private Group PSK profiles.

- Configuring PSK entries within the same profile:
  - You must use a unique name for each PSK entry.
  - You must use a unique passphrase for each PSK entry.

- Configuring PSK entries across different profiles that are configured with the same SSID:
  - You can create PSK entries with the same name but with a different passphrase.
  - You cannot create PSK entries with the same passphrase.
- Configuring PSK entries across different profiles with different SSIDs:
  - You can create PSK entries with the same name
  - You can create PSK entries with the same passphrase.

7.5.5.1.1.2 Manually Configure a PSK Entry

To manually create a new PSK entry, select **Configure PSK Entries** (the default) and click **Add Entry**.



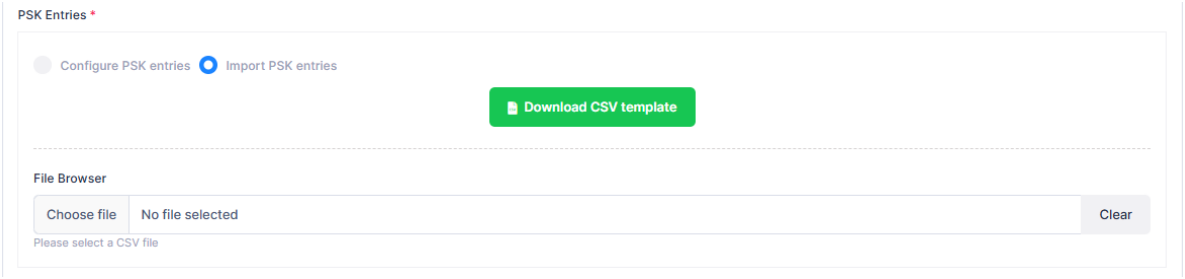
Enter the following information to configure the PSK entry (see Guidelines for Configuring PSK Entries (see page 750)):

- **Name** - Enter a unique name for the entry.
- **Passphrase** - Enter a unique PSK Passphrase for authentication.
- **Max Device Number** - The maximum number of devices for this PSK entry.
- **VLAN-ID** - The VLAN ID assignment for the PSK device. Note that either a VLAN ID or an Access Role Profile is required.
- **Access Role Profile** - Select the name of an existing Access Role Profile or click on **Create Access Role Profile** to create a new profile to use (see the Access Role Profile (see page 514) online help). Note that either an Access Role Profile or VLAN ID is required.

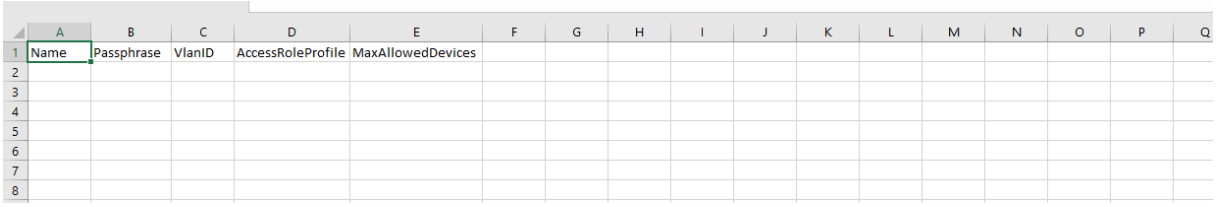
Click on **Add more entries** for each PSK Entry that you want to create. When you are done adding PSK entries, click on **Create** to create the profile configured with the PSK entries.

7.5.5.1.1.3 Import Multiple PSK Entries

To import multiple PSK entries, select **Import PSK Entries** and click on **Download XLSX template**. You are then prompted to specify where you would like to save the template file.



The following sample template file is an example of the template provided for adding multiple PSK entries:



	A	B	C	D	E
1	Name	Passphrase	VlanID	AccessRoleProfile	MaxAllowedDevices
2					
3					
4					
5					
6					
7					
8					

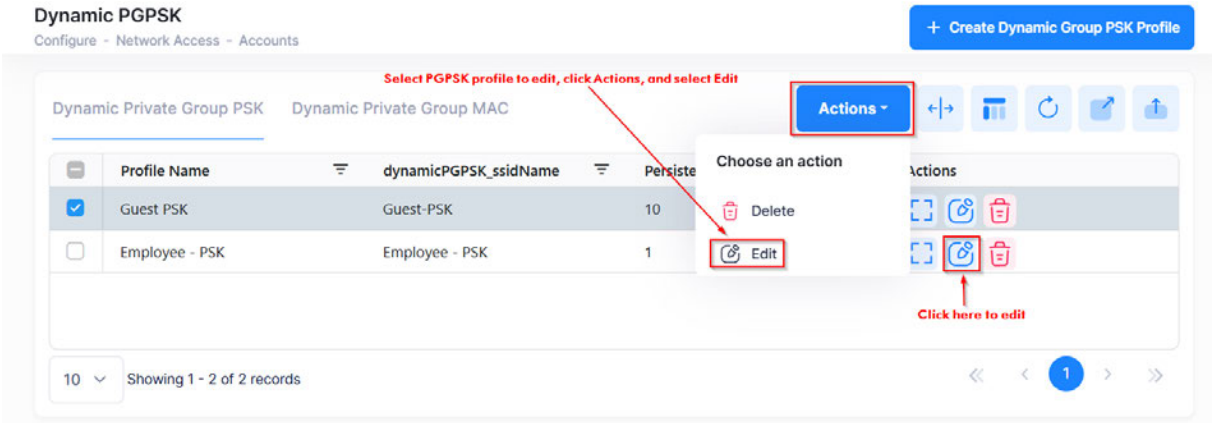
Fill out the template with information for each PSK entry that you want to import (see Guidelines for Configuring PSK Entries (see page 750)), then save the template file . Next, click in the **Choose File** field to find and select the existing template file to import.

Once the import is complete, the PSK Entries list is populated with the imported PSK entries. Click on **Create** to create the profile with the imported PSK entries.

7.5.5.1.2 Customizing a Dynamic Private Group PSK Profile

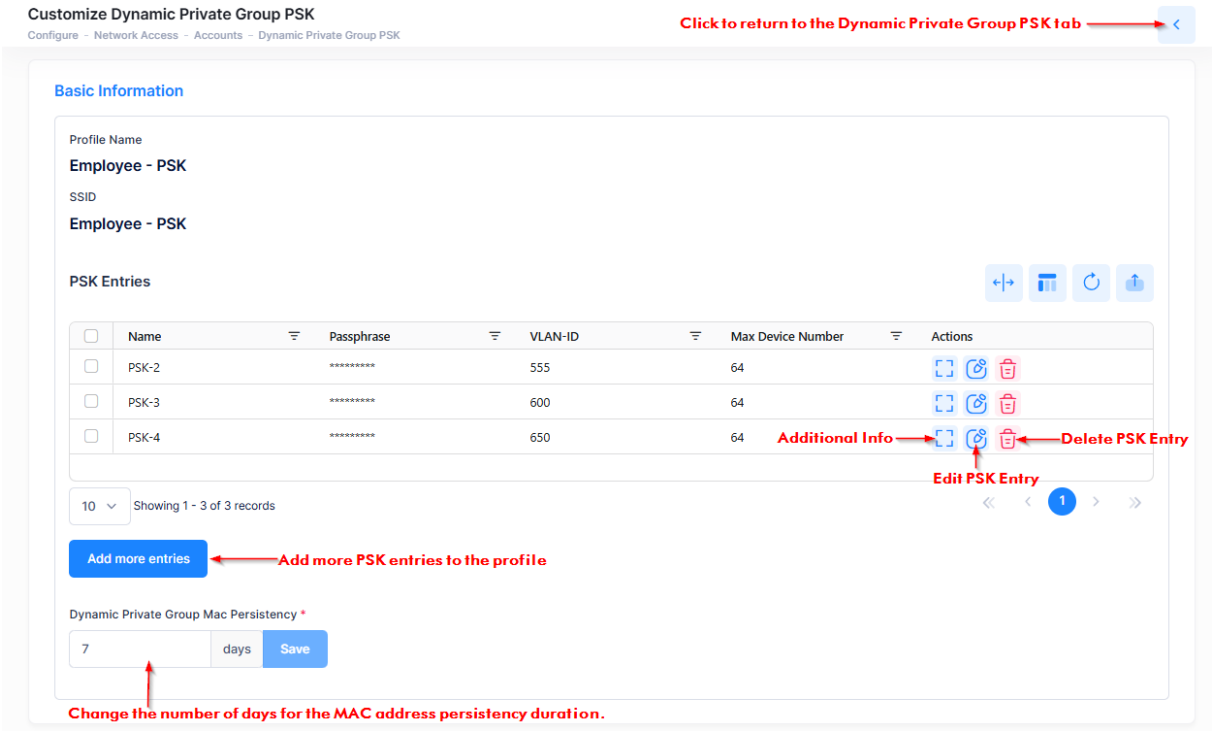
You can customize a Dynamic Private Group PSK profile by accessing the Customize Dynamic Private Group PSK screen. To access the Customize Dynamic Private Group PSK screen, use one of the following methods:

- Select the Dynamic Private Group PSK profile to edit by clicking on the checkbox next to the profile, click on **Actions**, then select **Edit** from the drop-down menu.
- Click on the pencil icon under the “Actions” column next to the profile that you want to edit.



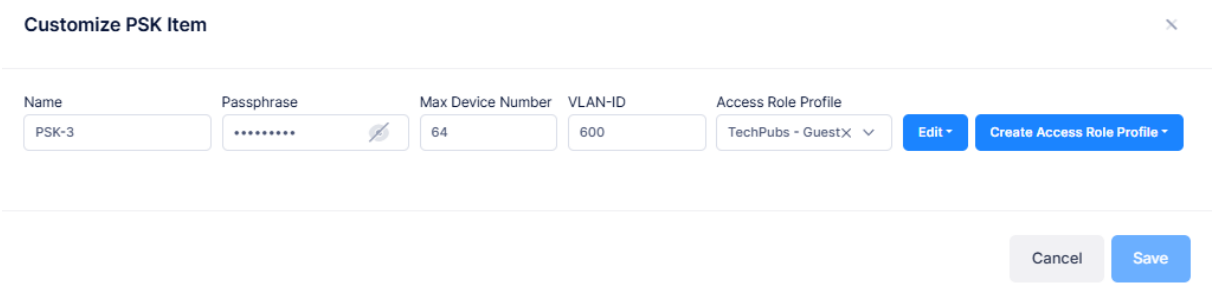
The following Customize Dynamic Private Group PSK screen opens. This screen displays information (see page 755) about PSK entries assigned to the Dynamic PGPSK profile. Use this screen to add more PSK entries (see page 756) to the profile, edit (see page 754)or delete (see page 755)existing PSK entries, and change the MAC Persistency duration (see page 757) for devices authenticated through the

Dynamic PGPSK profile. When you are finished customizing the Dynamic PGPSK profile, click on the arrow in the upper-right corner of the screen, as shown below.



7.5.5.1.2.1 Editing a PSK Entry

To edit a PSK Entry, select the entry and click on **Actions** to select **Edit** from the drop-down menu or click on the Edit icon under the “Actions” column next to the entry. The Customize PSK Items screen appears.



Change any of the PSK entry attributes for the following fields:

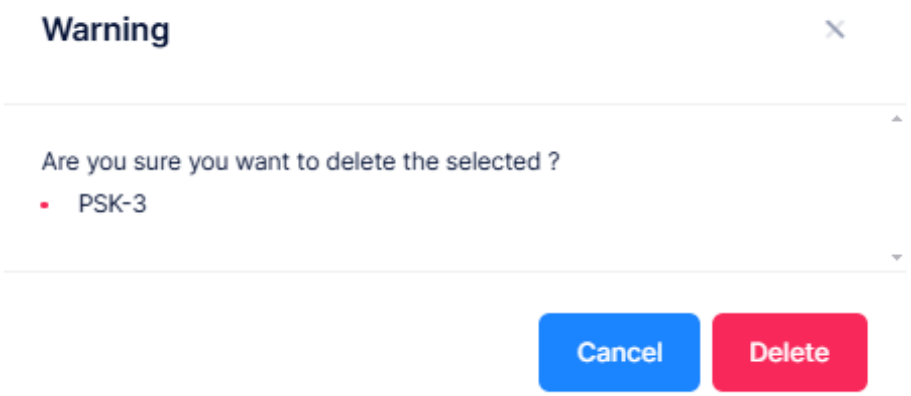
- **Name** - The name of the PSK entry.
- **Passphrase** - The PSK Passphrase used for authentication
- **Max Device Number** - The maximum number of devices that can authenticate with this PSK entry.
- **VLAN-ID** - The VLAN ID assignment for the PSK device.

- **Access Role Profile** - The Access Role Profile assignment for the PSK device. Click on **Edit** to edit the assigned Access Role Profile or click on **Create Access Role Profile** to create a new profile to use (see the Access Role Profile (see page 514) online help),

When you are done with editing the PSK entry, click on **Save** to retain your changes.

7.5.5.1.2.2 Deleting a PSK Entry

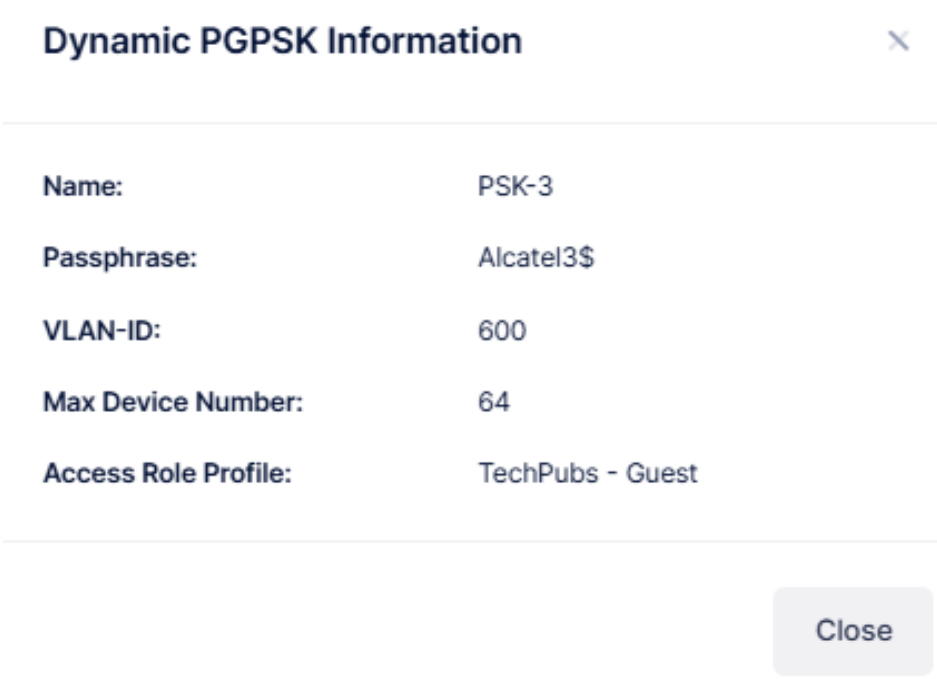
To delete a PSK Entry from the Dynamic PGPSK profile, select the entry and click on **Actions** to select **Delete** from the drop-down menu or click on the Delete icon under the “Actions” column next to the entry. The following confirmation prompt appears:



Click on **Delete** to remove the PSK entry from the Dynamic PGPSK profile.

7.5.5.1.2.3 Display PSK Entry Information

The PSK Entries list displays information for the PSK entries associated with the Dynamic PGPSK profile. To display information about a specific entry, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.

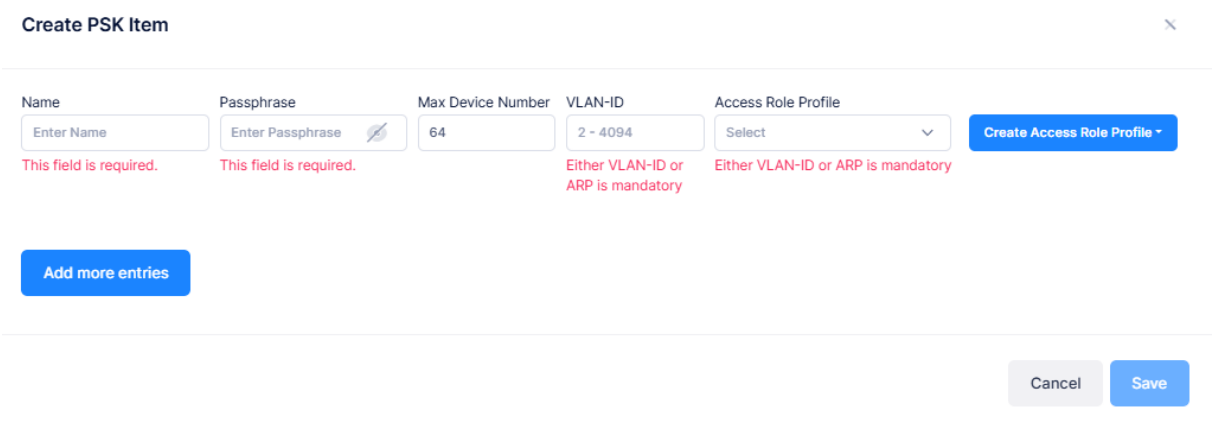


The following information is displayed for the PSK entry:

- **Name** - The name assigned to the PSK entry.
- **Passphrase** - The PSK Passphrase for authentication.
- **VLAN-ID** - The VLAN ID assignment for the PSK device.
- **Max Device Number** - The maximum number of devices that can authenticate with this PSK entry.
- **Access Role Profile** - The Access Role Profile assignment for the PSK device.

7.5.5.1.2.4 Adding PSK Entries

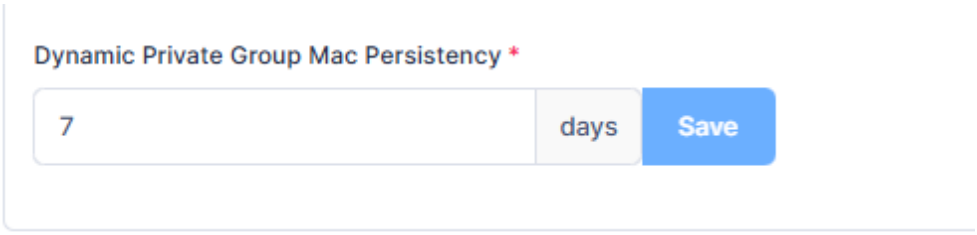
Customizing the Dynamic PGPSK profile also allows you to add more PSK entries to the profile. On the Customize Dynamic Private Group PSK screen, click on **Add more entries**. The Create PSK Item screen appears.



Complete the fields as described in Manually Configure a PSK Entry (see page 752). Click on **Add more entries** to add another PSK entry. When you are done adding one or more entries, click on **Save**. The new PSK entries are then added to the Dynamic PGPSK profile.

7.5.5.1.2.5 Changing the MAC Persistency Duration

On the Customize Dynamic Private Group PSK screen, you can also change the MAC Persistency duration value. By default, the duration is set to one day. You can specify a maximum duration up to 365 days maximum.

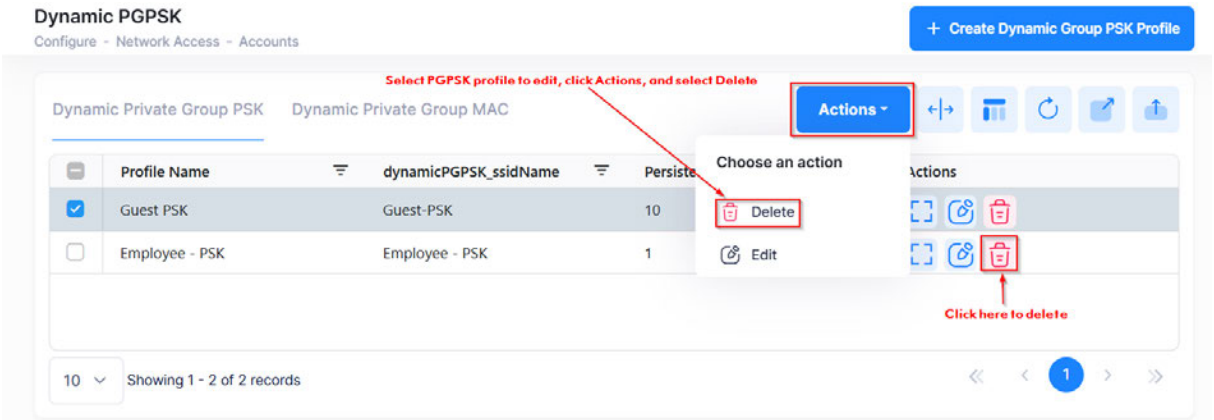


If you want to change the number days for the Dynamic Private Group MAC Persistency, enter the number of days and click on **Save**.

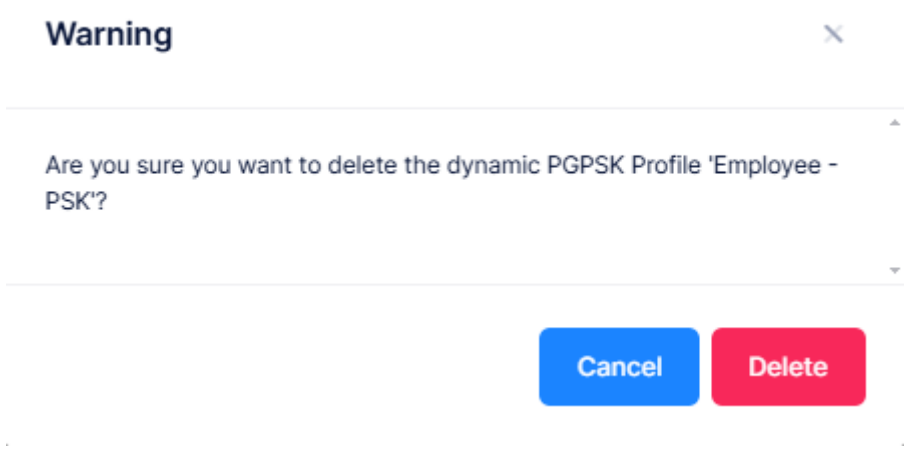
7.5.5.1.3 Deleting a Dynamic Private Group PSK Profile

To delete a Dynamic Private Group PSK profile, use one of the following methods to select the profile that you want to delete:

- Select the Dynamic Private Group PSK profile to delete by clicking on the checkbox next to the profile, click on **Actions**, then select **Delete** from the drop-down menu.
- Click on the delete icon under the “Actions” column next to the profile that you want to edit.



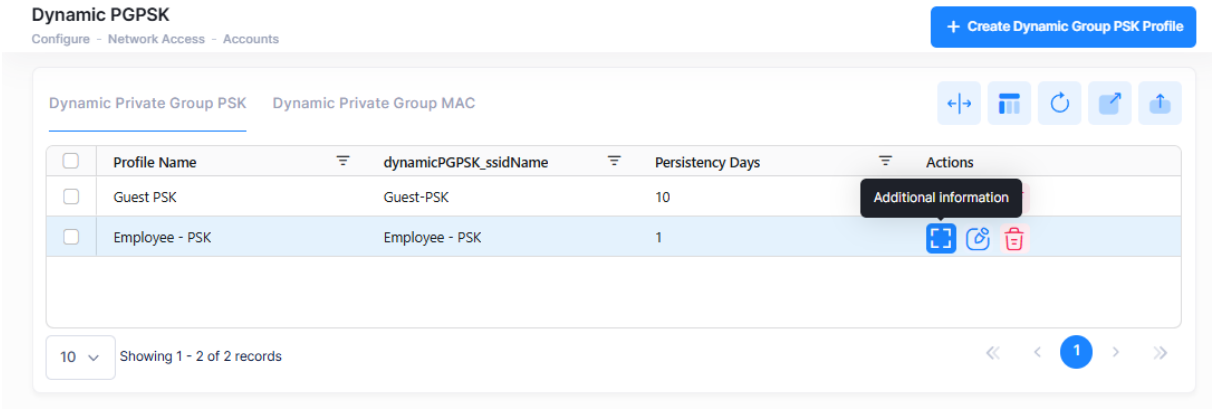
When you select the profile that you want to delete, the following confirmation pop-up appears:

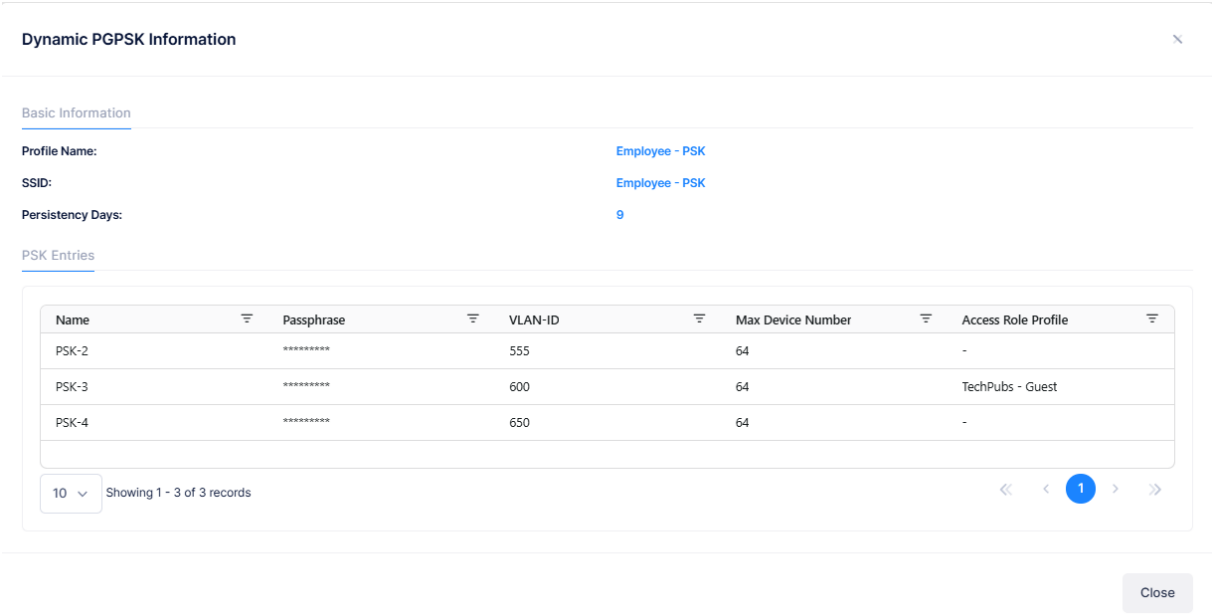


Click **Delete** to confirm that you want to delete the selected Dynamic Private Group PSK profile.

7.5.5.1.4 Display Dynamic PGPSK Profile Information

The Dynamic Private Group PSK (PGPSK) list displays information for the configured Dynamic PGPSK profiles. To display detailed information about a specific profile, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



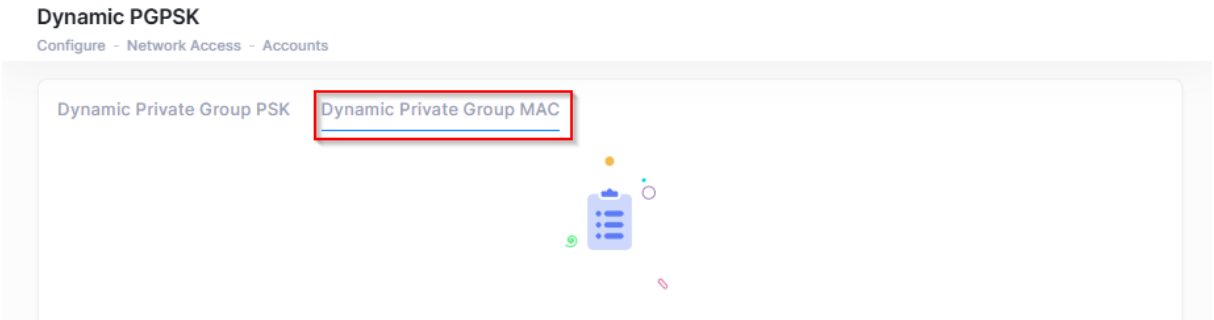


The following information is displayed for each Dynamic PGPSK profile:

- **Profile Name** - The unique name assigned to the profile.
- **SSID** - The name of the SSID assigned to the profile. Note that only SSIDs with the Dynamic Private Group PSK option enabled are available to assign to a profile.
- **Persistency Days** - The number of persistency days for the profile.
- **PSK Entries** - The PSK entries configured for the Dynamic PGPSK profile.

7.5.5.2 Using the Dynamic Private Group MAC Tab

The Dynamic Private Group PSK MAC tab provides a list of devices connected through UPAM PSK authentication. Use this tab to view devices that matched one of the passphrase entries in a Dynamic PGPSK profile. You can also delete and export Dynamic Private Group PSK MAC entries.



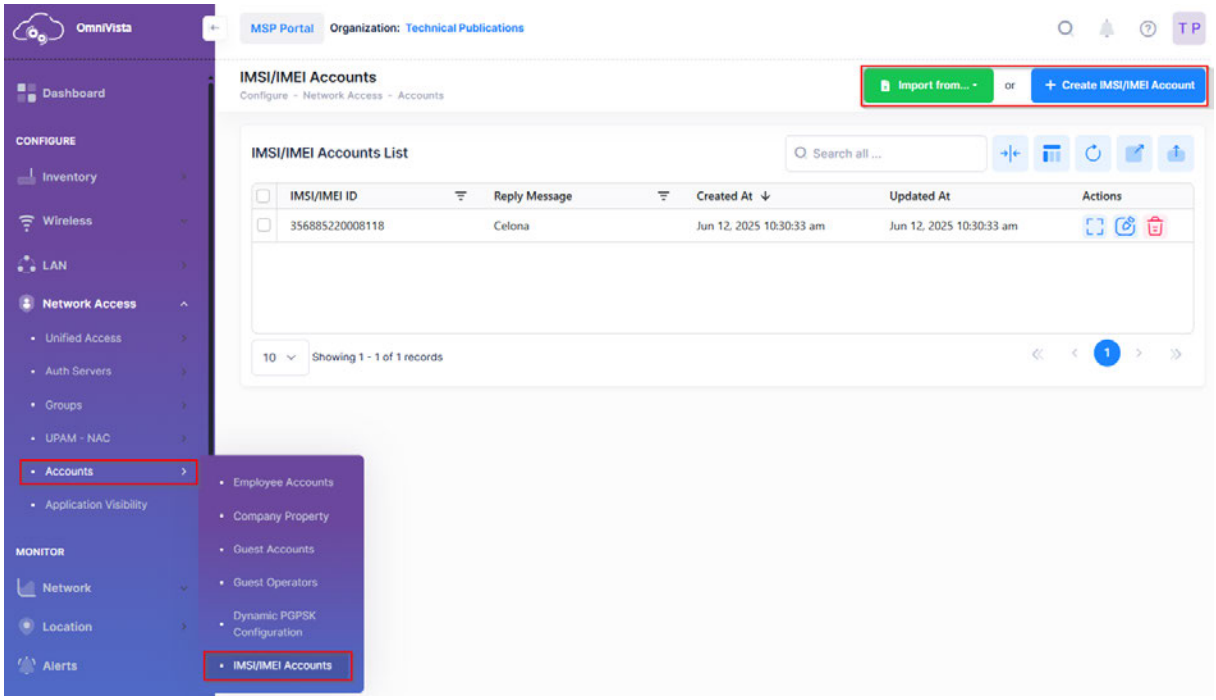
The Dynamic Private Group MAC Persistency (see page 751) setting configured for the PSK entry to which the device matched determines how long the MAC address remains in the Dynamic Private Group MAC database. During this time, the user will not have to enter the passphrase again to gain network access.

21 Oct 2025

7.5.6 IMSI/IMEI Accounts

UPAM integration with the Celona Private Wireless solution is implemented through configuration of an Access Policy with the IMSI/IMEI database selected as the Authentication Source. The Celona Edge first performs user authentication based on Sim. The users are then authorized by validating that the SIM card (IMSI) or the device (IMEI) has a corresponding entry in the UPAM IMSI/IMEI database.

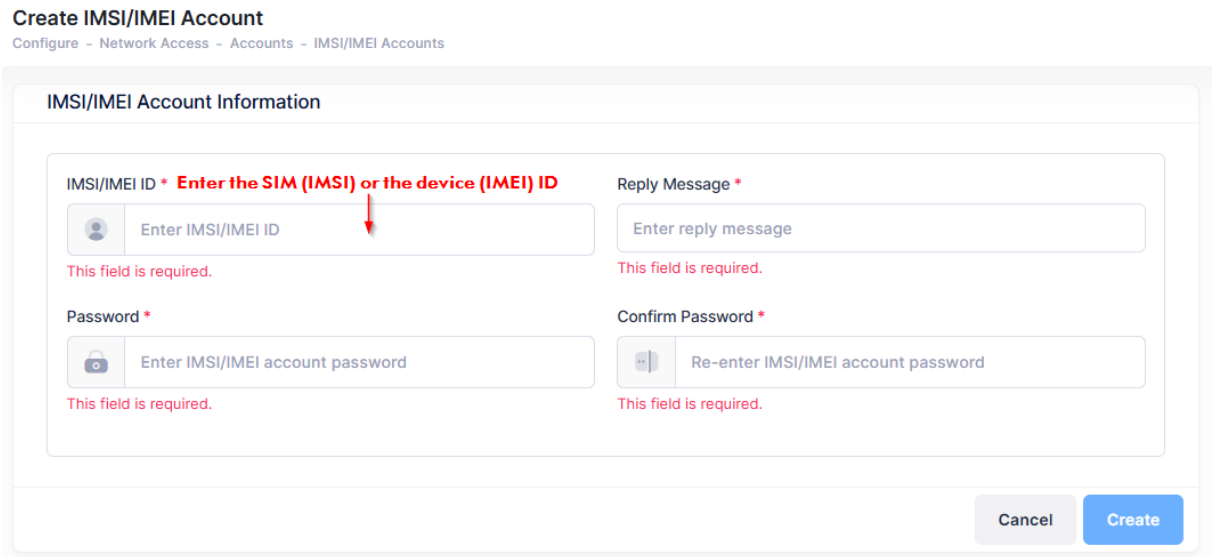
The IMSI/IMEI Accounts screen displays (see page 765) information about all of the configured IMSI/IMEI accounts in the UPAM database. This screen also allows you to create (see page 761), edit, and delete (see page 764)accounts. To access the IMSI/IMEI Accounts screen, click on **Network Access > Accounts > IMSI/IMEI Accounts** under the “Configure” section of the OmniVista Terra Menu (see page 45).



7.5.6.1 Creating an IMEI/IMSI Account

There are two methods for creating IMEI/IMSI Accounts for Celona device authorization: Import an Excel XLSX file (see page 762) with multiple IMEI/IMSI entries or manually create an account.

To manually add a new IMEI/IMSI Account, click on **Create IMEI/IMSI Account** to display the Create IMSI/IMEI Account screen.

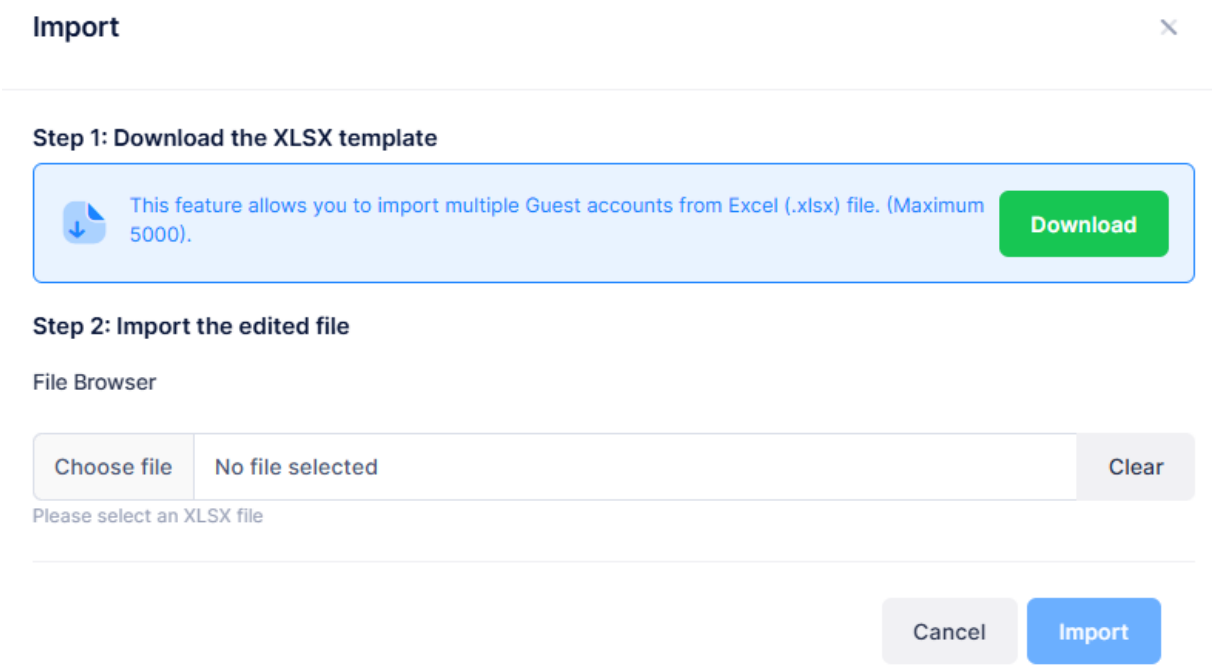


Complete the IMSI/IMEI Account Information as described below, then click **Create**.

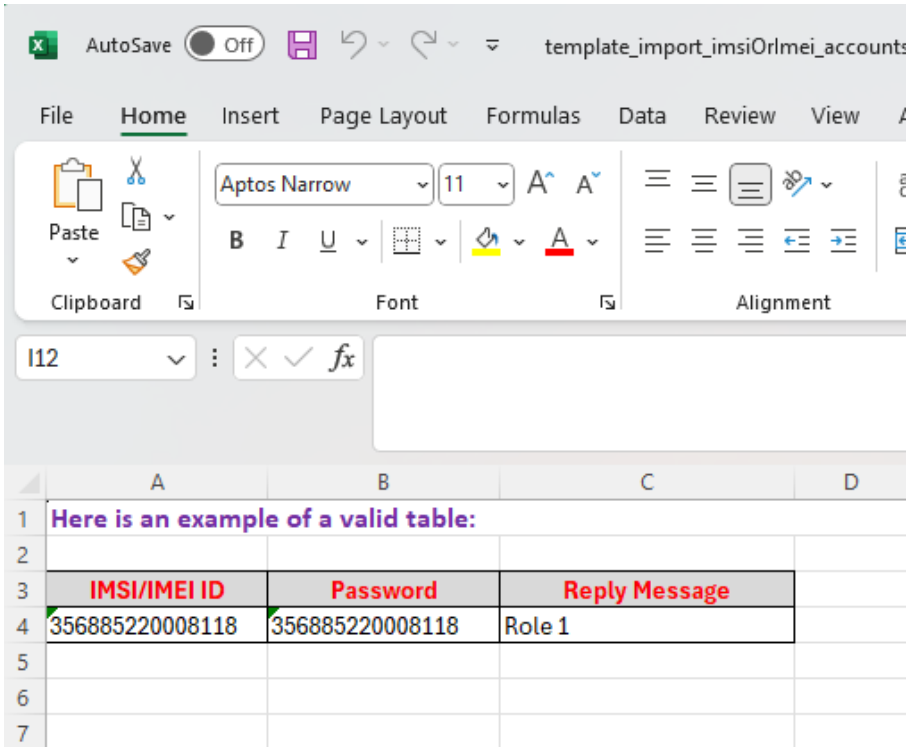
- **IMSI/IMEI ID** - Enter the SIM (IMSI) or the device (IMEI) ID for the Celona device.
- **Reply Message** - Enter the name of the Celona Role Profile to which the device is assigned for network access.
- **Password** - Enter the user password for the account.
- **Confirm Password** - Enter the user password again to confirm.

7.5.6.1.1 Import Multiple User Accounts from an Excel Sheet

To import multiple IMSI/IMEI accounts from an existing Excel sheet (.xlxs), click on **Import from…** and select **XLSX template file**. You will then be prompted to download an XLSX template file that contains steps on how to define the IMSI/IMEI account in the Excel file to create multiple accounts.



Step 1: Click on **Download** and specify where you would like to save the template file. When you open the template file, an example shows how to define each IMSI/IMEI account that you want to add to the UPAM database.



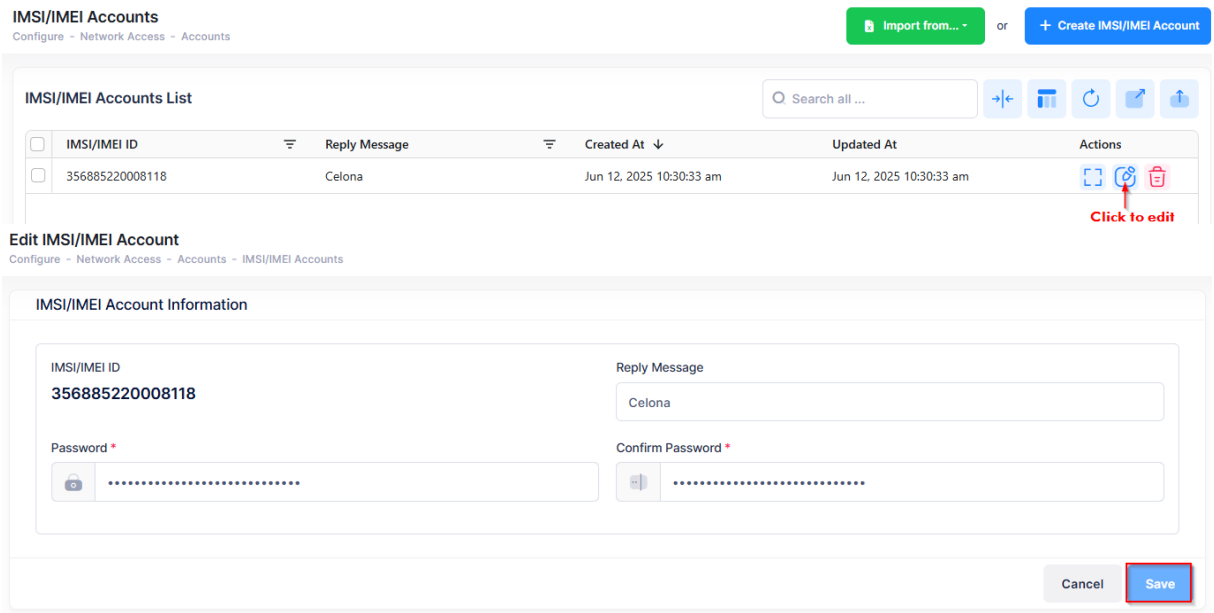
Step 2: Import the edited file

- **File Browser** - Click in this field to find and select the existing template file to import.

Once the Import form is complete, click on **Import**. The IMSI/IMEI Account list is populated with the imported IMSI/IMEI Accounts.

7.5.6.2 Editing an IMSI/IMEI Account

To edit an IMSI/IMEI Account, click on the Edit icon under the “Actions” column next to the account entry. The Edit IMSI/IMEI Account screen appears.

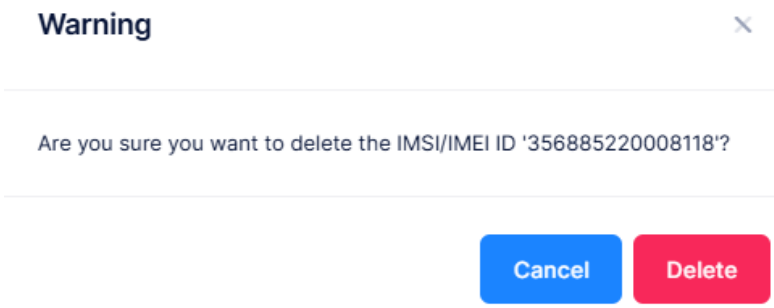


Edit the fields as described above (see page 761), then click on **Save**.

> Note that you can only change the value of the “Reply Message” and “Password/Confirm Password” fields; you cannot change the value of the “IMSI/IMEI ID” field.

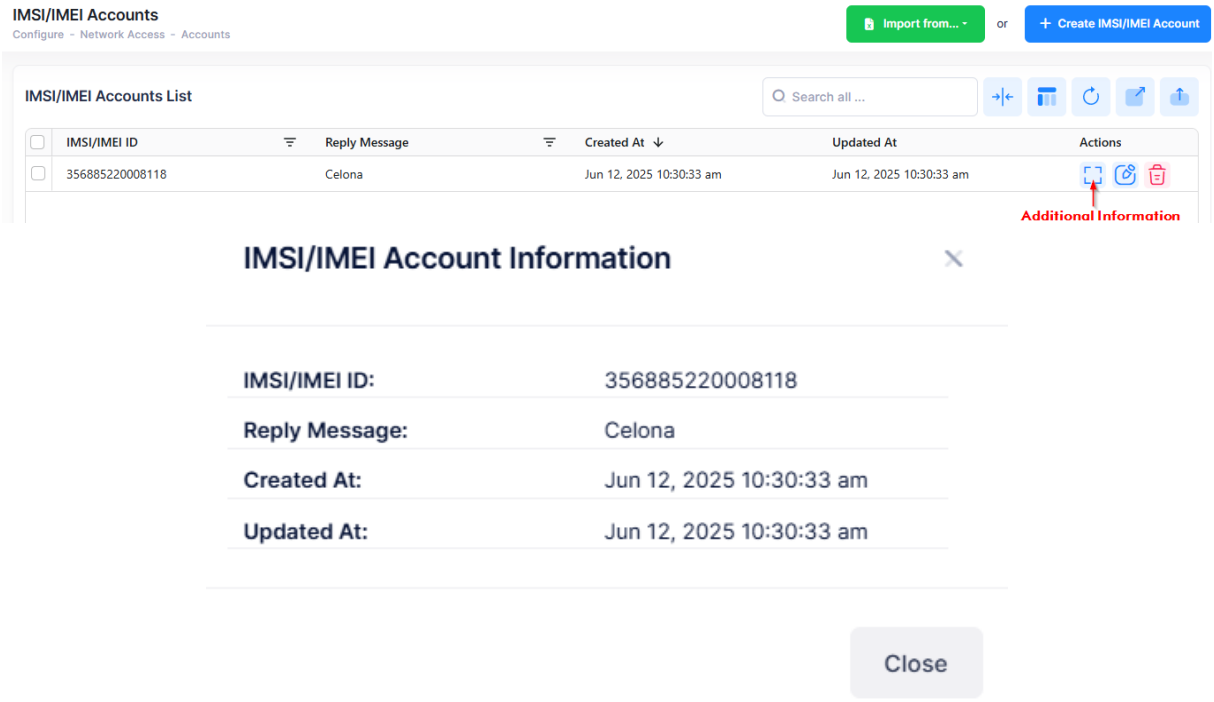
7.5.6.3 Deleting an IMSI/IMEI Account

Select an IMSI/IMEI Account from the list and click on the **Actions** button and select Delete from the drop-down menu, or click on the Delete icon under the “Actions” column. When the following confirmation prompt appears, click on **Delete** to delete the account.



7.5.6.4 Display IMSI/IMEI Account Information

The IMSI/IMEI Accounts list displays information for the configured IMSI/IMEI accounts. To display detailed information about a specific account, click on the Additional Information icon under the “Actions” column. The information displayed on this screen is defined below.



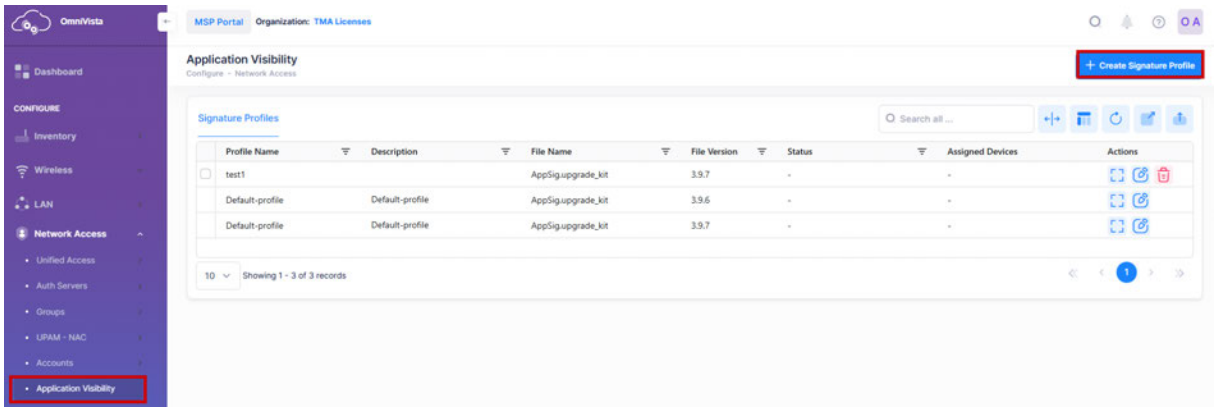
- **IMSI/IMEI ID** - The SIM (IMSI) or the device (IMEI) ID for the Celona device.
- **Reply Message** - The name of the Celona Role Profile to which the device is assigned for network access.
- **Created At:** - The date and time the account was created.
- **Updated At:** - The date and time the account information was updated.

21 Oct 2025

7.6 Application Visibility Signature Profiles

The Application Visibility Signature Profiles Screen displays all configured Signature Profiles and is used to create (see page 766), edit (see page 768) and delete (see page 770) profiles. Signature Profiles are created from a Signature File, which contains Application Signature information for individual applications/protocols as well application groups (pre-configured groups of related applications/ protocols).

To create an Application Visibility Signature Profile, navigate to the Application Visibility screen by clicking on **Network Access > Application Visibility** under the “Configure” section of the OmniVista Terra Menu (see page 45). The Application Visibility Signature Profiles screen displays.

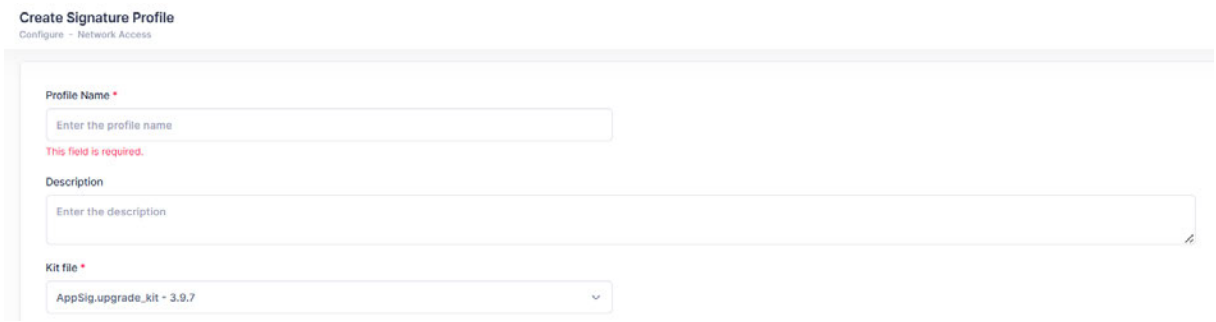


7.6.1 Creating a Signature Profile

Signature Profiles are created from a Signature File, which contains application signature information for individual applications/protocols and application groups. You create a Signature Profile by selecting one or more applications/application groups (or creating a custom group) that contain the applications/protocols you want to monitor/control. You then assign the Signature Profile to Access Points. Multiple Signature Profiles can be created from a single Signature File, each containing a different combination of applications/application groups. And a Signature Profile can be assigned to one or more Access Points. However, an Access Point can be assigned to only one Signature Profile.

To access this screen, click on **Create Signature Profile**, the following screen appears. The Create Signature Profile screen provides the following step-by-step process for creating a Signature Profile:

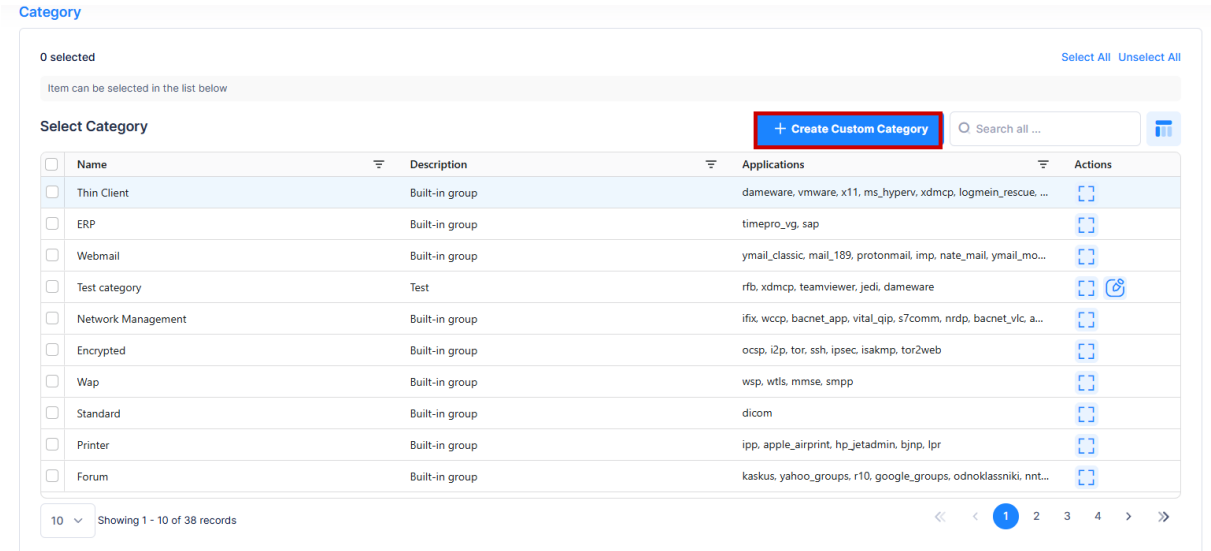
1. **Name and Description**



- **Profile Name -** Enter a Profile Name. Enter a name describing the profile you are creating.

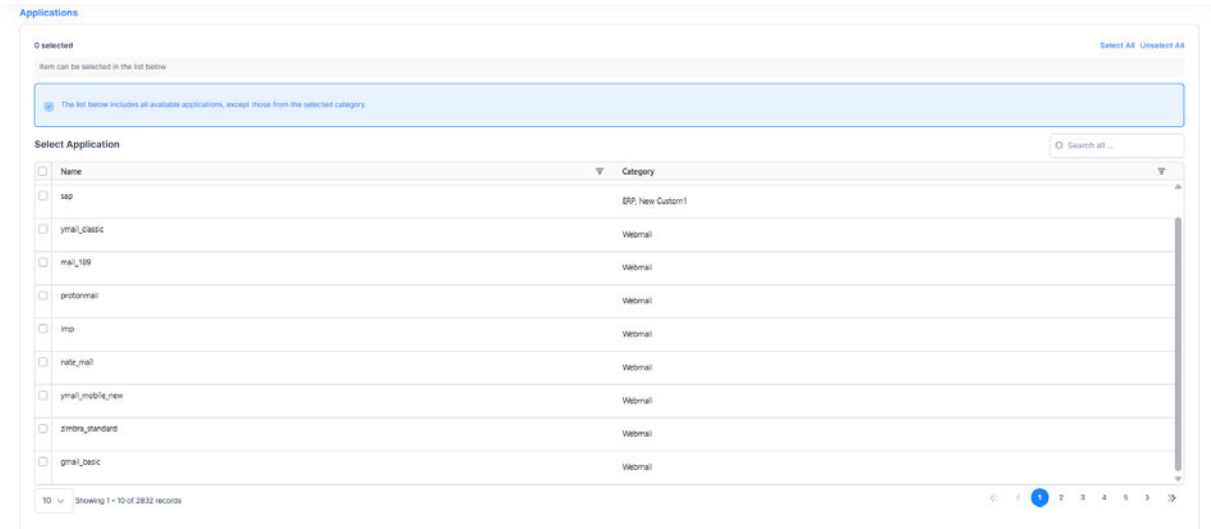
- **Description** - Enter a profile description.
- **Kit file** - Select a Signature File. Access Points use the AppSig.upgrade_kit Files. You can only select one Signature File at a time.

2. **Category**



This tab is used to select the Category of the Applications from the available list of Categories. Select the Category of the applications you want to include in the profile. You can also **Create Custom Category** by selecting the applications of your own choice.

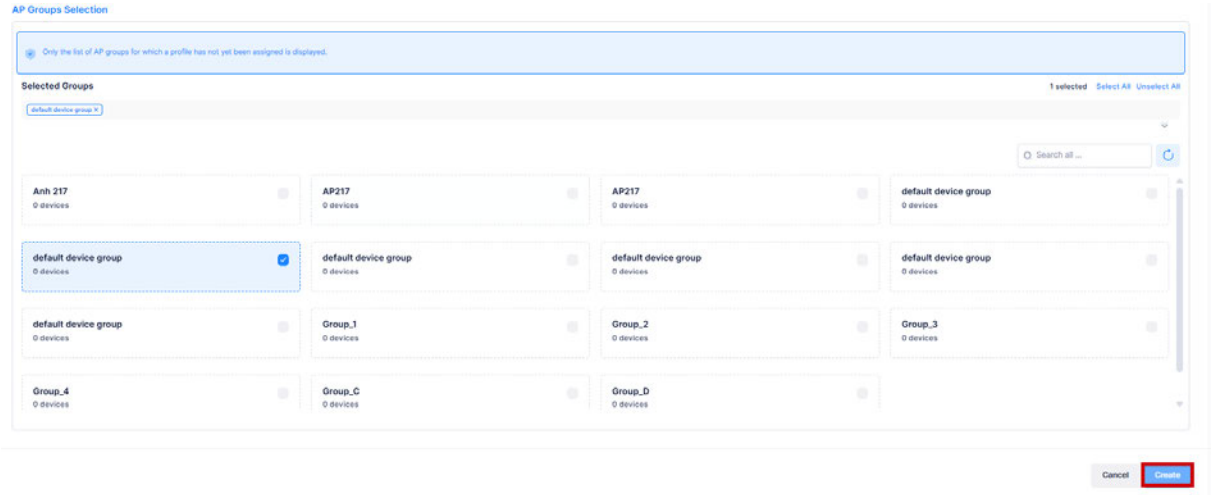
3. **Applications**



This tab is used to select Monitoring Applications from the available list of Applications you want to include in the profile. You can also add multiple Applications.

Note: The list only includes Applications that were not selected in the previous Select Category.

4. **AP Group Selection**



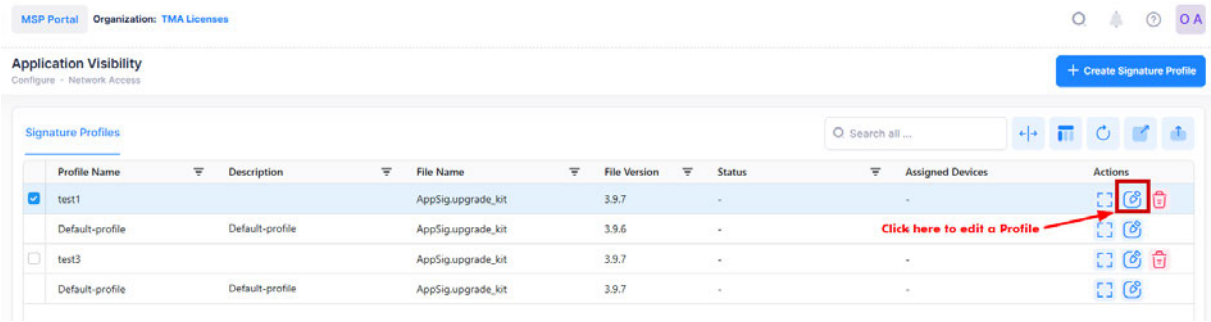
This tab is used for **AP Group Selection**, from the available list of AP Groups. You can Select the groups you want to include in the profile by clicking on the select button.

Note: The list of only those AP groups for which the profile is not been assigned yet will be displayed for selection.

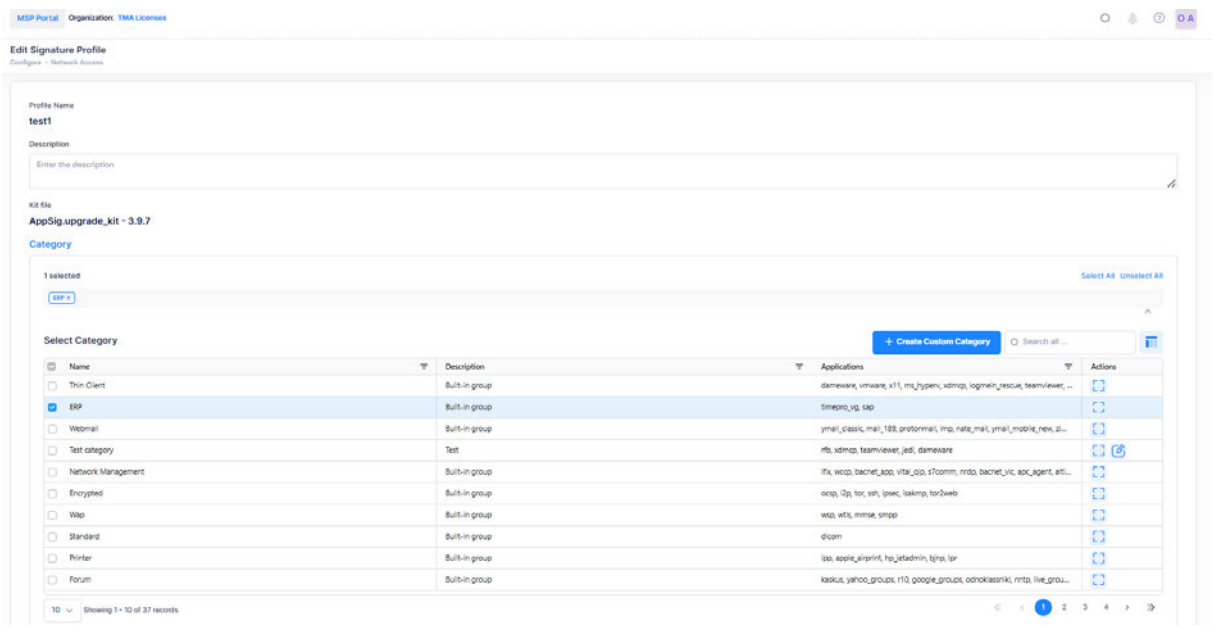
Now you can click on the **Create** button to create a Signature Profile.

7.6.2 Editing a Signature Profile

You can edit the parameter values for an existing Signature Profile by accessing the Edit Signature Profile screen. Click on the pencil icon under the “Actions” column next to the profile that you want to edit.



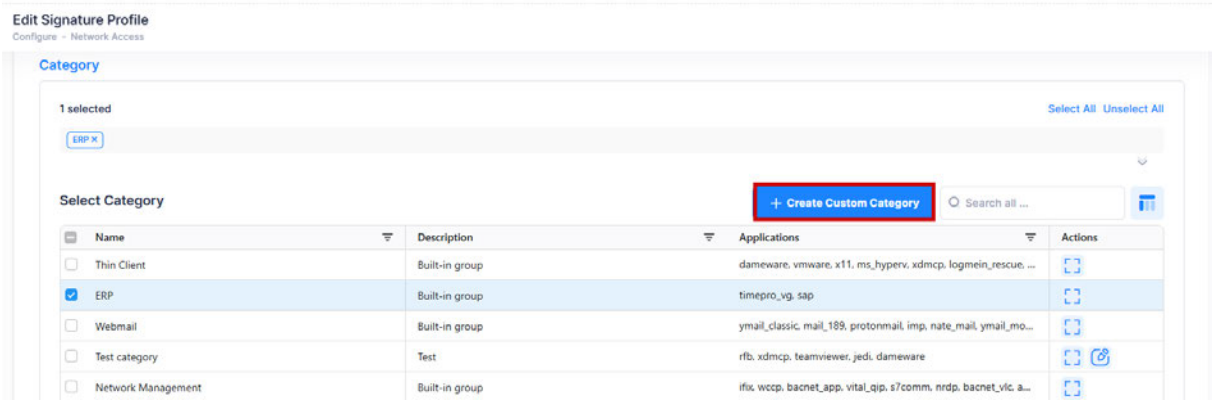
The following Edit Signature Profile screen displays. Edit the fields as described above, then click on **Save**.



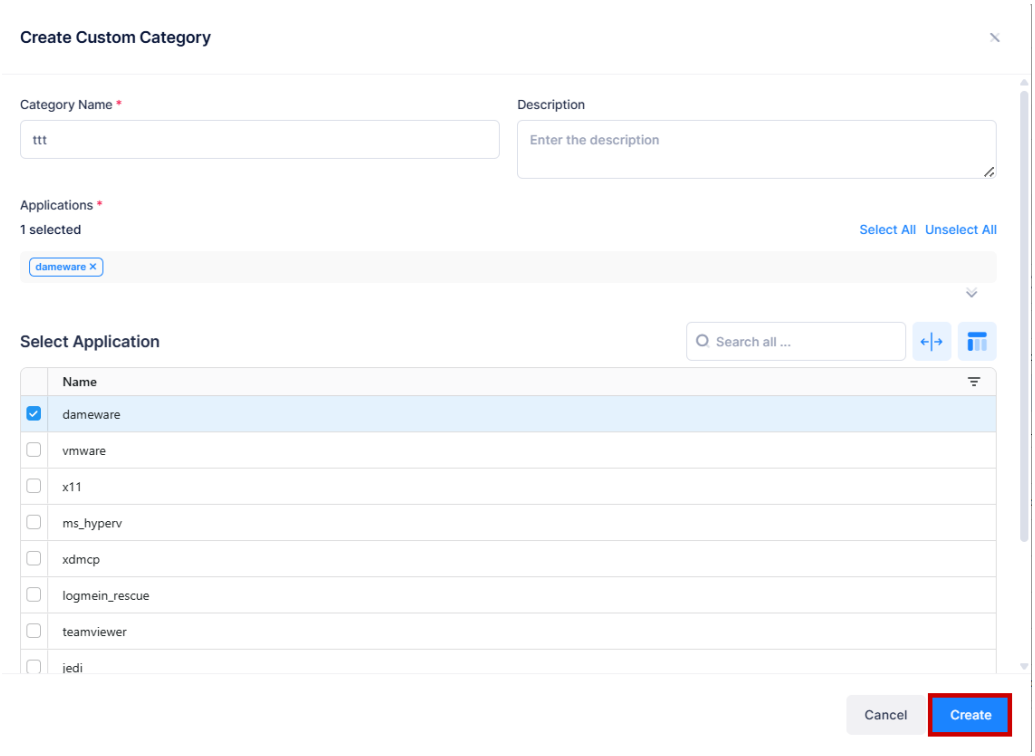
Note: The default Signature Profile cannot be modified. Therefore, you cannot remove the Application groups from the default selected list. You can only attach the devices to Default Profile.

7.6.2.1 Create Custom Category

You can customize the Category value by clicking on **Create Custom Category** while editing a Signature Profile as shown below:



The following screen will appears:



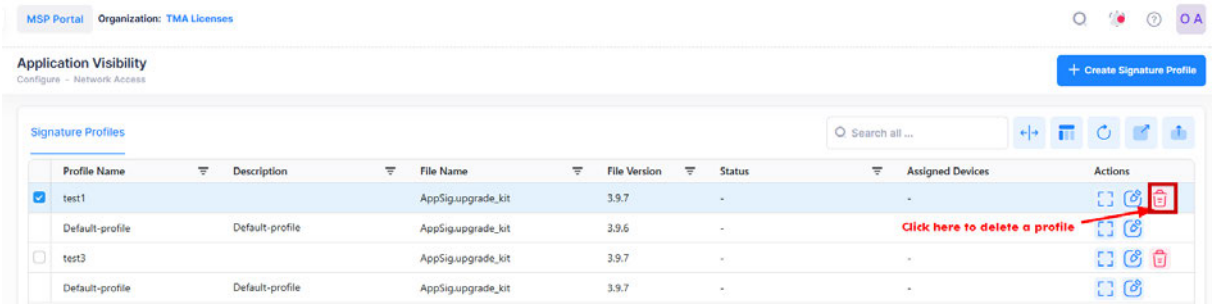
Edit the fields as described below, then click on **Create**.

- **Category Name** - Enter a name to the Category of Applications.
- **Description** - Enter a description for the Category.
- **Select Application** - Select the Applications from the available list to add in the Category list.

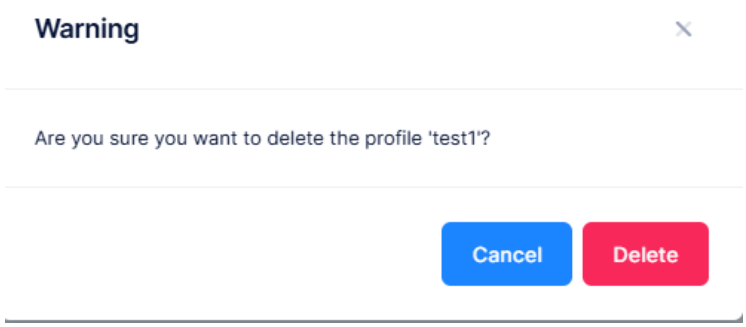
- Creating duplicate Categories is not allowed, therefore one or more Categories cannot contain the same list of Applications.
- A Custom Category, once created, is visible when Signature Profiles are created for the entire Organization.
- A Custom Category cannot be deleted, but it can be updated.

7.6.3 Deleting a Signature Profile

To delete Signature Profile, select the profile you want to delete, click on the trash can icon under the “Actions” column next to the profile that you want to delete.



The following confirmation prompt appears:



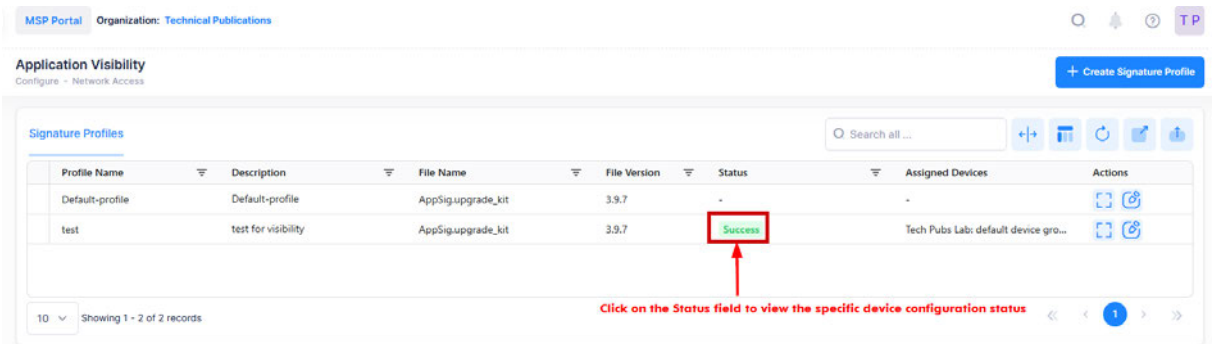
Click on **Delete** to confirm that you want to delete the Signature Profile.

Note:

- You cannot delete the existing Default Signature Profile.
- You can delete the custom Signature Profiles which are not assigned to devices.
- A Custom Signature Profile cannot be deleted if any AP groups or devices are assigned to it. To successfully delete the Profile, you must first remove any attached devices from the Profile list. Only after this step can you proceed with deleting the Profile.

7.6.4 Display a Signature Profile

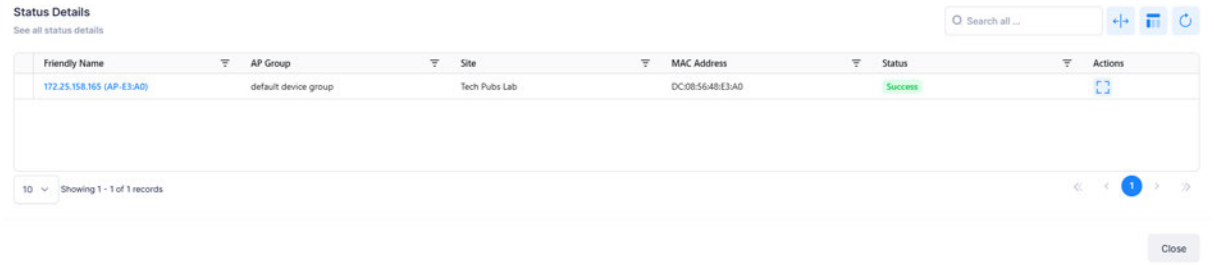
The Signature Profiles list displays information for the configured Signature Profiles. This screen also allows you to export, search and filter the data.



The following field value information will be displayed for each of the Signature Profile:

- **Profile Name -** The name of the profile assigned to the device.
- **Description -** A description for the profile.
- **File Name -** The name of the Signature File used in the profile.
- **File Version -** The file version of the Signature file used in the profile.
- **Status** - .The status of the profile(Success, fail or partial).
- **Assigned Devices -** List of the network devices to which the profile has been assigned.

To view the Device specific configuration status, click on the “Success” tab under the **Status** field. The following screen appears:



Note: Applications/Categories traffic is monitored using the Advanced Analytics section. To view statistics on Applications/Categories you have configured in a profile, go to the Application Visibility (see page 862) Screen. (**Monitor > Network > Analytics > Application Visibility**). Once you configure a profile and assign it to Access Points, the statistics for the Applications/Categories in the profile are displayed in graphical and table format.

21 Oct 2025

8 Monitoring Network Device Activity

OmniVista Terra provides the following applications and tools under the “Monitor” section of the OmniVista Terra Menu (see page 45) to help you monitor network components and device activity:

- **Network Analytics** (see page 774) - Analyze network metrics, generate reports on network utilization, review access records, and define custom dashboards to monitor specific metrics.
- **Location** (see page 943)- Use Wi-Fi heatmaps to design, verify, and troubleshoot installed Stellar Wi-Fi networks.
- **Alerts** (see page 948) - Monitor and analyze alerts received from network devices.
- **Diagnostic Tools** (see page 969) - Analyze network events, connect to devices, and collect log file information from network devices.

21 Oct 2025

8.1 Network Analytics

The following group of Network Analytics applications are accessed by clicking on the **Network** option under the “Monitor” section of the OmniVista Terra Menu (see page 45):

- Analytics (see page 775)
- Access Records (see page 878)
- Topology (see page 910)
- Analytics Reports and Custom Dashboards (see page 924)

21 Oct 2025

8.1.1 Advanced Analytics

OmniVista Terra provides the following advanced analytics to monitor and enhance the Wi-Fi user experience:

- Quality of Experience (QoE) Analytics (see page 776)
- Network Analytics (see page 789)
- Monitor WIPS Analytics (see page 818)
- Monitoring the Clients (see page 826)
- Monitoring Client Analytics (see page 846)
- Client Block List (see page 858)
- Application Visibility (see page 862)
- RF Details (see page 870)
- Network Analytics Summary (see page 873)

21 Oct 2025

8.1.1.1 Monitor QoE Analytics

Monitoring QoE analytics allows you to evaluate the actual end-user experience on the network.

OmniVista Terra provides six metrics to be monitored: **Successful Connects**, **Time To Connect**, **Roaming**, **Coverage, Available Capacity** and the **Device Uptime**. The information in this section describes how to utilize the following OmniVista Terra advanced analytics to monitor and evaluate the actual end-user experience on the network.

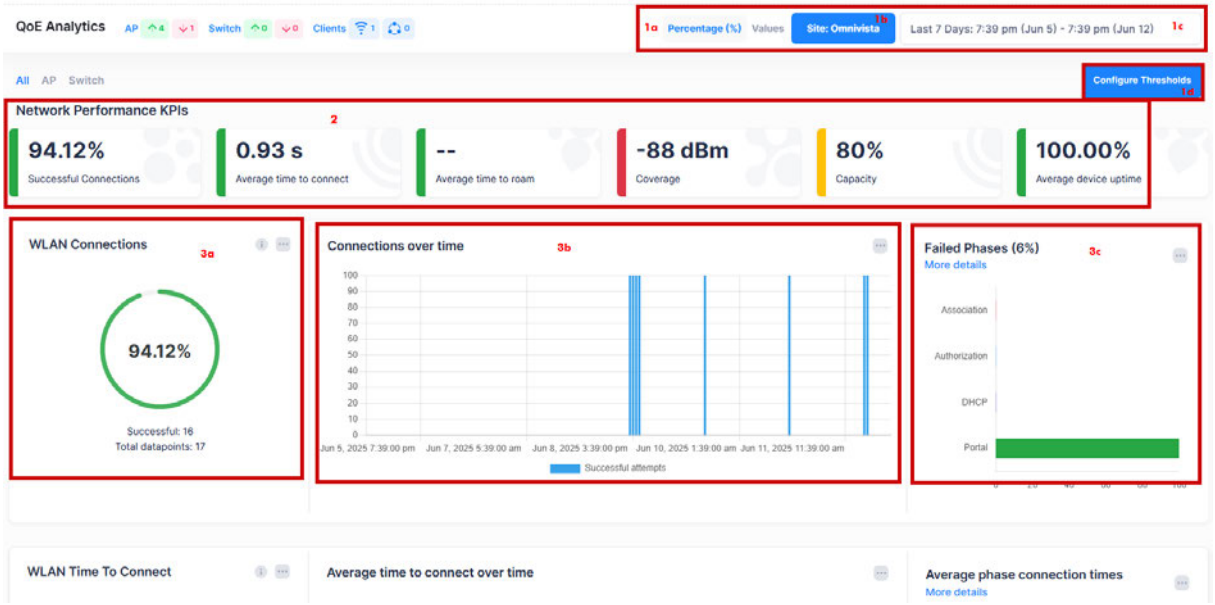
- Successful Connects
- Time To Connect (see page 781)
- Roaming (see page 782)
- Coverage (see page 783)
- Available Capacity (see page 784)
- Device Uptime (see page 785)
- Switch QoE (see page 786)
- QoE Metric Failures (see page 787)

21 Oct 2025

8.1.1.1.1 The QoE Dashboard

The QoE Dashboard is used to examine the overall QoE metric values for a specific set of Devices defined in a selected scope (for example, entire Organization, Sites, Buildings, Floors, or Access Points).

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switch Up and Switch Down Count in the Network.



The QoE Dashboard is divided into three different sections:

1. **The filter and actions section**: This section allows you to:
   a. Select the format of the data to be displayed: Percentage or Real Values.
   b. Select the scope of Devices for which you want to retrieve the QoE attribute values.
   c. Select the Time window during which you want to analyze the QoE attribute values.
   d. Configure the QoE Thresholds: for certain QoE attributes, you can adjust the threshold to match your expectations.
2. **The Network performance KPIs section**: This section allows you to take a quick look at the overall QoE attributes performance index.
3. **The QoE attributes detail section**: If you want to go deeper into the analysis of each QoE attribute value, you can scroll down to reach the QoE attribute details view. For each QoE attribute, three elements are available:
   a. **A large counter widget** representing the percentage of success reached for the QoE attribute compared to the threshold (if any).
   b. **A bar chart widget** representing the evolution of the QoE attribute value over time.
   c. **A Failed Phases bar chart widget** representing the categorization of the failures that occurred. (Not counted as a success case).

Use the QoE Dashboard to:

- Configure QoE Thresholds (see page 779)
- Understand the Successful Connects QoE Metric (see page 780)
- Understand the Time-to-Connect QoE Metric (see page 781)
- Understand the Roaming QoE Metric (see page 782)
- Understand the Coverage QoE Metric (see page 783)
- Understand the Available Capacity QoE Metric (see page 784)
- Understand the Device Uptime QoE Metric (see page 785)
- Understand Switch QoE Metric (see page 786)
- Analyze QoE Metric Failures (see page 787)

QoE metrics data is retained for 30 days.

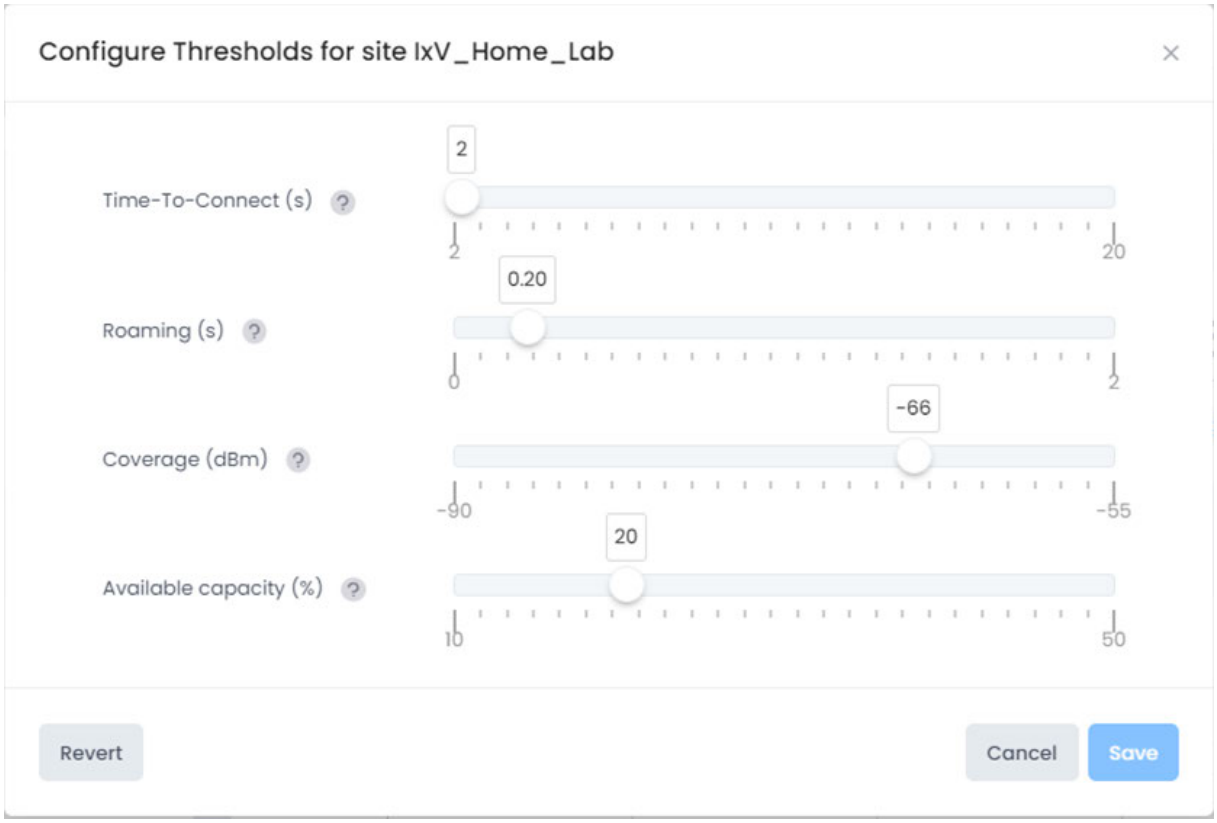
21 Oct 2025

8.1.1.1.2 Configure QoE Thresholds

QoE metrics are computed based on Threshold values configured at the Site level.

To change a threshold value, just click on the **Configure Thresholds** button on the QoE dashboard. This will open a modal window from which you can configure the threshold values for each of the following QoE metrics:

- **Time-to-Connect:** From 2 to 20s. Default: **2s**
- **Roaming**: From 0.2 to 2s. Default: **0.2s**
- **Coverage**: From -90 to -55dBm. Default: **-66dBm**
- **Available Capacity**: From 10 to 50%. Default: **20%**

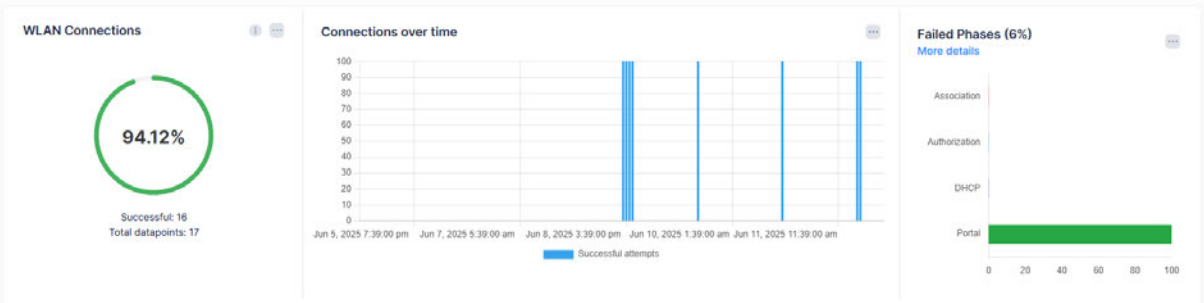


21 Oct 2025

8.1.1.1.3 Understanding the WLAN Successful Connections Metric

The “WLAN Connections” QoE metric indicates the number of connections **that succeeded in passing all the Authorization, Association, DHCP, and Portal phases** when a client connects to an Access Point.

There is no threshold value applied to this QoE metric, as it is just a counter that increases over time.



The “WLAN Connections” metric tracks failures in the following four phases:

- **Association** - Once authentication is complete, clients can associate with an Access Point for full network access. Association allows the Access Point to register each client so that frames are delivered correctly.
- **Authorization -** The phase during which the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected).
- **DHCP** - The phase where clients obtain a DHCP lease for an IP address, a subnet mask, and various DHCP options from DHCP servers in a four-step process:
  a. **DHCP DISCOVER:** The client broadcasts a request for a DHCP server.
  b. **DHCP OFFER:** DHCP servers on the network offer an address to the client.
  c. **DHCP REQUEST:** The client broadcasts a request to lease an address from one of the offering DHCP servers.
  d. **DHCP ACK:** The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.
- **Portal** - The failure occurred in the Captive Portal phase.

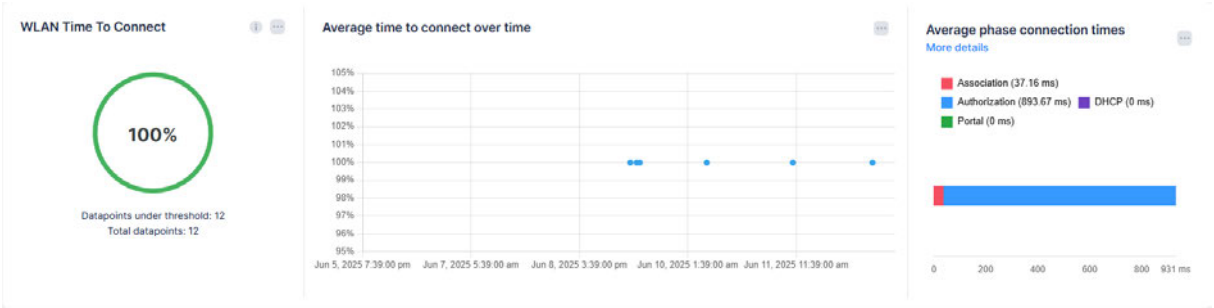
21 Oct 2025

8.1.1.1.4 Understanding the WLAN Time-to-Connect Metric

The “WLAN Time-to-Connect” QoE metric represents the sum of the times you need to pass each connection phases successfully.

There are four phases of connection: **Association, Authorization, DHCP,** and **Portal Authorization**. If the total time to connect takes longer than the selected threshold, the connection will be considered as a failure (failure to reach the goal). In this case, the phase that took longer than usual will be designated as the cause of the failure.

The threshold can be configured from 2s to 20s. The default threshold value is 2s.



The “ Average phase connection times” metric tracks failures in the following four phases:

- **Association -** Once authentication is complete, clients can associate with an access point for full network access. Association allows the Access Point to register each client so that frames are delivered correctly.
- **Authorization -** This phase refers to the phase in which the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected).
- **DHCP -** The DHCP phase refers to the phase where clients obtain a DHCP lease for an IP address, a subnet mask, and various DHCP options from DHCP servers in a four-step process:
  a. **DHCP DISCOVER:** The client broadcasts a request for a DHCP server.
  b. **DHCP OFFER:** DHCP servers on the network offer an address to the client.
  c. **DHCP REQUEST:** The client broadcasts a request to lease an address from one of the offering DHCP servers.
  d. **DHCP ACK:** The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.
- **Portal Authorization -** The failure occurred during the Captive Portal Authorization phase.

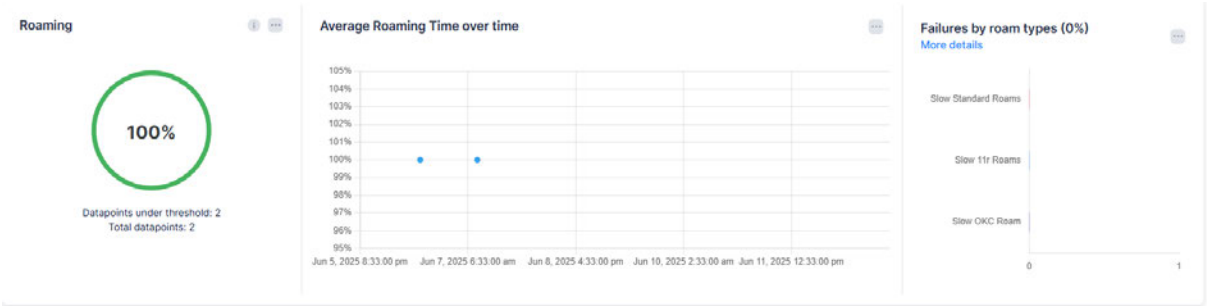
21 Oct 2025

8.1.1.1.5 Understanding the Roaming Metric

The “Roaming” QoE metric represents the percentage of successful roams between two Devices for clients within the defined threshold.

> A client decides to roam when it detects a better signal from a new Access Point compared to the one it is currently associated with. This behavior is normal, especially for mobile devices such as laptops, tablets, and mobile phones.

The threshold (which is the max target time it takes for a client to roam) can be configured from 0.2s to 2s. The default threshold value is 0.2s.



The “Roaming” metric tracks failures depending on the roaming technology used by the client:

- **Slow Standard Roams** - For PSK and Open Access clients.
- **Slow 11r Roams** - 802.11r is a standards-based fast roaming technology, supported by Apple iOS devices and some Android devices, that is leveraged when using a secure SSID. Learn more.
- **Slow OKC Roams** - OKC (Opportunistic Key Caching) is a technique available for authentication between multiple Access Points in a network where those Access Points are under common administrative control. Using OKC, a client who roams to any other Access Point in the network will not have to complete a full authentication exchange, but will instead just perform the four-way handshake to establish transient encryption keys.

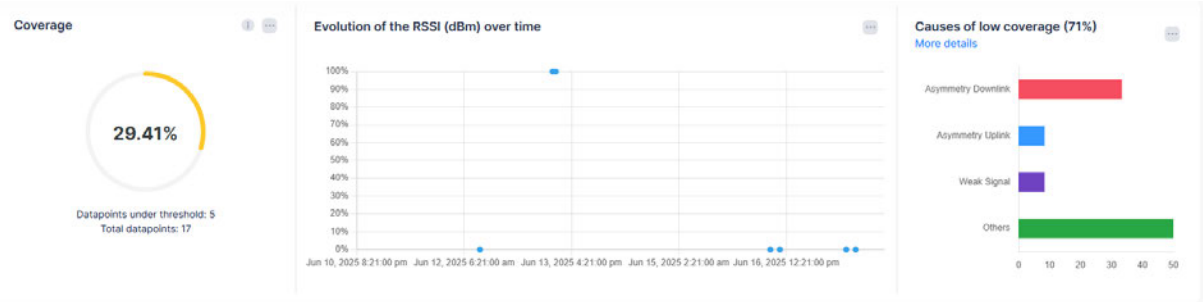
21 Oct 2025

8.1.1.1.6 Understanding the Coverage Metric

The “Coverage” QoE metric represents the percentage of time where the client signal is above the defined threshold.

When the client signal doesn’t reach the configured threshold value, the failure is classified among the list of classifiers: **Asymmetry Downlink, Asymmetry Uplink, Weak Signal,** or **Others.**

The threshold can be configured from -90 dBm to -55 dBm. The default threshold value is -66 dBm.



The “Coverage” metric tracks the following four kinds of failures:

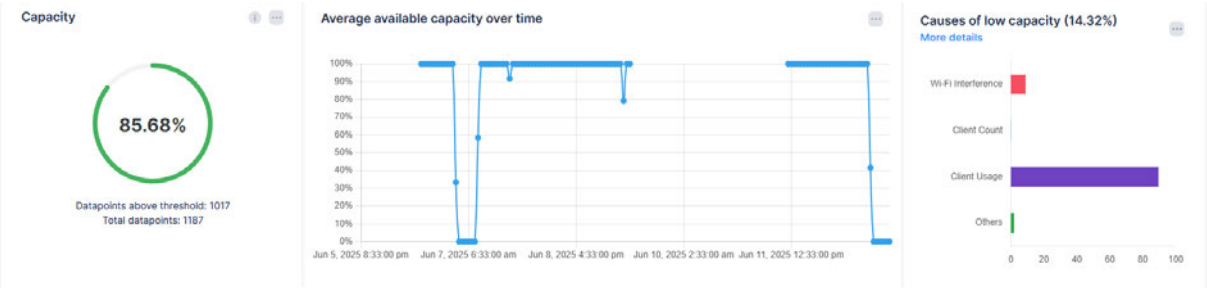
- **Asymmetry Downlink -** The failure is classified as an Asymmetry Downlink if any signal below -75dBm and the transmit power (txPower) of the Access Point is too weak from the transmit power of the Client.
- **Asymmetry Uplink -** The failure is classified as an Asymmetry Uplink if any signal below -75dBm and the transmit power (txPower) of the client is too weak from the transmit power of the Access Point.
- **Weak Signal -** any signal below -75dBm that doesn’t classify to Asymmetry Downlink and Asymmetry Uplink is classified as a Weak Signal failure.
- **Others -** any other records above -75dBm and below the configured threshold. (Note: If you put the threshold below -75 dBm, you will never get any failure classified as Others, they will be classified as Weak Signal first.)

21 Oct 2025

8.1.1.1.7 Understanding the Available Capacity Metric

The “Available Capacity” QoE metric tracks the percentage of time the available RF channel capacity was greater than the defined threshold.

The threshold can be configured from 10% to 50%. The default threshold value is 10%.



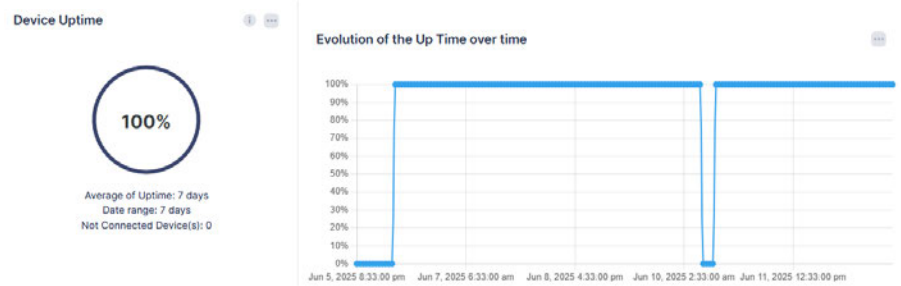
The “Available Capacity” metric tracks the following four kinds of causes of low capacity that will be counted if the Available Capacity starts to be less than the configured threshold:

- **Wi-Fi Interference -** One record is classified as a Wi-Fi Interference when the experienced capacity is below the configured threshold and the number of the Interfering Access Points is greater than 30 for the Access Point on which the client is currently connected to.
- **Client Count -** One record is classified as a Client Count when the number of clients currently connected to the Access Point is over 30.
- **Client Usage -** A Client Usage failure can occur when the data usage at the Access Point level is too large.
- **Others -** A failure is tracked as Others if it was not classified to one of the other three classifiers above.

21 Oct 2025

8.1.1.1.8 Understanding the Device Uptime Metric

The Device Uptime section provides information to help monitor and evaluate Device uptime and downtime. The Device Uptime widget displays the percentage of average uptime for all Devices within the defined scope (organization, site, building, set of devices and Access Points) and time interval.

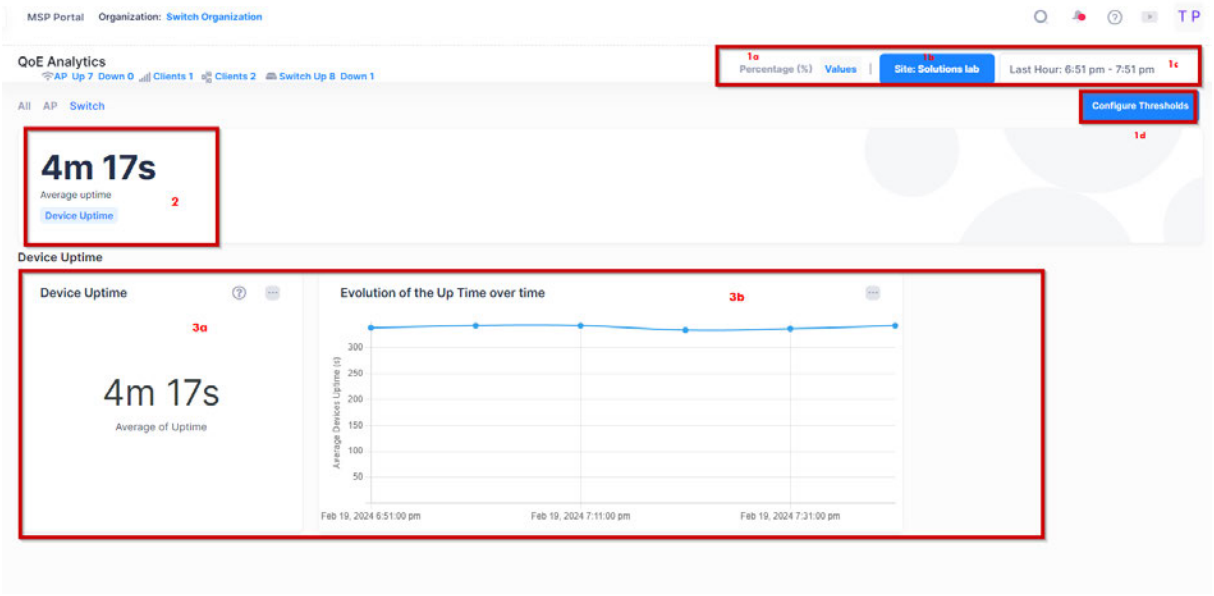


21 Oct 2025

8.1.1.1.9 Understanding Switch QoE Metric

The QoE Dashboard is used to examine the overall QoE metric values for a specific set of Switches or devices defined in a selected scope (for example, entire Organization, Sites, Buildings, Floors, or Devices).

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switch Up and Switch Down Count in the Network.



The Switch QoE Analytics Dashboard is divided into three different sections:

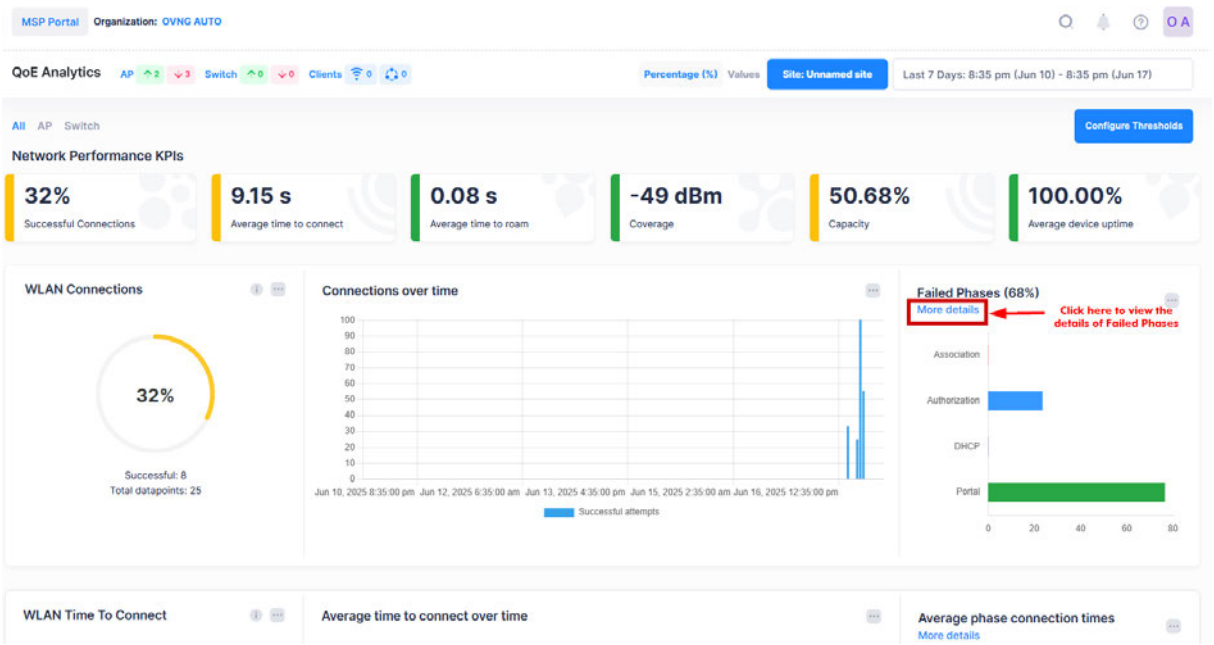
1. **The filter and actions section**: This section allows you to:
   a. Select the format of the data to be displayed: Percentage or Real Values.
   b. Select the scope of Devices for which you want to retrieve the QoE attribute values.
   c. Select the Time window during which you want to analyze the QoE attribute values.
   d. Configure the QoE Thresholds: for certain QoE attributes, you can adjust the threshold to match your expectations.
2. **The Switch attributes summary section**: This section allows you to take a quick look at the summary of Switch or device performance values.
3. **The Switch attributes detail section**: If you want to go deeper into the analysis of each Switch or Device attribute value, you can scroll down to reach the QoE attribute details view. For each QoE attribute, two elements are available:
   a. **A large counter widget** representing the percentage of the uptime of all Devices in the selected scope.
   b. **A line chart widget** representing the evolution of the QoE attribute value over time. For example, here it represents the evolution of the Device Uptime over time.

8.1.1.1.10 Analyze QoE Metric Failures

From the QoE Dashboard page (see page 777), you may want to further analyze the failures that occurred in one of the tracked QoE metrics.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, Switch Up, Switch Down Count, number of Live Wireless and Wired Clients connected in the Network.

Click on the **More details** button in the “Failed Phases” block of the QoE metric for which you want to analyze the failures:

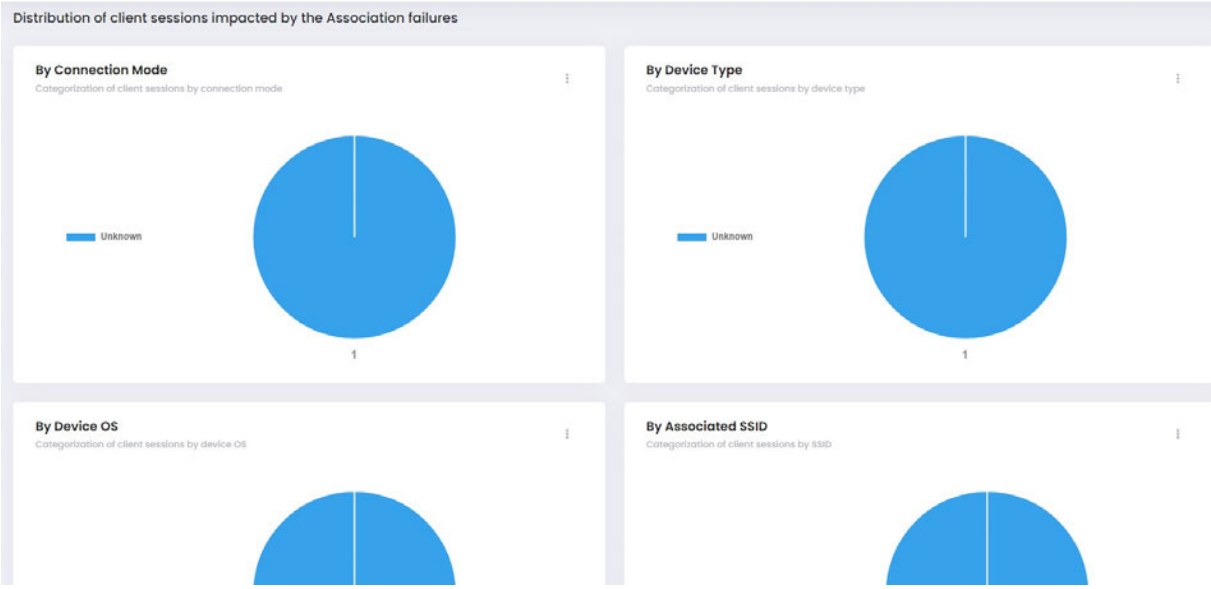


The Failure Classifiers dashboard appears. This page is divided into four parts:

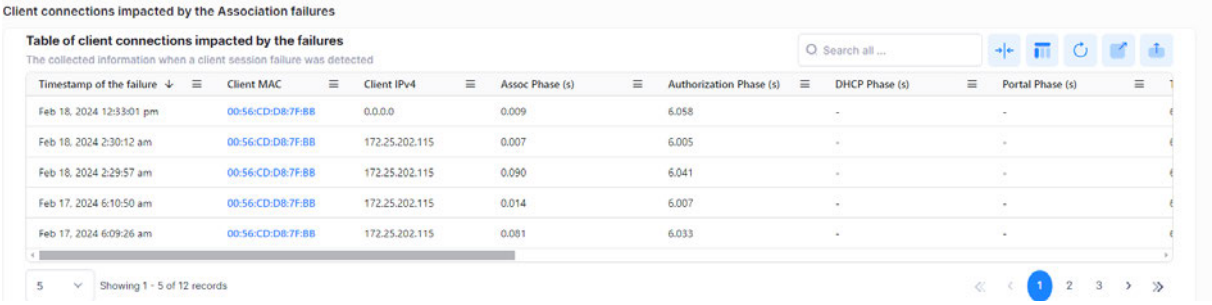
- **The Summary widget** - This widget gives a summary of the number of client sessions that experienced a failure in one of the tracked classifiers.
- **The Timeline of failures** - This widget represents a timeline allowing us to know at which timestamp the failures occurred.
- **The distribution of client sessions impacted by the selected classifier failures** - This section contains pie charts that give the distribution of client sessions impacted by the selected classifier failures.
- **Table of client connections impacted by the failures** - This section contains a table displaying the list of client sessions impacted by the failures.

To switch between the available classifiers, simply click on one of the available classifiers in the red block. The Failure Classifiers dashboard will be automatically refreshed.

14 **Timeline of Failures**



15 **Distribution of Client sessions impacted by the Association failures**



16 **Table of Client connections impacted by the failures**

21 Oct 2025

8.1.1.2 Monitor Network Analytics

Monitoring network analytics allows you to evaluate WiFi and Wired Clients network performance using WLAN metrics (such as AP uptime, AP health, session metrics, Device health). The information in this section describes how to utilize the following OmniVista Terra advanced analytics to monitor and evaluate the WiFi and Wired Clients network performance:

- Network Analytics Dashboard (see page 790)
- Configure Network Analytics Thresholds (see page 792)
- Device List (see page 802)
- Channel Distribution (see page 796)
- Channel Utilization (see page 797)
- Device Health (see page 799)
- Switch Network Analytics (see page 808)

21 Oct 2025

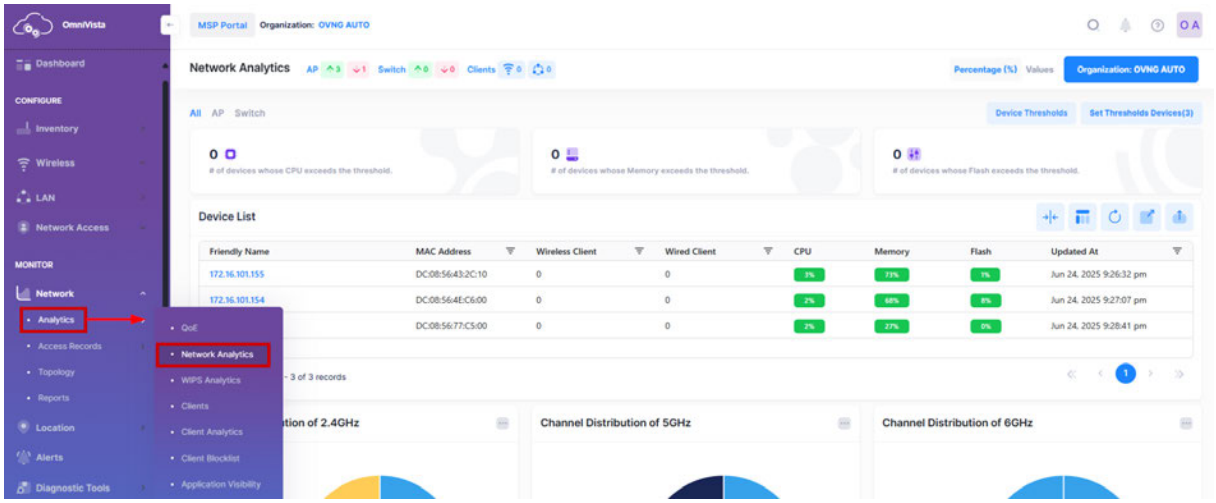
8.1.1.2.1 Network Analytics Dashboard

The Network Analytics Dashboard provides an overview of WLAN and Wired metric values for Access Points and Switches. The scope of Access Points or Switches to monitor is defined using the display filters to specify an entire organization, site, building, or a set of Access Points. To access the Network Analytics Dashboard, click on **Network > Analytics > Network Analytics** under the “Monitor” section of the OmniVista Terra Menu (see page 45).

There are three options available to monitor the Network Analytics from this screen:

- **All** - Displays Analytics of all devices (Access Points and Switches).
- **AP** - Displays Analytics of Access Points.
- **Switch** - Displays Analytics of Switches.

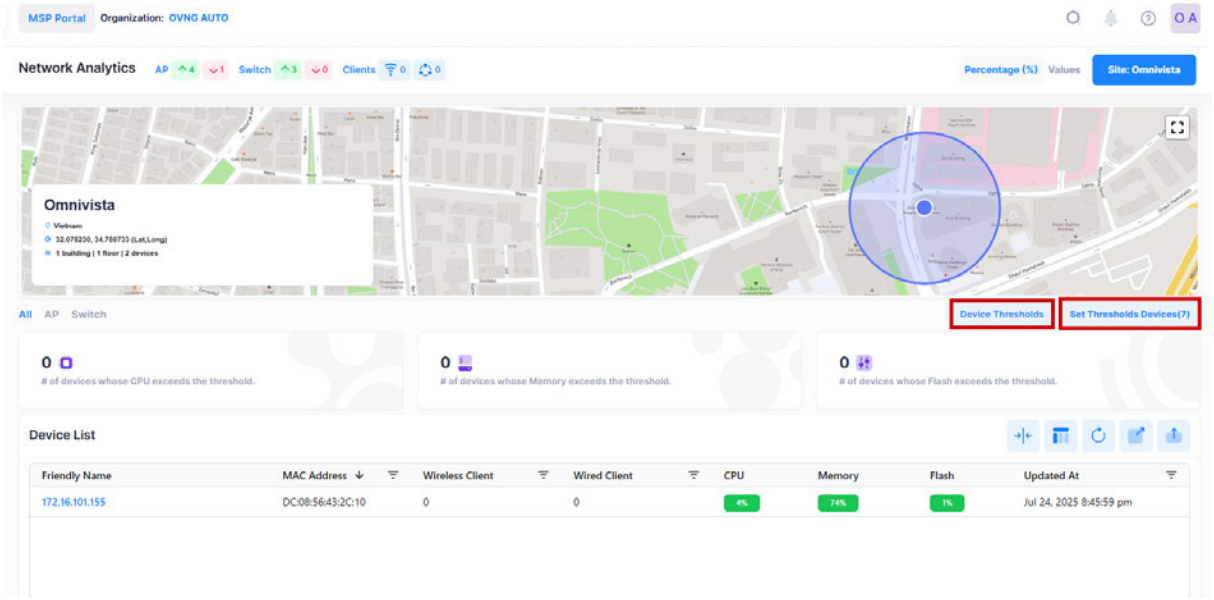
By default, **All** devices are selected. Click on **All**, **AP**, or **Switch** to view the related device performance analytics.



Use the Network Analytics Dashboard to monitor and evaluate the following metric values:

- Network Analytics Summary (see page 873)
- Device List (see page 802)
- Channel Distribution (see page 796)
- Channel Utilization
- Device Health (CPU/Memory/Flash) (see page 799)
- Switch Network Analytics (see page 808)

Use the **Device Thresholds** and **Set Thresholds Devices** metrics to configure and evaluate the Access Points and Switches Health threshold values. The CPU and memory health threshold values are configurable for a specific Access Point device; the CPU, memory, and flash health threshold values are configurable for all Access Points and Switches associated with a specific Site. Note that device threshold values take precedence over Site threshold values. See the Configure Network Analytics Thresholds (see page 792) online help for more information.



Use the Access Points and Switches Health metrics to watch for sustained usage that is close to the threshold values and identify peak usage rates.

Note: Changing any of the default Site or device threshold values will recalculate all three parameters of the Access Point Health dashboard and will change the threshold line in the Access Point Health Table**.** It is used to count number of healthy Access Points that are available now corresponding to the new threshold values.

21 Oct 2025

8.1.1.2.2 Configure Network Analytics Thresholds

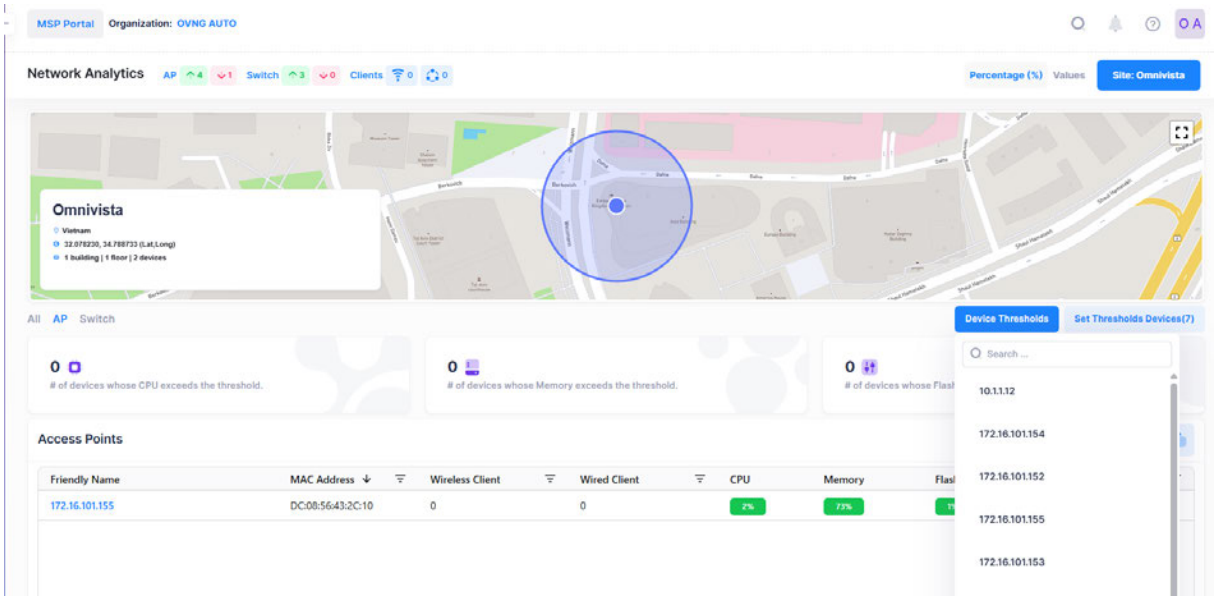
Network Analytics are computed based on usage threshold values configured at Organizational level and Site level. To change a usage threshold value, click on the respective button on the Network Analytics Dashboard as described below.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients connected in the Network, total number of Switches, Switches Up and Down Count.

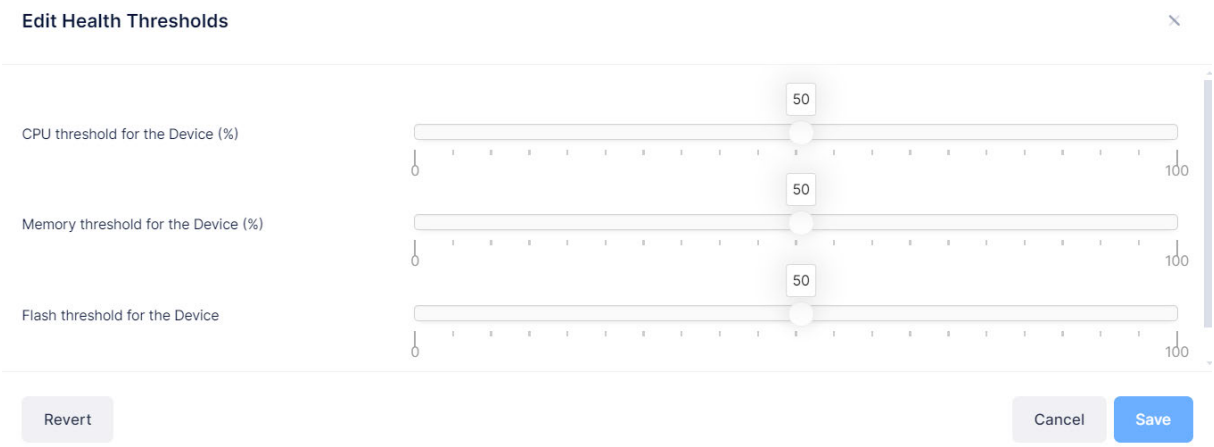
8.1.1.2.2.1 Configure Device Health Thresholds for Access Points

The Access Points Health analytics for CPU, Memory and Flash Health metrics can also be computed based on Device threshold values of the devices. The Device Thresholds button appears when you selects an Organization level/Site level/Building level or Floor level to view the Access Points Health.

To set a device threshold for the Access Points, click on the **Device Thresholds** button on the Access Points Health Dashboard. This opens the window in which you can select the Access Points for which you want to edit the threshold values.



When you click on one of the Access Points, it opens the " Edit Health Thresholds" window from which you can edit the following threshold values for the Device:

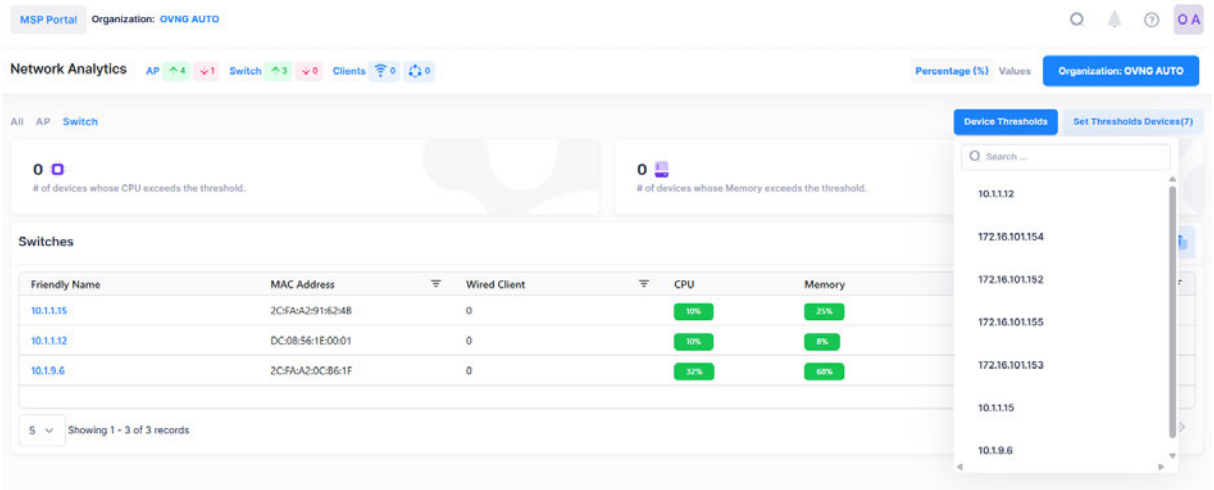


After changing any of the threshold values, click the **Save** button. To revert thresholds to their default values, click the **Revert** button.

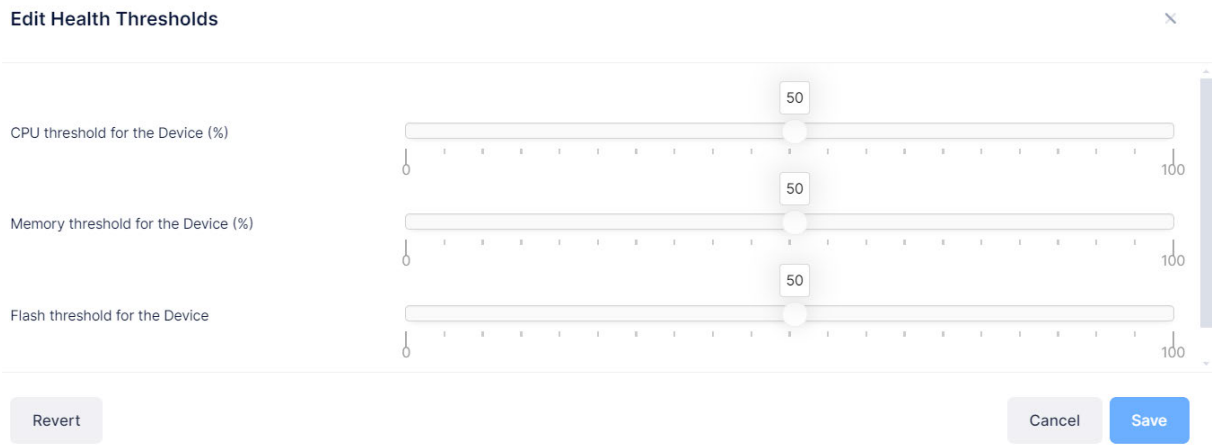
8.1.1.2.2.2 Configure Device Health Thresholds for Switches

The Switches Health analytics for CPU, Memory and Flash Health metrics can also be computed based on Device threshold values of the devices. The Device Thresholds button appears when you selects an Organization level/Site level/Building level or Floor level to view the Switch Health.

To set a device threshold for the Switch, click on the **Device Thresholds** button on the Device Health Dashboard. This opens the window in which you can select the Switch/device for which you want to edit the threshold values.



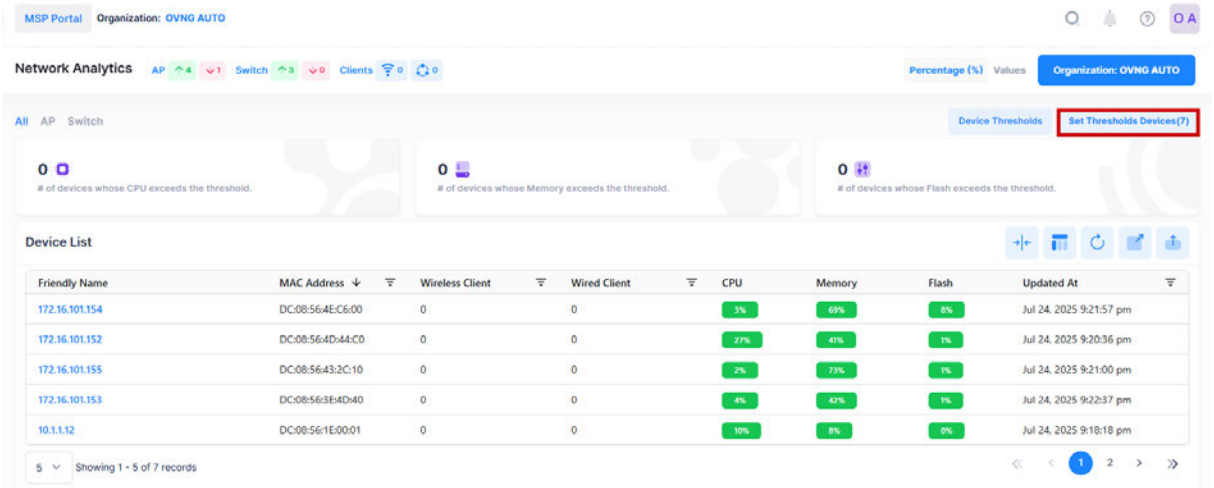
When you click on one of the Switch IP, it opens the “ Edit Health Thresholds” window from which you can edit the following threshold values for the Device:



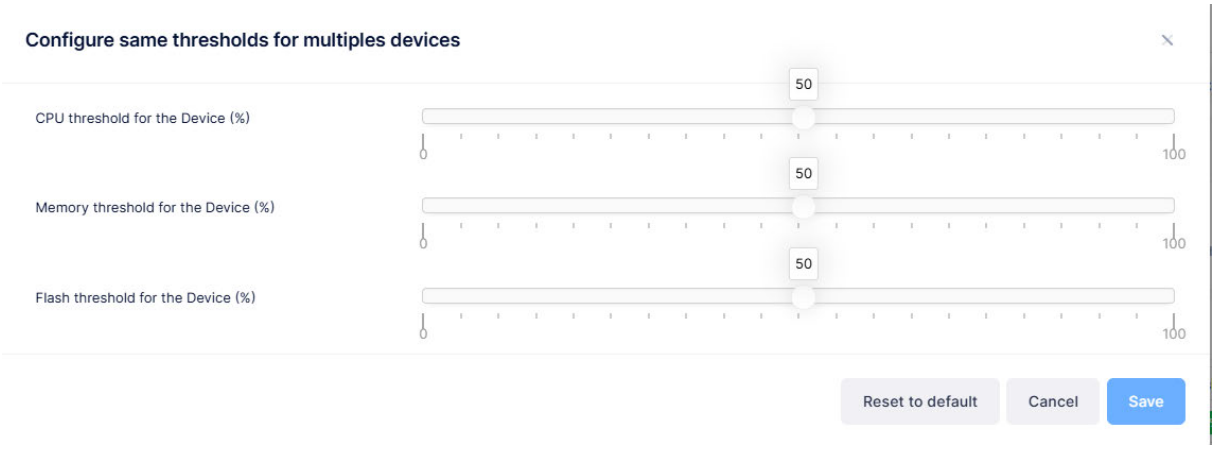
After changing any of the threshold values, click the **Save** button. To revert thresholds to their default values, click the **Revert** button.

8.1.1.2.2.3 Set Health Thresholds for multiple Devices

To set the same thresholds for multiple devices simultaneously you can click on the **Set Thresholds Devices** button. The Set Thresholds Devices button appears next to the Device Thresholds button when you are looking at a specific Site or Organization to view the Device Health as shown below:



To set same thresholds value for multiple devices for a specific Site, click on the **Set Thresholds Devices** button. The following screen appears from which you can edit the following threshold values for the Access Points:



After changing any of the threshold values, click the **Save** button. To revert thresholds to their default values, click the **Reset to default** button.

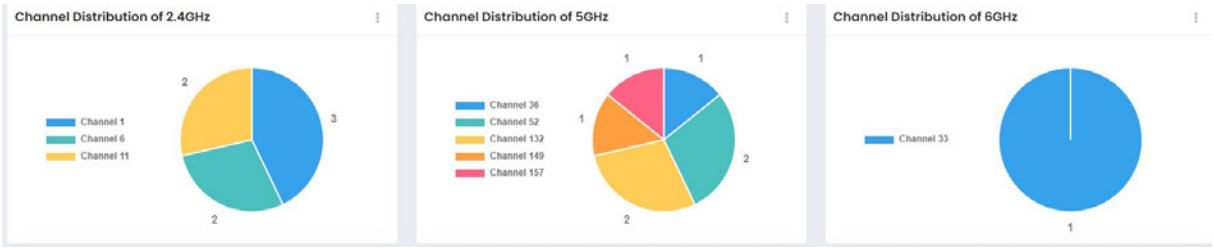
Notes:

- The Site health threshold is a global threshold that applies to all the devices belonging to that Site. It can be overridden by the device health threshold which is configured with the Device Thresholds option.
- The Site health threshold is also used to compute the Health Reports for Analytics Reports. (see page 925)
- OmniVista Terra sends the commands to configure the Thresholds on OV managed devices.
- You can select only one device at a time to configure the Thresholds values.

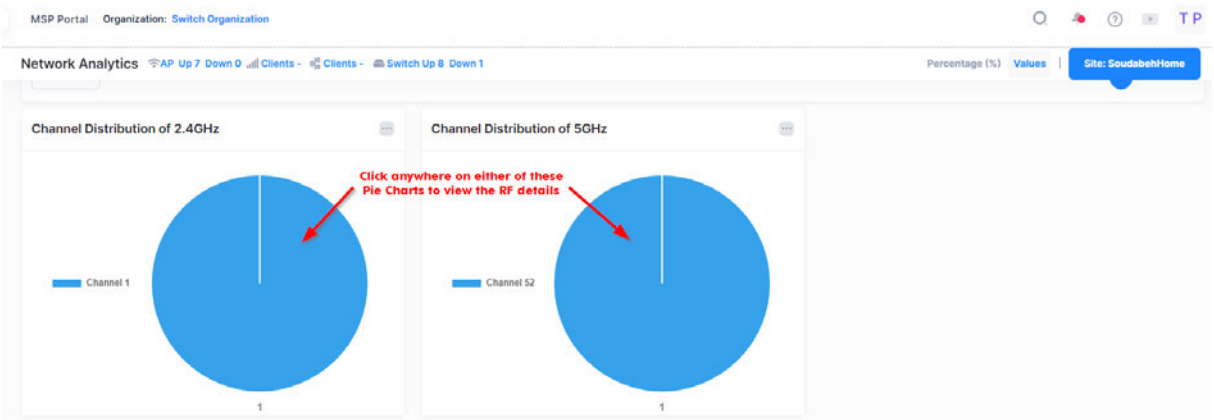
21 Oct 2025

8.1.1.2.3 Channel Distribution Metrics

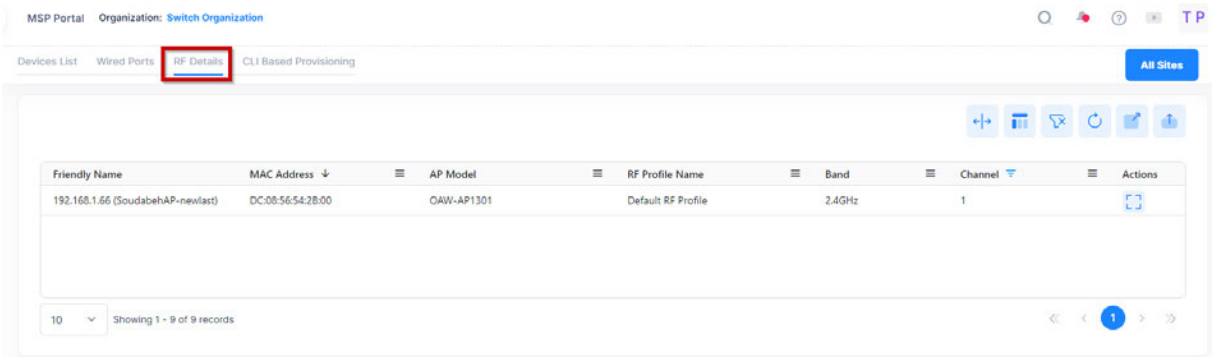
The Channel Distribution section of the Network Analytics Dashboard (see page 790) includes widgets for 2.4GHz, 5GHz and 6GHz frequency bands that show the channels that are being used within each frequency band. Use this information combined with Channel Utilization metrics to check that there is a fair distribution of wireless and wired communications among all of the channels.



You can click on any of the sections of either of these above shown Pie charts of 'Channel Distribution' to view the Device RF details:



When you click on the Pie Chart, you are redirected to the **RF Details** screen, which displays Radio Frequency attributes for managed devices. View the online help Device Catalog (see page 170) for more information.

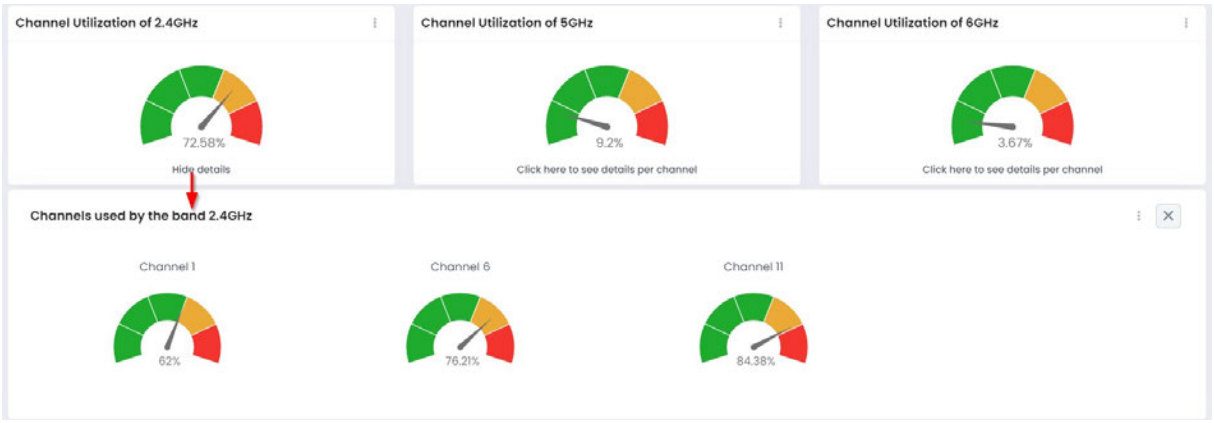


21 Oct 2025

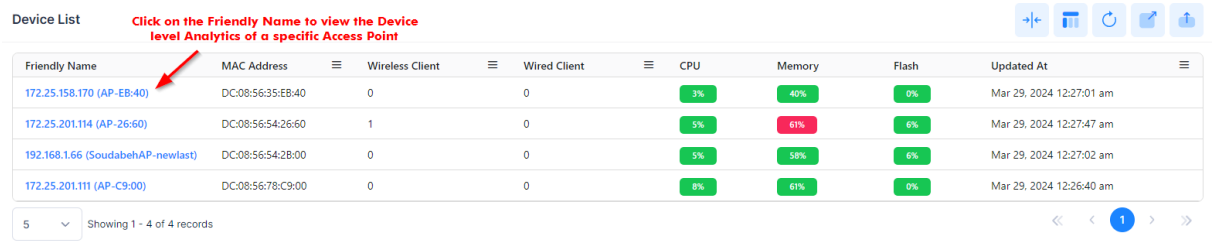
8.1.1.2.4 Channel Utilization Metrics

The Channel Utilization section of the Network Analytics Dashboard (see page 790) includes widgets for 2.4GHz, 5GHz and 6GHz frequency bands that show an average percentage of channel usage within each band. Use this information combined with Channel Distribution (see page 796) metrics to check that there is a fair distribution of wireless and wired communications among all of the channels.

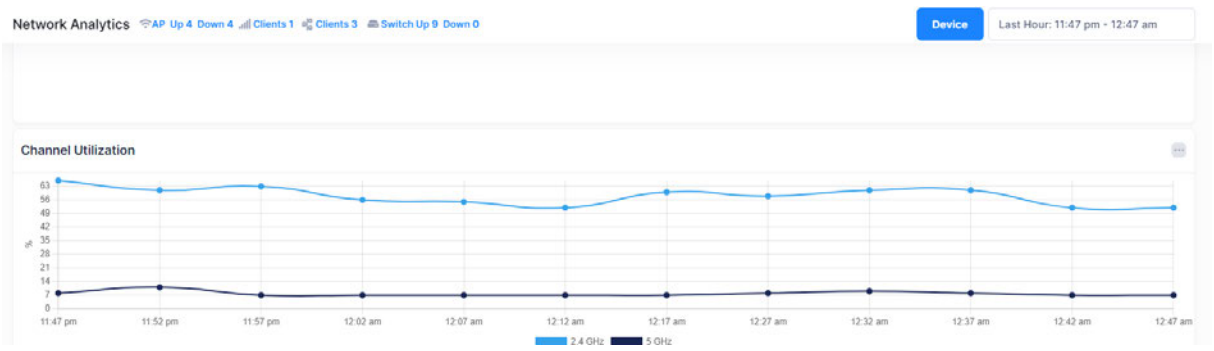
To get more detailed information for each channel within the frequency band, click on **Click here to see details per channel** at the bottom of the widget.



You can click on a “Friendly Name” from Device List (see page 802) table to view the historic trend of Channel Utilization on a device as shown below.



Then you will be directed to the below screen to view the history trend of Channel Utilization.



21 Oct 2025

8.1.1.2.5 Device Health (CPU / Memory / Flash) Metrics

The Device Health section of the Network Analytics Dashboard (see page 790) provides the information to help monitor and evaluate the latest Device Health status metrics.

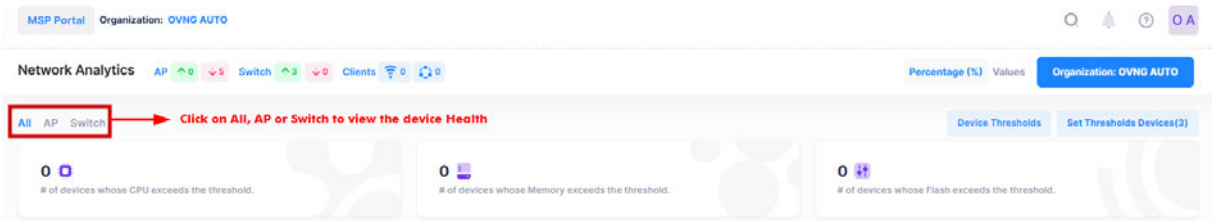
There are three options available to view the Device Health from this screen:

- **All** - Displays a list of all devices (Access Points and Switches).
- **AP** - Displays a list of Access Points.
- **Switch** - Displays a list of Switches.

By default, all devices are selected. Click on **All**, **AP**, or **Switch** to view the related device health performance.

From this screen, you can perform any of the following actions:

- Monitor Access Point Health Trend (see page 799)
- Monitor Switch Health Trend (see page 800)

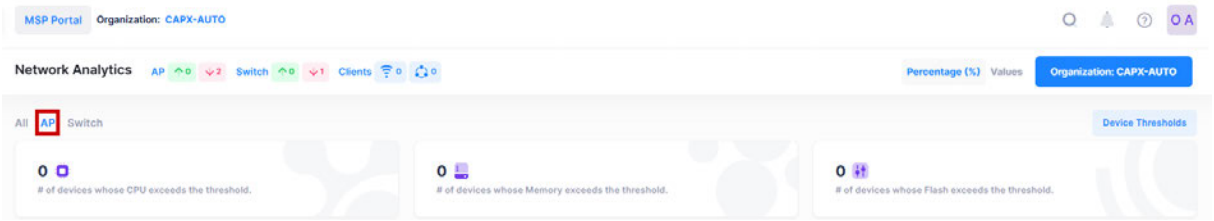


The CPU and memory health threshold values are configurable for a specific device; the CPU, memory, and flash health threshold values are configurable for all Devices associated with a specific Site. Note that device threshold values take precedence over Site threshold values. See the Configure Network Analytics Thresholds (see page 792) online help for more information.

8.1.1.2.5.1 Access Points Health Trend

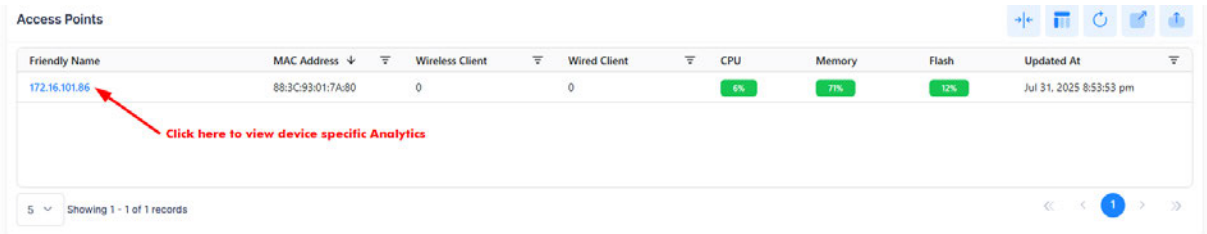
The Access Point Health section provides the following information to help monitor and evaluate Device health:

- The number of Devices with CPU usage that exceeds the threshold value.
- The number of Devices with memory usage that exceeds the threshold value.
- The number of Devices with flash usage exceeds the threshold value.

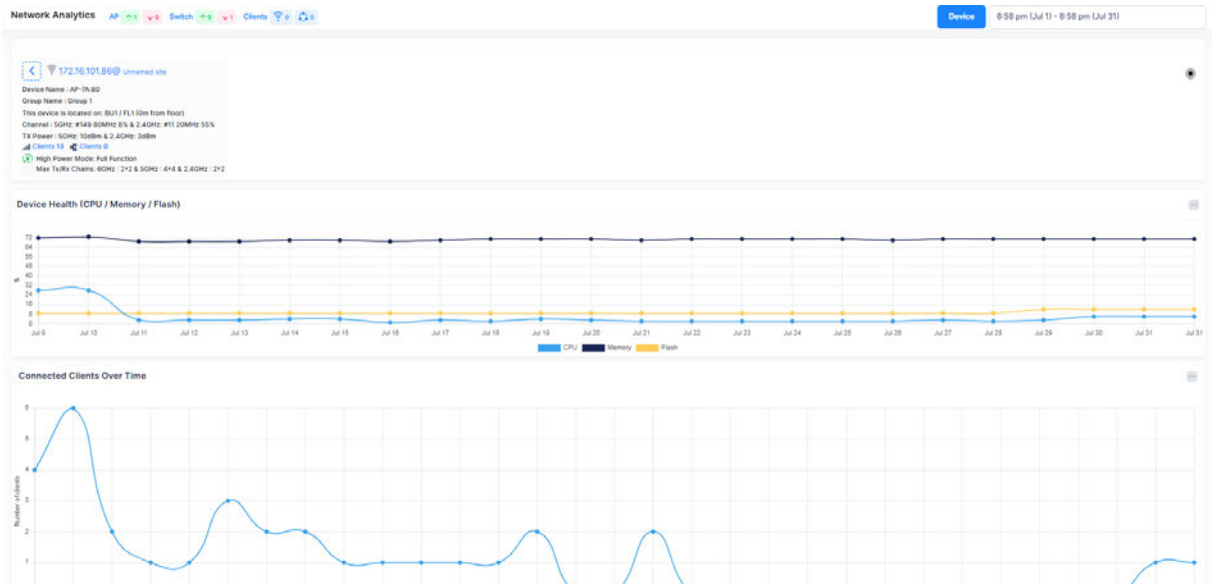


To view the latest percentage-wise status of CPU, memory, and flash usage for the devices, go to the “Device List” table.

You can click on a specific Friendly Name in the “Device List” Table, then you will be directed to the **Device Detail Single view page** which displays the history trend of Device Health Metrics as shown below.



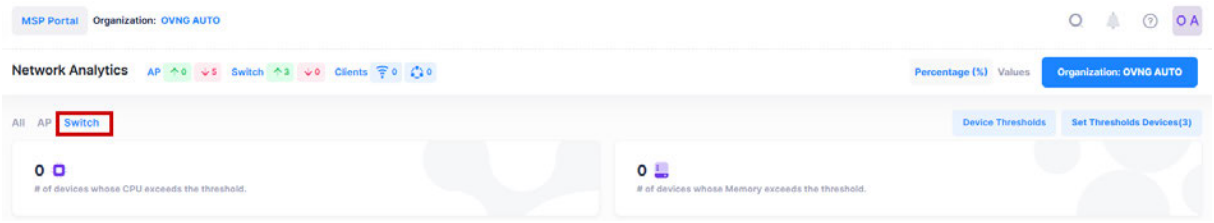
The Device Level Health Trend is shown below for specific Device which is selected for a selected time window range.



8.1.1.2.5.2 Switch Health Trend

To view the **Switch Health Metrics**, select the **Switch** tab to monitor and evaluate the following Switch Health metrics as shown below:

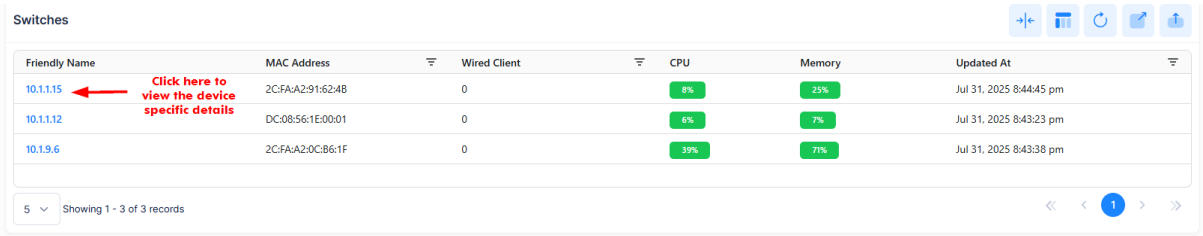
- The number of Devices with CPU usage that exceeds the threshold value.
- The number of Devices with memory usage that exceeds the threshold value.



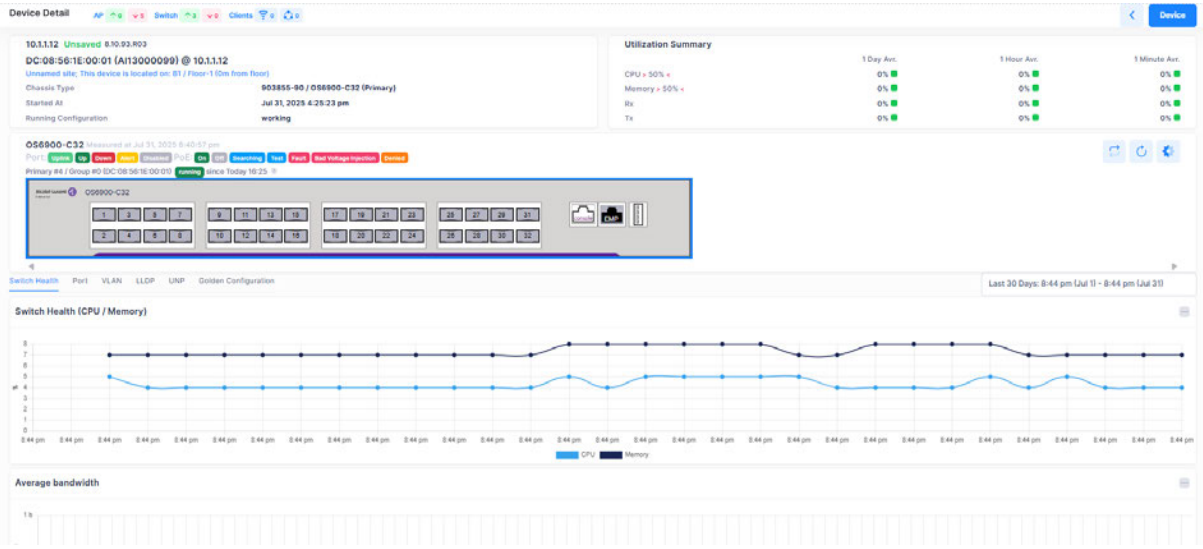
Note: The Switches do not report the Flash Health values to the OmniVista Terra.

To view the latest percentage-wise status of CPU and memory usage for the devices, go to the “Device List” table.

By Clicking on a specific Friendly Name in the “Device List” Table, you will be directed to the **Device Detail Single view page** which displays the various parameters of Switch Health Metrics as shown below.



It will redirects you to the **Device Detail** screen for Switches. The Switch Level Health Trend is shown below for specific Device which is selected for a selected time window range.



Note: The number of devices over the threshold is computed between the Device Threshold and the Health Threshold values. (if the device is not listed in Device Threshold)

21 Oct 2025

8.1.1.2.6 Device List

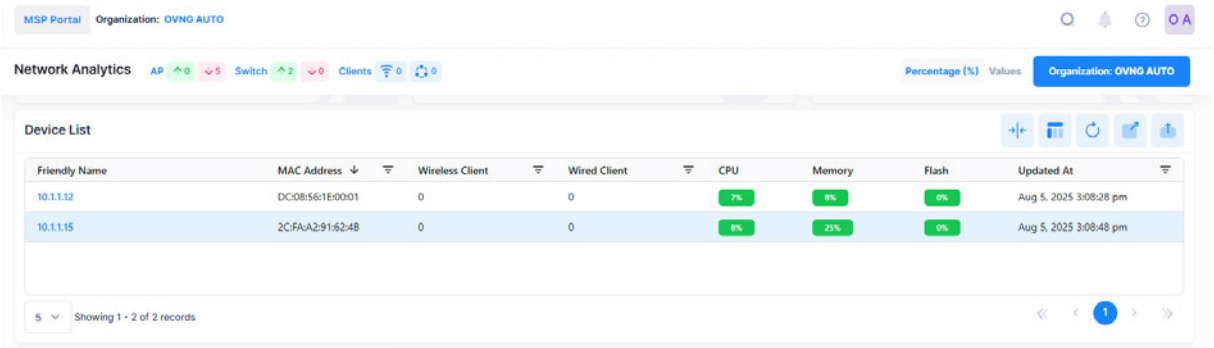
The Device List section of the Network Analytics Dashboard (see page 790) provides information to help monitor and evaluate the Device or Access Points performance metrics which also includes the Wireless and Wired Clients Device uptime.

Data displayed can be exported into a CSV, PDF or Excel sheet format. You can also switch to full-screen mode for a better display.

By default, all devices are selected. Click on **All**, **AP**, or **Switch** to view the related device detailed performance.

From this screen, you can perform any of the following actions:

- Monitor Access Point Network Analytics (see page 805)
- Monitor Switch Network Analytics (see page 808)

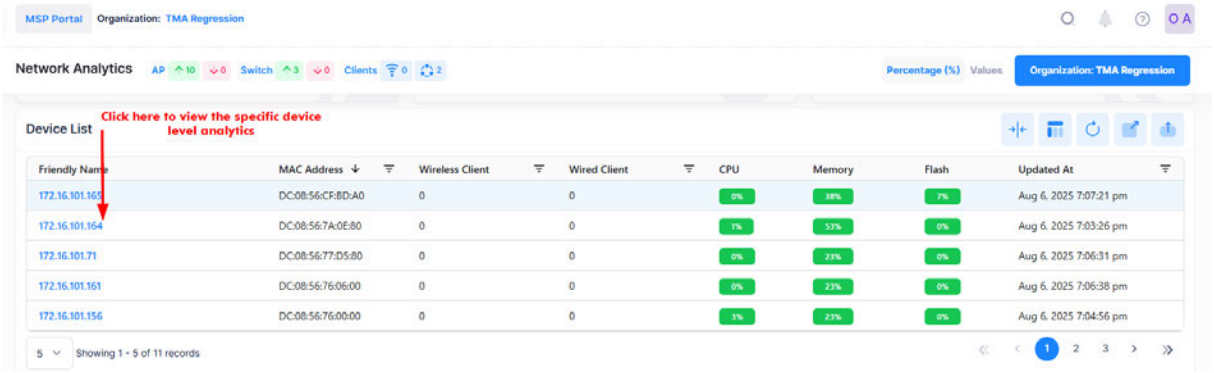


The Device List field values provide the following information:

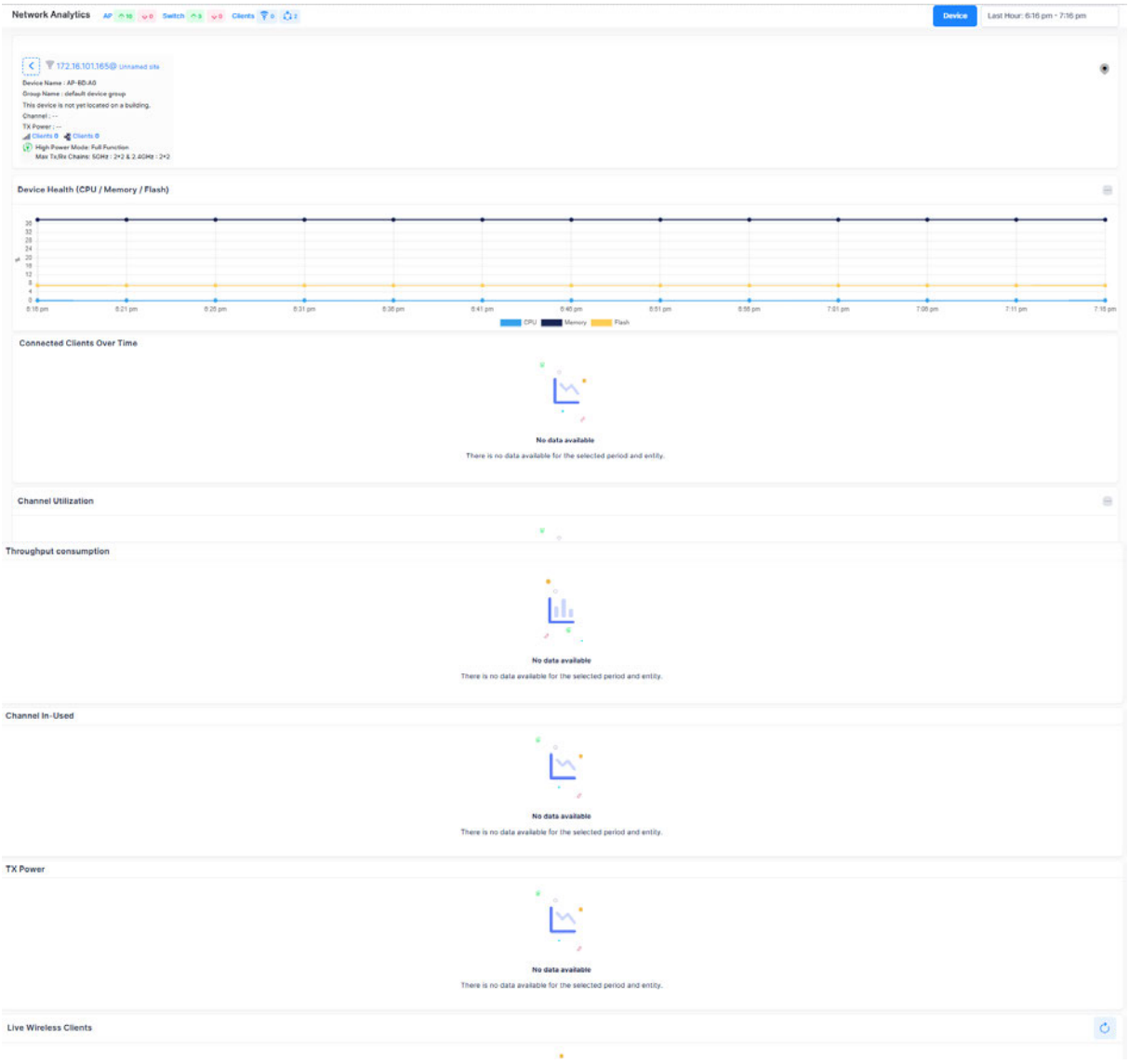
- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **MAC Address -** The Access Point MAC address.
- **Wireless Client -** The number of Wireless Clients connected to the Access Point.
- **Wired Client -** The number of Wired Clients connected to the Access Point.
- **CPU -** The CPU Usage of the Access Point device.
- **Memory -** The Memory Usage of the Access Point device.
- **Flash -** The Flash Usage of the Access Point device.
- **Updated At -** The time of the last event received from the Access Point that was used to calculate the Uptime or downtime.

Note: The Device List table displays only those Access Points or Switches which are fully connected and managed with OmniVista Terra services. The Devices must be sending the Analytics data and it should not be disabled by the user. The Access Points which are not active will not be displayed here.

To explore specific Device Level Analytics, click on the specific ‘Friendly Name’ in the Device List Table to view the detailed Analytics of a particular Access Point or Switch device as shown below.



The Device level Network Analytics screen displays filters on the dashboard to define the scope of activity that you want to monitor within a specific window of time.



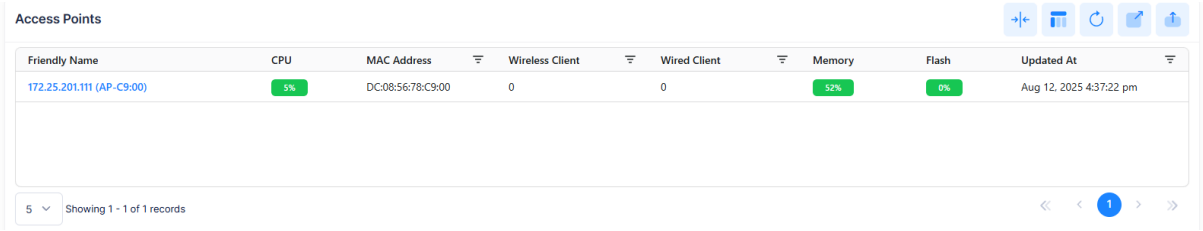
Note: The ‘Current’ Access Point Uptime and Downtime with the count of Live Wireless and Wired Clients connected and other Network Analytics is shown as a summary at the top and the ‘Historical’ charts are displayed below the Summary view.

21 Oct 2025

8.1.1.2.6.1 AP Network Analytics

The Access Point Network Analytics section of the Network Analytics Dashboard (see page 790) provides information to help monitor and evaluate the Access Points performance metrics.

Data displayed can be exported into a CSV, PDF or Excel sheet format. You can also switch to full-screen mode for a better display.

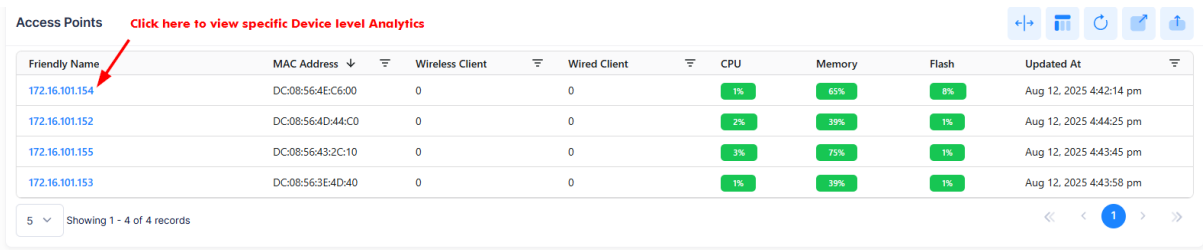


The Access Points field values provide the following information:

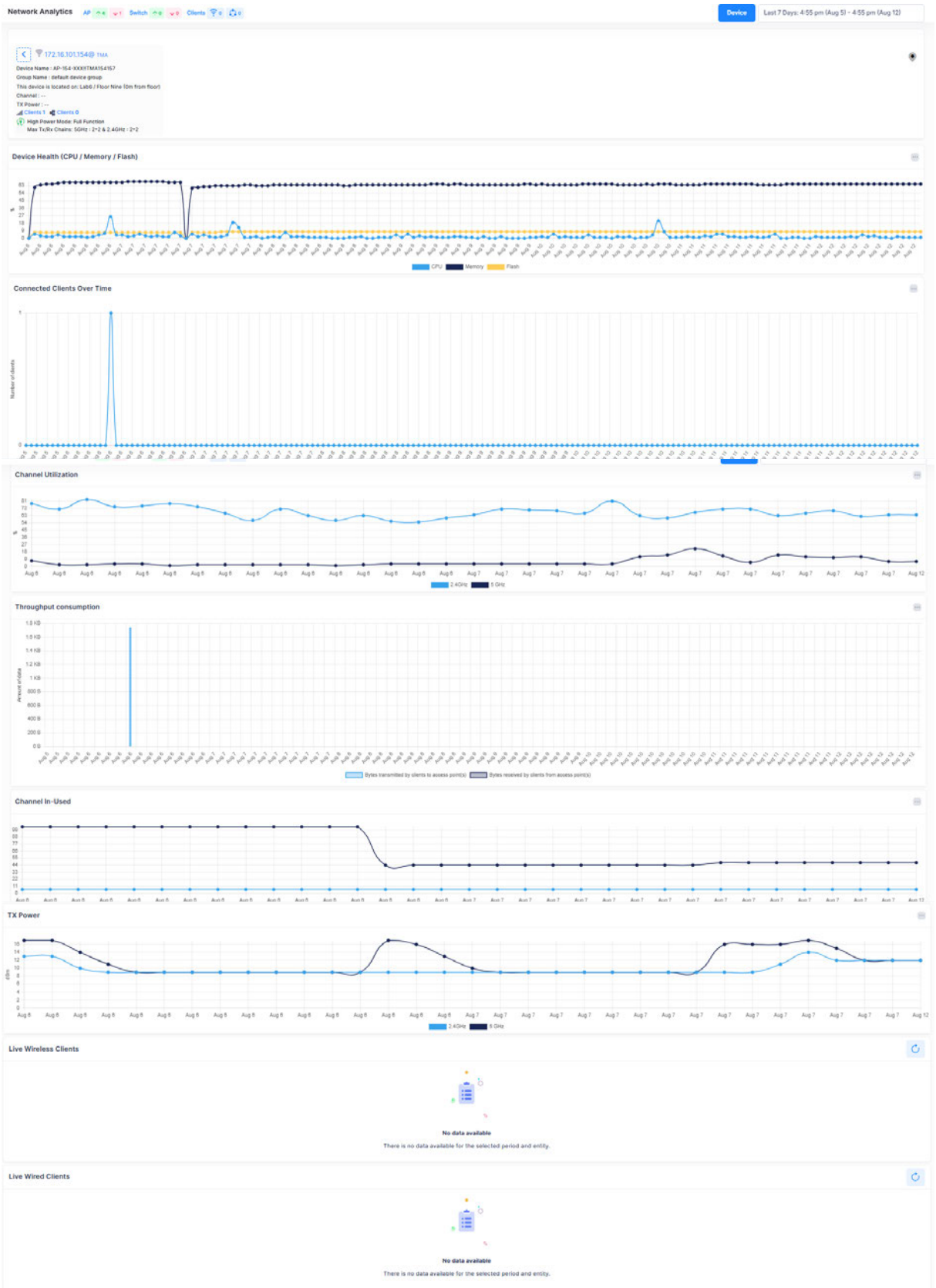
- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **MAC Address -** The Access Point MAC address.
- **Wireless Client -** The number of Wireless Clients connected to the Access Point.
- **Wired Client -** The number of Wired Clients connected to the Access Point.
- **CPU -** The CPU Usage of the Access Point device.
- **Memory -** The Memory Usage of the Access Point device.
- **Flash -** The Flash Usage of the Access Point device.
- **Updated At -** The time of the last event received from the Access Point that was used to calculate the Uptime or downtime.

Note: The Access Points table displays only those Devices which are fully connected and managed with OmniVista Terra monitoring agent. The Devices which are not active will not be displayed here.

To explore specific Device Level Analytics, click on the specific 'Friendly Name' in the Device List Table to view the detailed Analytics of a particular Access Point as shown below.



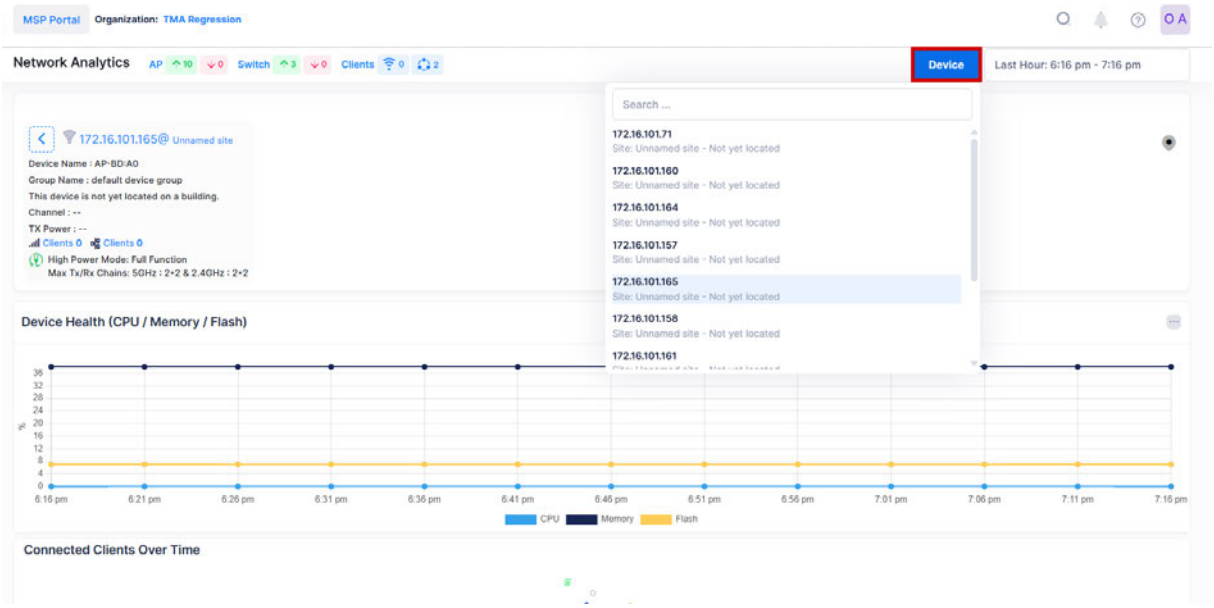
The Device level Network Analytics screen displays filters on the dashboard to define the scope of activity that you want to monitor within a specific window of time.


Network Analytics
Device
Device Health (CPU / Memory / Flash)
Connected Clients Over Time
Channel Utilization
Throughput consumption
Channel In-Used
TX Power
Live Wireless Clients
No data available
There is no data available for the selected period and entity.
Live Wired Clients
No data available
There is no data available for the selected period and entity.

The following parameters can be monitored by using above Charts and Tables to evaluate the Device Analytics Trend.

- Device Health Trend (CPU/Memory/Flash)
- Number of Current Connected Clients Over Time
- Current Channel Utilization 2.4 GHz/5 GHz/6 GHz
- Current Channel In-Use Trend 2.4 GHz/5 GHz/6 GHz
- Throughput Consumption
- Current Tx Power 2.4GHz/5GHz/6 GHz
- Live Wireless Clients
- Live Wired Clients

When you click on the **Device** button, it displays a drop-down list of the Access Points on the Access Points list. You can choose another Access Points from the list by selecting an Access Point from the menu, to view the device level analytics of other devices without returning to the Network Analytics screen as shown below.



21 Oct 2025

8.1.1.2.6.2 Switch Network Analytics

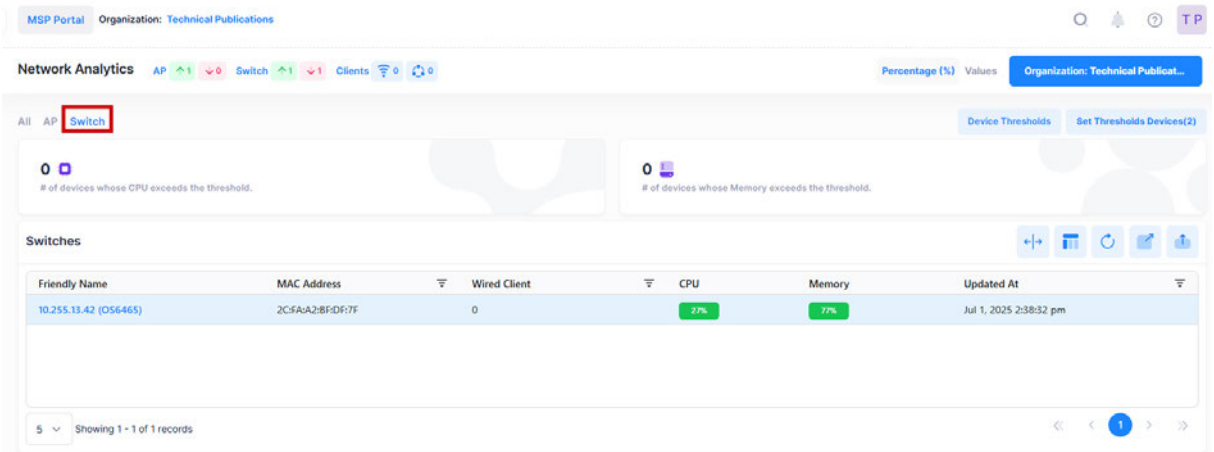
The Switch Network Analytics section of the Network Analytics Dashboard (see page 790) provides information to help monitor and evaluate the Switches performance metrics.

The top section provides the following information to help monitor and evaluate Device health:

- The number of devices with CPU usage that exceeds the threshold value.
- The number of devices with memory usage that exceeds the threshold value.

The CPU and memory health threshold values are configurable for a specific device; the CPU and memory health threshold values are configurable for all devices associated with a specific Site. Note that device threshold values take precedence over Site threshold values. See the Configure Network Analytics Thresholds (see page 792) online help for more information.

Data displayed can be exported into a CSV, PDF or Excel sheet format. You can also switch to full-screen mode for a better display.

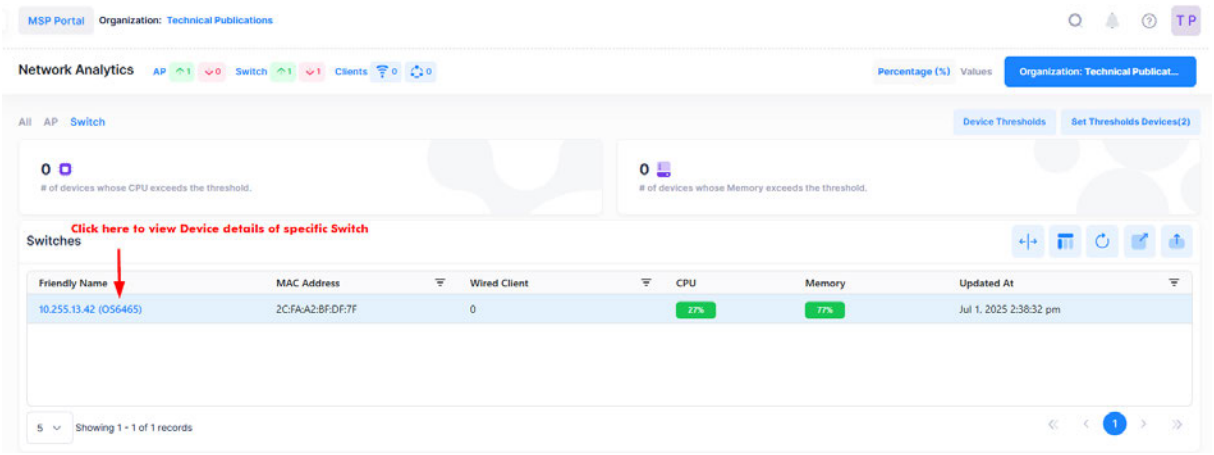


The Switches field values provide the following information:

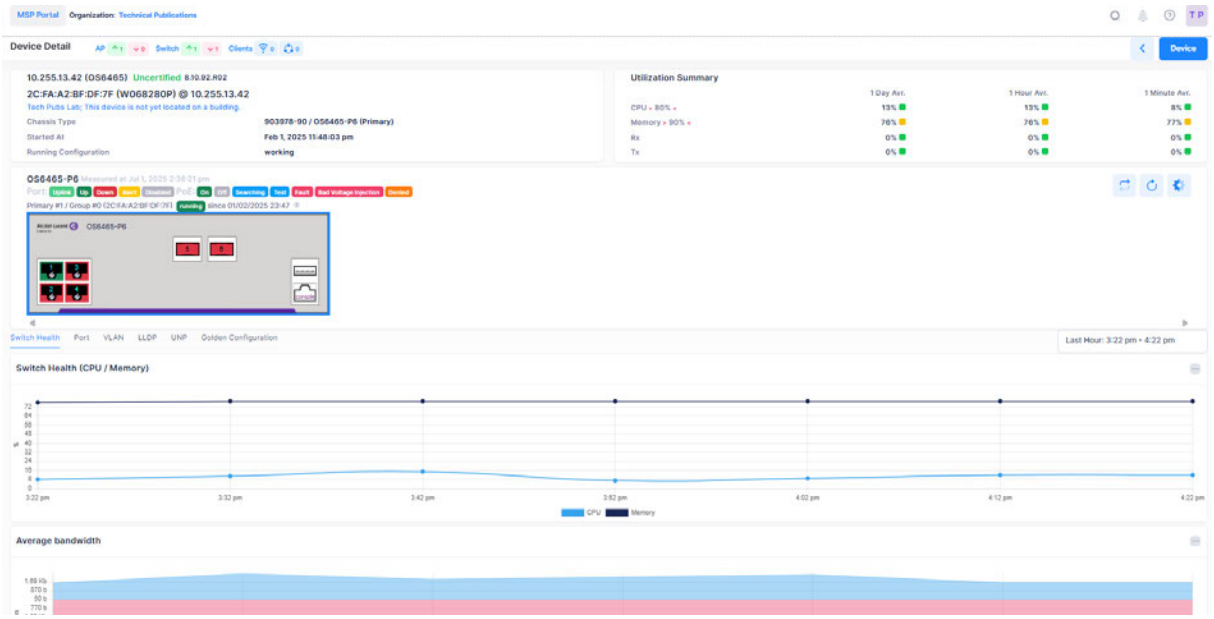
- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **MAC Address -** The Switch MAC address.
- **Wired Client -** The number of Wired Clients connected to the Switch.
- **CPU -** The CPU Usage of the Switch device.
- **Memory -** The Memory Usage of the Switch device.
- **Updated At -** The time of the last event received from the Switch that was used to calculate the Uptime or downtime.

Note: The Switches table displays only those Devices which are fully connected and managed with OmniVista Terra monitoring agent. The Devices which are not active will not be displayed here.

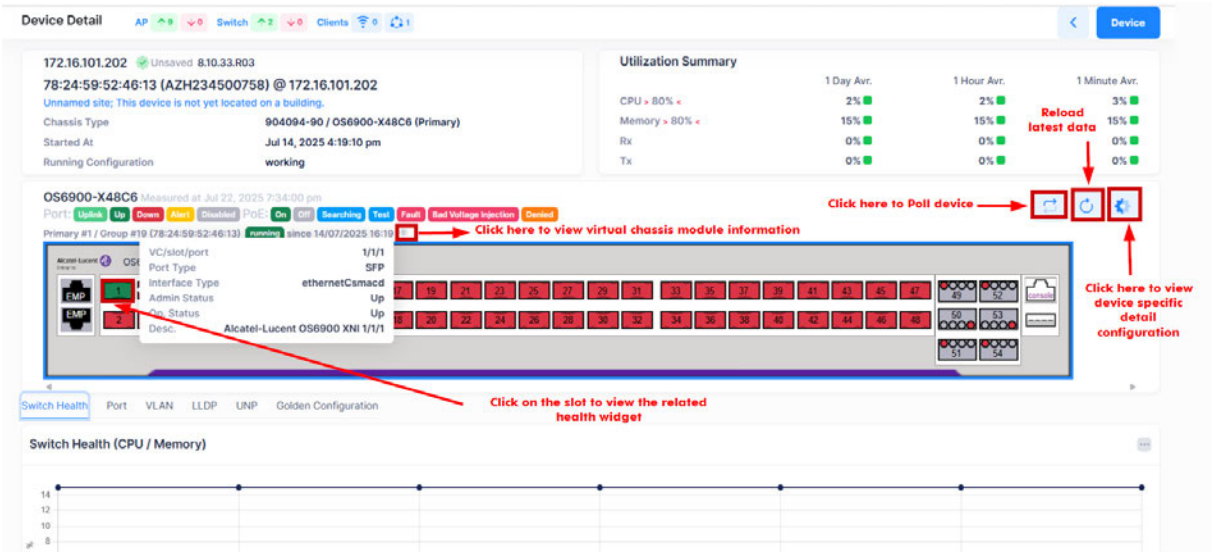
To explore specific Device Level Analytics, click on the specific ‘Friendly Name’ in the Switches Table to view the detail Device Analytics of selected Switch as shown below.



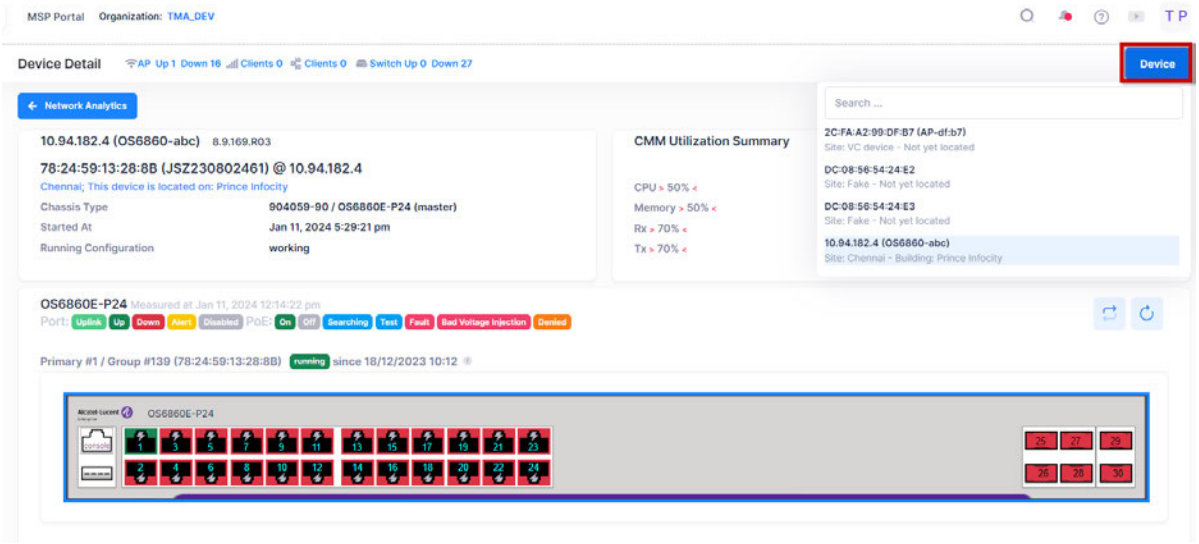
The Switch primary and secondary face plate along with Virtual Chassis slots appears with Switch details like Device Name, Model, IP address, serial number, chassis type and running status and is displayed at the top of the screen as shown below. The Virtual Chassis 1 is selected by default as shown in blue color.



You can click on any of the slot on the Switch faceplate to view the related widget for Switch health performance.



To view device level analytics for another switch without returning to the Network Analytics screen, click on **Device** in the upper-right corner of the screen. A drop-down list of devices is displayed from which you can select another switch, as shown below.

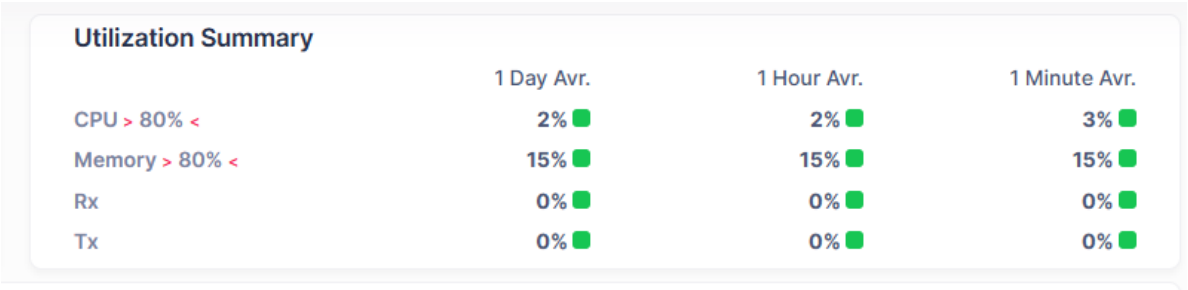


On the Device Detail screen, you can monitor the following parameters using charts and tables to evaluate the Switch Health Trend.

- CMM Utilization Summary (see page 811)
- Switch Health (CPU/Memory) (see page 811)
- Average Bandwidth (see page 811)
- Port Level Health and Statistics (see page 811)
- Configured VLANs (see page 814)
- LLDP Links (see page 815)
- Live UNP Clients (see page 815)
- Golden Configuration (see page 815)

CMM Utilization Summary

The CMM Utilization Summary table at the top-right of the Device Detail screen displays the summary of CPU, Memory, Tx and Rx Average utilization for the Switch.



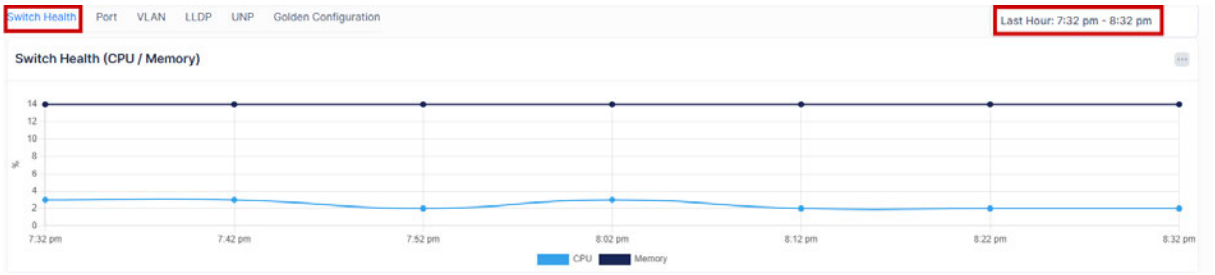
Switch Health

Click on the **Switch Health** tab at the bottom section of the Device Detail screen to view metrics on the switch CPU/Memory usage and the average bandwidth.

Switch Health (CPU/Memory)

The Switch Health (CPU/Memory) graph is used to evaluate the percentage of Switch CPU and Memory usage for the selected time window range.

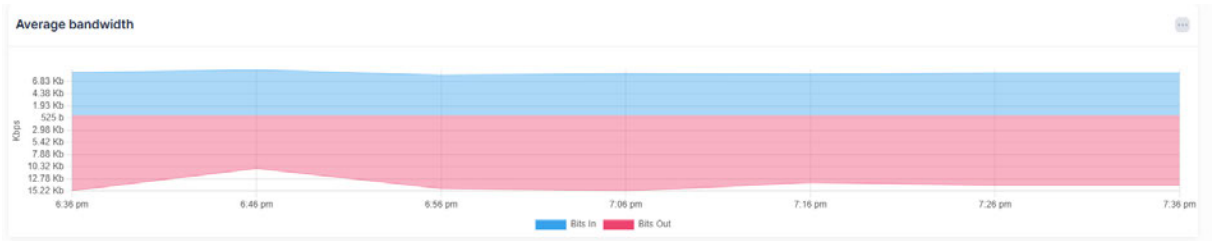
Data displayed in the line chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.



Average Bandwidth

The Average bandwidth section includes a graph representing the number of bytes received and transmitted by Clients to Switch over time.

Data displayed in the bar chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.



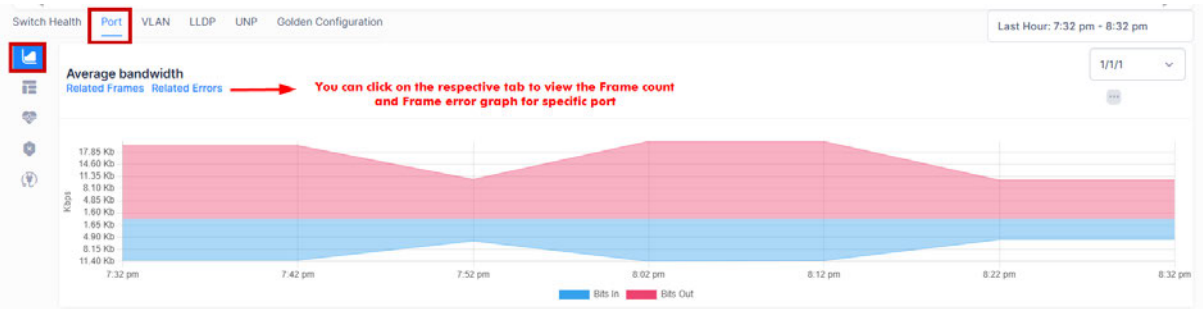
Port Level Health and Statistics

Click on the **Port** tab at the bottom section of the Device Detail screen to monitor the following parameters during the specified time window range.

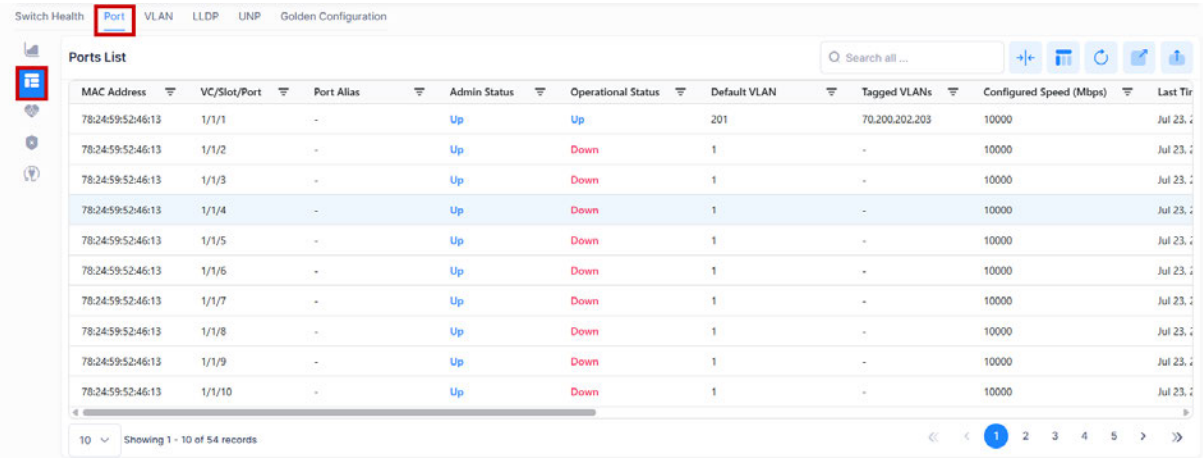
By default, the Average bandwidth graph is displayed which represents the Bytes-in and Bytes-out counter of the Switch over the selected time range. The graph displays the health of the 1/1/1 port by default. However, you can select another port from the drop-down list to view the health analytics of another port.

You can also view the other related charts from this screen as shown below.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



- **Ports List** - Displays the list of active Switch ports and their respective TX and RX Health information.

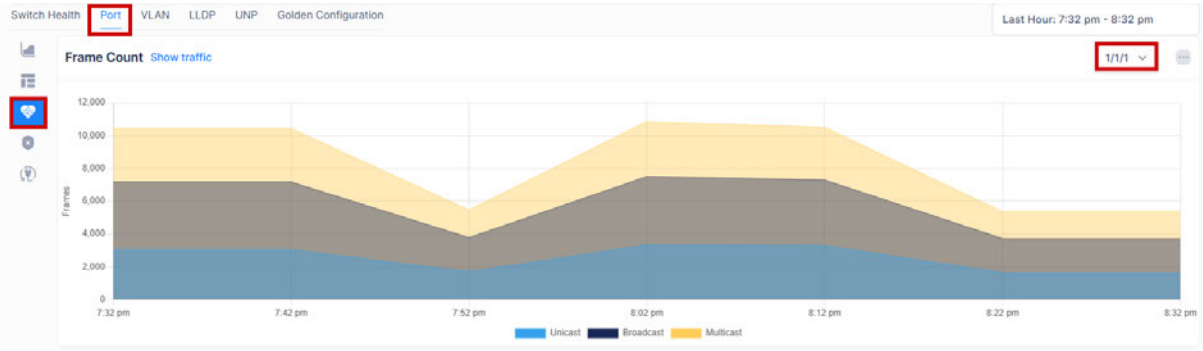


For each Port in the list, the following attribute values are provided:

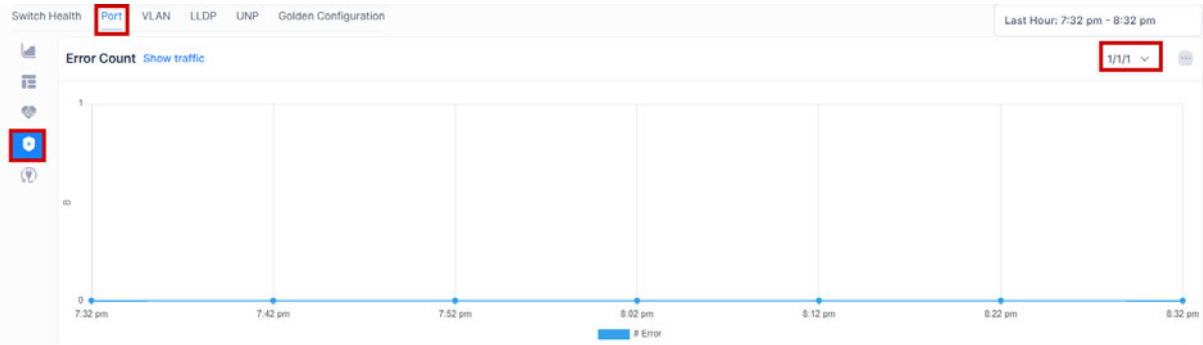
1. **MAC Address -** MAC address of the port.
2. **VC/Slot/Port -** The Virtual chassis/slot/port number.
3. **Port Alias -** The user-defined alias for the port.
4. **Admin Status** - Admin status of the port (Up or down).
5. **Operational Status** - Operational status of the port.
6. **Default VLAN** - The default Virtual LAN configured on the port.
7. **Tagged VLANs -** Displays the list of tagged VLANs.
8. **Configured Speed (Mbps)** - The configured interface line speed, in Mbps. If the port is set to "Auto", the switch automatically sets the line speed to match the attached device.

9. **Last time link changed** - The last time the configuration for the interface was changed.
10. **Number of status Change** - The total number of times the configuration of the interface has changed.
11. **Negotiated Speed (Mbps)** - The actual speed of the port.
12. **LAG Port Member** - The Link Aggregation Port(s) on the device, if applicable.
13. **UNP Name** - The Access Role Profile assigned to the port, if applicable.
14. **UNP Status** - Indicates whether or not UNP is Enabled/Disabled on the port.
15. **Port Split Status** - The split port status of the switch (Auto, 40GB, or 4 x 10GB). If the port is on a non-supported device, the field will display "False".
16. **VFL Port -** Indicates whether or not the port is a VFL port (True/False).

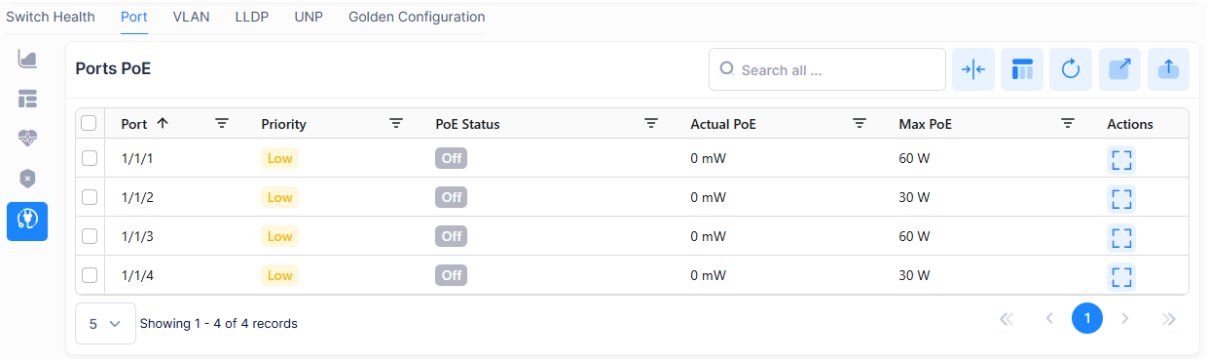
- **Frame Count** - Displays the Unicast, Broadcast and Multicast frame count for the selected port over the selected time range. The health of port 1/1/1 is displayed by default. However, you can select another port from the drop-down list to view the health analytics of another port.



- **Error Count** - The line chart displays the error count for the selected port over the selected time range. It displays the health of the 1/1/1 port by default. However, you can select another port from the drop-down list to view the health analytics of another port.



- **Ports PoE -** Displays the list of PoE ports on the Switch.



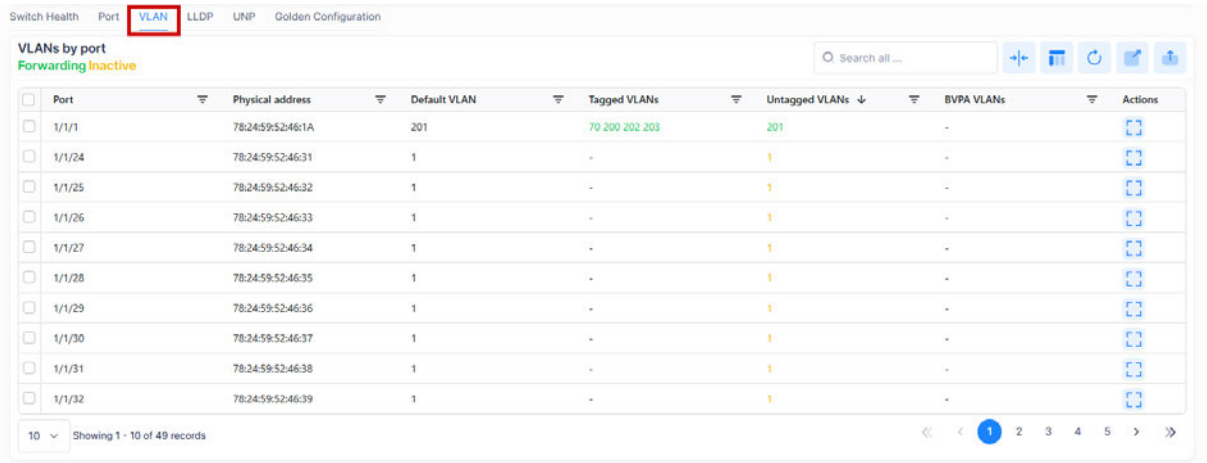
For each PoE Port in the list, the following attribute values are provided:

1. **Port** - The Virtual chassis/slot/port number.
2. **Priority** - The priority of the PoE.
3. **PoE Status** - The status of PoE (Enable/Disable).
4. **Actual PoE** - The current PoE wattage.
5. **Max PoE** - The maximum allowed PoE wattage.

Configured VLANs by Port

Click on the **VLAN** tab at the bottom section of the Device Detail screen to monitor the following parameters during the specified time window range.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



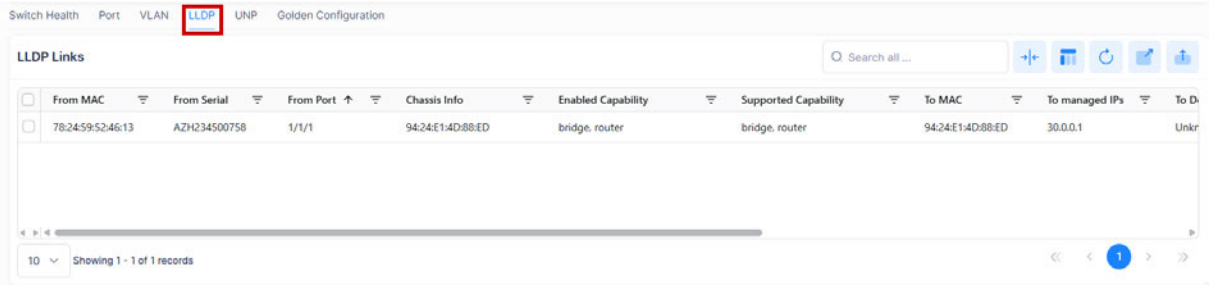
For the VLANs by port in the list, the following attribute values are provided:

1. **Port** - The chassis/slot/port number of the port.
2. **Physical address** - The MAC address of the Switch.
3. **Default VLAN** - The default VLAN configured on the port.
4. **Tagged VLANs** - The list of tagged VLANs.
5. **Untagged VLANs** - The list of untagged VLANs.
6. **BVPA VLANs** - The BVPA VLANs.

LLDP Links

Click on the **LLDP** tab at the bottom section of the Device Detail screen to monitor the LLDP connections to the switch.

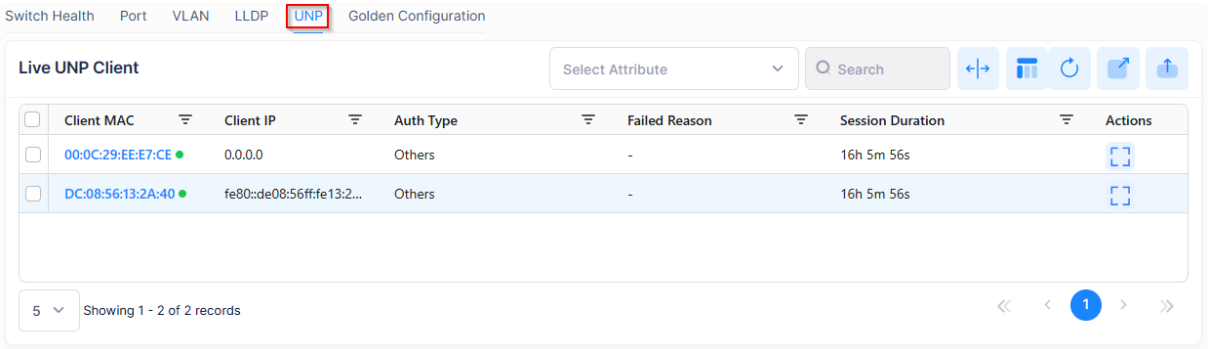
Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



Live UNP Client

Click on the **UNP** tab at the bottom section of the Device Detail screen to monitor the Live UNP Clients connected to the current Switch.

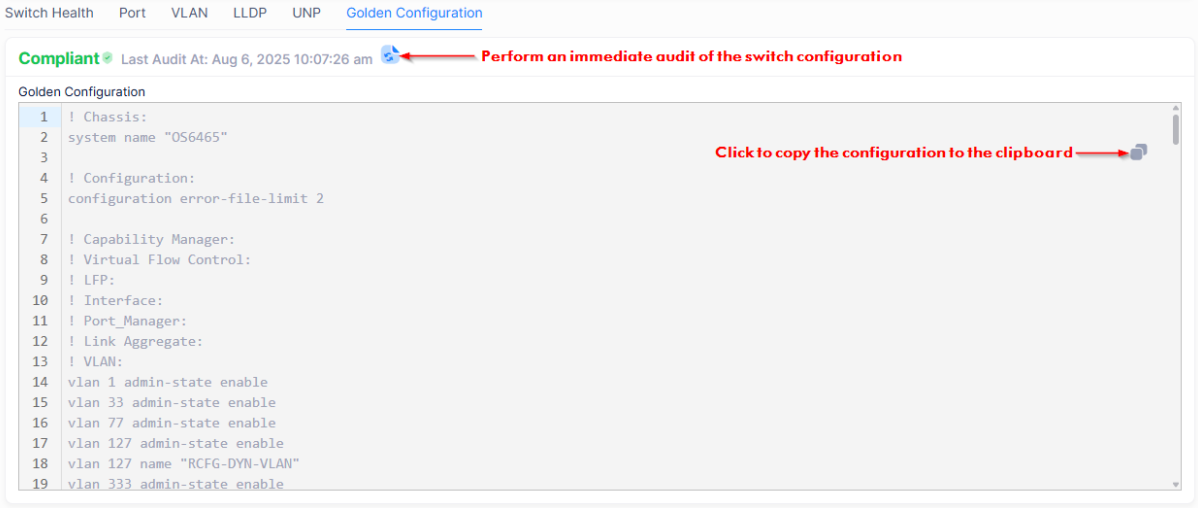
Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



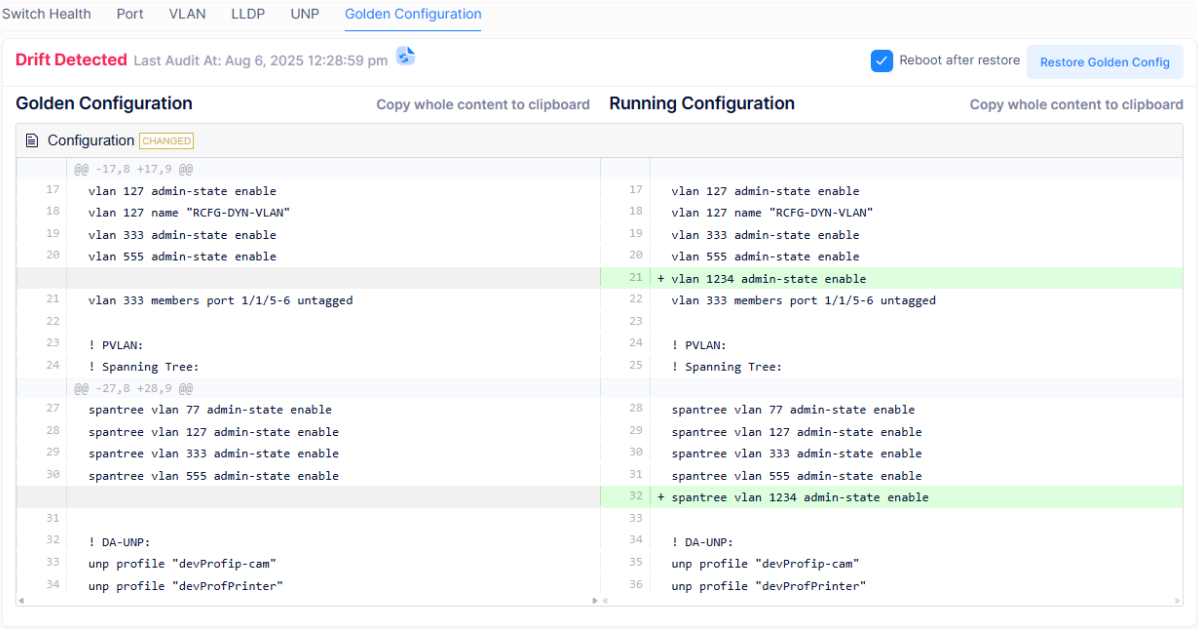
Golden Configuration

Click on the **Golden Configuration** tab to view the Golden Configuration for the switch. If a Golden Configuration was not designated for the switch, nothing is displayed for this tab.

If there is a Golden Configuration, the following is displayed:



If a difference between the Running Configuration and the saved Golden Configuration is detected, a comparison between the saved Golden Configuration and the current Running Configuration is displayed. Objects removed are highlighted in red; objects added are highlighted in green. For example:



You can perform any of the following actions from the Golden Configuration tab:

- View the differences between the saved Golden Configuration and the Running Configuration.
- Copy the Golden and/or Running Configuration to the clipboard.
- Determine the date and time the Drift was detected.
- Perform an immediate audit of the switch configuration.
- Click on **Restore Golden Config** to restore the Golden Configuration as the device configuration for the switch. By default, the “Reboot after restore” option is selected. Consider the following when you select this action:

- **Restore Golden Configuration with the “Reboot after restore” option selected**
  The Golden Configuration is copied to the switch as the new Running Configuration and reloads the switch.
- **Restore Golden Configuration with the “Reboot after restore” option is not selected**
  The Golden Configuration is copied to the vcboot.cfg of the switch as the new configuration file and the switch is not reloaded. The current Running Configuration for the switch remains.

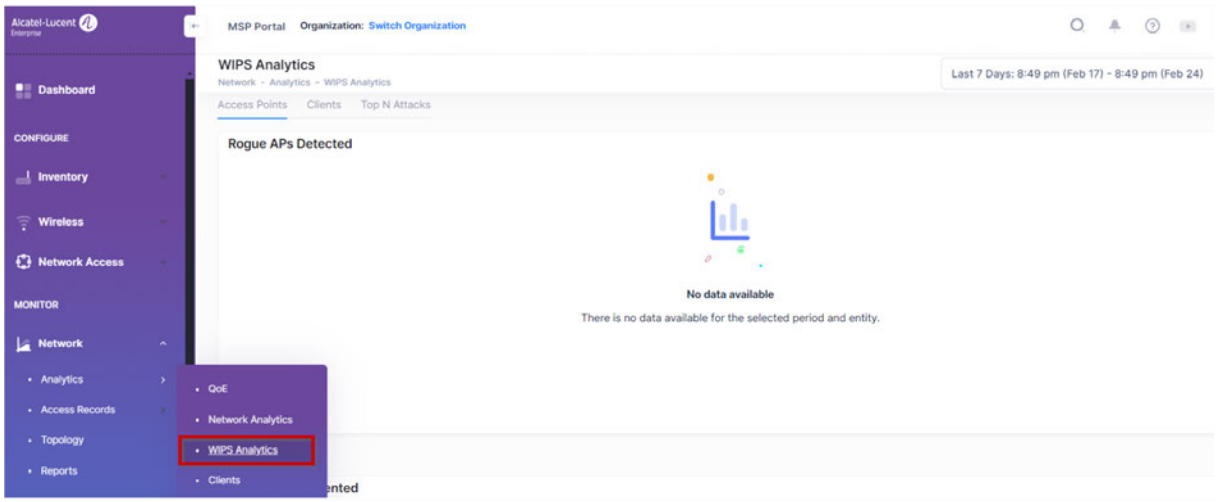
Please see Auditing the OmniSwitch Golden Configuration (see page 248) online help for more information.

21 Oct 2025

8.1.1.3 Monitor WIPS Analytics

An 802.11 network is open and borderless, making it vulnerable to attack (e.g., rogue APs, unauthorized clients, DoS attacks). The Wireless Intrusion Protection System (WIPS) application monitors the wireless radio spectrum for the presence of unsafe access points and clients, and can take countermeasures to mitigate the impact of foreign intrusions. WIPS provides an overview of wireless network threats/intrusions for Stellar APs, and enables users to set up policies to detect threats and take countermeasures.

To access the WIPS Analytics Summary, click on **Network > Analytics > WIPS Analytics** under the “Monitor” section of the OmniVista Terra Menu.



It provides the following screen to monitor the WIPS analytics for Access Points and Clients.

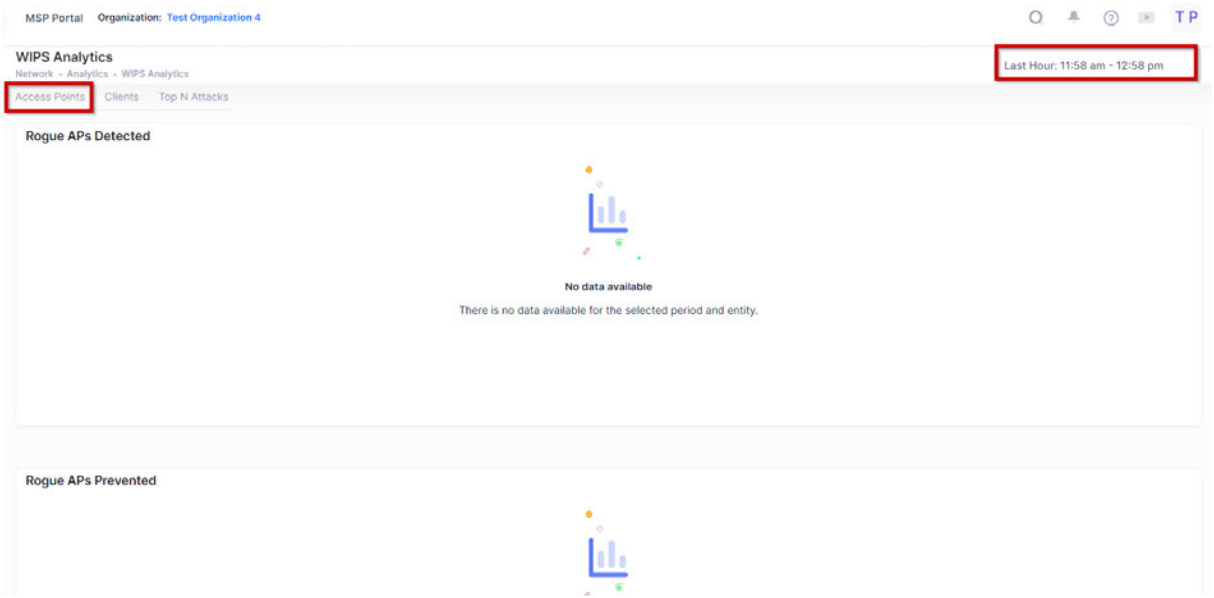
- WIPS Access Points Analytics (see page 819)
- WIPS Clients Analytics (see page 821)
- Monitor Top N Attacks (see page 823)

21 Oct 2025

8.1.1.3.1 WIPS Access Points Analytics

The “WIPS Access Points” section of the Monitor WIPS Analytics (see page 818) dashboard includes widgets that show the the number of Rogue Access Points Detected and Rogue Access Points Prevented and the Rogue Access Points Table associated with the managed devices during the specified time window range.

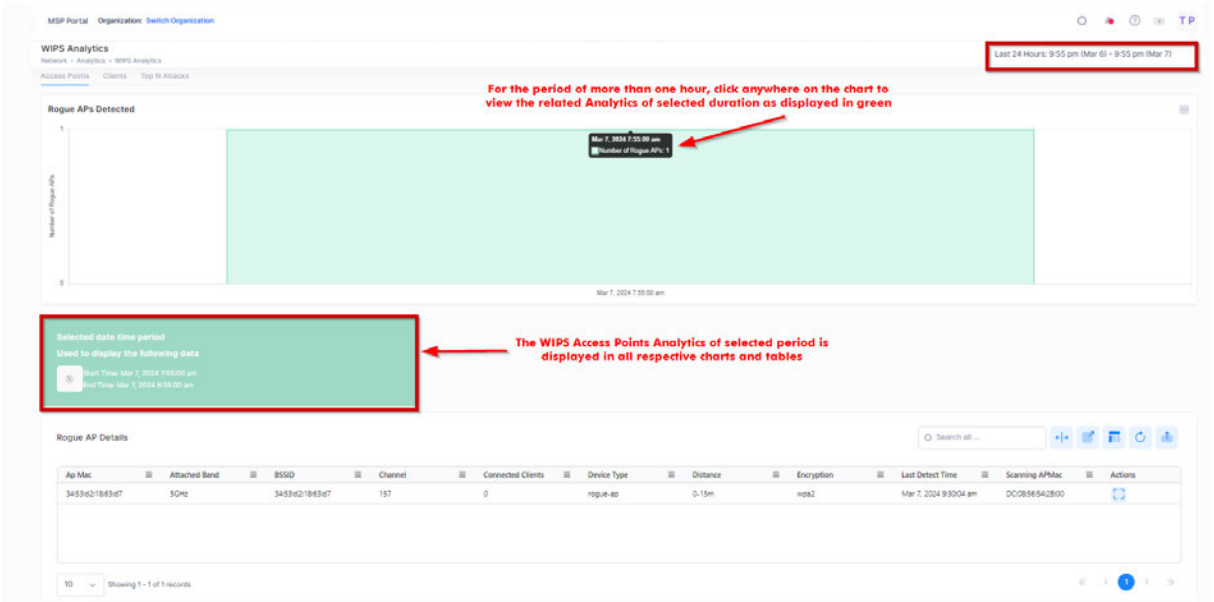
Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



The “Select time” option is used to select the date and period by clicking on one of the bars from the chart to display the other related WIPS Access Points metrics on the screen.

By default, the bar chart selects and displays the latest available Rogue Access Points details for the last hour range. The time interval between two points in the chart is 5 minutes when the last hour is selected from the filter, but the ‘Rogue AP Details’ table displays data for the complete last hour. The Chart bar data is not clickable for the last hour’s time duration.

However, for other ranges (like 6,12 ,24 hour, etc.), the time interval between two points is one hour, and by default, the latest data point is selected. You can click anywhere on the bar chart to see the detailed Analytics and all related Chart details for a specific time duration as shown below:



For each Rogue Access Points table, the following attribute values are provided:

- **AP MAC -** MAC address of the rogue access point.
- **Attached Band** - The frequency band associated with the access point.
- **BSSID** - BSSID of the interfering AP.
- **Channel -** Working channel of the rogue access point.
- **Connected Clients** - The number of clients connected with the rogue access point.
- **Device type** - The type of the Device.
- **Distance -** Distance between the rogue client and the detecting AP.
- **Encryption -** Encryption method of the SSID to which the rogue access point is associated.
- **Last Detect Time -** The latest time that the interfering AP was seen by the valid AP.
- **Scanning APMac** - MAC address of the valid AP that detected the interfering AP.

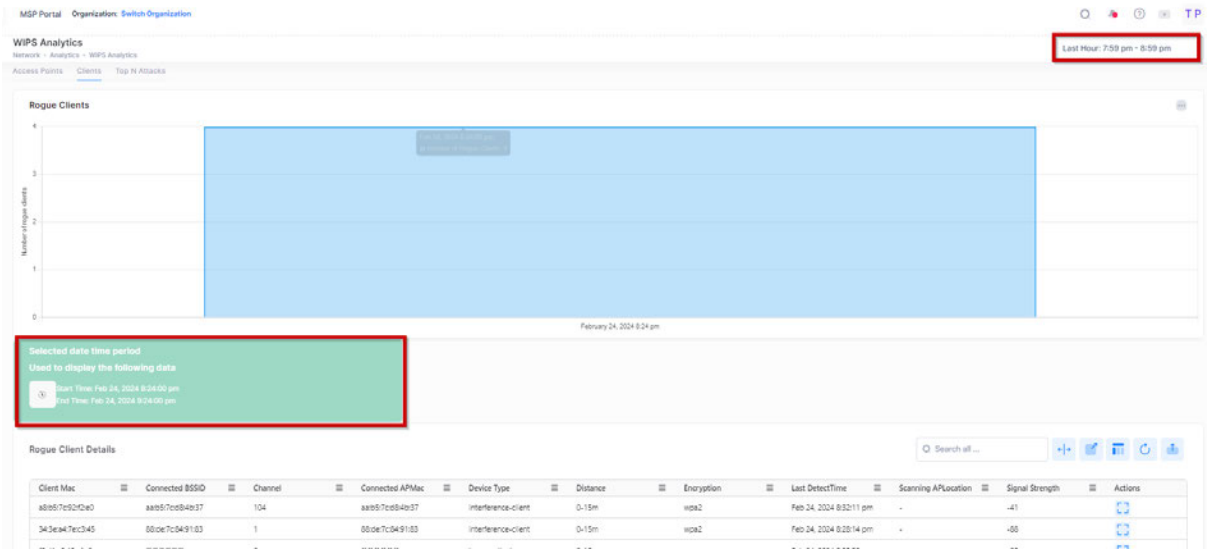
See the Intrusive APs (see page 382) Online help for more information.

21 Oct 2025

8.1.1.3.2 WIPS Clients Analytics

The “WIPS Clients” section of the Monitor WIPS Analytics (see page 818) dashboard includes widgets that show the the Rogue Clients, Blocklisted Clients and DeAuth Clients Table associated with the managed devices during the specified time window range.

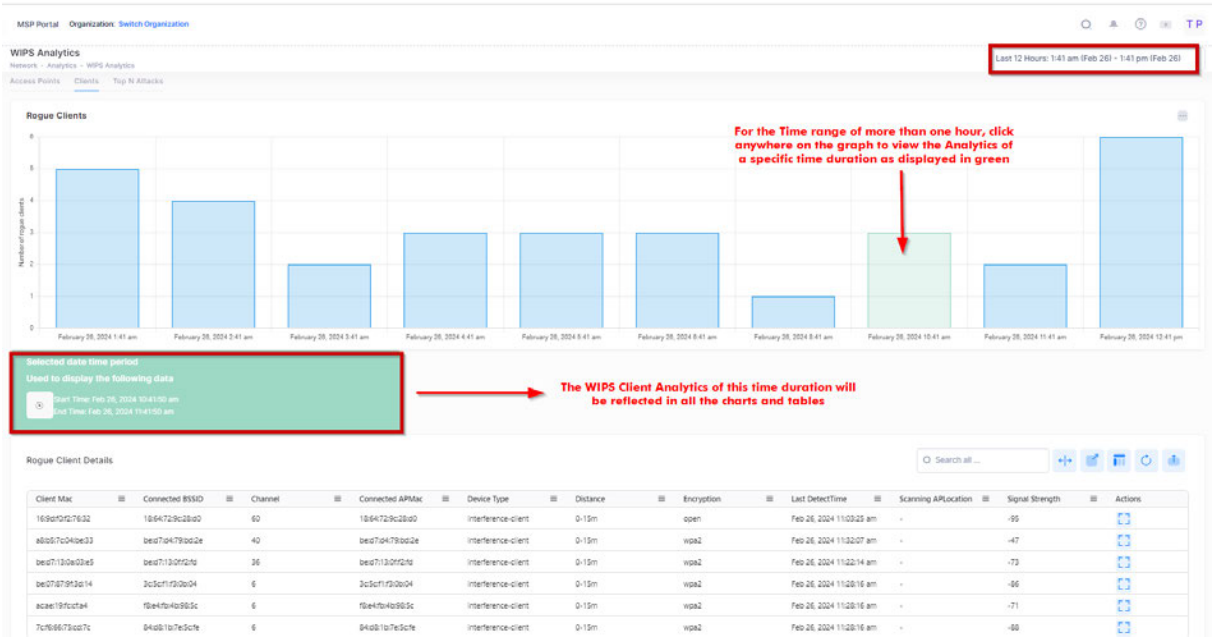
Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



The “Select time” option is used to select the date and period by clicking on one of the bars from the chart to display the other related WIPS Client Analytics metrics on the screen.

By default, the bar chart selects and displays the latest available Client details for the last hour range. The time interval between two points in the chart is 5 minutes when the last hour is selected from the filter, but the ‘Rogue Client Details’ table displays data for the complete last hour. The Chart bar data is not clickable for the last hour’s time duration.

However, for other ranges (like 6,12 ,24 hour, etc.), the time interval between two points is one hour, and by default, the latest data point is selected. You can click anywhere on the bar chart to see the detail Analytics and all related Chart details for a specific time duration as shown below:



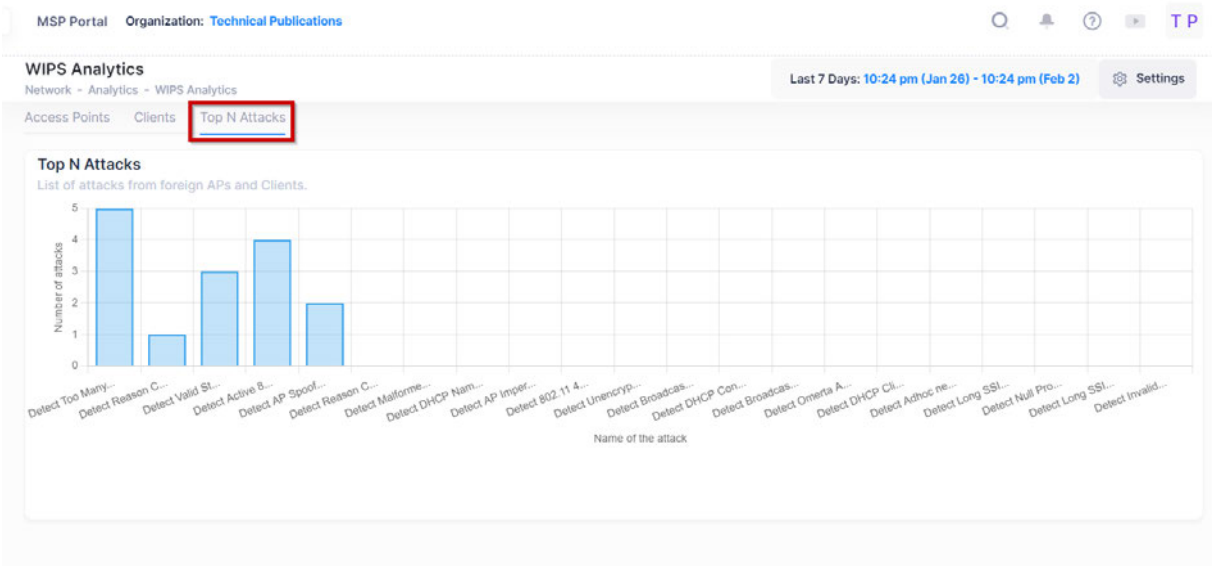
For each Rogue client details table, the following attribute values are provided:

- **Client MAC -** MAC address of the rogue client.
- **Connected BSSID** - BSSID of the interfering AP to which the client is associated.
- **Connected SSID -** ESSID to which the rogue associated.
- **Channel -** Working channel of the rogue client.
- **Connected APMac** - MAC address of the valid AP that detected the interfering AP.
- **Device type** - The type of the device.
- **Distance -** Distance between the rogue client and the detecting AP.
- **Encryption -** Encryption method of the SSID to which the rogue client is associated.
- **Signal Strength -** RSSI of the rogue client.
- **Last Detected Time -** The latest time that the rogue client was seen by the detecting AP.
- **Scanning AP Location** - Location of the valid AP that detected the interfering AP.
- **Reason** - Indicates the reason for classifying the foreign AP as a rogue AP:
  - Signal Strength is Too Strong, Reducing Network Performance
  - Channel is Switching Too Often
  - Broadcasting Conflicted SSID, Misleading User Connection
  - Matching the Keyword of Suspected SSID
  - Matching the Suspected MAC OUI
- **Time Stamp from scanning AP** - The first time when the rogue client was seen by the detecting AP.

21 Oct 2025

8.1.1.3.3 WIPS Top N Attacks

The WIPS Top N Attacks Screen displays information about wireless attacks on the network including AP attacks (see page 823) and Client attacks (see page 385). To access the WIPS Top N Attacks screen, click on **Network > Analytics > WIPS Analytics** and select **Top N Attacks** tab under the “Monitor” section of the OmniVista Terra Menu (see page 45).



The Top N Attacks screen provides a chart of Wireless attacks observed in the network from foreign Access points and Clients based on the type of attack detected during the specified time window range. The graph displays the top 5 attacks (by default) observed in the network.

Below is the list of multiple attacks originating from foreign APs and the attacks originating from wireless clients.

- **Detect AP Spoofing -** An AP Spoofing attack involves an intruder sending forged frames that are made to look like they are from a valid AP.
- **Detect Broadcast De-authentication -** A de-authentication broadcast attempts to disconnect all clients in range. Rather than sending a spoofed de-authentication frame to a specific MAC address, this attack sends the frame to a broadcast address.
- **Detect Broadcast Disassociation -** By sending disassociation frames to the broadcast address (FF:FF:FF:FF:FF:FF), an intruder can disconnect all stations on a network for a widespread DoS.
- **Detect Adhoc Networks using VALID SSID -** If an unauthorized ad hoc network is using the same SSID as an authorized network, a valid client may be tricked into connecting to the wrong network. If a client connects to a malicious ad hoc network, security breaches or attacks can occur.
- **Detect Long SSID -** Detects long SSIDs with more than 32 characters in the name.
- **Detect AP Impersonation -** In AP impersonation attacks, an AP assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for person-in-the-middle attacks, a rogue AP attempting to bypass detection, or a Honeypot attack.
- **Detect Adhoc Networks -** An ad hoc network is a collection of wireless clients that form a network among themselves without the use of an AP. If the ad hoc network does not use encryption, it may expose sensitive data to outside eavesdroppers. If a device is connected to a

wired network and has bridging enabled, an ad-hoc network may also function like a rogue AP. Additionally, ad-hoc networks can expose client devices to viruses and other security vulnerabilities.

- **Detect Wireless Bridge -** Wireless bridges are normally used to connect multiple buildings together. However, an intruder could place (or have an authorized person place) a wireless bridge inside the network that would extend the corporate network somewhere outside the building. Wireless bridges are somewhat different from rogue APs in that they do not use beacons and have no concept of association. Most networks do not use bridges. In these networks, the presence of a bridge is a signal that a security problem exists.
- **Detect Null Probe Response -** A null probe response attack has the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. Many popular NIC cards will lock up upon receiving such a probe response.
- **Detect Invalid Address Combination -** In this attack, an intruder can cause an AP to transmit de-authentication and disassociation frames to its clients. Triggers that can cause this condition include the use of broadcast or multicast MAC address in the source address field.
- **Detect Reason Code Invalid of De-authentication -** De-authentication packets with invalid reason code will be classified as an attack.
- **Detect Reason Code Invalid of Disassociation -** Disassociation packets with invalid reason code will be classified as an attack.
- **Detect Valid Station Mis-association** - This feature does not detect attacks, but rather monitors valid wireless clients and their association within the network. Valid client mis-association is potentially dangerous to network security. The four types of mis-association monitored are:
  - **Valid Client Associated to a Rogue -** A valid client that is associated to a rogue AP
  - **Valid Client Associated to an Interfering AP -** A valid client that is associated to an interfering AP
  - **Valid Client Associated to a Honeypot AP -** A honeypot is an AP that is not valid but is using an SSID that has been designated as valid
  - **Valid Client in Ad Hoc Connection Mode -** A valid client that has joined an ad hoc network
- **Detect Omerta Attack -** Omerta is an 802.11 DoS tool that sends disassociation frames to all clients on a channel in response to data frames. The Omerta attack is characterized by disassociation frames with a reason code of 0x01. This reason code is “unspecified” and is not be used under normal circumstances.
- **Detect Unencrypted Valid Client -** A valid client that is passing traffic in unencrypted mode is a security risk. An intruder can sniff unencrypted traffic (also known as packet capture) with software tools known as sniffers. These packets are then reassembled to produce the original message.
- **Detect 802.11 40MHZ Intolerance Setting -** When a client sets the HT capability “intolerant bit” to indicate that it is unable to participate in a 40MHz BSS, the AP must use lower data rates with all of its clients. Network administrators often want to know if there are devices that are advertising 40MHz intolerance, as this can impact the performance of the network.
- **Detect Active 802.11n Greenfield Mode -** When 802.11 devices use the HT operating mode, they can’t share the same channel as 802.11a/b/g clients. Not only can they not communicate

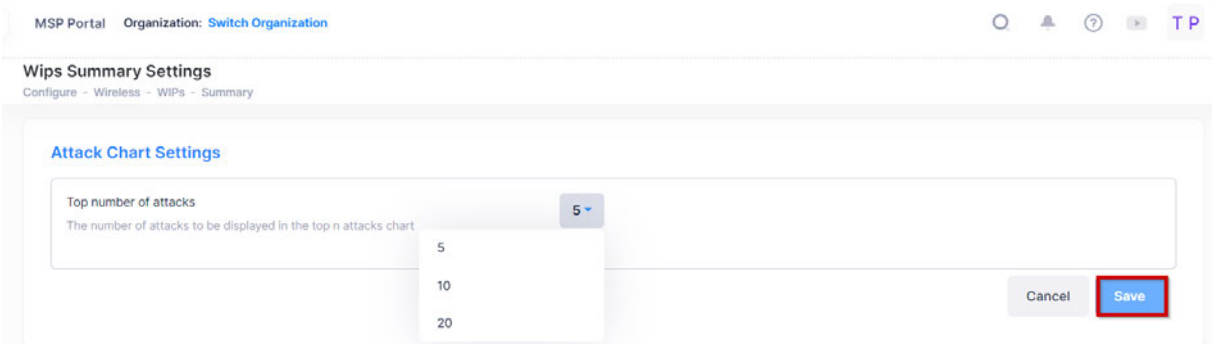
with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.

- **Detect DHCP Client ID -** A client which sends a DHCP DISCOVER packet containing a Client-ID tag (Tag 61) which doesn't match the source MAC of the packet may be doing a DHCP denial-of-service to exhaust the DHCP pool.
- **Detect DHCP Conflict -** Clients which receive a DHCP address and continue to use a different IP address may indicate a mis-configured or spoofed client.
- **Detect DHCP Name Change -** The DHCP configuration protocol allows clients to optionally put the hostname in the DHCP Discover packet. This value should only change if the client has changed drastically (such as a dual-boot system). Changing values can often indicate a client spoofing/MAC cloning attack.
- **Detect Too Many Auth Failure Client -** Client which attempts to connect to Stellar AP but fails to pass the authentication for too many times, indicating an attack client.
- **Detect Malformed Frame-Assoc Request -** Some wireless drivers used in access points do not correctly parse the SSID information element tag contained in association request frames. A malicious association request with a null SSID can trigger a DoS or potential code execution condition on the targeted device.
- **Detect Long SSID At Client -** Detect long SSID in the wireless environment based on packets sent by clients.
- **Detect Reason Code Invalid of De-authentication -** Detect invalid De-authentication Reason Code.
- **Detect Reason Code Invalid of Disassociation -** Detect invalid Disassociation Reason Code.

8.1.1.3.3.1 WIPS Summary Settings

You can set the number of attacks to be displayed in the Top N Attacks by clicking on the **settings** tab at the top of the screen, it redirects you to the WIPS Summary Settings screen.

You can change the Attack Chart settings from here by selecting the top number of attacks from the drop-down list. (By default = 5, or 10 or 20). Click on the **Save** button to apply the changes.

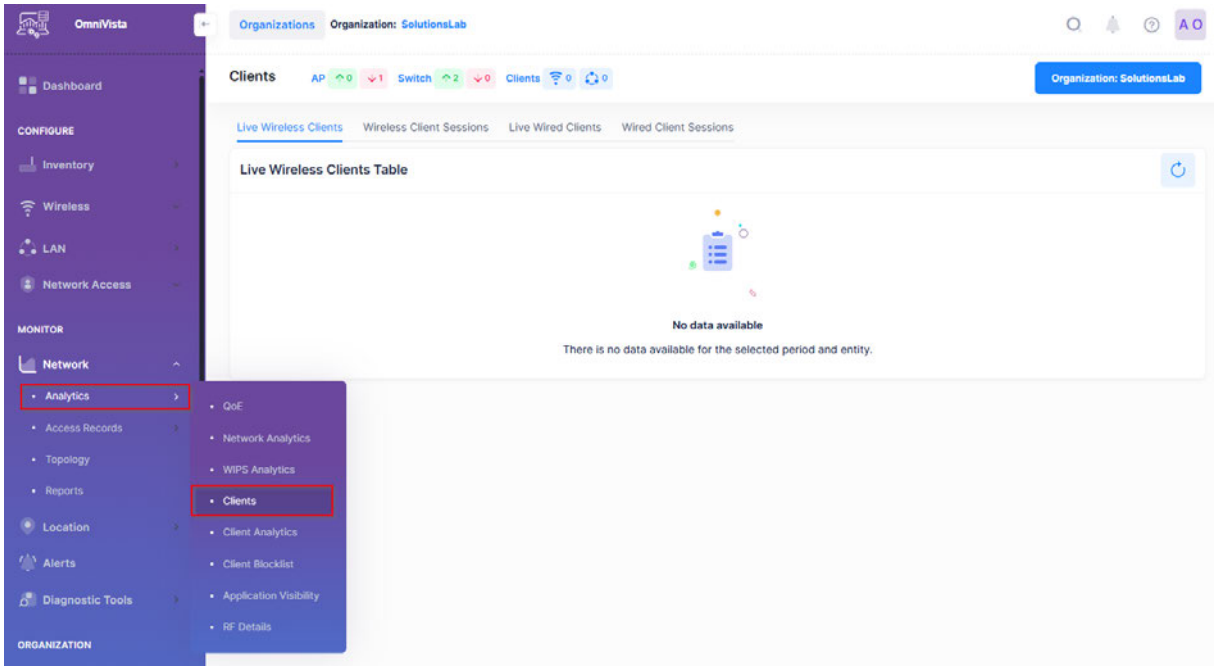


See the Wireless Attacks (see page 385) Online help for more information.

21 Oct 2025

8.1.1.4 Monitor Clients

Use the display filters on the dashboard to define the scope of client activity that you want to monitor based on the organization/ sites/ building/ floors or Devices.



The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the Network.

Further, the Clients Dashboard is divided into four sections to monitor the Live wireless and wired Clients activities:

- **Live Wireless Clients** (see page 827)
- **Wireless Client Sessions** (see page 833)
- **Live Wired Clients** (see page 837)
- **Wired Client Sessions** (see page 841)

Note that the information gathered for “Device Type” and “Device OS” fields in any of the above sections depends on the information provided by the AP Client. As a result, these fields may appear blank based on the capability of the Client to provide the information.

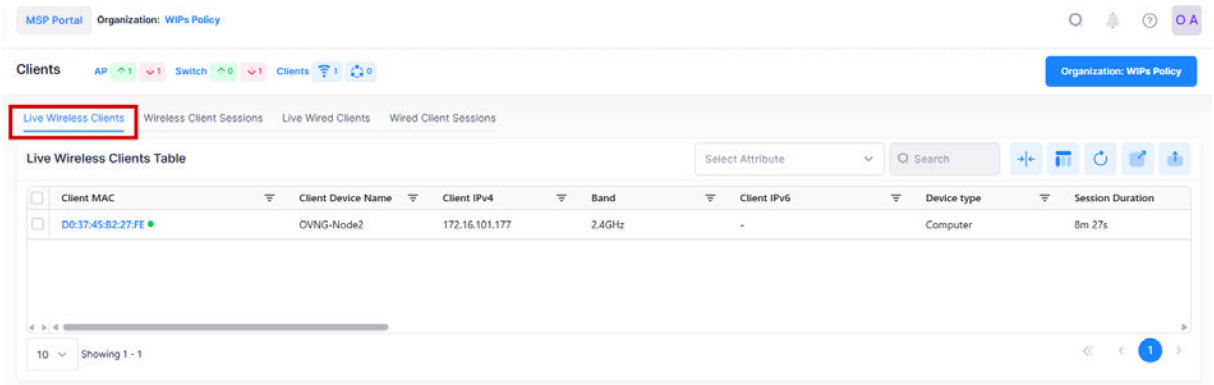
21 Oct 2025

8.1.1.4.1 Monitor Live Wireless Clients

The “Live Wireless Clients” section of the Monitor Clients (see page 826) Dashboard displays a list of the unique online wireless clients associated with the managed Devices.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the Network.

Data displayed can be exported into a CSV, PDF or Excel sheet format. You can also switch to full-screen mode for a better display.



For each client in the list, the following attribute values are provided:

- **Client Device Name** - The Name of the Device (Or device hostname as determined by the Access Point).
- **Client IPV4** - The IPv4 address of the client, if applicable.
- **Client MAC -** The MAC Address of the client**.** (Please note: most mobile devices use random MAC Address for each new connection to avoid tracking).
- **Client IPV6** - The IPv6 address of the client, if applicable.
- **AP Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Device Type** - If determined, the Device Type of the client. (e.g: Mobile, Computer, ...). It is not always available.
- **Session Duration** - The length of time during which the Session was active.
- **Session Start Time** - The date and time on which the Session was started.
- **Device OS** - If determined, the Operating System of the client’s device.
- **AP IP Address** - The current (or last) IP address of the Access Point to which the client is associated.
- **AP MAC** - The MAC address of the Access Point to which the client is associated.
- **AP Model** - The model type of the Access Point (e.g., OAW-AP1221, OAW-AP1251, …).
- **AP Name** - The name of the Access Point.
- **AP Version** - The Version set in the Edit Device page of the Access Point.
- **Site Name** - The Site Name.

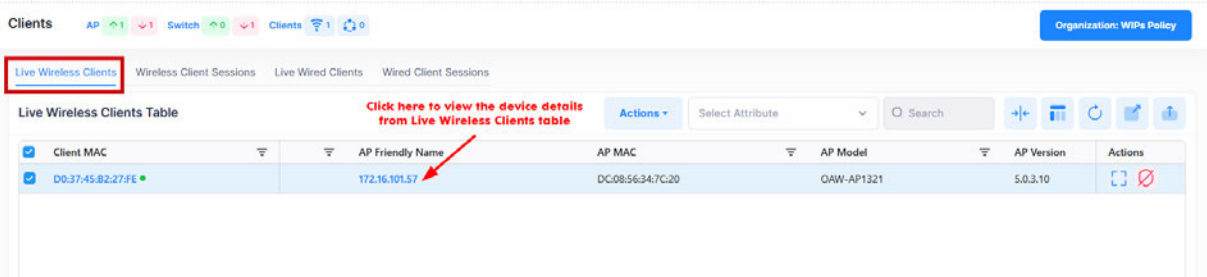
- **AP Location** - The physical location of the Access Point connected to the client.
- **Portal Username** - The username used to connect to the portal.
- **802.1X Username** - The 802.1X username configured for the client, if applicable.
- **Auth Type** - The authentication type used by the client (e.g., WPA2_WPA, PSK, …)
- **Band** - The radio band through which the client attached to the AP (2.4GHz or 5GHz).

Sometimes, for short sessions (lasting less than five minutes), some information may be missing because it could not be determined.

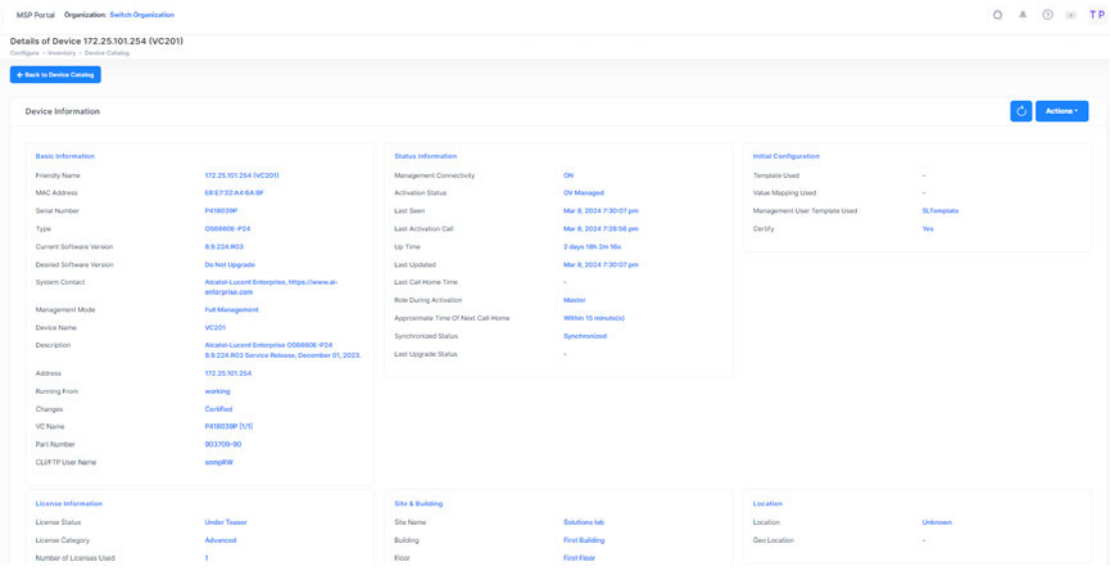
Note: The **Device Type** value is determined on the basis of User-Agent field that is reported in the HTTP header from the client. However, this may not accurately represent the type of device always. This happens when websites accessed by the client device use different value of User-Agent. Some websites set User-Agent to a different value for content optimization, compatibility or other reasons.

8.1.1.4.1.1 View Device Information from Live Wireless Clients Table

To view the Device Information from the Live Wireless Clients Table, click on the 'AP Friendly Name' in the table as shown below:

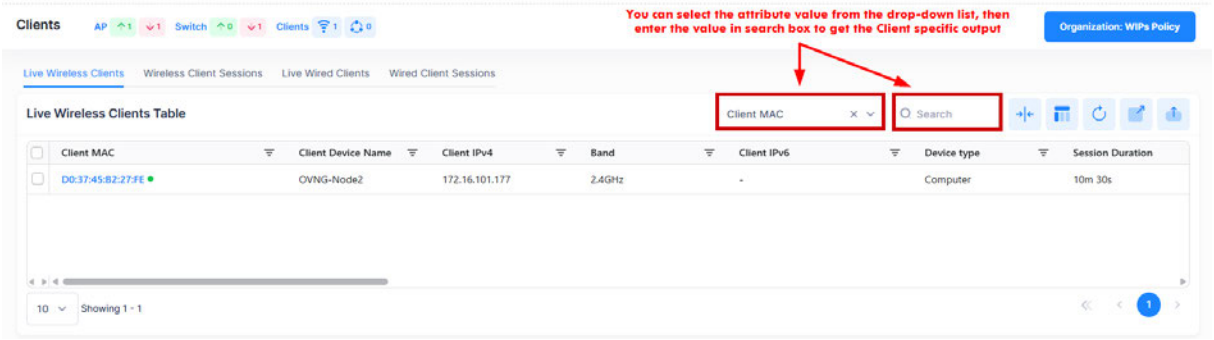


It will redirect you to the 'Device Catalog' screen displaying the Device Information of the selected device. See the Device Catalog (see page 170) online help for more information.



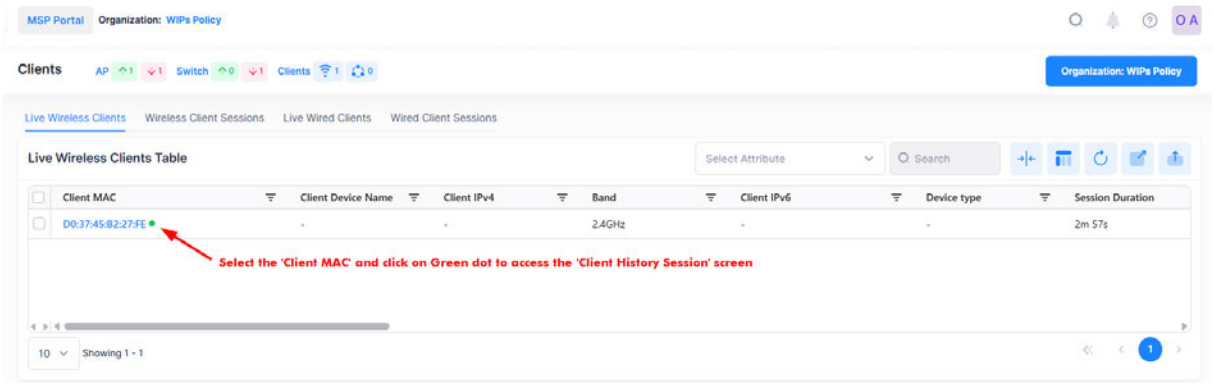
8.1.1.4.1.2 Search Live Wireless Client by an Attribute Value

You can search for Wireless Clients that are live in the network by using the Select Attribute and Search box option. The search results are refined based on the attribute value selected from the available drop-down list (802.1X Username/Client IPv4/Client MAC or Portal Username). Only those Wireless Clients that contain the matching searched values are displayed in the results.



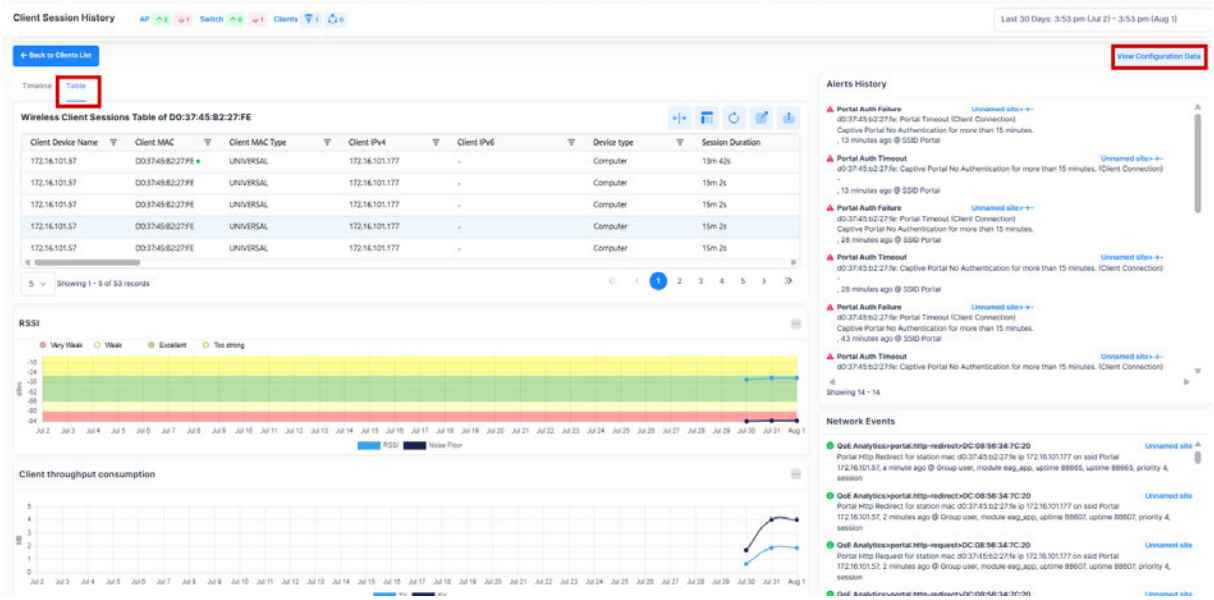
8.1.1.4.1.3 View Wireless Client Session History

If you want to see more details of the Client activity and Client session history for a particular device, then follow the steps as shown below:



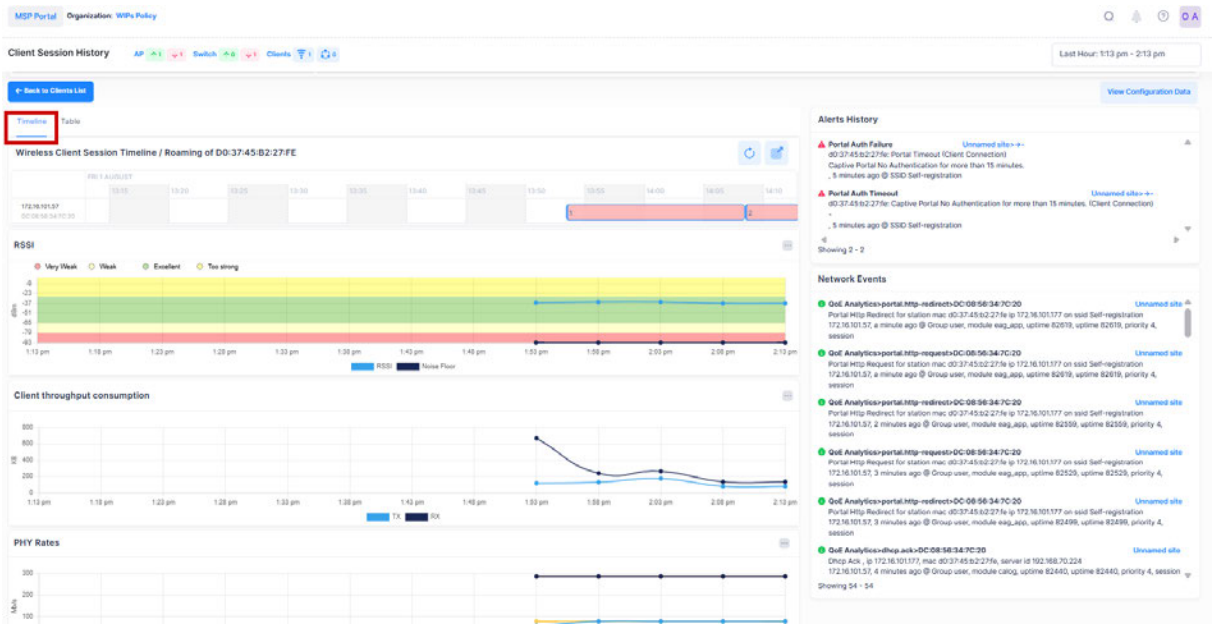
When you click on the MAC address of the selected Client, a new window opens dedicated to displaying information for the selected client. As shown below, this new window displays a summary of activities and session timelines for the individual client. You can also view the device configuration details from this screen by clicking on **View Configuration Data** tab.

There are two display modes to monitor Clients sessions history: Table and Timeline.



17 **Table mode of Client Sessions History**

The geo coordinates displayed in the background reflects the latest Access Point of the currently connected client for the selected time period. Additionally, it displays the graphical information such as RSSI, number of Alerts received, Network Events List, total session duration, Physical Rates for the Client, data usage etc.



18 **Timeline mode of Client Sessions History**

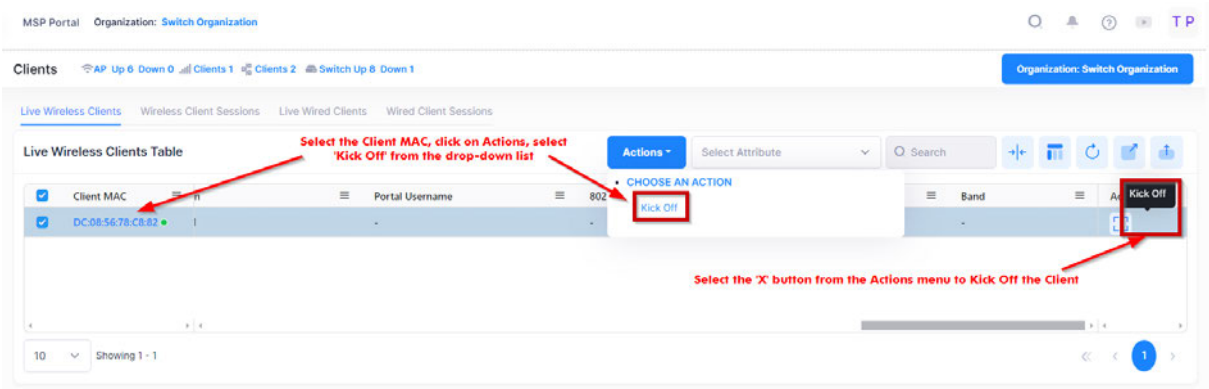
The timeline mode displays a chart of the individual client sessions with the unique roaming ID to monitor the various Access Point sessions based on the selected time period duration. See the Monitor Wireless Client Sessions (see page 833) online help for more information.

- The above Client pages are not accessible from Clients screen; they are only accessible when the user clicks on a specific client in the Clients Table.
- Client Sessions data is retained for 400 days.

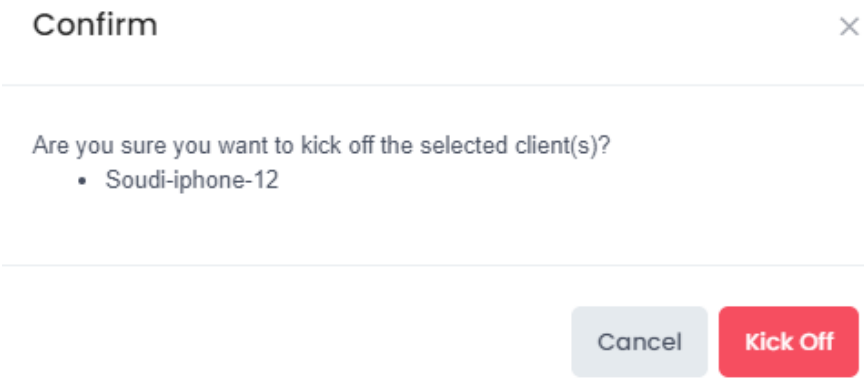
8.1.1.4.1.4 Kick Off Clients

To kick a Wireless Live Client off the network, use one of the following methods to select the Clients you want to log off the network:

- Select the Client MAC on the checkbox next to the Clients Table, click on **Actions**, then select **Kick Off** from the drop-down menu.
- Click on the “X” icon under the “Actions” column next to the table entry for the client that you want to Kick Off.



When you select the Client(s) you want to Kick off, the following confirmation prompt appears:



Click on **Kick Off** to confirm that you want to Kick Off the Client(s).

Note: The Kick-Off operation sends a disconnect action to the Client device, causing it to disconnect. However, if the Client's behavior is to initiate reconnection, then the Client will once again appear on the network. This behavior varies depending on the Client devices and is considered as normal in OmniVista Terra 10.

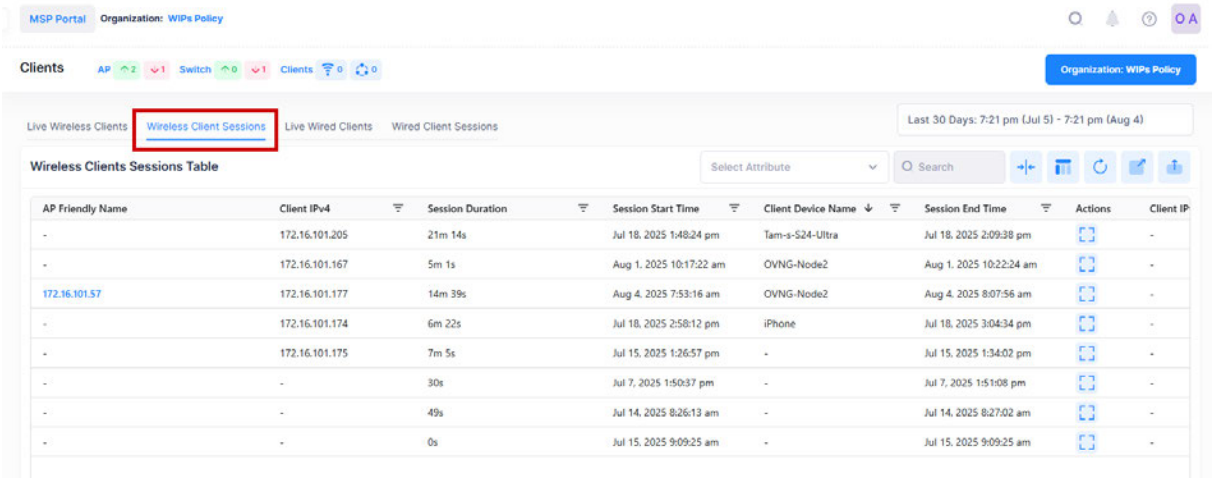
21 Oct 2025

8.1.1.4.2 Monitor Wireless Client Sessions

The “Wireless Client Sessions” section of the Monitor Clients (see page 826) dashboard includes widgets that show the wireless client sessions Table associated with the managed devices during the specified time window range.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count and number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the Network.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



For each historical wireless client session, the following attribute values are provided:

- **Client Device Name** - The client Device Name.
- **Client MAC** - The MAC Address of the client.
- **Client IPV4** - The IPv4 address of the client, if applicable.
- **AP Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Client IPV6** - The IPv6 address of the client, if applicable.
- **Device Type** - If determined, the Device Type of the client. (e.g: Mobile, Switch, Computer, ...)
- **Session Duration** - The length of time during which the Session was active
- **Session Start Time** - The date on which the Session was started
- **Session End Time** - The date on which the Session was stopped
- **Device OS** - If determined, the Operating System of the client’s device
- **AP IP Address** - The IP Address address of the Access Point to which the client is associated
- **AP MAC** - The MAC address of the Access Point to which the client is associated
- **AP Model** - The model type of the Access Point (e.g., OAW-AP1221, OAW-AP1251, …)
- **AP Name** - The name of the Access Point
- **AP Version** - The Version set in the Edit Device page of the Access Point
- **Site Name** - The Site Name

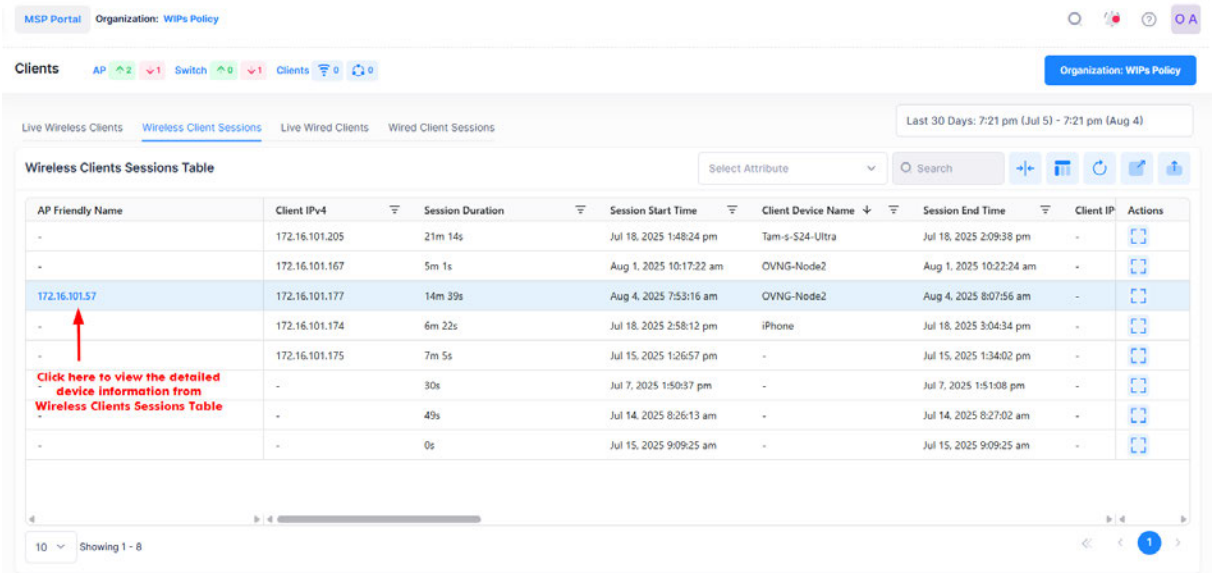
- **AP Location** - The physical location of the Access Point connected to the client.
- **Portal Username** - The username used to connect to the portal.
- **802.1X Username** - The 802.1X username configured for the client, if applicable.
- **Auth Type** - The authentication type used by the client (e.g., WPA2_WPA, PSK, …)

Notes:

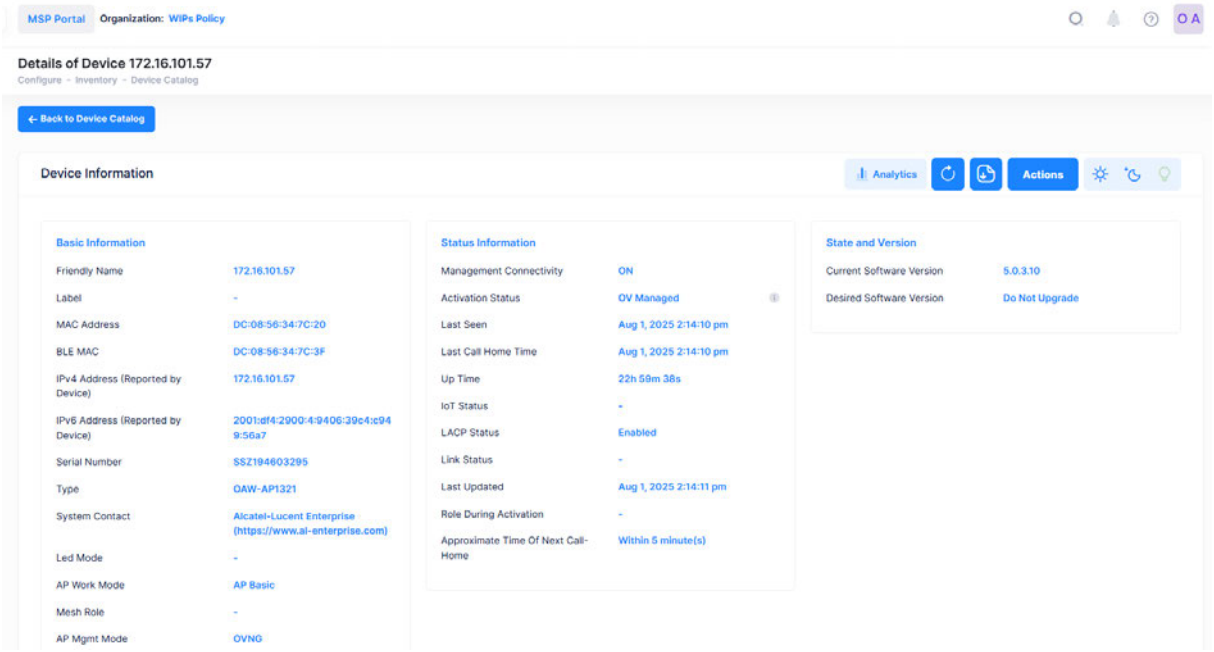
- The Wireless Clients Sessions table displays the history of closed Clients sessions as well as live Clients Sessions.
- The Green dot in the table represents the live Clients which are connected in the Network.
- If the 'Client Device Name' is not available, it should be learned from the corresponding entry in the 'Company Property' list table, if it exists.

8.1.1.4.2.1 View Device Information from Wireless Client Sessions Table

To view the Device Information from the Wireless Client Sessions Table, click on the ‘Friendly Name’ in the table as shown below:

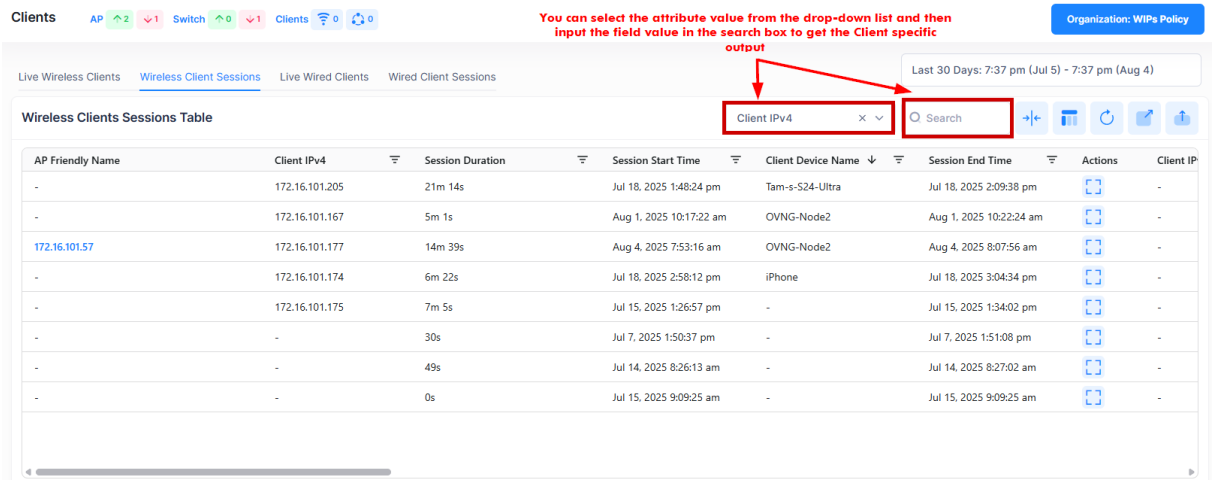


It will redirect you to the ‘Device Catalog’ screen displaying the Device Information of the selected device. See the Device Catalog (see page 170) online help for more information.



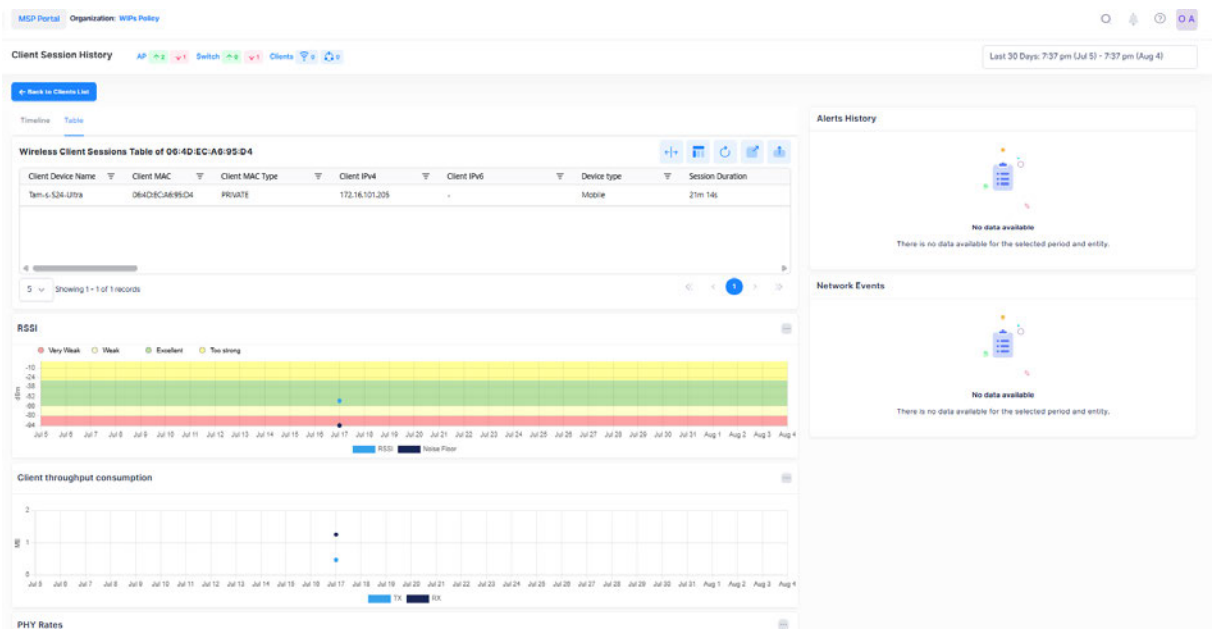
8.1.1.4.2.2 Search Wireless Client Sessions by an Attribute Value

You can search for any of the possible field values or attribute values that exist in the Wireless Clients Sessions Table List by using the Select Attribute and Search option. The search results are refined based on the attribute value selected from the available drop-down list (802.1X Username/Client IPv4/ Client MAC or Portal Username). Only those Wireless Clients that contain the matching searched attributes are displayed in the search results.



8.1.1.4.2.3 View Client Session History

If the user want to see more details of the Client activity and Client session history for a particular device, then click on the MAC address of the selected Client, a new window opens dedicated to displaying information for the selected client. As shown below, this new window displays a summary of activities and session timelines for the individual client.



For each of the Client, you can Monitor the following Client details:

- **RSSI -** It is the received signal intensity measured in dBm for the particular Client. The “Noise Floor” displays the detected noise floor value in dBm for the Client.
- **Client Throughput Consumption** - It displays the data usage of the Client in bytes.
- **PHY Rates -** It displays the detected physical Rates for the Client. The Rx WiFi/Tx WiFi rate represents the maximum speed supported by the Client in Bytes/second. The Tx/Rx rate displays the data rate reported by the Access points in Bytes/second.
- **Alerts Entry List -** It displays the Alerts for the Client all devices within the Organization scope and specified timeframe and updated in real-time.
- **Network Events -** The Network Events screen displays configured events received from device and provides basic event information (for example, severity, date/time received).

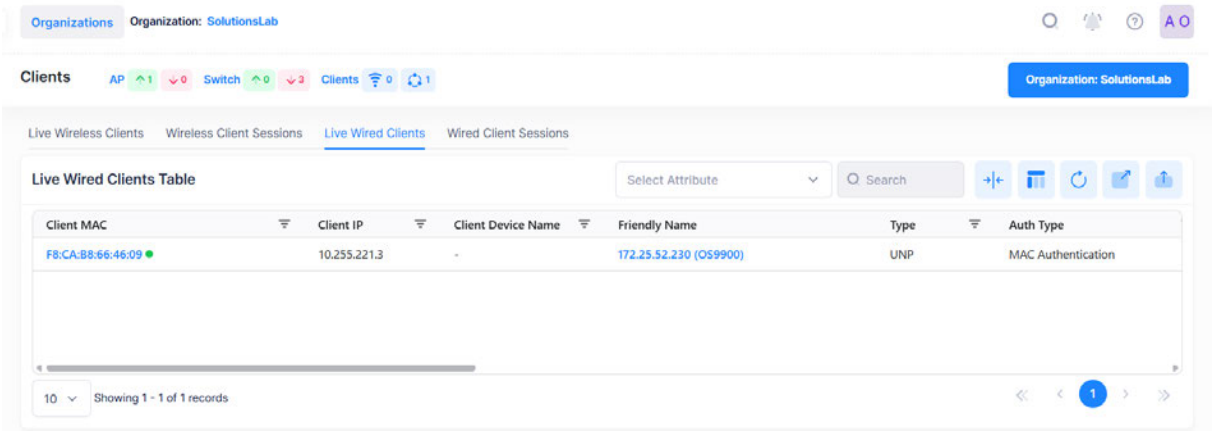
21 Oct 2025

8.1.1.4.3 Monitor Live Wired Clients

The “Live Wired Clients” section of the Monitor Clients (see page 826) dashboard displays a list of unique live wired clients associated with managed devices.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the network.

Data displayed in the list can be exported into a CSV, PDF or Excel sheet format. You can also switch the list to full-screen mode for a better display.



For each Client in the list, the following attribute values are provided:

- Switch Clients are displayed only if they are connected to a UNP port.
- Stellar Access Points connected to a UNP port are displayed as UNP clients.
- Wired clients not connected to a UNP port (non-UNP Clients) are not included in this list.

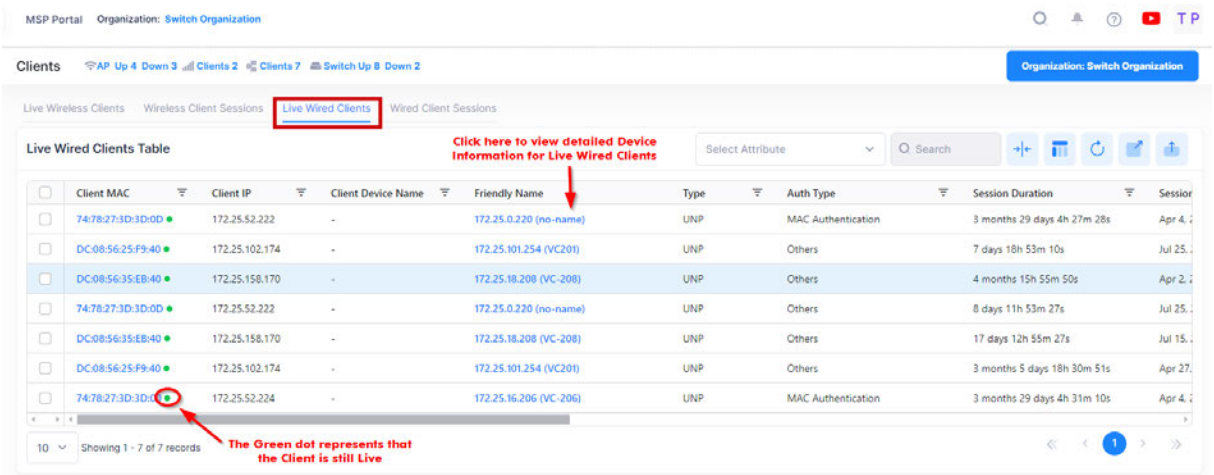
- **Client Device Name** - The name of the device (or device hostname as determined by the Access Point).
- **Client IP Address** - The IP address of the client, if applicable.
- **Client MAC -** The MAC address of the client. (Please note: most mobile devices use a random MAC address for each new connection to avoid tracking).
- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Type** - Indicates if the Client is wired to an Access Point or connected to a Switch as a UNP Client.
- **Device Type** - If determined, the Device Type of the client (e.g: Mobile, Computer, ...). This information is not always available.
- **Session Duration** - The length of time during which the Session was active.
- **Session Start Time** - The date and time on which the Session was started.

- **Session End Time** - The date and time on which the Session was stopped. (No value in this field indicates the session is ongoing).
- **Device MAC** - The MAC address of the device to which the client is wired.
- **Site Name** - The Site name of the device to which the client is wired.
- **Switch SN.** - The serial number of the Switch to which the wired Client is connected (applicable for UNP Clients only).
- **Client username** - The username used by the Client or UNP profile used by the wired Client (This value can be the same as the Client MAC address value in case MAC authentication is used by the Client).
- **Tx Total -** The total number of bytes transmitted by the Client to the device.
- **Rx Total** - The total number of bytes received by the Client from the device.
- **VLAN** - The VLAN through which the Client accesses the network.
- **Port** - The name of the port.

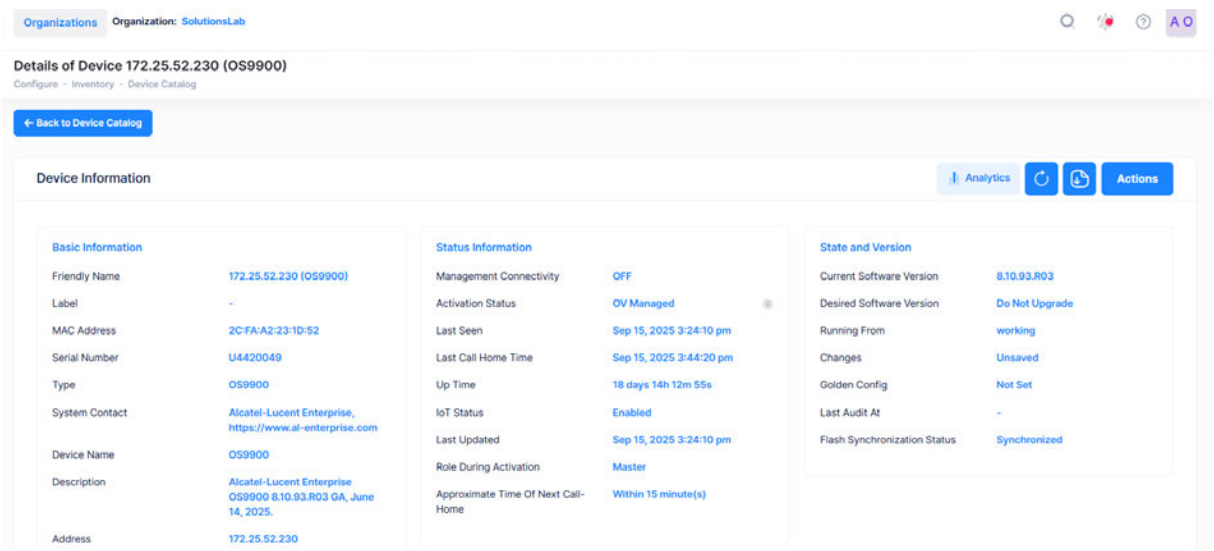
Sometimes, for short sessions (lasting less than five minutes), some information may be missing because it could not be determined.

8.1.1.4.3.1 View Device Information from Live Wired Clients Table

To view the Device Information from the Live Wired Clients Table, click on the “Friendly Name” in the table as shown below.

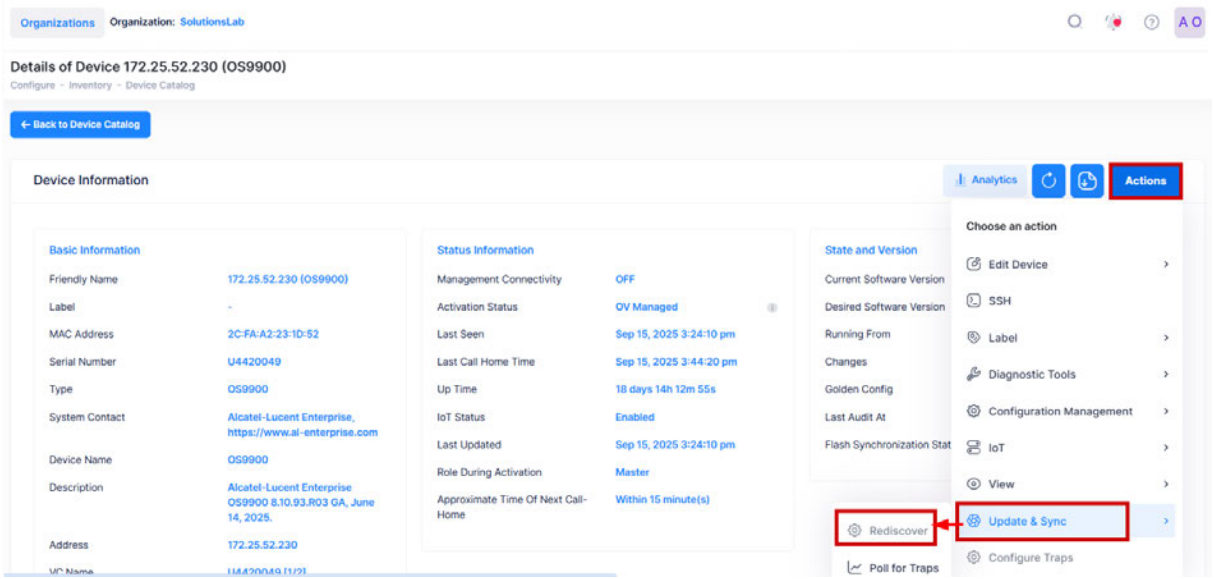


You are then redirected to the Device Details screen for the selected device. See the Device Catalog (see page 170) online help for more information.



Note: If the Live Wired Clients Table continues to show a green dot for a disconnected Client, follow the steps shown below to rediscover the device and update the Live Wired Clients Table.

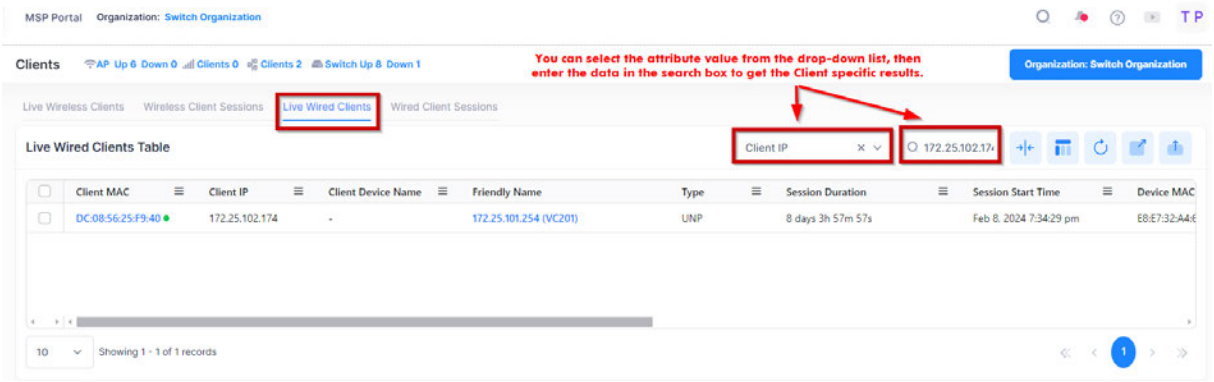
- Click the “Friendly Name” in the Live Wired Clients Table to view the Device Detail screen.
- Click on **Actions** and hover your cursor over **Update and Sync**, then select **Rediscover** from the drop-down menu.
- The Live Wired Clients Table will update with the device's latest status.



8.1.1.4.3.2 Search Live Wired Clients by Attribute Value

You can search for Wired Clients that are live in the network by using the Select Attribute and Search box option. The search results are refined based on the attribute value selected from the available

drop-down list (Client IP/Client MAC or Client Username). Only those Wired Clients that contain the matching searched attributes are displayed in the search results.



8.1.1.4.3.3 View Wired Clients Session History

If you want to see more details of the Wired Client activity and Client session history for a particular device, then click on the MAC address of the selected Client, a new window opens dedicated to displaying information for the selected client. See the Monitor Wired Client Sessions (see page 841) online help for more information.

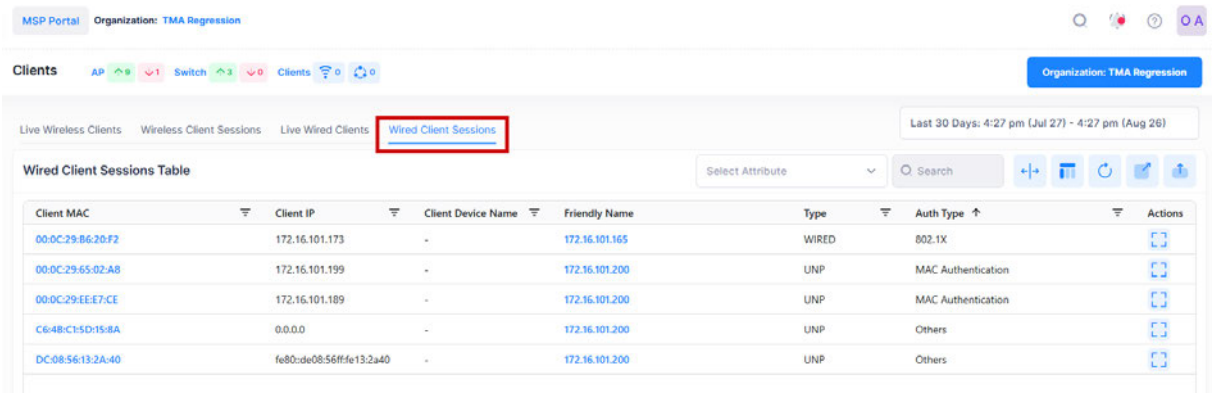
21 Oct 2025

8.1.1.4.4 Monitor Wired Client Sessions

The “Wired Client Sessions” section of the Monitor Clients (see page 826) dashboard displays a list of wired clients sessions. The Wired Client Sessions Table lists sessions associated with managed Devices connected through wired ports during the specified time window range.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the Network.

Data displayed in the list can be exported into a CSV, PDF or Excel sheet format. You can also switch the list to full-screen mode for a better display.



For each historical wired client session, the following attribute values are provided:

> Switch Client sessions are displayed only if the Clients are connected to UNP ports. Wired client sessions for Clients not connected to a UNP port (non-UNP Clients) are not included in this list.

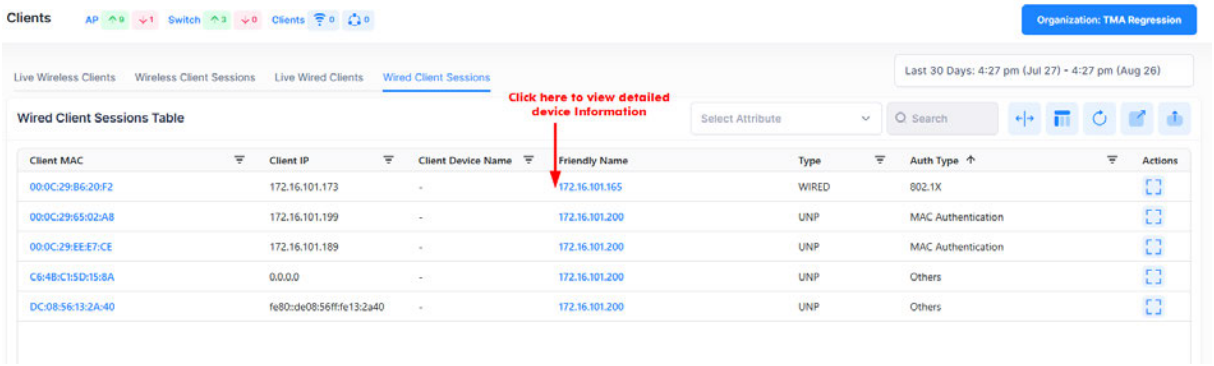
- **Client Device Name** - The client Device Name.
- **Client MAC** - The MAC Address of the client.
- **Client IP** - The IP address of the client, if applicable.
- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Type** - It provides the information that the Client is wired to an Access Point or connected to a Switch as a UNP Client.
- **Auth Type** - The authentication type used by the client
- **Session Duration** - The length of time during which the Session was active.
- **Session Start Time** - The date and time on which the Session was started.
- **Session End Time** - The date and time on which the Session ended.
- **Device MAC** - The MAC address of the Device to which the Client is wired.
- **Switch SN**. - The serial number of the Switch to which the wired Client is connected (applies only to UNP Clients).

- **Port** - The name of the port.
- **VLAN** - The VLAN which is in use.
- **Site Name** - The Site Name of the Device to which the client is wired.
- **Client Username** - The username used by the Client or UNP profile used by the wired Client (This value can be the same as the Client MAC address value in case MAC authentication is used by the Client).

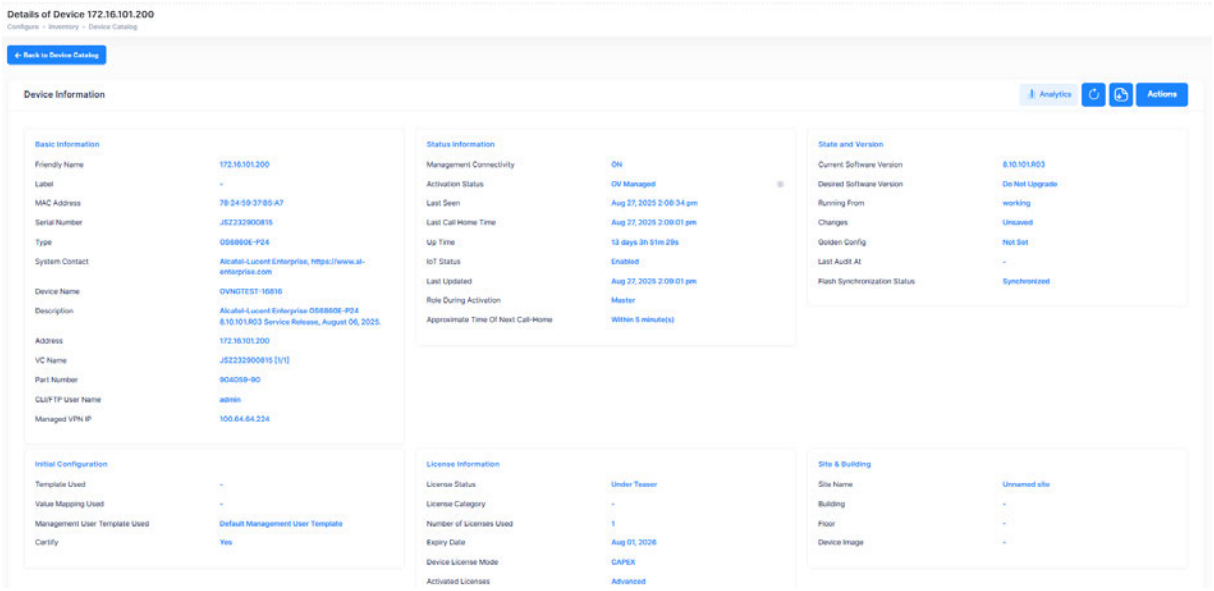
- The Wired Client Sessions table displays the history of closed Clients sessions as well as live Client Sessions.
- The Green dot in the table represents the live Clients which are connected in the Network.

8.1.1.4.4.1 View Device Information from Wired Client Sessions Table

To view the Device Information from the Wired Client Sessions Table, click on the 'Friendly Name' in the table as shown below:

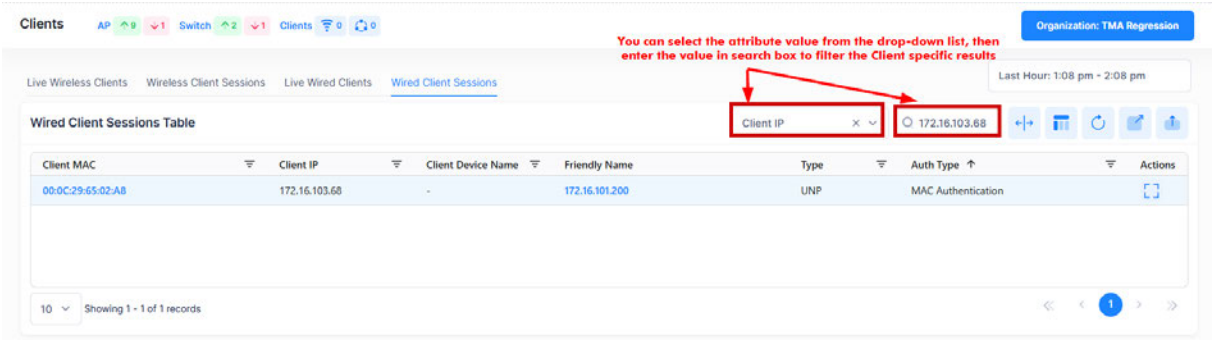


It will redirect you to the 'Device Catalog' screen displaying the Device Information of the selected device. See the Device Catalog (see page 170) online help for more information.



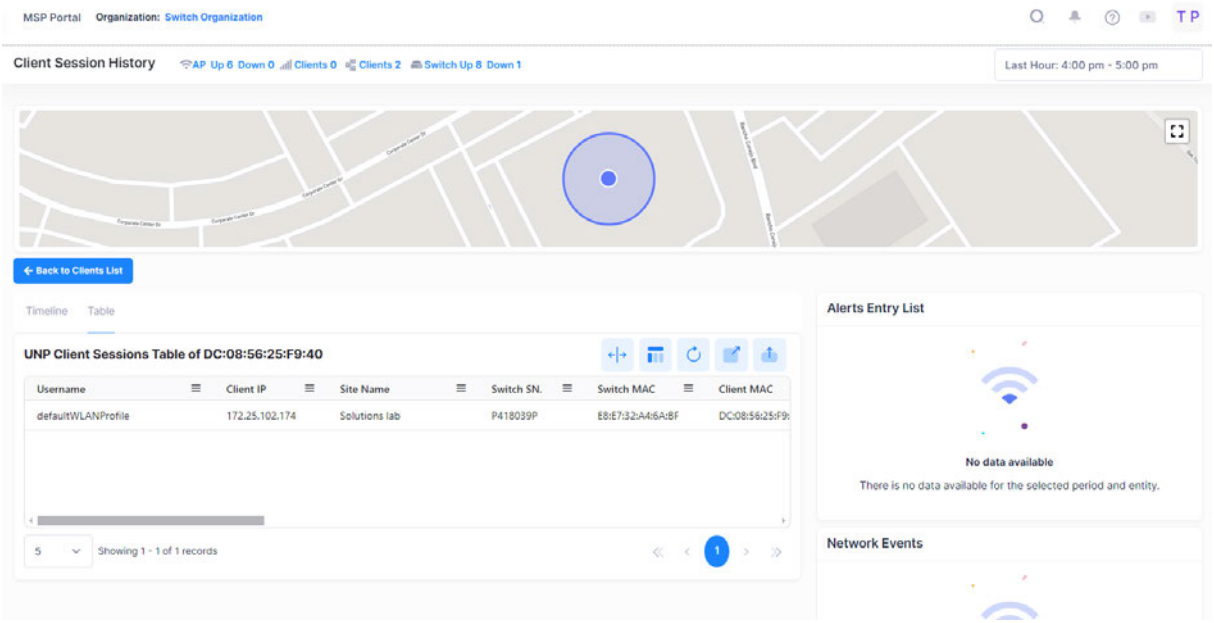
8.1.1.4.4.2 Search Wired Client Sessions by Attribute Value

You can search for Client sessions that exist in the Wired Client Sessions Table List by using the Select Attribute and Search option. The search results are refined based on the attribute value selected from the available drop-down list (Client IP/Client MAC or Client Username). Only those Wired Clients that contain the matching searched attributes are displayed in the search results.



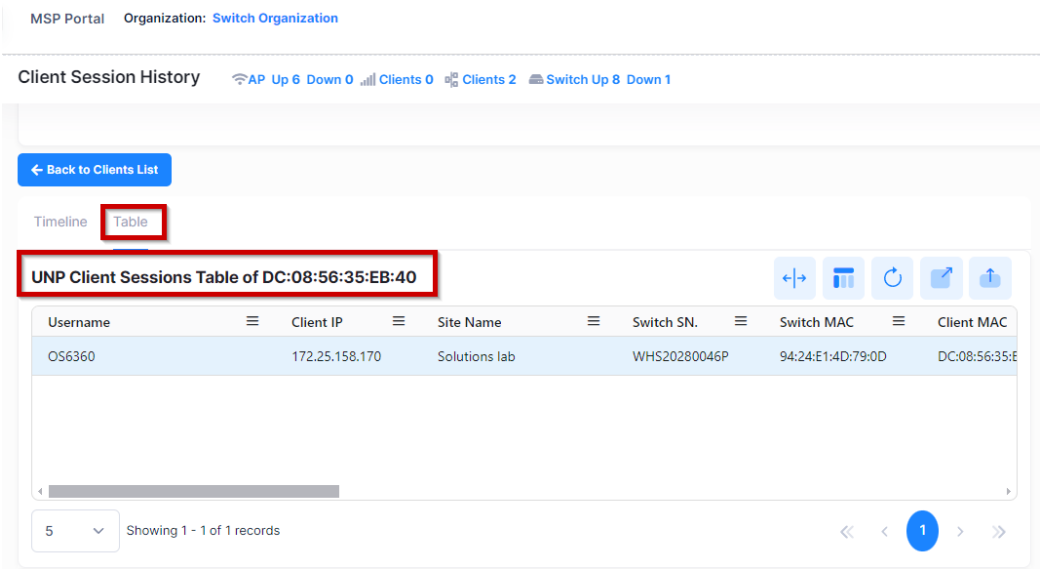
8.1.1.4.4.3 View Client Sessions History

If you want to see more details of the Client activity and Client session history for a particular device, then click on the MAC address of the selected Client, a new window opens dedicated to displaying information for the selected client. As shown below, this new window displays a summary of activities and session timelines for the individual Client.



For each of the Client, you can Monitor the following Client details:

- **UNP Client Sessions Table of Device -** It displays the Session detail of UNP Clients which are wired to the Switch or Clients which are wired to the Access Point of a device as shown below:

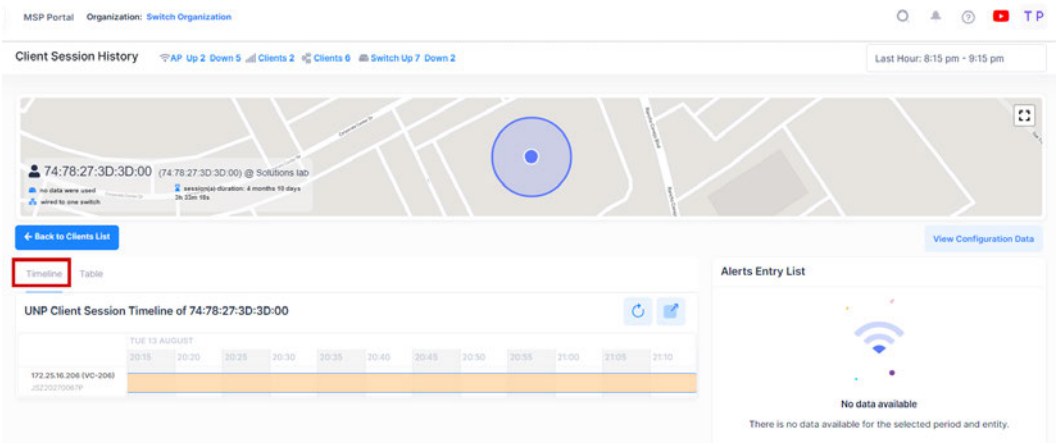


For each UNP session, the following attribute values are provided:

- **Username** - The username used by the Client or UNP profile used by the wired Client (This value can be the same as the Client MAC address value in case MAC authentication is used by the Client).
- **Switch MAC** - The MAC Address of the Device to which the Client is wired.
- **Client MAC** - The MAC Address of the client.
- **Client IP** - The IP address of the client, if applicable.
- **UNP Profile** - The UNP Profile of the Client.

- **Type** - It provides the information that the Client is wired to an Access Point or connected to a Switch as a UNP Client.
- **Session Duration** - The length of time during which the Session was active.
- **Session Start Time** - The date and time on which the Session was started.
- **Session End Time** - The date and time on which the Session ended.
- **Switch SN**. - The serial number of the Switch to which the Client wired with (applicable for UNP Clients only).
- **Port** - The name of the port.
- **VLAN** - The VLAN which is in use.
- **Authentication Type** - The authentication type used by the client (e.g., WPA2_WPA, PSK, …)
- **Site Name** - The Site Name of the Device to which the client is wired.
- **Tx Total -** The total number of bytes transmitted to the client during the session.
- **Rx Total** - The total number of bytes received by the client during the session.
- **Tx Packets -** The total number of packets transmitted to the client during the session.
- **Rx Packets -** The total number of packets received by the client during the session.

- **Wired Client Session History** - It displays the Wired Session History detail of Clients which are wired to the Switch or Clients which are wired to the Access Point of a device as shown below:



- **Alerts Entry List -** It displays the Alerts for the Client all devices within the Organization scope and specified timeframe and updated in real-time.
- **Network Events -** The Network Events screen displays configured events received from device and provides basic event information (for example, severity, date/time received).

21 Oct 2025

8.1.1.5 Monitor Client Analytics

Monitoring client analytics allows you to determine the characteristics of the clients that are currently connected or have been connected to your WiFi network. The information in this section describes how to utilize the OmniVista Terra Client Analytics Dashboard (see page 847) to monitor the following client metrics:

- Connected Clients Over Time (see page 849)
- Client Distribution (see page 850)
- Client Throughput Consumption
- Connected Duration Within the Hourly Selection (see page 855)
- Devices Per-User (see page 857)

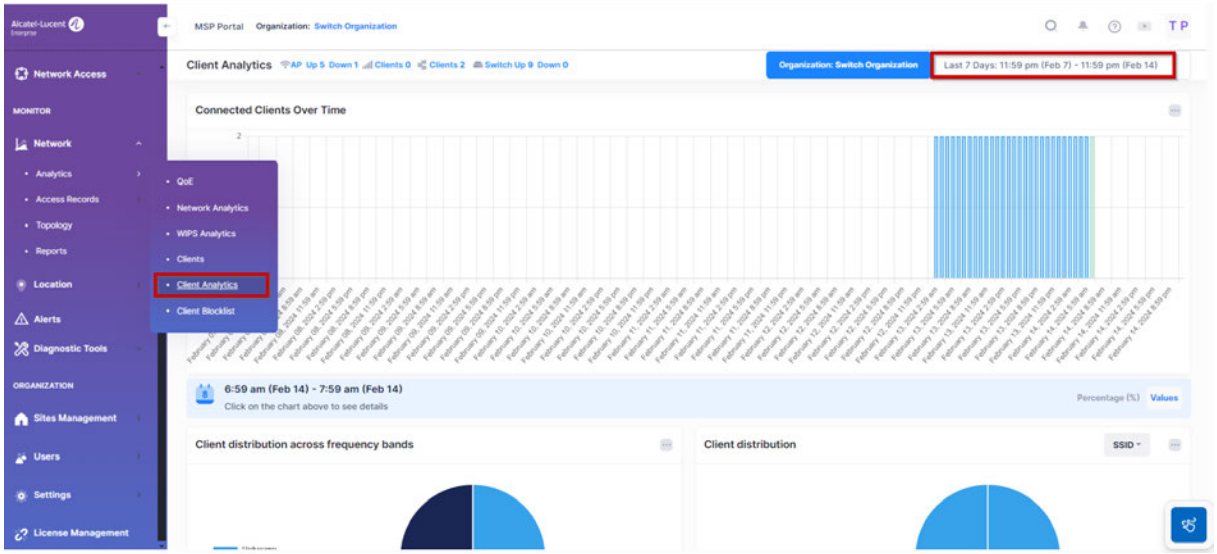
21 Oct 2025

8.1.1.5.1 Client Analytics Dashboard

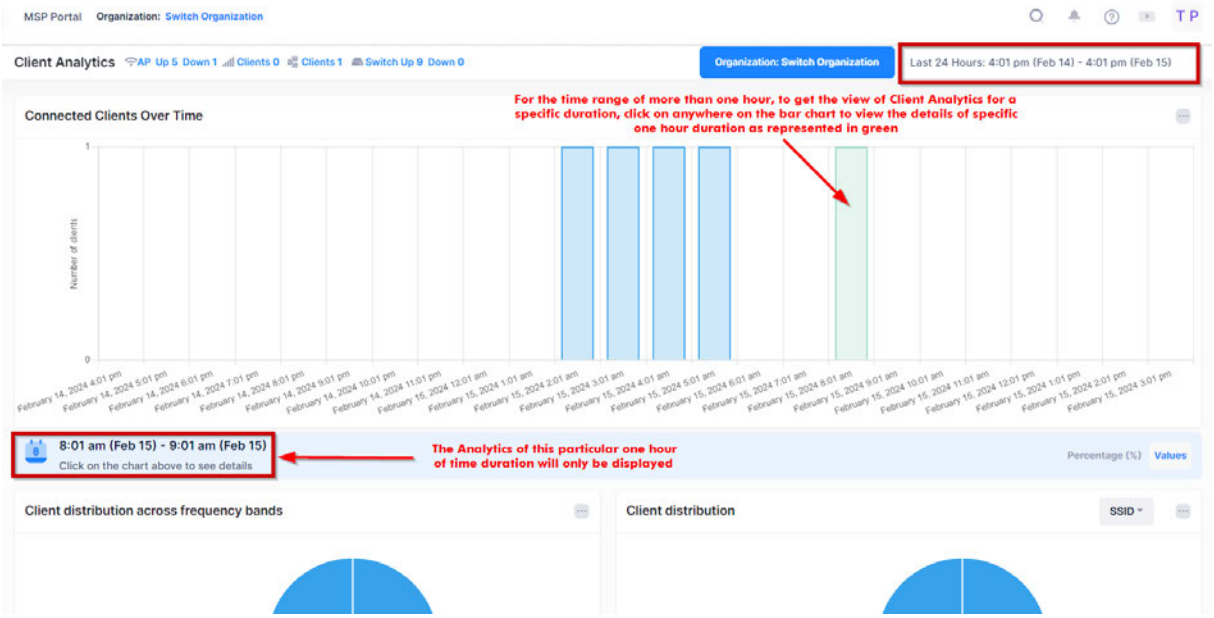
The Client Analytics Dashboard provides an overview of Client metric values. To access the Client Analytics Dashboard, click on **Network > Analytics > Client Analytics** under the “Monitor” section of the OmniVista Terra Menu (see page 45).

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the Network.

Adjust the display filters on the dashboard by selecting either the entire Organization, specific Sites, Building, Floors, or even Access Points to display metrics related to Clients that are connected to the managed Access Points located within the selected scope. You can also select a period of time during which metrics are retrieved.



The **Connected Clients Over Time** bar graph display changes with different Time filter selections. If you select the last one hour time window range, then all the chart attributes are displayed by default. However, if you select a longer range of time period, such as the last 6 hours or last 7 days, to get the view of all the other related pie charts for a specific duration, click on a date time period on one of the bars in the chart, which represents a single hour (indicated in green rectangle) as shown below.



Use the Client Analytics Dashboard to monitor and evaluate the following metric values:

- Connected Clients Over Time (see page 849)
- Client Distribution (see page 850)
- Client Throughput Consumption (see page 854)
- Connected Duration Within the Hourly Selection (see page 855)
- Devices Per-User (see page 857)

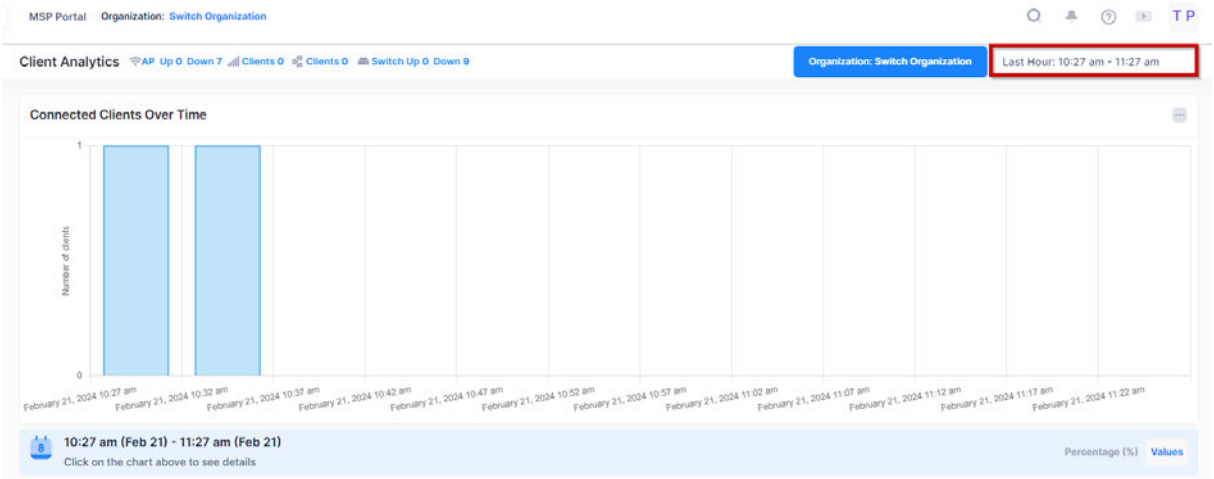
Note: The time range which can be selected to view the latest Client Analytics metrics should not be more than 7 days. You cannot customize the range to view client analytics metrics for the last 30 days period.

21 Oct 2025

8.1.1.5.2 Connected Clients Over Time

The Connected Clients Over Time section of the Client Analytics Dashboard (see page 847) includes widgets that shows the graphical display of the number of clients connected to managed Access Points during the specified time window. The “Select time” option is used to select the date and period by clicking on one of the bars from the chart to display the other related Client Analytics metrics on the screen. By default, the bar chart selects and displays the latest available Client details for the last hour range.

The Network Analytics Summary (see page 873) at the top of the dashboard displays the total number of Access Points, Access Points Up, Down Count, number of Live Wireless and Wired Clients, total number of Switches, Switches Up and Down Count in the Network.



Note: The Chart bar data is not clickable for the last hour’s time duration. However, more than one hour, you can click anywhere on the bar chart to see the detail Analytics and all related Chart details for a specific time duration.

Data displayed in the chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.

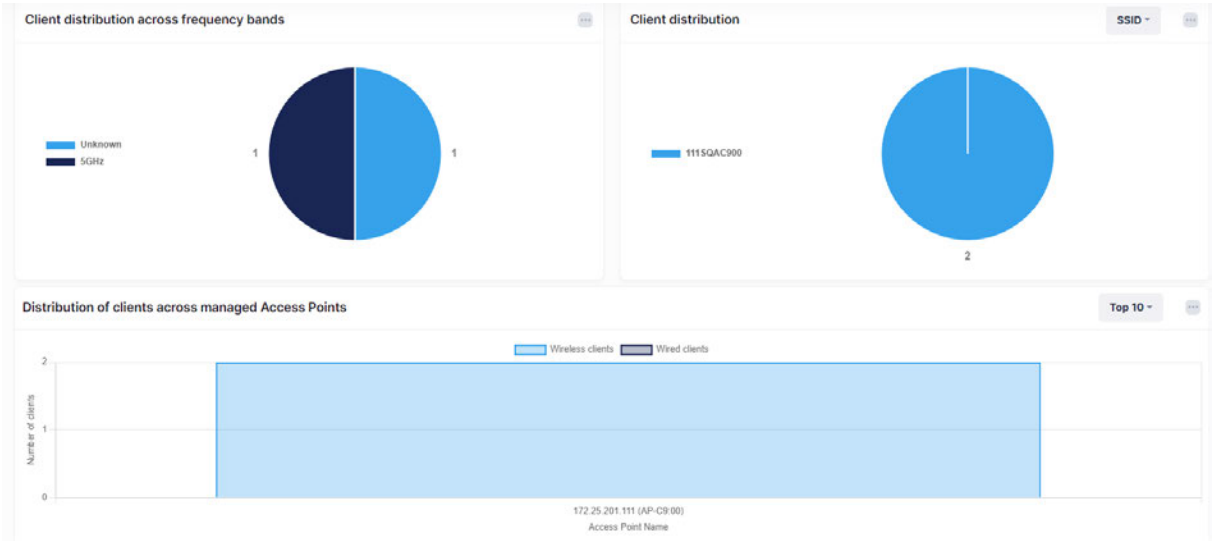
Note: Do not select a time range to view the latest Client Analytics metrics that is more than 7 days. You cannot specify a custom time range to view the Connected Clients Over Time metrics for the last 30-day period.

21 Oct 2025

8.1.1.5.3 Client Distribution

The Client Distribution section of the Client Analytics Dashboard (see page 847) includes widgets that show the distribution of connected clients on the 2.4 GHz, 5 GHz, and 6 GHz bands that allows you to analyze the number of clients connected on each Access Point.

Data displayed in each widget can be exported into a CSV or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



19 **Client Distribution Widgets**

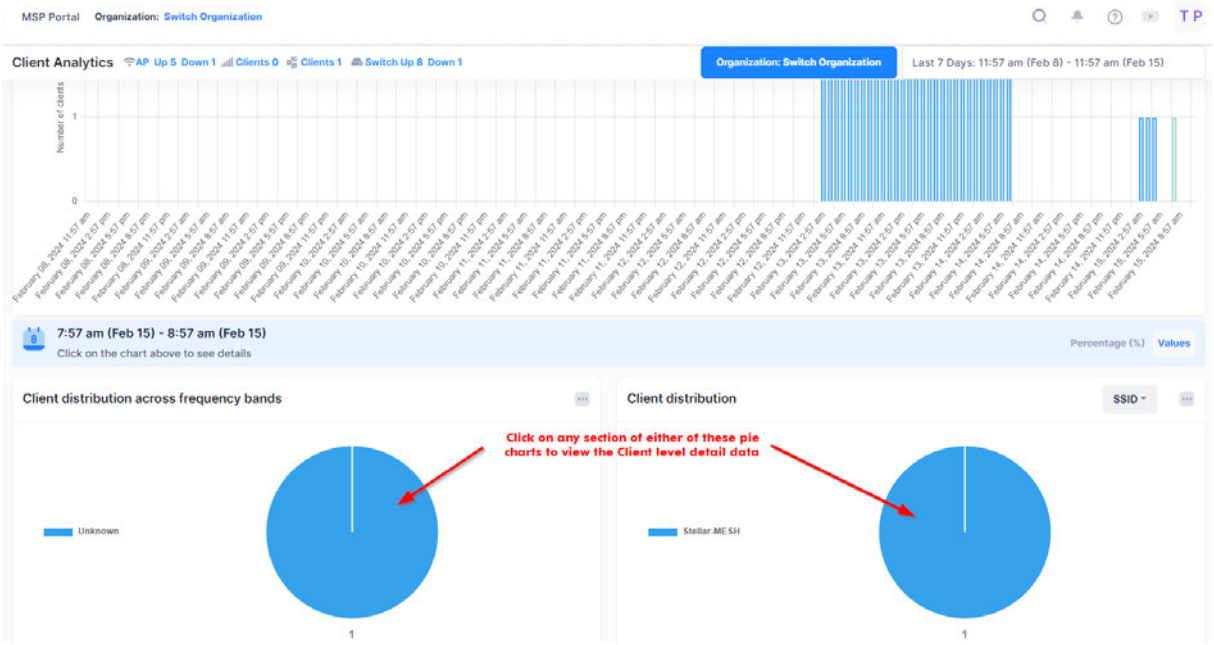
The Client Distribution across frequency bands widget:

Use this widget to find out how many clients have been connected on each Frequency Band.

The Categorization of Client Distribution:

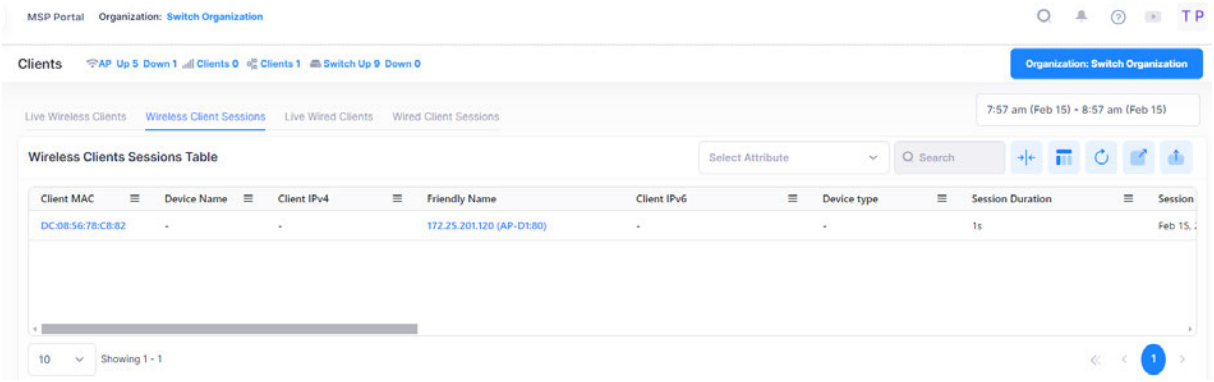
Use this widget to determine the distribution of clients based on Connection Mode, Client Device Type, Device OS, Health and Associated SSID.

You can click on any of the sections of either of these below shown Pie charts of ‘Client Distribution’ to view the Client level data:



The Client distribution regarding health is determined by the Client's RSSI level, which serves as an indicator of overall health. The classification is as follows: Excellent (RSSI >= -55 dBm), Good (RSSI >= -70 dBm), Fair (RSSI >= -80 dBm), and Poor (for all other values).

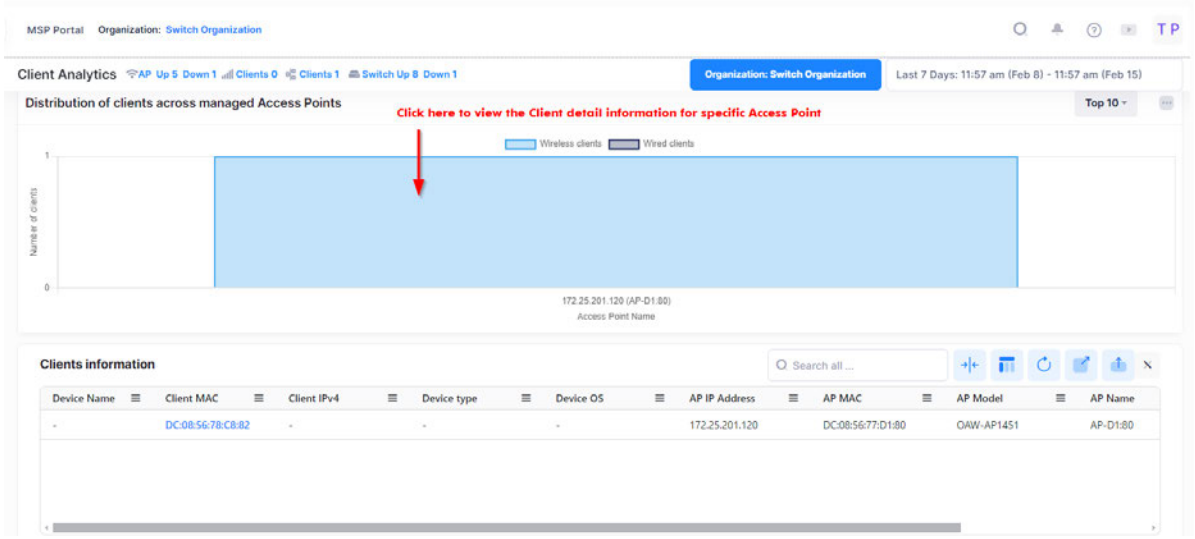
When you click on the Pie Chart, you are redirected to the Wireless Clients Sessions screen (see page 833), which displays a list of Wireless Client Sessions Table associated with the managed Access Points during the specified time window range.



The distribution of clients across managed Access Points widget:

Use this widget to quickly understand which Access Point has the highest number of Wireless and Wired clients currently connected to it. The widget displays the Top 10 Access Points by default, but you can change this value from the drop-down menu located on the top right corner of the widget.

If you want to view the detailed Clients information connected to a particular managed Access Points, then click on one of the bar for which of the Access point you want to get the detailed Clients Information as shown below:



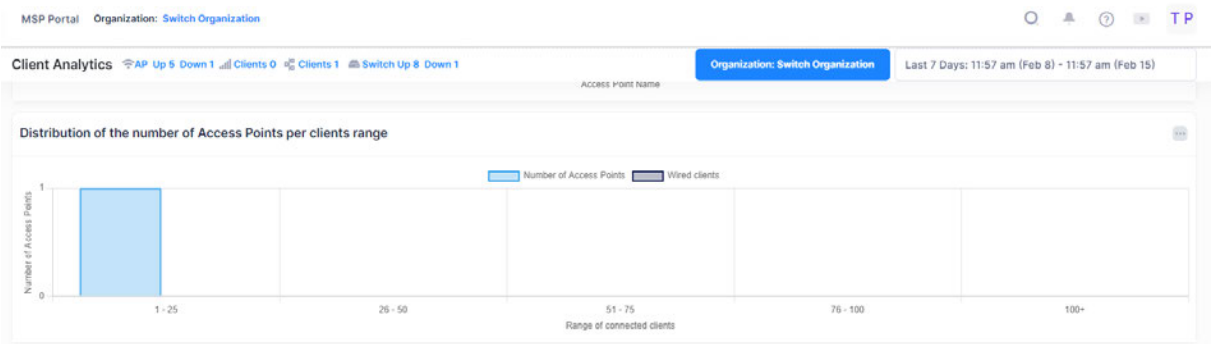
For each Client, the following attribute values are provided:

- **Device Name** - The Client Device Name.
- **Client MAC** - The MAC Address of the Client.
- **Client IPV4 Address** - The IPv4 address of the Client, if applicable.
- **Device Type** - If determined, the Device Type of the Client. (e.g: Mobile, Computer, ...)
- **Device OS** - If determined, the Operating System of the Client's device.
- **AP IP Address** - The IP Address address of the Access Point to which the Client is associated.
- **AP MAC** - The MAC address of the Access Point to which the Client is associated.
- **AP Model** - The model type of the Access Point (e.g., OAW-AP1221, OAW-AP1251, ...)
- **AP Name** - The name of the Access Point.
- **AP Version** - The Version set in the Edit Device page of the Access Point.

Data displayed in each widget can be exported into a CSV or Excel sheet format. You can also switch the widgets to full-screen mode for a better display. The table can be closed if you don't want to view the Client Information by selecting the 'X' button.

The distribution of the number of Access Points per clients range widget:

Use this widget to determine the number of clients connected to Access Points per client range : 0, 1-25, 26-50, 51-75, 76-100, 100+



Note that the information gathered for “Device Type” and “Device OS” depends on the information provided by the AP Client. As a result, these fields may appear blank based on the capability of the Client to provide the information.

21 Oct 2025

8.1.1.5.4 Client Throughput Consumption

The Throughput Consumption section of the Client Analytics Dashboard (see page 847) includes a Bar Chart widget representing the number of bytes received and transmitted by Clients to Access Points over time.

Data displayed in the bar chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.

20 Throughput Consumption Chart

21 Oct 2025

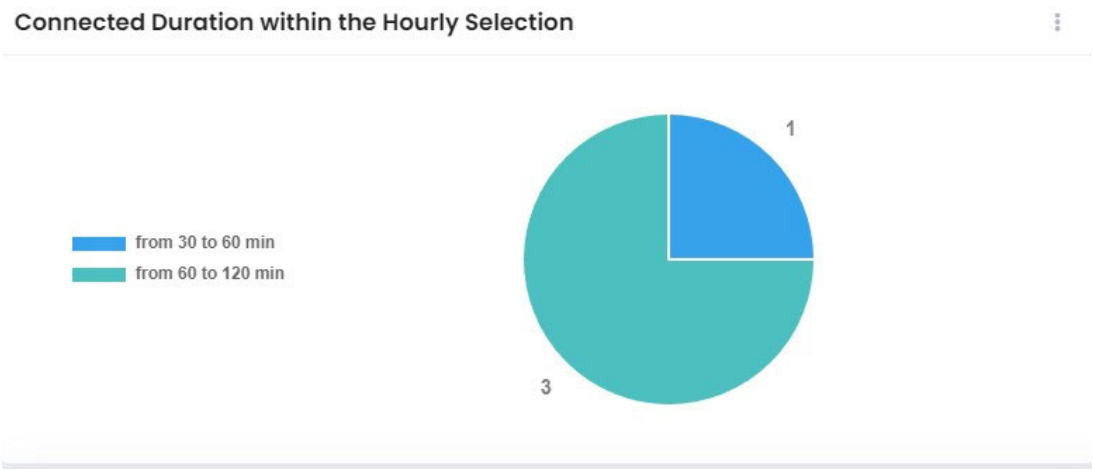
8.1.1.5.5 Connected Duration Within the Hourly Selection

The Connected Duration within the Hourly Selection section of the Client Analytics Dashboard (see page 847) displays widgets that display statistics about the average duration of client sessions for the chosen hour range.

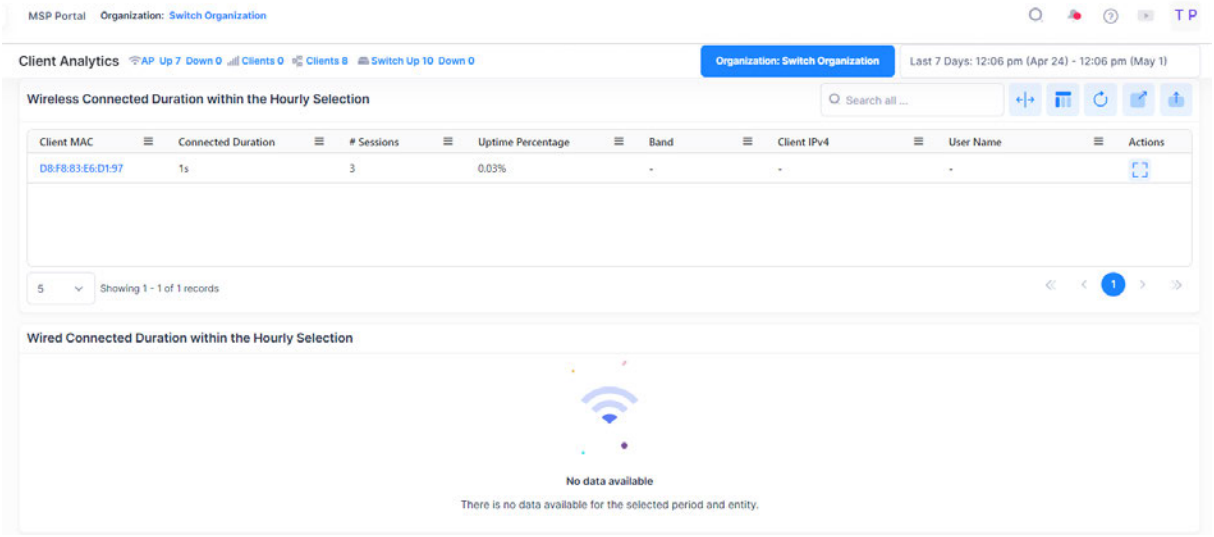
The Connected Duration within the Hourly Selection pie chart provides the distribution of the session duration across five predefined time windows:

- From 0 to 10 min
- From 10 to 30 min
- From 30 to 60 min
- From 60 to 120 min

Data displayed in the pie chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.



The Connected Duration within the Hourly Selection tables provide an overview of all sessions that occurred in the selected hour range for each of Wireless and Wired Clients. Data displayed in the table can be exported into a CSV, Excel sheet, or PDF format.



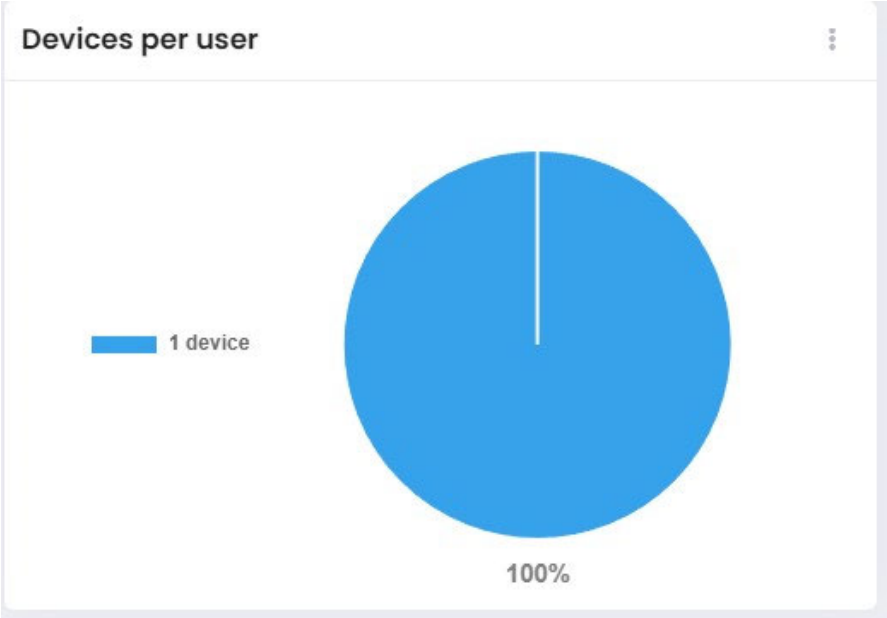
For each historical client session, the following attributes are displayed in the duration table:

- **Client MAC** - The MAC Address of the client.
- **Connected Duration** - The total amount of time for all the client sessions.
- **# Sessions** - Total number of client sessions.
- **Uptime Percentage** - The percentage Uptime of the Client sessions.
- **Band** - The radio band through which the client attached to the AP (2.4GHz or 5GHz).
- **Client IPV4 Address** - The IPV4 address of the client, if applicable.
- **User Name** - The user name of the client.
- **Device Name** - The name of the client device.
- **Device Type** - If determined, the Device Type of the client. (e.g: Mobile, Computer, ...).

21 Oct 2025

8.1.1.5.6 Number of Devices Per-User

The Devices per-user section of the Client Analytics Dashboard (see page 847) displays a pie chart that shows the number of devices used on average for each user connected to Access Points in your network.



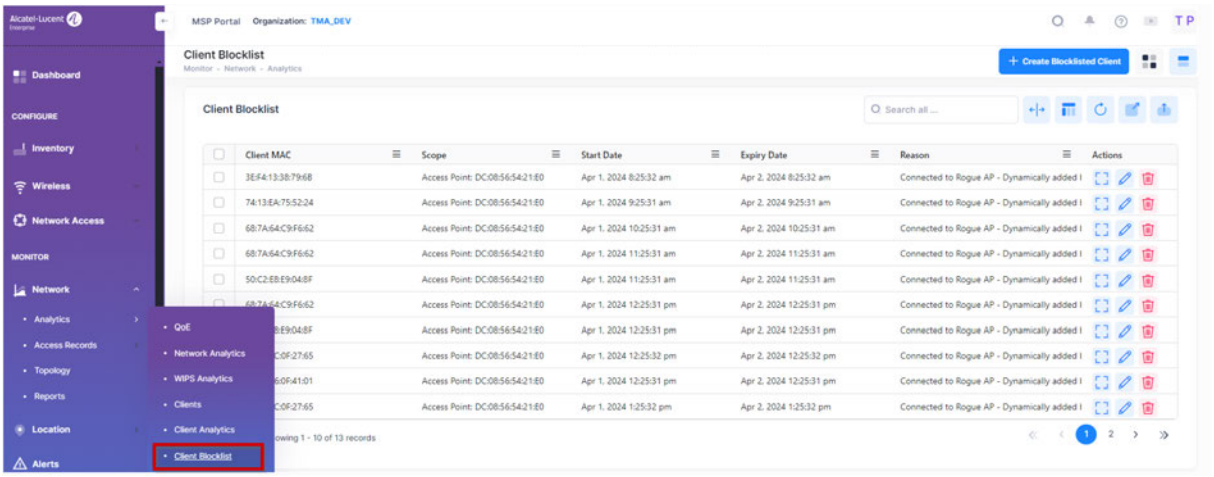
Note: This chart only displays devices per user when the SSID is portal or 802.1X. It will not display the number of devices per user if the SSID is open or PSK.

21 Oct 2025

8.1.1.6 Client Blocklist

The Client Blocklist screen displays information (see page 858) about all clients that have been added to the Blocklist (either manually or as a result of a WIPS policy). This screen is also used to manually add clients to the Blocklist (see page 859), edit clients on the Blocklist (see page 860), and delete clients from the Blocklist (see page 860).

The Client Blocklist screen is accessed by clicking on **Network > Analytics > Client Blocklist** under the “Monitor” section of the OmniVista Terra Menu (see page 45).

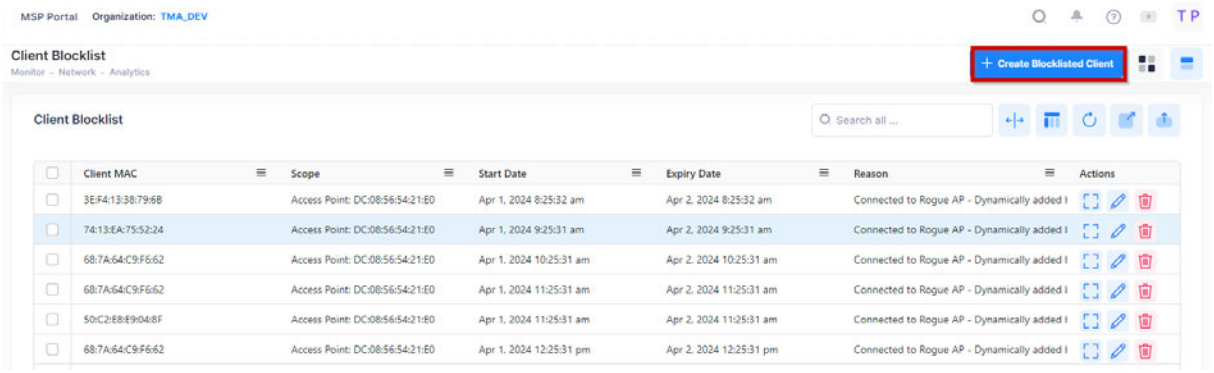


8.1.1.6.1 Client Blocklist

- **Client MAC -** MAC address of the client in the Blocklist.
- **Scope** - Client MAC address is blocked from access to the entire Organization or blocked from acccess to a specific Site within the Organization.
- **Start Date -** The starting date for the blocklisting. During the duration, the client is not allowed to access to the wireless network.
- **Expiry Date -** The expiration date for the blocklisting. The client can access the wireless network after the expiration date.
- **Reason -** The reason why the client was added to the Blocklist.
  - Manually Add - Added into the Blocklist by the user. The “Reason” field is optional when manually adding a client to the Blocklist.
  - Garbing Legal Accessing Client - Dynamically added by the WIPS policy.
  - Signal Strength is Too Strong, Reducing Network Performance - Dynamically added by the WIPS policy.
  - Channel Switching Too Often - Dynamically added by the WIPS policy.
  - Broadcasting Conflicted SSID, Misleading User Connection - Dynamically added by the WIPS policy.
  - Matching the Keyword of Suspected SSID - Dynamically added by the WIPS policy.
  - Matching the Suspected MAC OUI - Dynamically added by the WIPS policy.
  - Have Attacking Behavior - Dynamically added by the WIPS policy.

8.1.1.6.2 Manually Adding a Client to the Blocklist

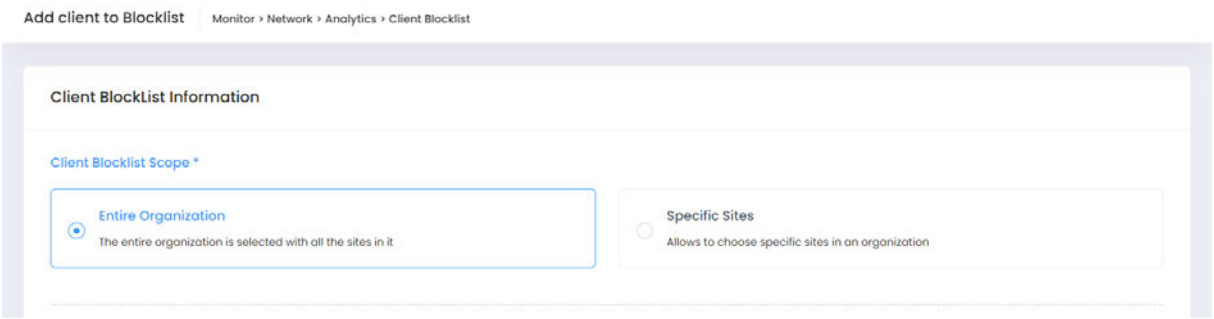
Click on **Create Blocklisted Client** to access the Add Client to Blocklist form. Complete the fields as described below, then click on the **Create Blocklisted Client** button. Repeat to add additional clients.



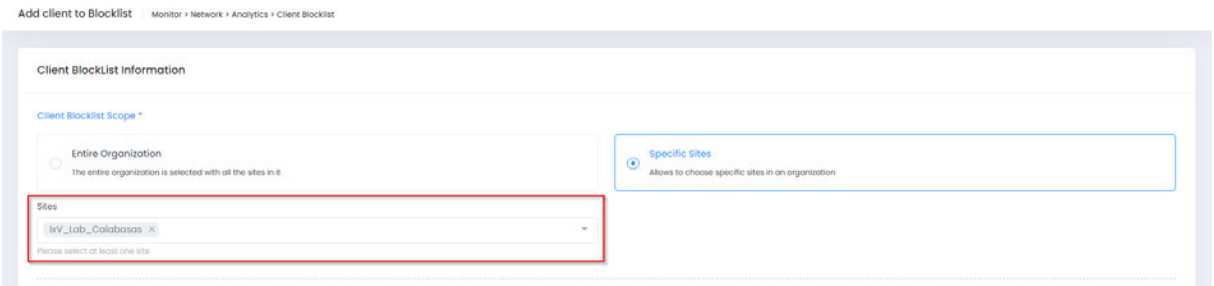
8.1.1.6.2.1 Client Blocklist Scope

The first section of the Add Client to Blocklist form is where you select the scope of the blocklist action:

- **Entire Organization (Default)** - Blocks client MAC address from all Sites within the Organization.
- **Specific Sites** - Blocks client MAC address from selected Sites within the Organization.



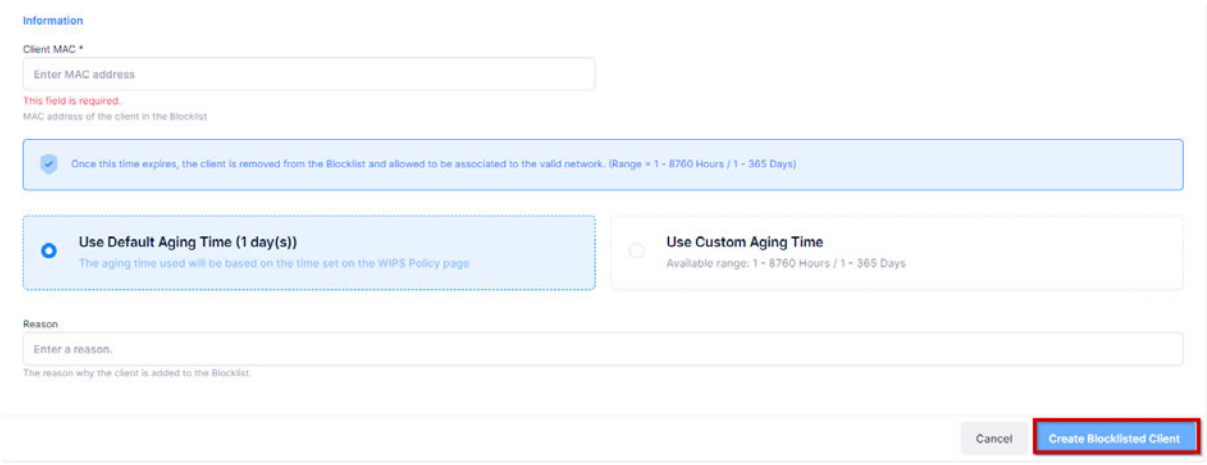
If you select the Specific Sites option, an additional “Sites” field is displayed, where you select the specific Sites for the blocklist action.



Click on the drop-down list and select Sites from the Organization. To remove a selected Site, click on the “x” next to the Site name.

8.1.1.6.2.2 Information

The next section of the Add Client to Blocklist screen is where you enter information about the client that you want to blocklist.



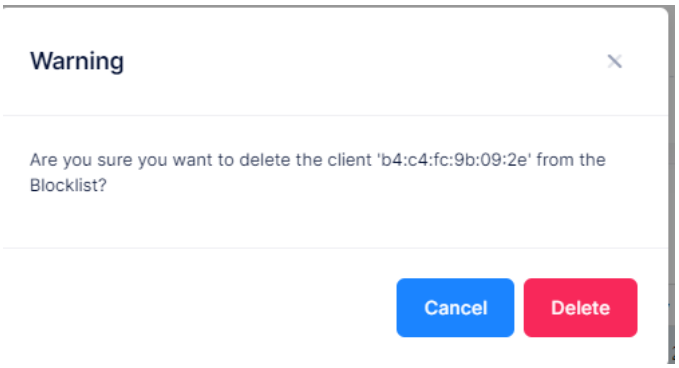
- **Client MAC -** The MAC Address of the client.
- **Aging Time -** The amount of time the client will remain on the Blocklist. Once this time expires, the client is removed from the Blocklist and allowed to be associated to the valid network. You can select one of two options to define the aging time:
  - **Use Default Aging Time** - The aging time is based on the time set for the WIPS Policy (see page 376).
  - **Use Custom Aging Time** - Define a custom time range for the aging time (Range = 1 - 8760 Hours/1 - 365 Days).
- **Reason (Optional)-** The reason the client was added to the Blocklist.

8.1.1.6.3 Editing a Client on the Blocklist

You can edit the Client Block List Scope, a client's Aging Time, or the Reason a client was blocklisted. Select a client in the Blocklist and click on the Edit icon. Edit the field(s) as described above (see page 859) and click on the **Save** button.

8.1.1.6.4 Deleting a Client from the Blocklist

Select the client in the Blocklist and click on the Delete icon. The following prompt appears on the screen.



Click on **Delete** at the confirmation prompt.

21 Oct 2025

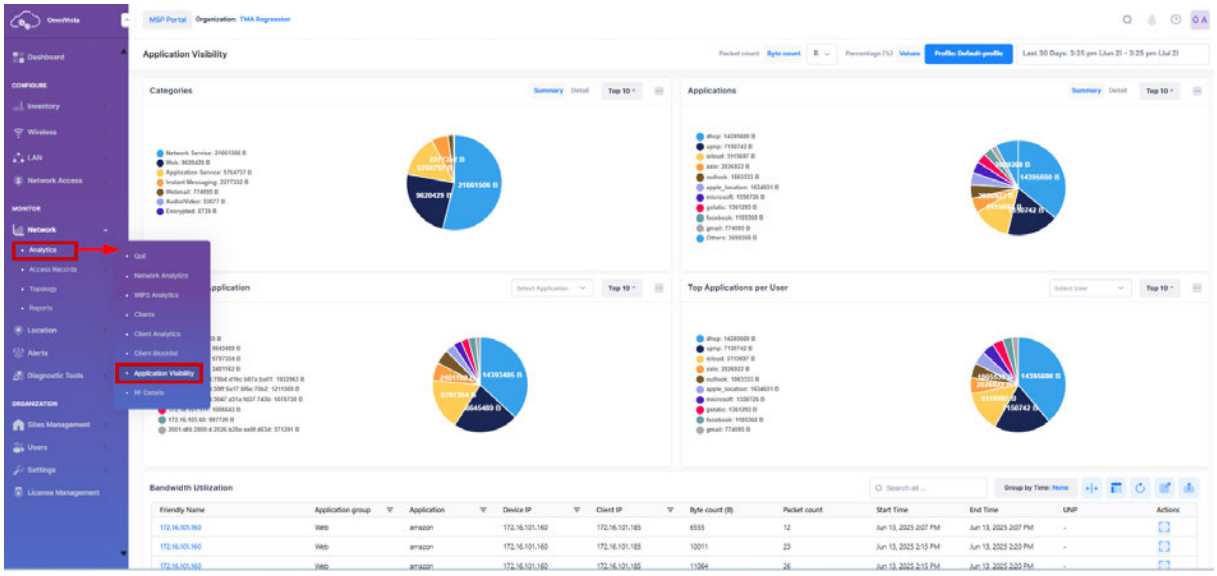
8.1.1.7 Application Visibility

The Application Visibility Application identifies application/protocol flows based on Application Signatures that identify an associated application or protocol. To enable Application Visibility, you create a Signature Profile (see page 766) that includes all of the signatures for applications/protocols that you want to monitor/control, and apply that profile to Access Points.

To access the Application Visibility Dashboard, click on **Network > Analytics > Application Visibility** under the “Monitor” section of the OmniVista Terra Menu (see page 45).

The Application Visibility Analytics dashboard provides the following analytics data:

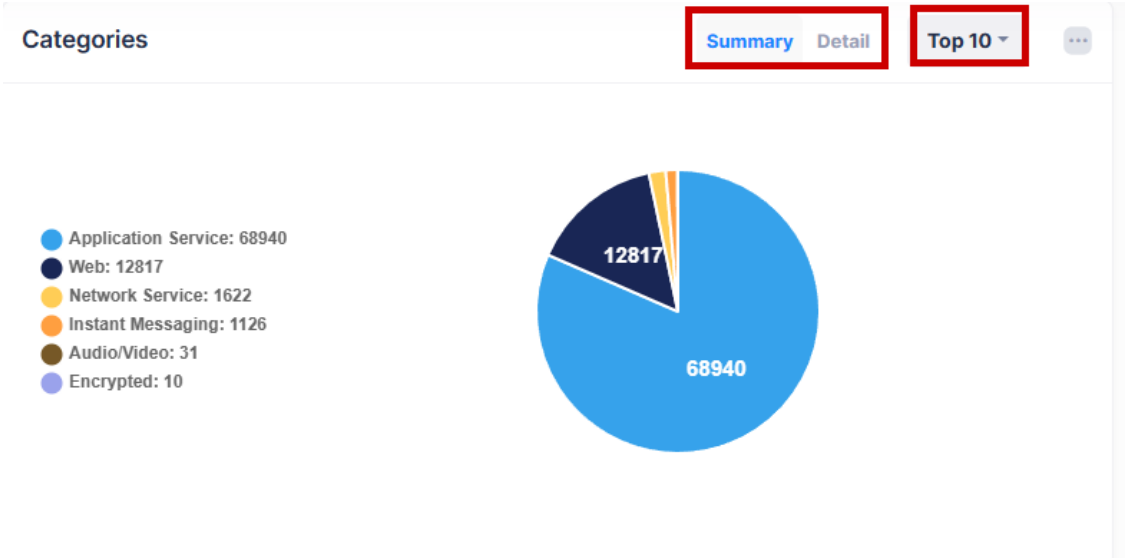
- Category Bandwidth usage (see page 862).
- Application Bandwidth usage (see page 863).
- Top users per Application (see page 864).
- Top Application per user (see page 865).
- Tabular view of Bandwidth Utilization (see page 866).



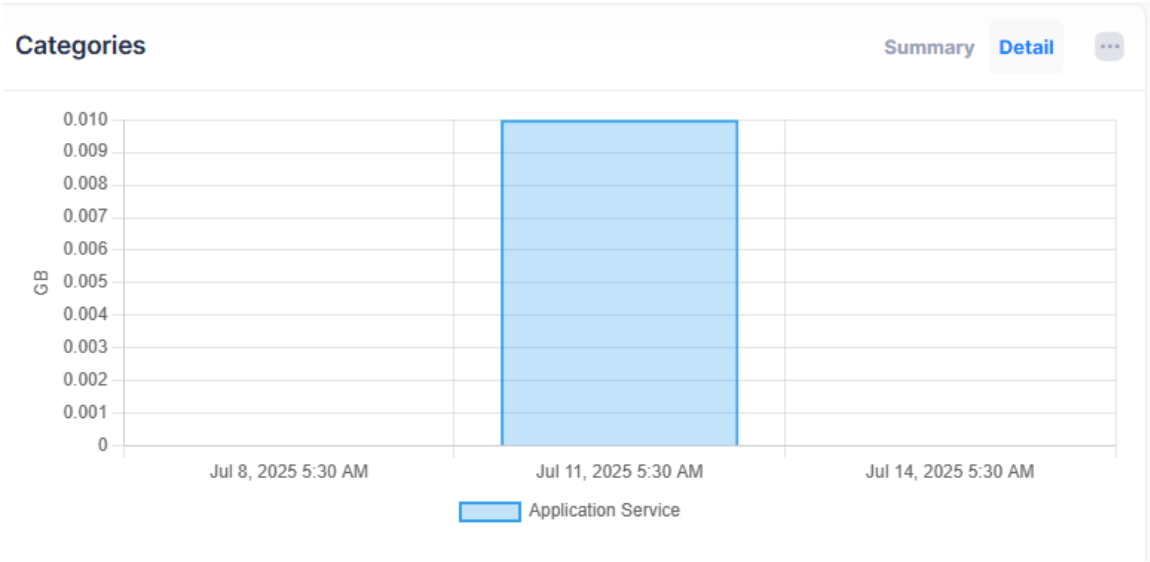
8.1.1.7.1 Category Bandwidth Usage

The Category Bandwidth Usage screen displays traffic flow information for Application groups discovered on the network, and the number of network resources being used by each application for the selected Access Points and configured time period. By default, the Summary view is displayed but you can toggle to the **Detail view** by clicking on the respective tab. By default, Top 10 Categories bandwidth usage are displayed.

Data displayed in the chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.



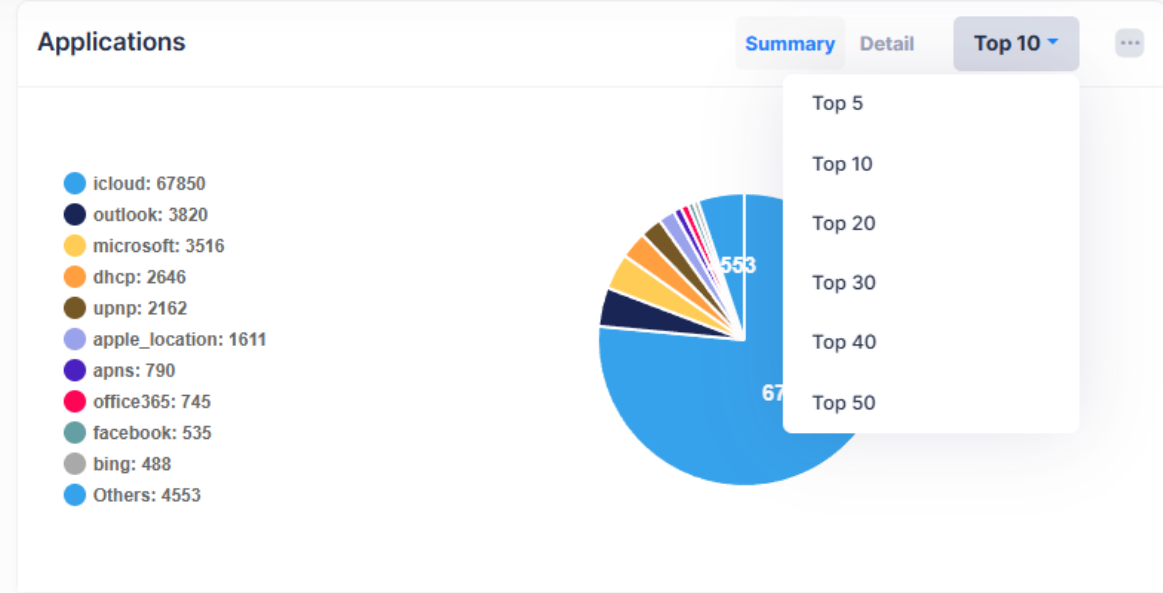
By clicking on a specific Category in the Pie chart, you can view the Detail traffic flow for the Category as shown below:



8.1.1.7.2 Application Bandwidth Usage

The Application Bandwidth usage screen displays packet or byte count information for Applications discovered on the network over the configured period of time, and the percentage of network resources being used by each application for the selected devices and configured time period. You can also view the detail bar chart of the Application information or Top N Applications usage by clicking on the respective tab. By default, Top 10 Applications bandwidth usage are displayed.

Data displayed in the chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.

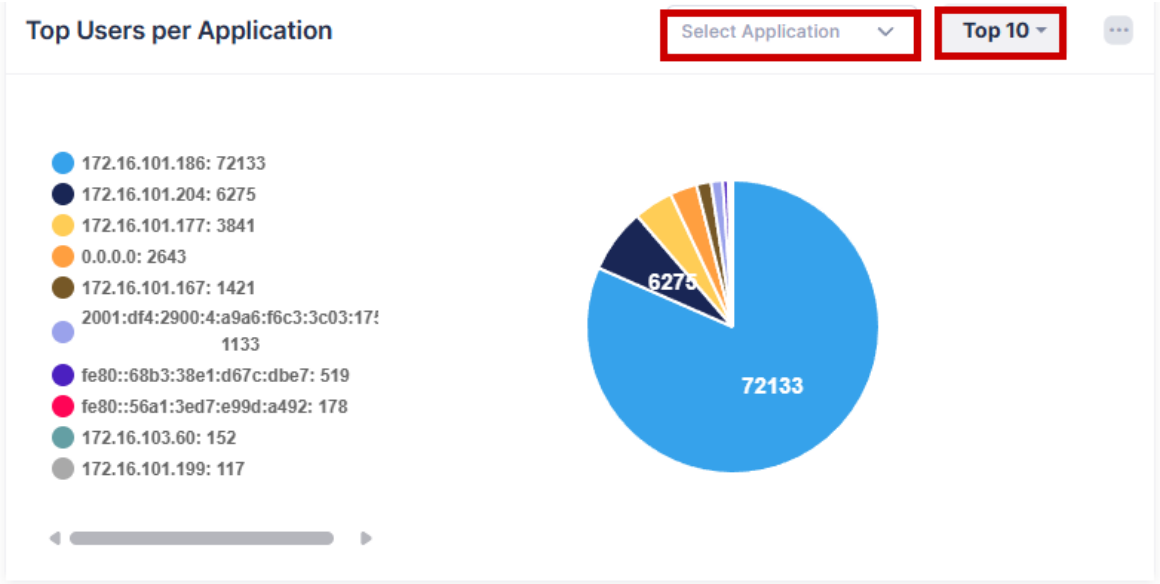


8.1.1.7.3 Top Users per Application

The Top Users per Application screen displays the top users (IP address) for the selected application. You can also select an application from the **Select Application** drop-down menu to display the top users for the selected Application. You can also view the Top N Users for each Application from this tab.

By default, the summary view is displayed on the screen but by clicking anywhere on the pie chart, you can access a detailed view of the data presented in a bar chart format for the specified time period. And you can also select or deselect an application(s) in the legend to add/remove the application(s) from the display. Click on the back arrow, to go to summary view.

Data displayed in the chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.

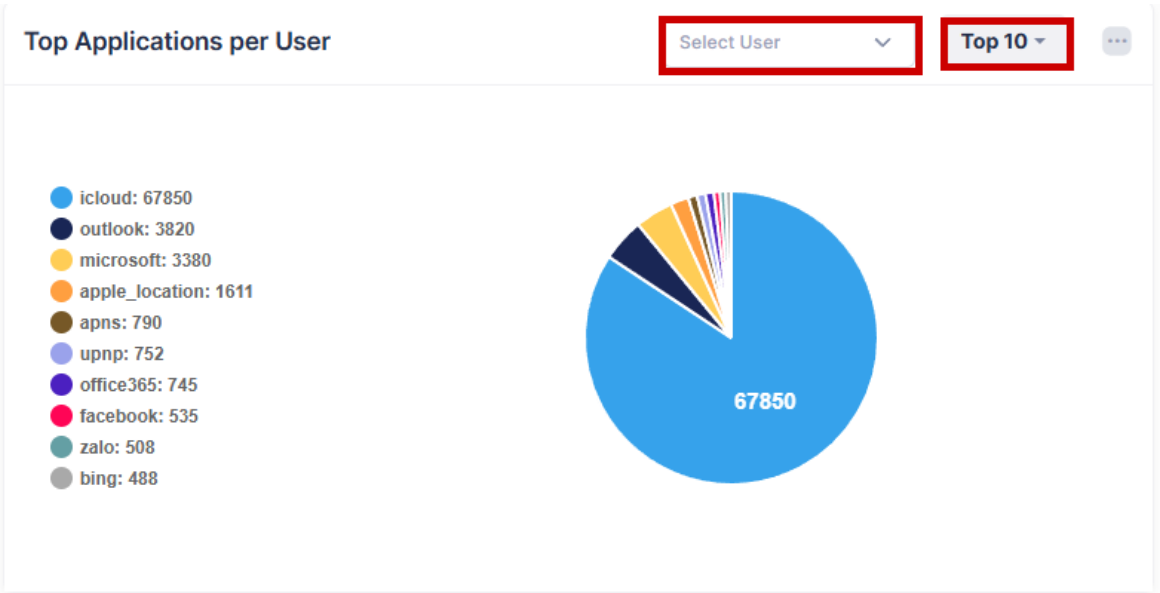


8.1.1.7.4 Top Applications per User

The Top Applications per User screen displays the top Applications for the selected user (IP address). Select a User (IP address) from the **Select User** drop-down menu to display the top Application for the selected user.

You can also view the Top N Applications per user from this tab. By default, the summary view is displayed on the screen but by clicking anywhere on the pie chart, you can access a detailed view of the data presented in a bar chart format for the specified time period. And you can also select or deselect an user(s) in the legend to add/remove the user(s) from the display. Click on the back arrow, to go to summary view.

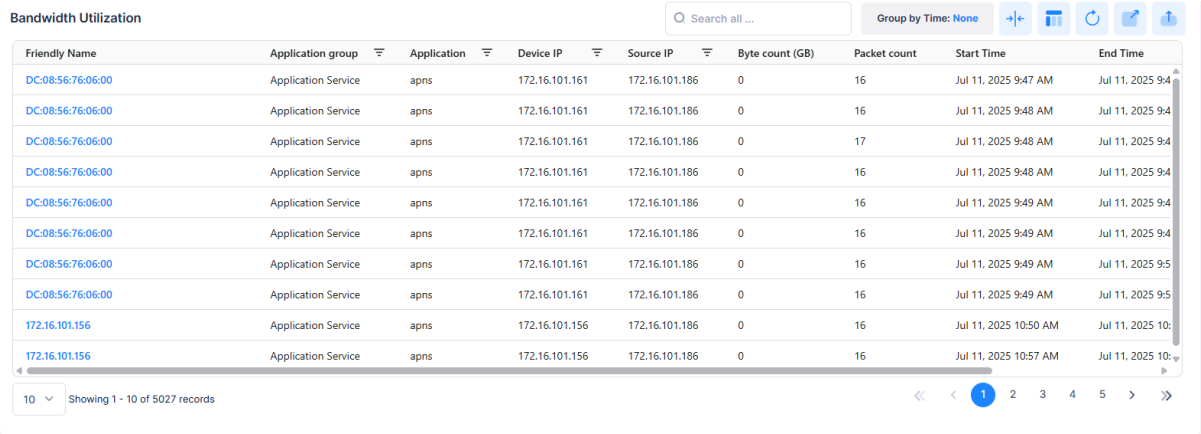
Data displayed in the chart widget can be exported into a CSV or Excel sheet format. You can also switch the widget to full-screen mode for a better display.



8.1.1.7.5 Tabular view of Bandwidth Utilization

The Bandwidth Utilization table displays the flow data with the Access Point to which the source (client) generating the flows was connected.

Data displayed can be exported into a CSV, PDF or Excel sheet format. You can also switch to full-screen mode for a better display.

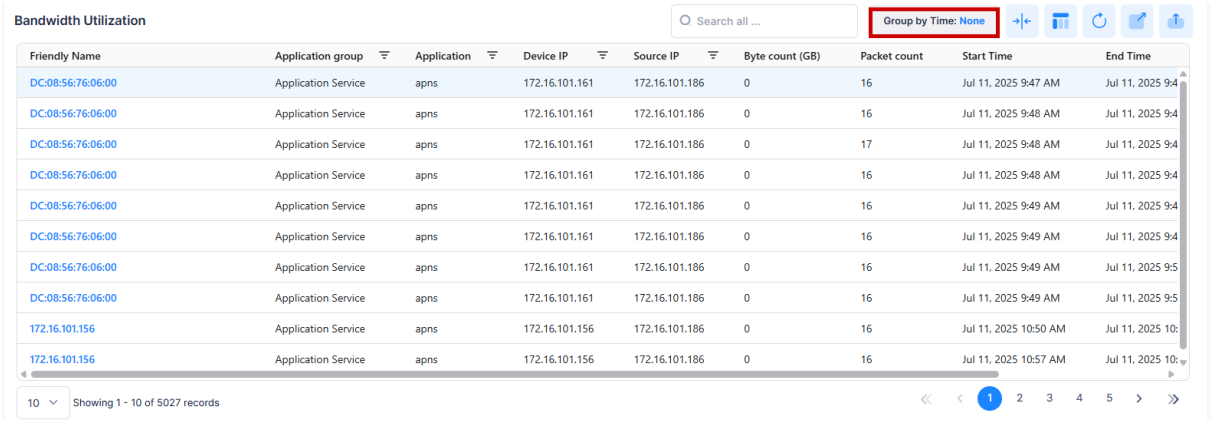


The Bandwidth Utilization table provides the following information for each of the device:

- **Friendly Name -** The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Application group** - Displays flow information for all Application groups included in the Signature Profile(s) of the selected devices.
- **Application** - Displays flow information for all Applications included in the Signature Profile(s) of the selected devices.
- **Device IP** - The IP address of the device.
- **Source IP** - The source IP address.
- **Byte count(MB**) - Displays the data unit for the byte count. By default is MB.
- **Packet count** - The count of the packet flow for specified time period.
- **Start Time** - The start date and time of the flow data.
- **End Time** - The end date and time of the flow data.
- **UNP** - The UNP profile associated with the device.

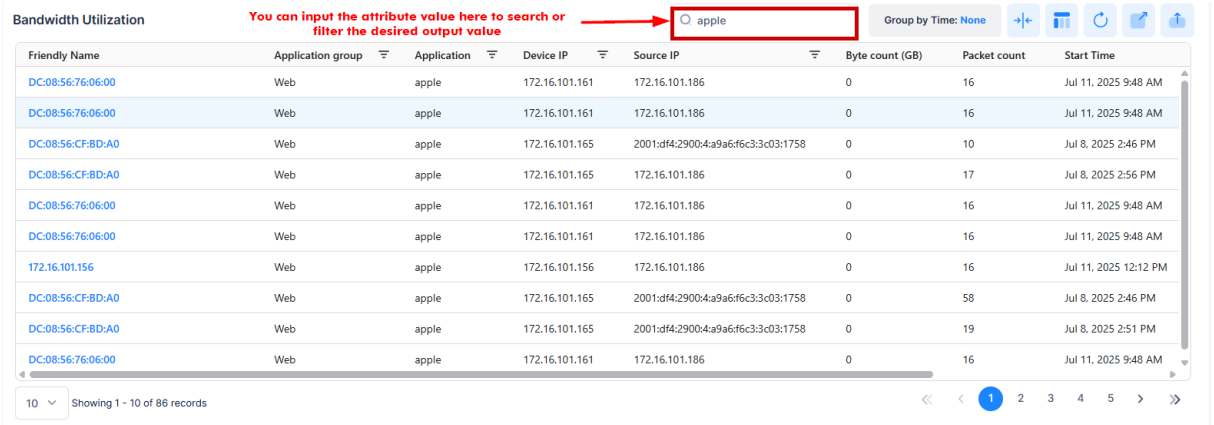
8.1.1.7.5.1 Group by Time

The Group by Time display option allows you to select a range of time to display flow data for each hour of each day for each application. To select the time range for the Group by Time, click on **Group by Time** and select from 5 minutes up to 24 hours from the drop-down menu. By default, the “None” option is selected, which displays the detail view of the flow data of all the applications for whole day without any grouping of time range.



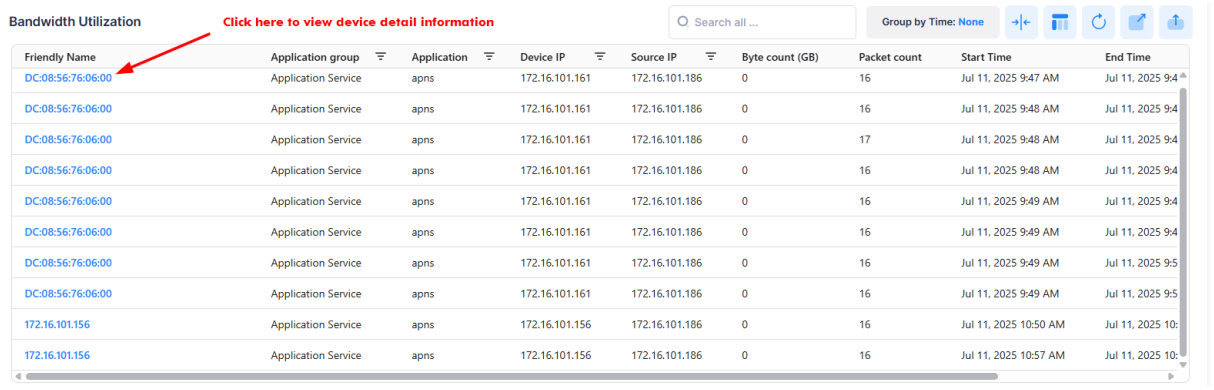
8.1.1.7.5.2 Search by an Attribute value

You can search for the specific Applications or Applications Groups by using the Search box option. The search results are refined based on the attribute value selected from the available list (Application/Application group/Device IP/Source IP). Only those output that contain the matching searched values are displayed in the results as shown below.

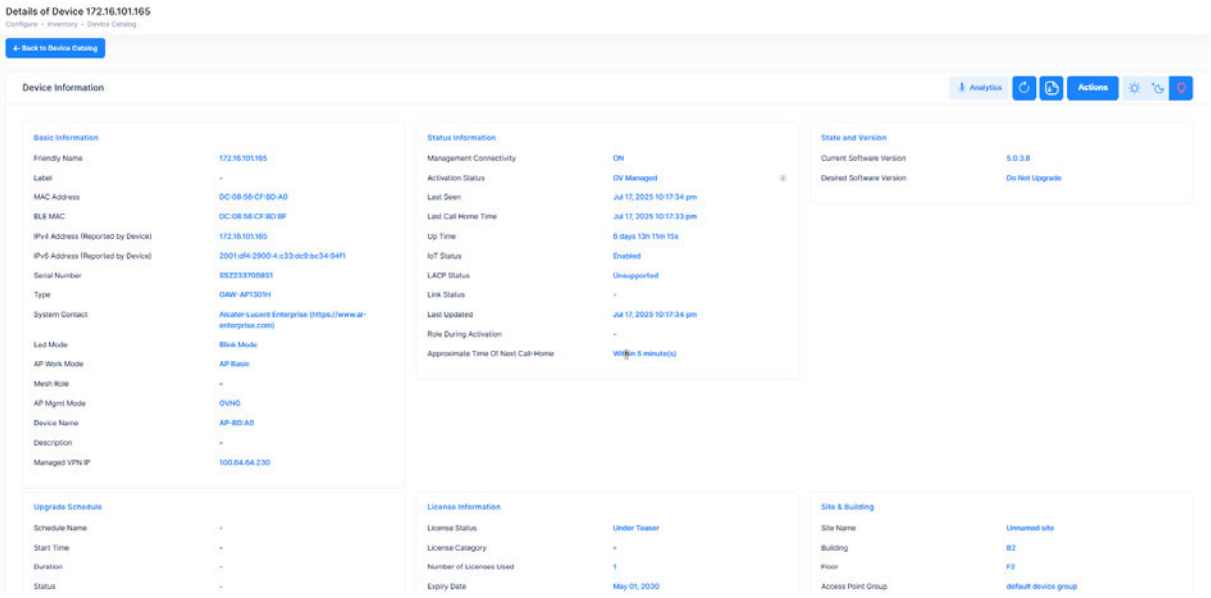


8.1.1.7.5.3 View Device Detail Information

The Bandwidth Utilization table displays information for the flow data for the configured devices. To display detailed device information about a specific device, click on the Friendly Name as shown below.



The following screen appears:



21 Oct 2025

8.1.1.7.6 Application Visibility - FAQs/Troubleshooting

8.1.1.7.6.1 When can I see an Application Visibility report after enabling DPI?

AP polls and updates DPI records every 15 minutes, OmniVista Terra polls for data every 15 minutes. So wait for 30 minutes before you can see data on the OmniVista Terra DPI page.

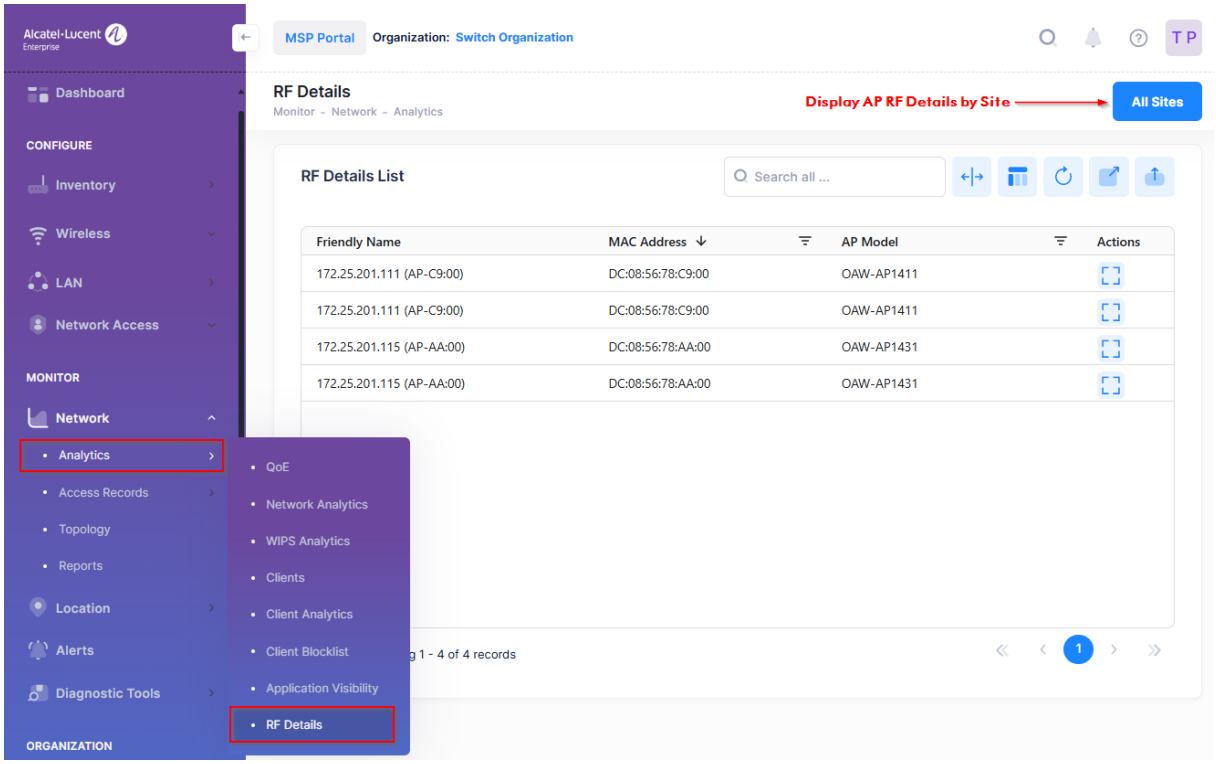
8.1.1.7.6.2 What is the impact of Daylight Saving Time (DST) with DPI reports?

Reports may show a time difference of an hour.

21 Oct 2025

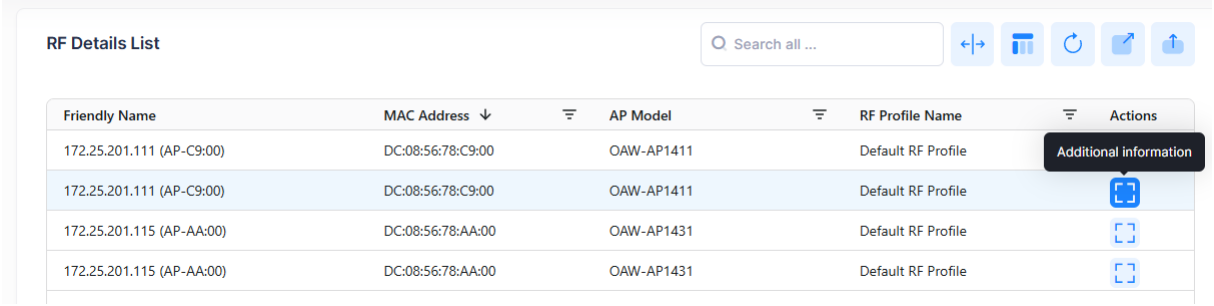
8.1.1.8 Radio Frequency Details

Click on **Network > Analytics > RF Details** to display Radio Frequency attributes (see page 870) for managed AP devices. On the RF Details screen, you can select if you want view RF Details for all Sites or for a specific Site within the Organization.



8.1.1.8.1 Displaying RF Details Information

Click the Additional Information icon next to a RF Details entry to display the Additional Information screen. The information displayed on this screen is defined below.



- **Friendly Name** - The name assigned to the AP device is derived from the Preferred Device Naming convention specified in the user preference settings. (see page 26)By default, the Friendly Name is set to IP Address (System Name).
- **Site Name** - The name of the Organization Site to which the device belongs.
- **MAC Address** - The MAC address of the AP device.
- **AP Model** - The Access Point model number.
- **RF Profile Name** - The name of the Radio Frequency profile to which the device was assigned. The RF profile is assigned to a provisioning configuration (see page 313), which provides configuration information for the AP Group to which the AP belongs. You can also change the RF Profile at the device level through the Device Catalog Edit Device (see page 217) menu (Group/ RF Profile, Assigned Site). Note that changing the RF Profile at the device level takes precedence over the profile assigned through the Provisioning Configuration.
- **Band** - The working radio band (2.4G, 5G Low, 5G High, 5G All, 6G).
- **Channel** - The working channel of the radio.
- **Channel Width** - The channel width setting. Controls how broad the signal is for transferring data.
  - **2.4G -** 20MHz/40MHz
  - **5G -** 20MHz/40MHz/80MHz/160MHz.
  - **6G** - 20MHz/40MHz/80MHz/160MHz
- **Channel Utilization** - The channel usage within each band.
- **TX power (EIRP)** - The Effective Isotropically Radiated Power radio frequency for the AP.

- **TX Chain Mask** - The TX chains that are active during transmission.
- **Avg Noise Floor** - The measure of the signal created from the sum of all noise sources and unwanted signals within a measurement system, where noise is defined as any signal other than the one being monitored.
- **Timestamp** - The last date and time OmniVista Terra received RF details for the AP.

21 Oct 2025

8.1.1.9 Network Analytics Summary

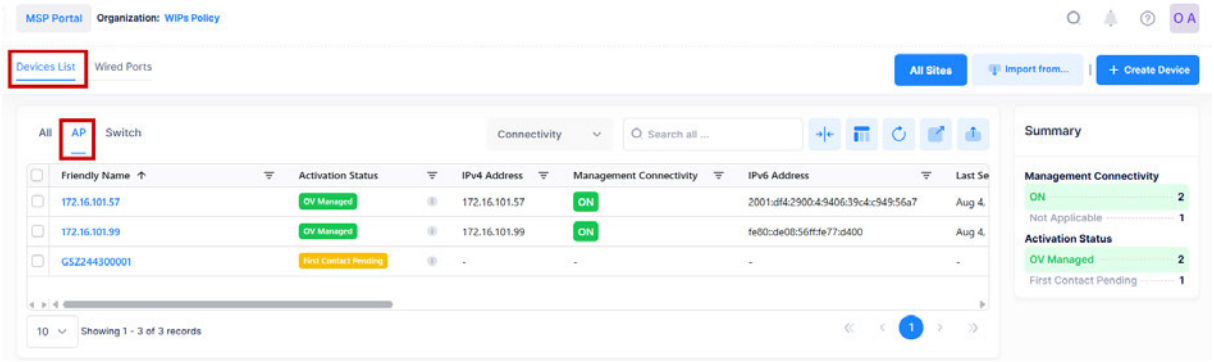
The Network Analytics Summary displays a summary of the following parameters at the top of the Dashboard:

- Total number of Access Points (see page 873)
- Access Points Up Count (see page 873)
- Access Points Down Count (see page 874)
- Number of Live Connected Wireless Clients (see page 874)
- Number of Live Connected Wired Clients (see page 875)
- Total number of Switches (see page 875)
- Switch Up Count (see page 876)
- Switch Down Count (see page 876)

8.1.1.9.1 Access Points Count

Displays the total number of Access Points connected in the Network, as shown below.

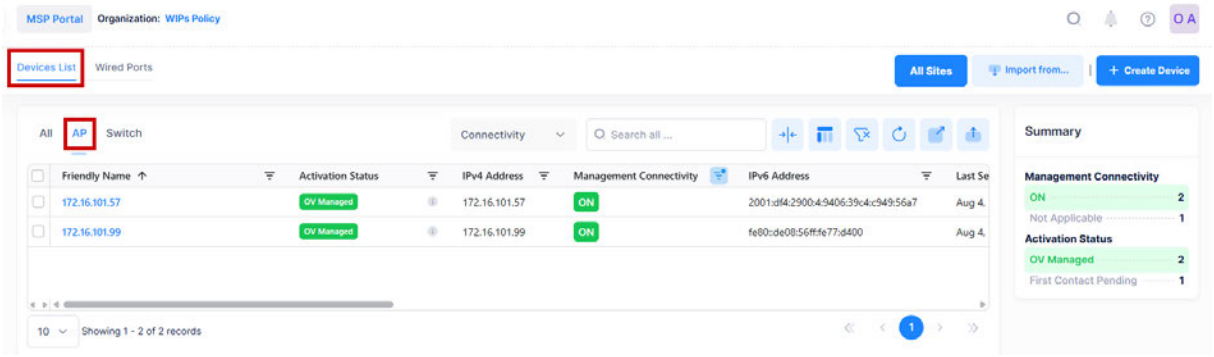
When you click on the Access Point Counter, you are redirected to the Devices List screen (see page 802), which displays a list of total devices that are connected to the Network.



8.1.1.9.2 Access Points Up Count

Displays the number of Access Points that are Up (Management Connectivity status is “On” or “Not Applicable”), as shown below.

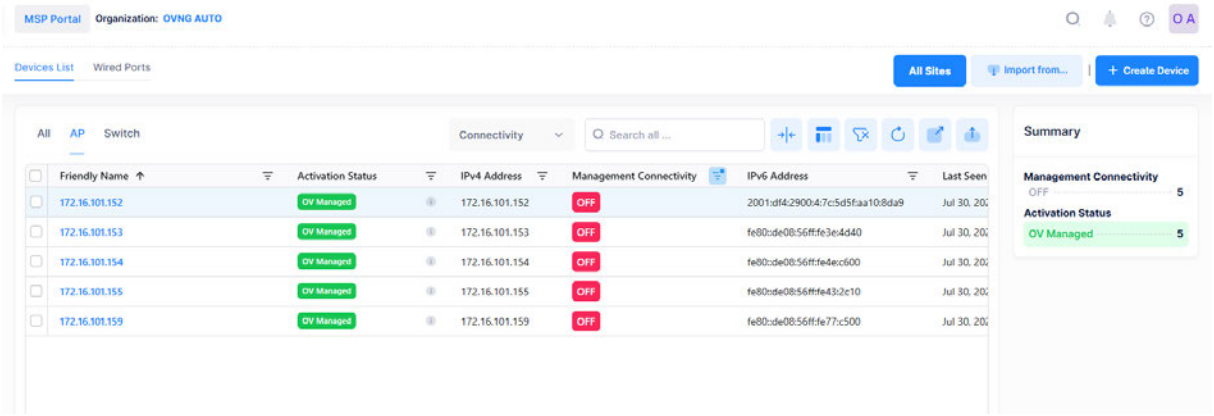
When you click on the Access Point Up Counter, you are redirected to the Devices List screen (see page 802), which displays a list of only those devices that are up.



8.1.1.9.3 Access Points Down Count

Displays the number of Access Points that are down (Management Connectivity status is Off), as shown below.

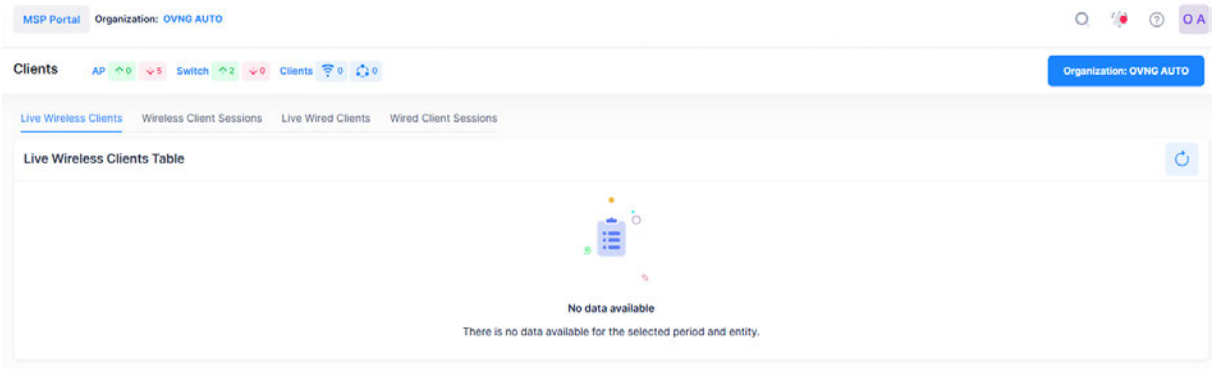
When you click on the Access Point Down Counter, you are redirected to the Devices List screen (see page 802), which displays a list of only those devices that are down.



8.1.1.9.4 Live Connected Wireless Clients

Displays the number of currently connected Live Wireless Clients in the Network as shown below.

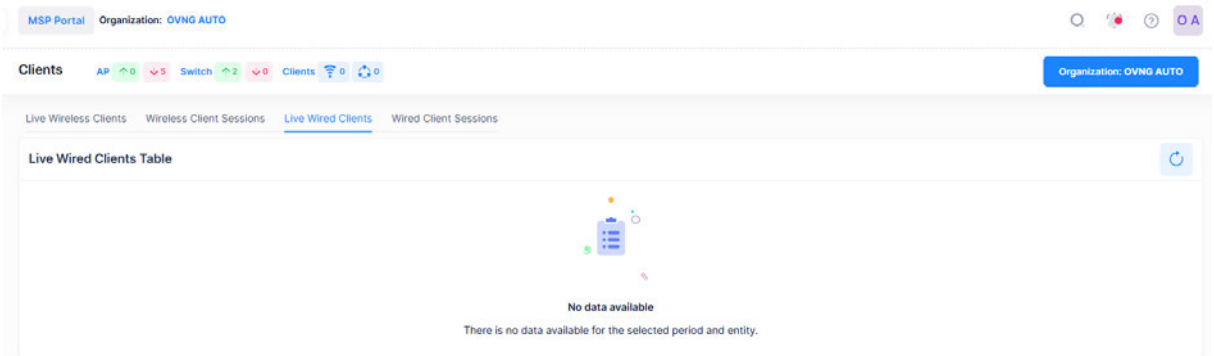
When you click on the Wireless Clients Counter, you are redirected to the Clients screen, which displays a list of Live Wireless Clients (see page 827) that are currently connected to the network.



8.1.1.9.5 Live Connected Wired Clients

Displays the number of currently connected Live Wired Clients in the Network as shown below.

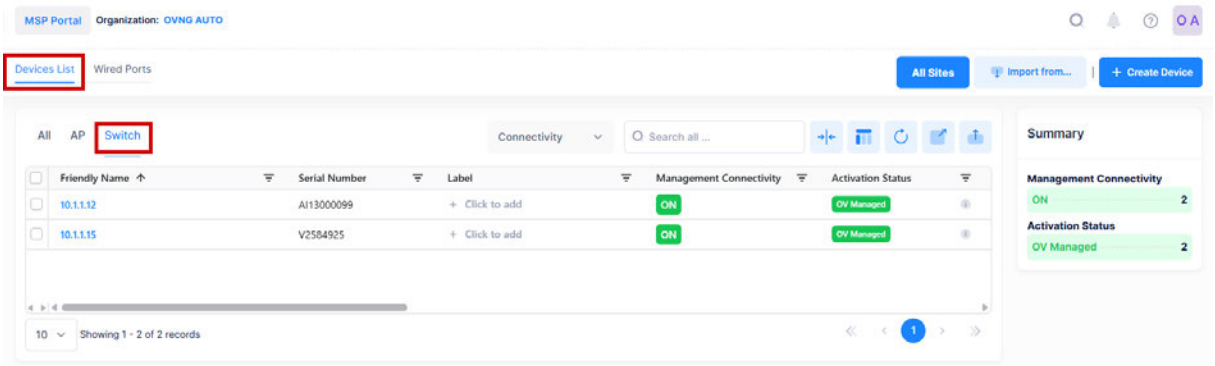
When you click on the Wired Clients Counter, you are redirected to the Clients screen, which displays a list of Live Wired Clients (see page 837) that are currently connected to the network.



8.1.1.9.6 Switch Count

Displays the total number of Switches connected in the Network, as shown below.

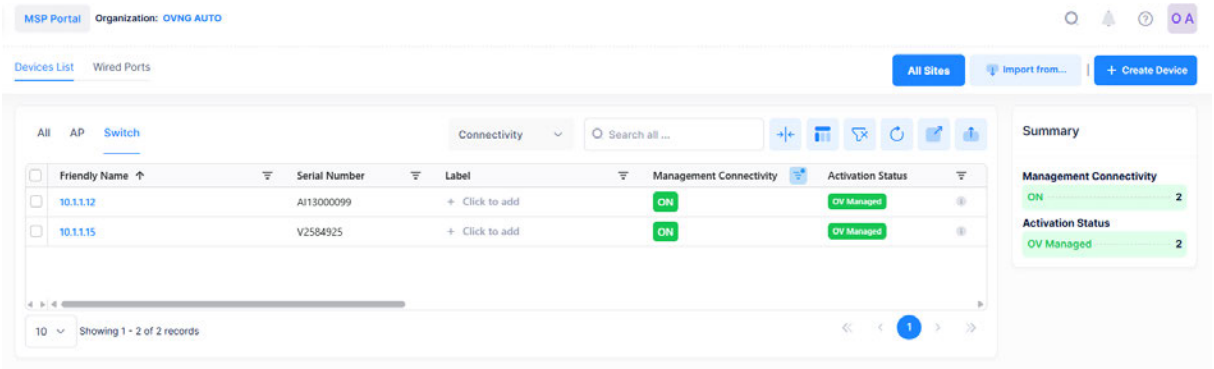
When you click on the Switch Counter, you are redirected to the Devices List screen (see page 802), which displays a list of total switches that are connected to the Network.



8.1.1.9.7 Switch Up Count

Displays the number of Switches that are Up (Management Connectivity status is “On” or “Not Applicable”), as shown below.

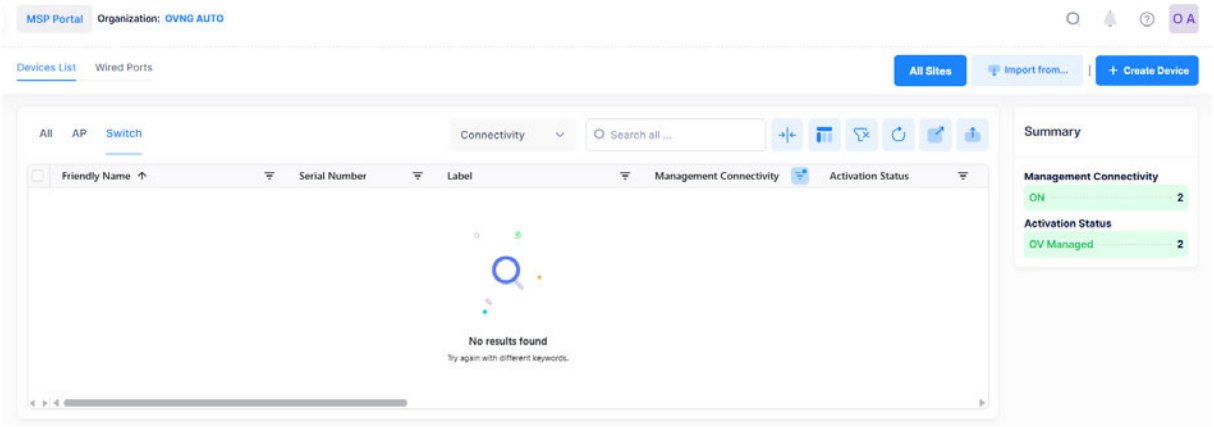
When you click on the Switch Up Counter, you are redirected to the Devices List screen (see page 802), which displays a list of only those switches that are up.



8.1.1.9.8 Switch Down Count

Displays the number of Switches that are down (Management Connectivity status is Off), as shown below.

When you click on the Switch Down Counter, you are redirected to the Devices List screen (see page 802), which displays a list of only those switches that are down.


MSP Portal
Organization: OVNG AUTO
Devices List
Wired Ports
All Sites
Import from...
+ Create Device
All
AP
Switch
Connectivity
Search all ...
Friendly Name
Serial Number
Label
Management Connectivity
Activation Status
No results found
Try again with different keywords.
Summary
Management Connectivity
ON
2
Activation Status
OV Managed
2

21 Oct 2025

8.1.2 Access Records

To monitor the access records of clients, click on **Network > Access Records** under the “Monitor” section of the OmniVista Terra Menu (see page 45). The following list of available Access Records to monitor displays:

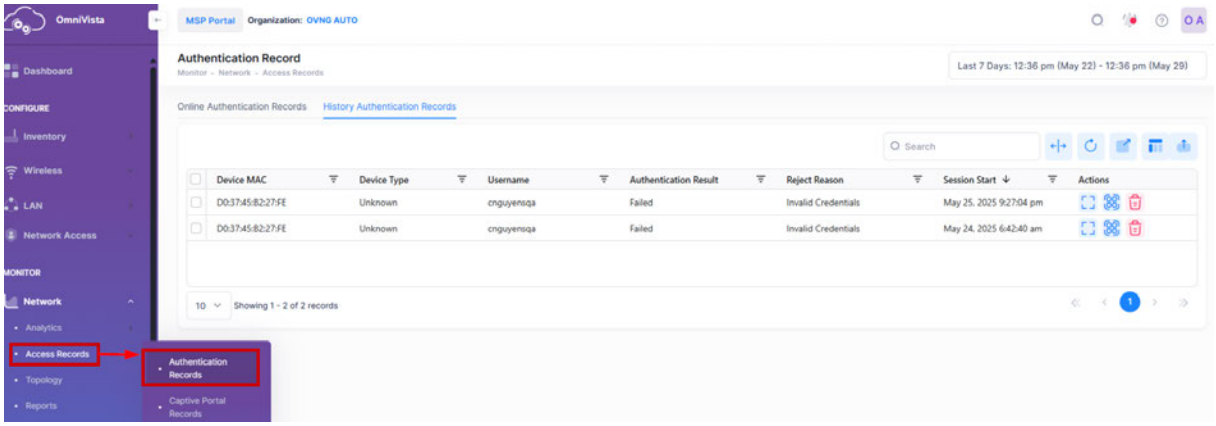
- **Authentication Records** (see page 879) - Displays authentication information for all devices authenticated through UPAM. There is an option to view authentication records for clients currently online and an option to review historical client records. Use this information to troubleshoot authentication failures.
- **Captive Portal Records** (see page 889) - Displays Captive Portal information for all devices authenticated through UPAM. Use this information to check the results of Captive Portal authentication and in case of failure, check the reason UPAM rejected the access request.
- **Self-Registration Requests** (see page 892) - Displays a list of guest requests for self-registration. This screen is used to review, approve or reject self-registration requests from Guest Users.
- **Guest Devices** (see page 894) - Displays a list of all guest devices that have authenticated through UPAM.
- **BYOD Devices** (see page 900) - Displays a list of all BYOD devices authenticated through UPAM.
- **IoT Devices** (see page 904) - Displays a list of all endpoint devices that connect to the network (for example, PCs, Tablets, Smartphones). You can display a summary of the IoT device inventory or customize the display by classification/authentication, location, or profiling data.

21 Oct 2025

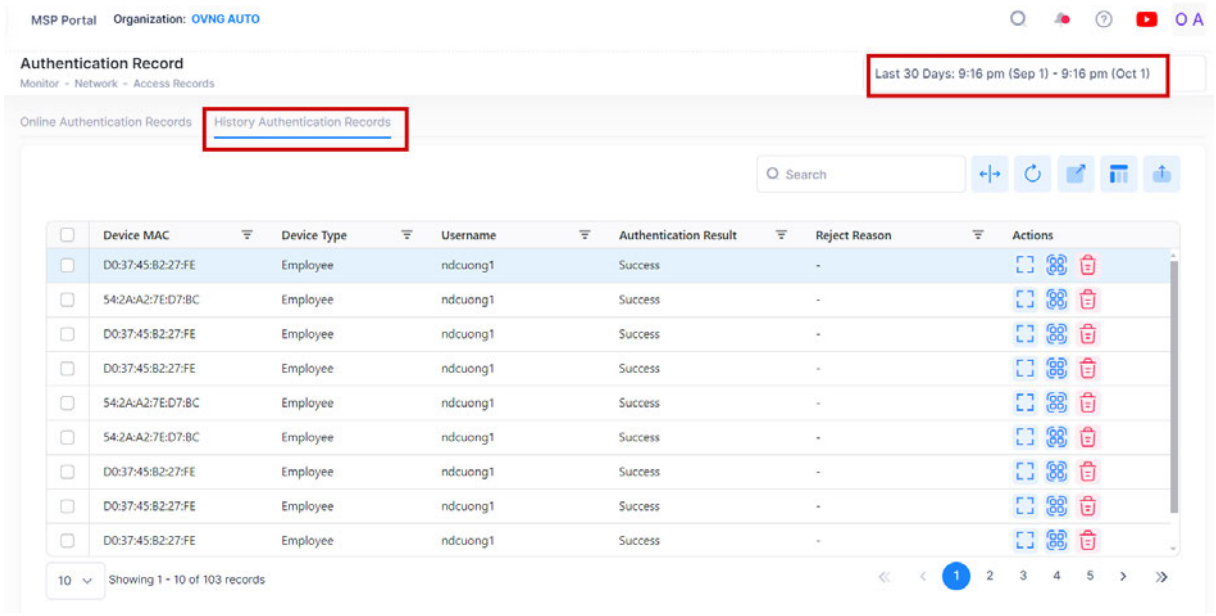
8.1.2.1 Authentication Records

The Authentication Records screen displays a list of all devices authenticated through UPAM. There is an option to view authentication records for clients currently online and an option to review historical client records. You can also display additional information (see page 884) about a specific Authentication Record. Use this information to troubleshoot authentication failures.

To access the Authentication Records screen, click on **Network > Access Records > Authentication Records** under the “Monitor” section of the OmniVista Terra Menu (see page 45).



By default, the Online Authentication Records List is displayed on the Authentication Records screen. This is a list of clients currently online. Click on the **History Authentication Records** tab to see a history of client authentication records. You can also select a specific time window range from the date range to filter the history of Authentication Records by starting time. For example:



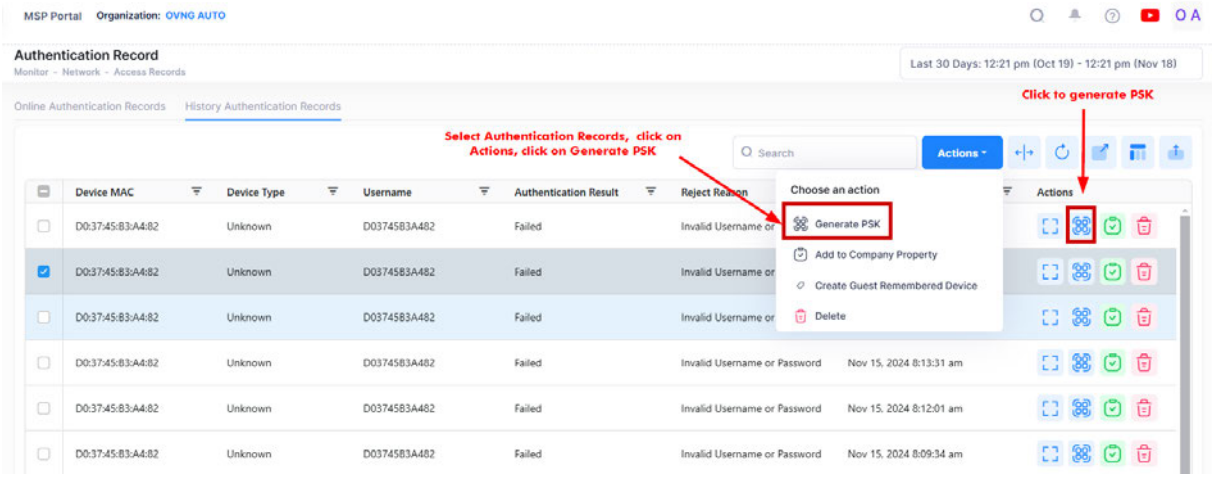
On the History Authentication Records screen, you have the following additional options:

- Generate a PSK for a device(s). (see page 880)
- Generate an Employee Account (see page 881)

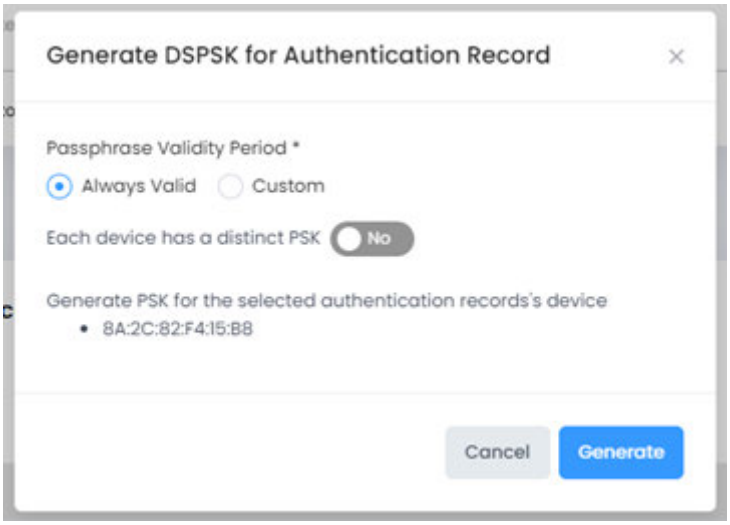
- Add to Company Property (see page 882)
- Create Guest Remembered Device manually (see page 883)
- Immediately log a user out of the network. (see page 884)The user will have to log in again to connect to the network.
- Search History Authentication Records by an Attribute Value (see page 887)

8.1.2.1.1 Generate a PSK

To generate a PSK for one or more devices, select the records in the History Authentication Records List and click on **Actions**, then select **Generate PSK** from the drop-down menu. You can also click on the Generate PSK icon under the “Actions” column next to an individual record.



The Generate DSPSK for Authentication Record modal opens.

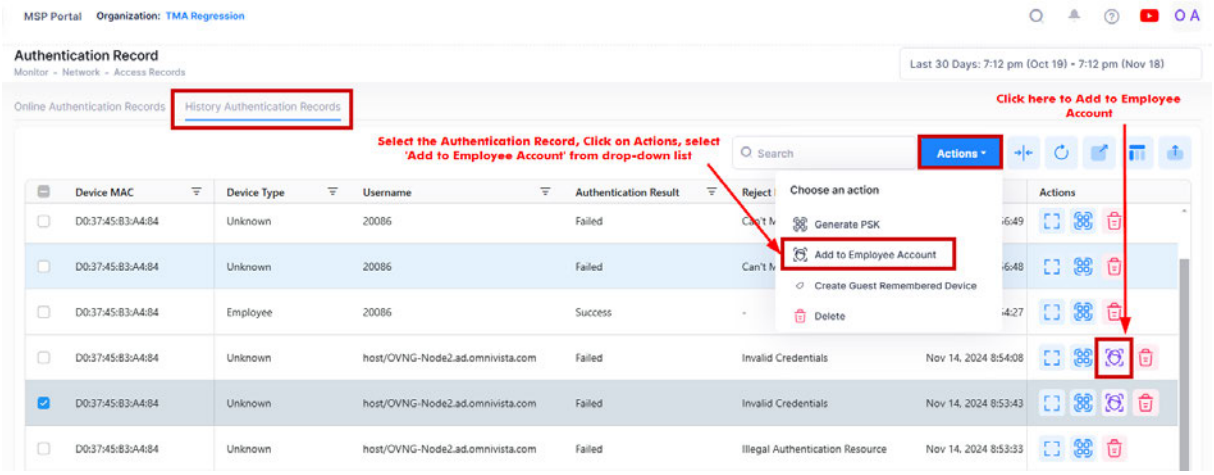


Select the Passphrase Validity Period (Always Valid or Custom) and whether each device will have a distinct PSK, then click on **Generate**. The device(s) associated with the record(s) will be added to the Company Property List as Device Specific PSK Devices. The PSK Passphrase for the device(s) is automatically generated by OmniVista Terra based on the device MAC Address and Session Time. The PSK Passphrase can be obtained and printed from the Company Property Screen. You can generate a

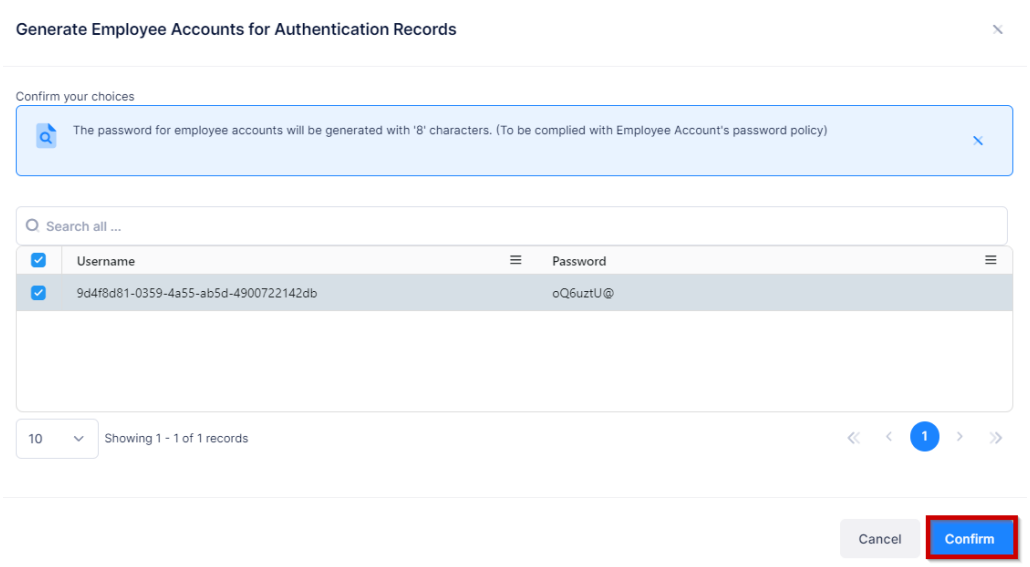
PSK for any Authentication Record. See the Company Property online help (see page 716) for more information.

8.1.2.1.2 Generate an Employee Account

To generate the Employee Accounts for the Authentication Records, select the records in the History Authentication Records list and click on **Actions**, then select **Add to Employee Account** from the drop-down menu. You can also click on the Add to Employee Account icon under the “Actions” column next to an individual record.



The Add to Employee Account will open below screen.



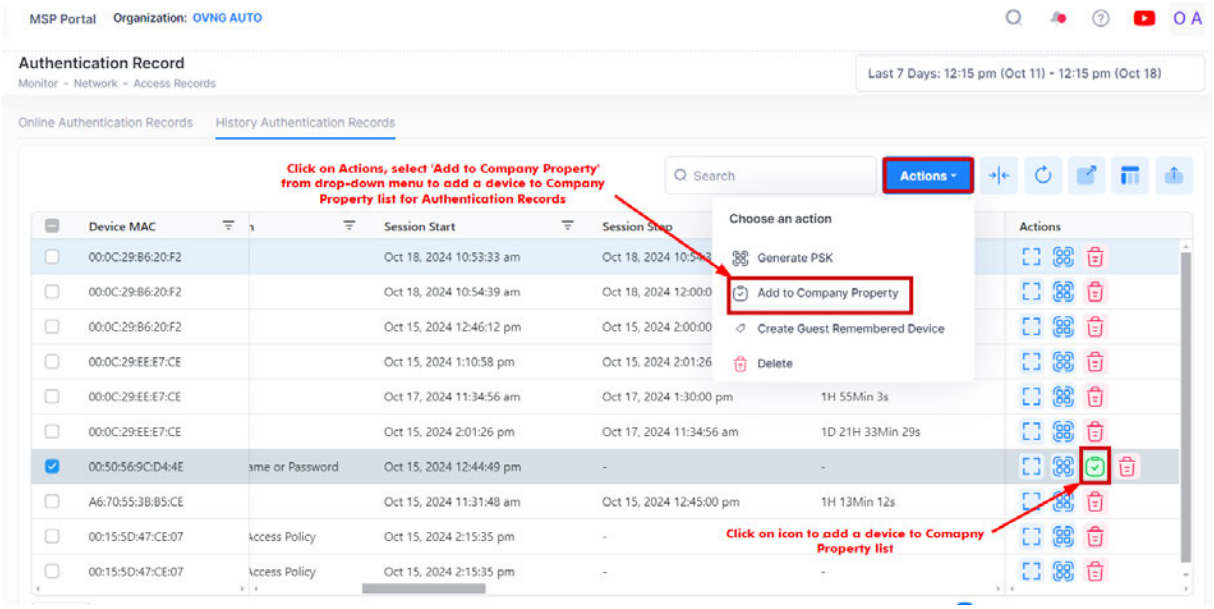
Click on **Confirm** to generate the Employee Account for an User in the Authentication Records.

- The password for employee accounts will be generated with '8' characters. (To be complied with Employee Account's password policy).
- You can also search and add multiple Authentication Records from the list to generate the Employee account.

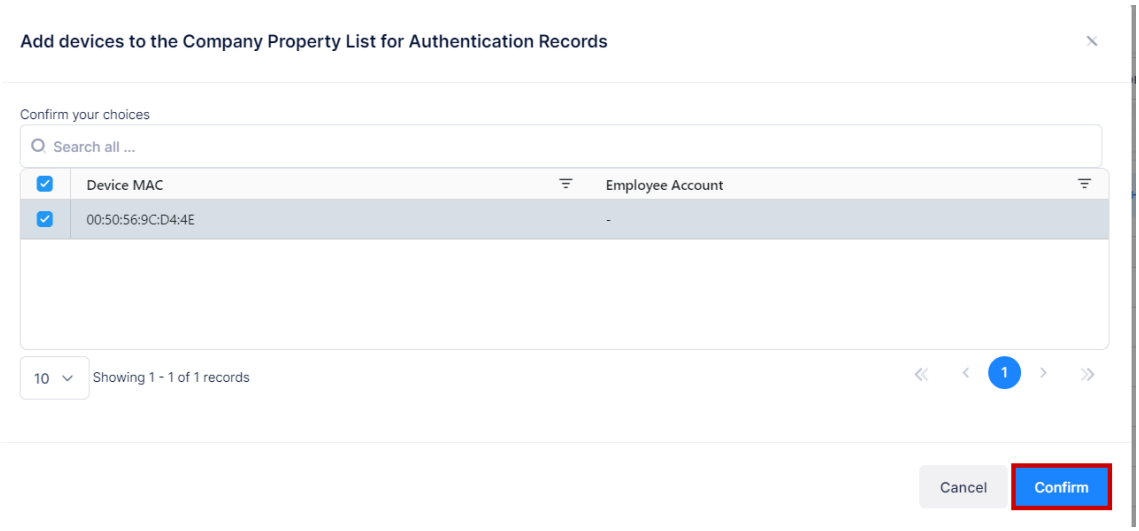
- The **Add to Employee Account** action button appears under all of the following conditions together:
  - Authentication Result = Failed
  - Authentication Resource = Local Database
  - Authentication Type = 802.1X or Portal

8.1.2.1.3 Add to a Company Property

To add network devices to Company Property list for Authentication records, select the records in the History Authentication Records list and click on **Actions**, then select **Add to Company Property** from the drop-down menu. You can also click on the Add to Company Property icon under the “Actions” column next to an individual record.



The Add to Company Property List will open below screen.



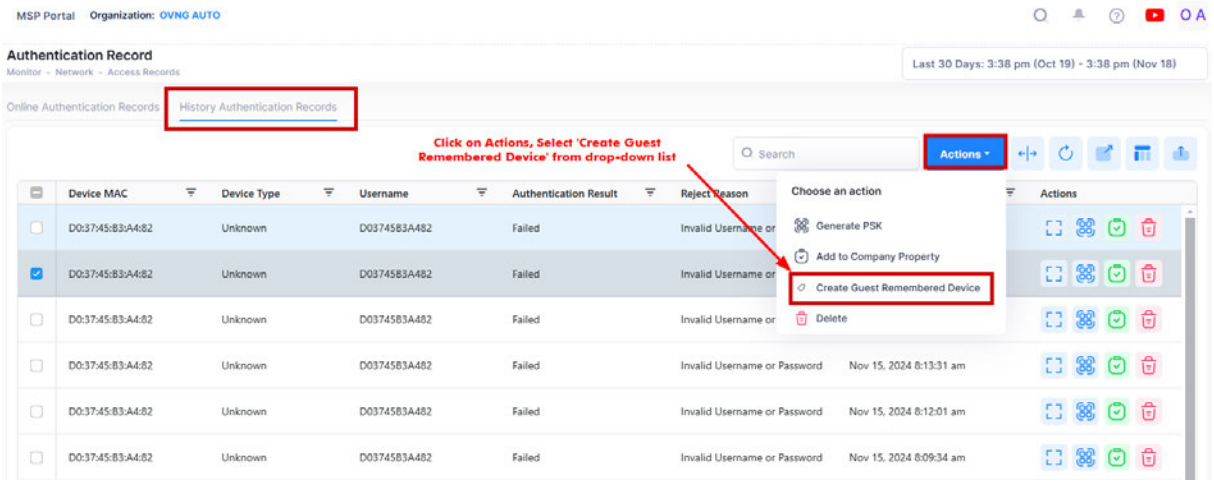
Click on **Confirm** to add the device to the Company Property List for the Authentication Records.

Note: The **Add to Company Property** action button appears under all of the following conditions together:

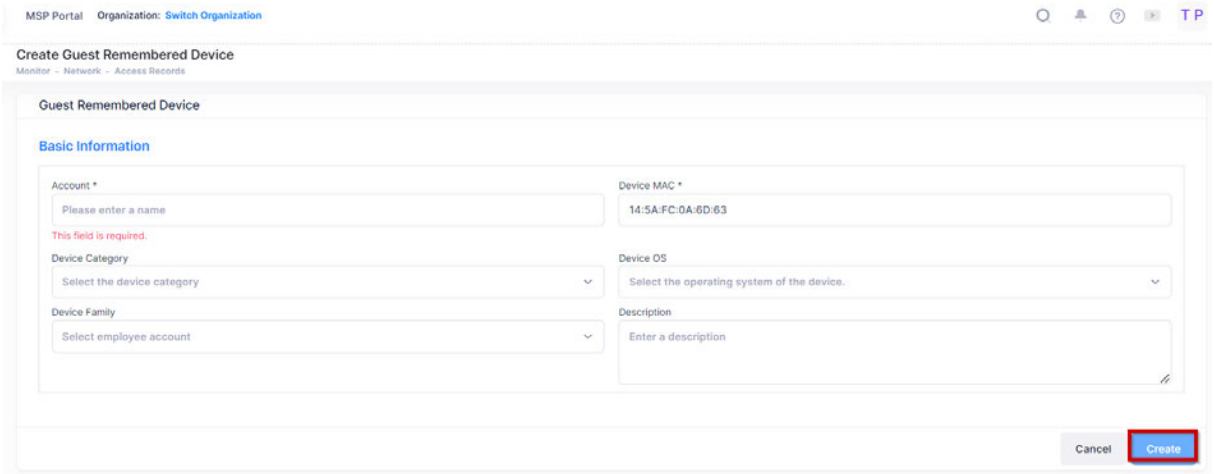
- Authentication Result = Failed
- Authentication Resource = Local Database
- Authentication Type = MAC

8.1.2.1.4 Create Guest Remembered Device

To create a Guest Remembered Device for the Authentication Records, select the records in the History Authentication Records list and click on **Actions**, then select **Create Guest Remembered Device** from the drop-down menu.



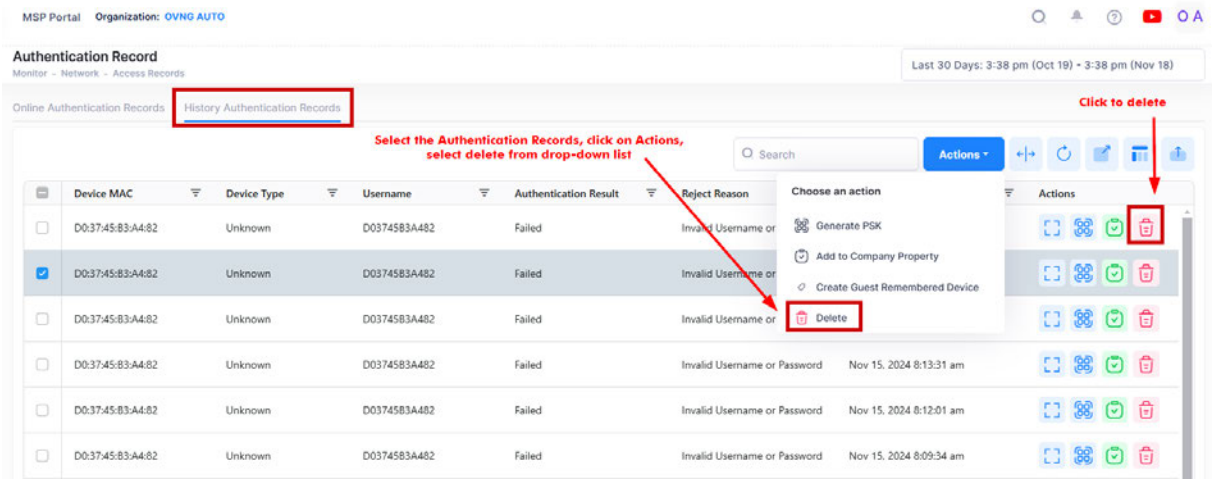
It directs you to Create Guest Remembered Device Screen as shown below:



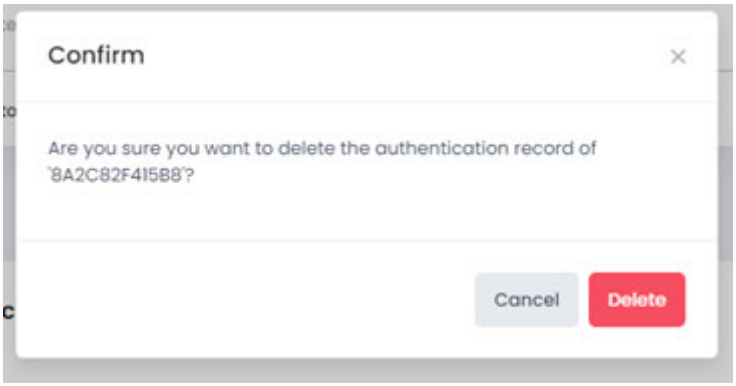
Enter the required information in the fields and click on **Create** button to create the Guest Remembered Device for the Authentication Records.

8.1.2.1.5 Log a User Out of the Network (Delete)

To delete an Authentication Record for one or more devices, select the records in the History Authentication Records List and click on **Actions**, then select **Delete** from the drop-down menu. You can also click on the Delete icon under the “Actions” column next to an individual record.

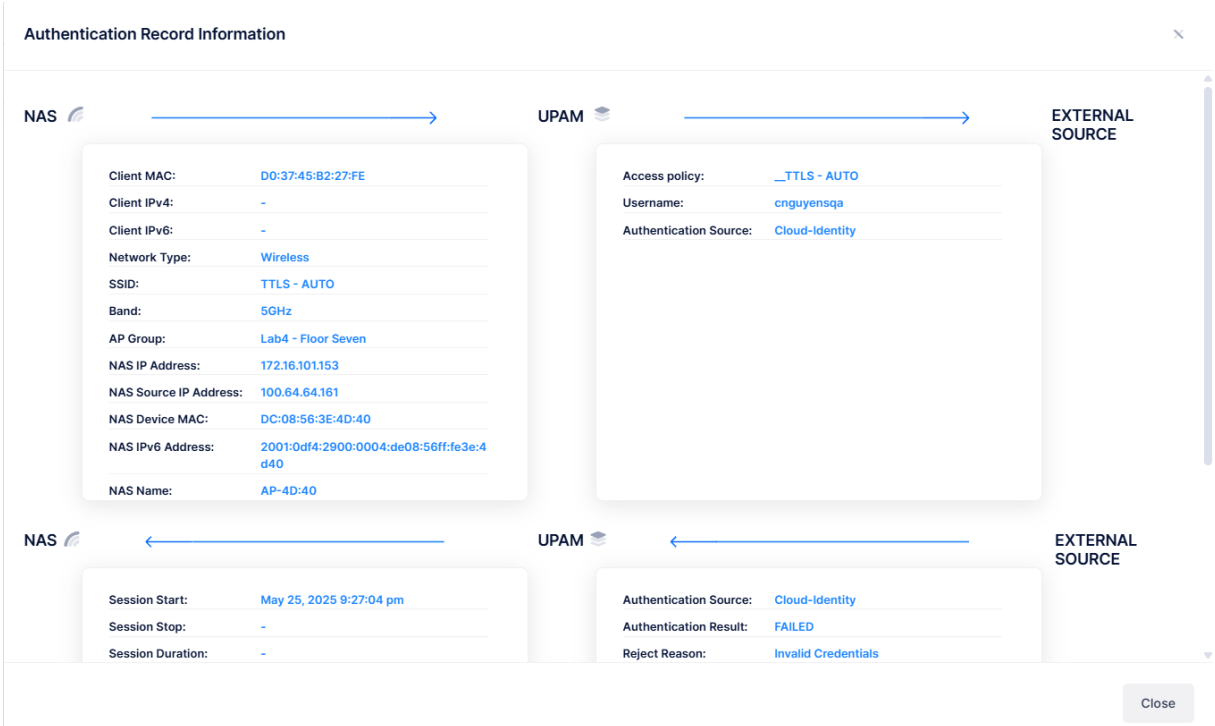


Click **Delete** on the following confirmation prompt. Note that when you delete an Authentication Record, you are logging the user associated with that record out of the network.



8.1.2.1.6 Authentication Records List

The Authentication Record List displays basic information for all Authentication Records. Click on the Additional Information icon under the “Actions' column next to a list entry to display detailed Authentication Record Information. The following screen appears:



The Authentication Record field values provide the following information:

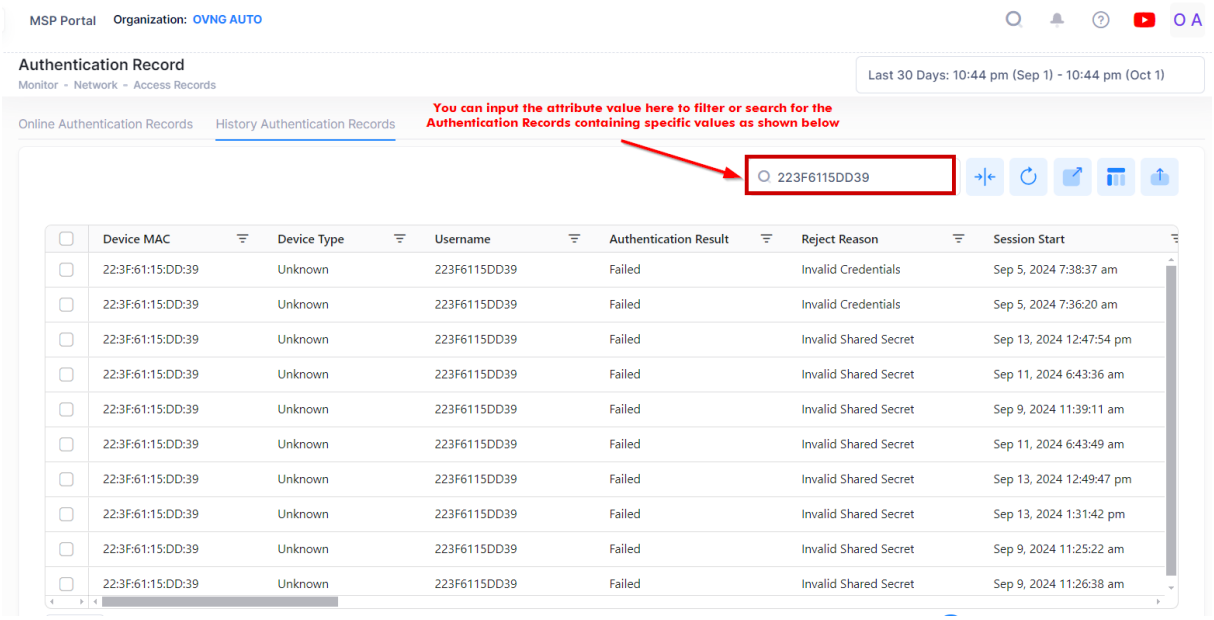
- **Client MAC** - The MAC address of the user device requesting authentication.
- **Client IPv4** - The IPv4 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **Client IPv6** - The IPv6 address of the client of the user device requesting authentication. Note that IP addresses are displayed only if they are known at the time the RADIUS Accounting packets are sent/received. For MAC Authentication, the Accounting Start packets typically do not contain client IP addresses.
- **SSID** - The access device SSID.
- **Band** - The frequency band used for NAS Client.
- **AP Group** - AP Group through which you accesses the network.
- **Device Type** - The type of the device.
- **Username** - User name of the device requesting authentication.
- **Authentication Result** - Result for the user authentication request (Success, Failed).
- **Reject Reason** - Reason for rejecting the authentication request from user device:
  - Overdue license
  - Invalid username or password
  - Cannot match access policy according to the authentication request.
- **Session Start** - The time when the user passed authentication and a connection session was created.
- **Session Stop** - The time when the connection session was terminated..

- **Session Time** - It specifies the maximum number of seconds of service provided prior to session termination..
- **Account Terminate Cause** - The reason for which the connection session was terminated..
- **Account Session ID** - Unique accounting ID that makes it easy to match start and stop records in a log file. The start and stop records for a given session must have the same account session ID.
- **Account Multi Session ID** - This is a unique accounting ID to make it easy to link together multiple related sessions in a log file.
- **Authentication Type** - The type of authentication used for the device (e.g., MAC, 802.1X)
- **Authentication method** - The method used for the device Authentication.(e.g., PAP, EAP-MD5, EAP-PEAP, EAP-TLS).
- **Auth Resource** - User profile database used in authentication, including none, local database, LDAP/AD and external RADIUS server, can refer to the authentication strategy definition.
- **Network Type** - The type of network used for device authentication. (Wireless or Wired).
- **NAS IP Address** - The identifying IP address of the NAS.
- **NAS Source IP Address** - The source IP address of the NAS.
- **NAS IPv6 Address** - The IPv6 address of the NAS.
- **NAS Name** - The Alcatel device name.
- **Packet Arrival** - The date and time at which the packet is received.
- **Packet Type** - The specific type of RADIUS message being transmitted between the client (NAS) and the RADIUS server.
- **EAP Method** - The specific method of Extensible Authentication Protocol (EAP) technique used within RADIUS to perform user authentication.
- **Alcatel Tenant ID** - It is the unique identifier of a specific tenant.
- **Alcatel Device SSID** - Wireless service broadcast by the NAS and connected by user device (only valid for wireless access).
- **NAS ID** - NAS Identifier, identify the NAS originating the Access-Request.
- **NAS Port Type** - The type of physical port type of the NAS authenticating the user:
  - Wireless-IEEE 802.11
  - Ethernet.
- **Called Station ID** - Allows the NAS to send the phone number the user called, using Dialed Number Identification (DNIS) or similar technology inside the Access-Request packet:
  - For Switch - Switch MAC Address.
  - For AP - radio_MAC_address:SSID_NAME.
- **NAS Port** - The physical port number of the NAS authenticating the user.
  - For Switch - if index.
  - For AP - Wireless radio index.
- **Service Type** - It is a standard attribute (Service-Type) used in RADIUS authentication requests and responses to specify the type of service being requested or provided to the user.
- **Alcatel Port desc** - The NAS Port description.

  - For Switch - Port description.
  - For AP - WLAN service.
- **NAS Port ID** - The NAS authenticating the user.
  - For Switch - chassis/slot/port
  - For AP - WLAN service.
- **Framed MTU** - The Maximum Transmission Unit to be configured for the user when it is not negotiated by some other means (e.g., PPP). It is a fixed value = 1400.
- **Alcatel Device MAC** - MAC address of the NAS to which the user device is attached.
- **Alcatel Device Name** - System name of the NAS to which the user device is attached.
- **Alcatel Device Location** - Location of the NAS.
- **NAS Device MAC** - The MAC address of the NAS Device.
- **Access Device SSID** - Wireless service broadcast by the NAS and connected by user device (only valid for wireless access).
- **Total UPAM Transactions** - The total time taken to complete RADIUS authentication.
- **Access Policy** - Name of the Access Policy for the user.
- **Web Access Policy** - Guest Strategy or BYOD Strategy.
- **Final Access Role Profile** - Access Role Profile assigned by NAS and in effect on the user device, but not the Access Role Profile returned by UPAM.

8.1.2.1.7 Search History Authentication Records by an Attribute Value

You can search for history Authentication records by using the Search box option. The search results are refined based on the attribute value selected from the available list (Device MAC/Nas Device MAC/ Access Device SSID or Username). Only those records that contain the matching searched values are displayed in the results.

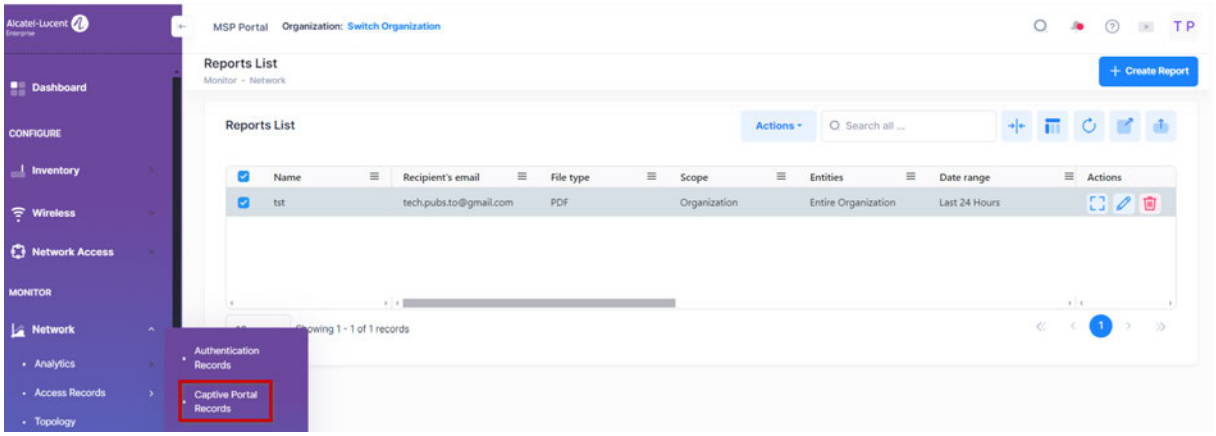


21 Oct 2025

8.1.2.2 Captive Portal Records

The Captive Portal Records screen displays Captive Portal information (see page 889) for all devices authenticated through UPAM. You can use this information to check the results of Captive Portal authentication and in case of failure, check the reason UPAM rejected the access request.

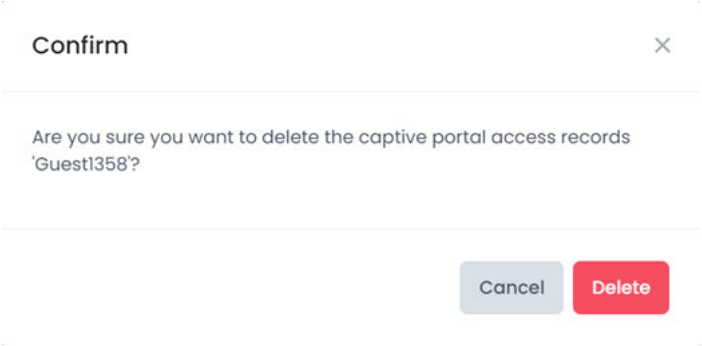
To access the Captive Portal Records screen, click on **Network > Access Records > Captive Portal Records** under the “Monitor” section of the OmniVista Terra Menu (see page 45).



8.1.2.2.1 Deleting a Captive Portal Record

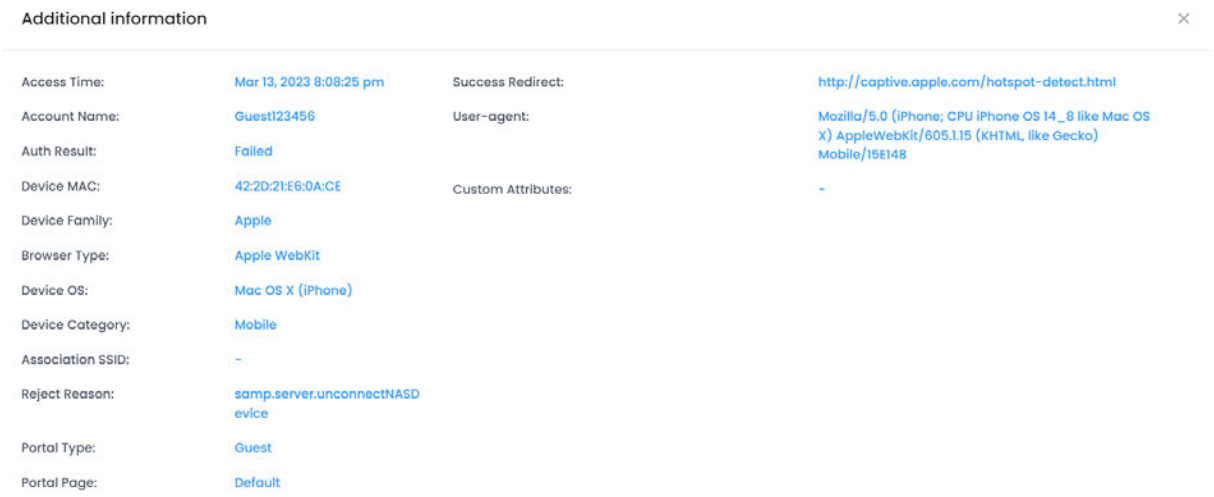
To delete a Captive Portal Record for one or more devices, select the records in the Captive Portal Records List and click on **Actions**, then select **Delete** from the drop-down menu. You can also click on the Delete icon under the “Actions” column next to an individual record.

Click **Delete** on the following confirmation prompt.



8.1.2.2.2 Captive Portal Records List

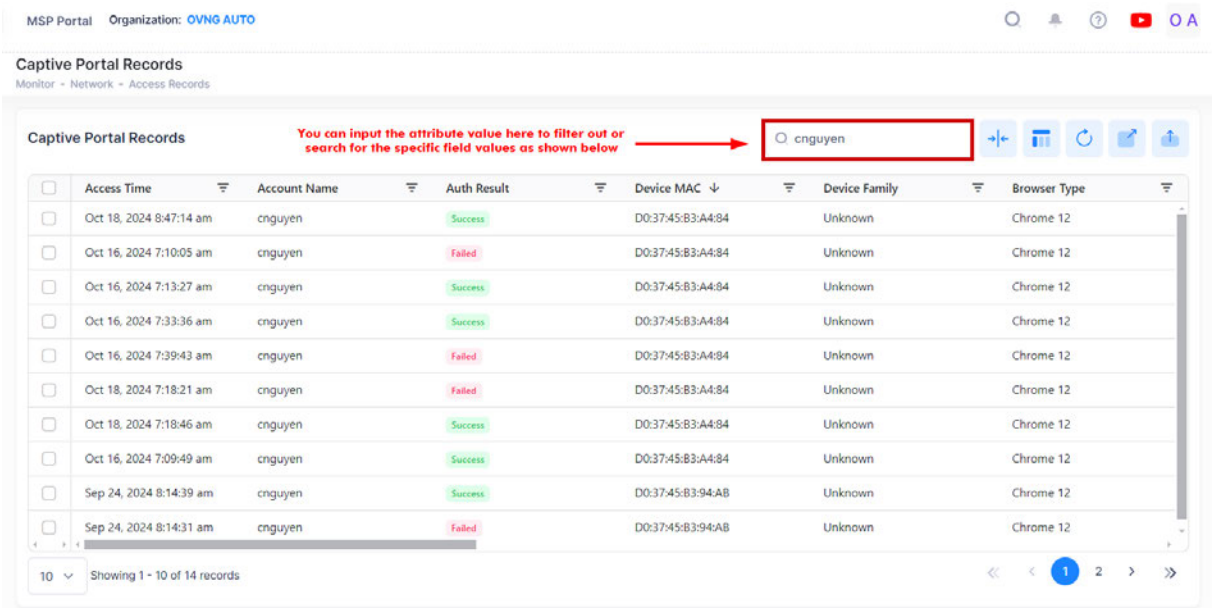
The Captive Portal Access Record List provides basic information. Click on the Additional Information icon under the “Actions' column next to a list entry to display detailed Captive Portal Access Record information.



- **Access Time** - The date and time the device sent the access request.
- **Account Name -** User name of the device requesting authentication.
- **Auth Result -** Result for the user authentication request (Success, Failed).
- **Device MAC -** MAC address of the user device requesting Captive Portal authentication.
- **Device Family -** Production vendor of the user device.
- **Browser Type -** The browser on the device that used to login the network by user.
- **Device OS -** Operating system of the user device.
- **Device Category -** Category of the user device (for example, “mobile”).
- **Association SSID -** Wireless network to which the user device is associated.
- **Reject Reason -** The the reason UPAM reject the access request.
- **Portal Type -** The Captive Portal usage (BYOD/Guest).
- **Portal Page -** The Captive Portal template name.
- **Success Redirect -** The redirect URL to which the browser goes after successful Captive Portal authentication.
- **User-agent -** The browser and device used to access the network.
- **Custom Attributes** - Custom attributes will show if you configured **Custom Attributes** in Guest Access Strategy (see page 633).

8.1.2.2.3 Search Captive Portal Records by an Attribute Value

You can search for Captive Portal records by using the Search box option. The search results are refined based on the attribute value selected from the available list (Device MAC/Association SSID or Account Name). Only those records that contain the matching searched values are displayed in the results.


MSP Portal
Organization: OVNG AUTO
Captive Portal Records
Monitor - Network - Access Records
Captive Portal Records
You can input the attribute value here to filter out or search for the specific field values as shown below
cnguyen
Access Time
Account Name
Auth Result
Device MAC
Device Family
Browser Type
Oct 18, 2024 8:47:14 am cnguyen Success D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 16, 2024 7:10:05 am cnguyen Failed D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 16, 2024 7:13:27 am cnguyen Success D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 16, 2024 7:33:36 am cnguyen Success D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 16, 2024 7:39:43 am cnguyen Failed D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 18, 2024 7:18:21 am cnguyen Failed D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 18, 2024 7:18:46 am cnguyen Success D0:37:45:B3:A4:84 Unknown Chrome 12
Oct 16, 2024 7:09:49 am cnguyen Success D0:37:45:B3:A4:84 Unknown Chrome 12
Sep 24, 2024 8:14:39 am cnguyen Success D0:37:45:B3:94:AB Unknown Chrome 12
Sep 24, 2024 8:14:31 am cnguyen Failed D0:37:45:B3:94:AB Unknown Chrome 12
10
Showing 1 - 10 of 14 records
1
2

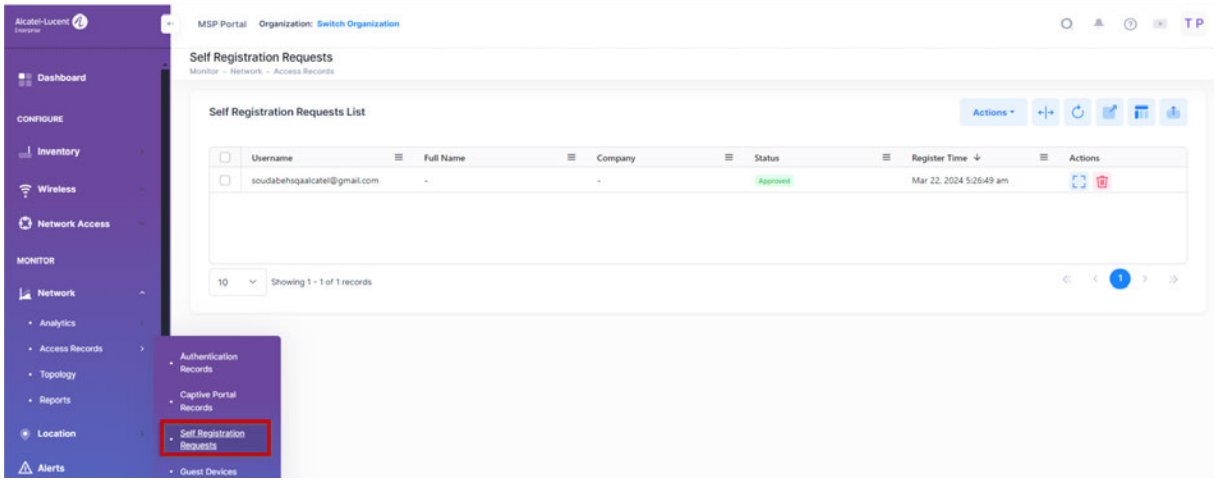
21 Oct 2025

8.1.2.3 Self-Registration Requests

The Self-Registration Requests screen is used to review, approve or reject self-registration requests from Guest Users. If “Self Registration” and “Approved by Sponsor” are enabled in the Guest Access Strategy (see page 633), a guest user must summit a request email to enroll with the required information. The self-registration request sent by guest user can be taken care of by the Administrator, Guest Operator or Employee sponsor, using the Approve or Reject operation.

To access the Self-Registration Requests screen, click on **Network > Access Records > Self Registration** requests under the “Monitor” section of the OmniVista Terra menu (see page 45).

To approve or reject a Self-Registration Request, select the request in the Self-Registration Requests List and click on the **Approve** or **Reject**.



8.1.2.3.1 Self-Registration Request List

- **Username -** Name of the guest user. If the self-registration request is approved, the guest name will be used as the login account for the guest user.
- **Full Name -** Full name of the guest user.
- **Company -** Company name of the guest user.
- **Register Time -** Date and Time when the guest user submitted the self-registration request.
- **Employee Email -** Email address of the employee being visited.
- **Employee Visited -** Name of the employee being visited.
- **Employee Phone Number -** Phone number of the employee being visited.
- **Reason for visit -** The purpose for this visit by the guest.
- **Status -** Status for the guest self-registration request.
  - **Unchecked -** The request needs to be checked by the Administrator or Guest Operator.
  - **Approved -** The request is approved by the Administrator/Guest Operator/Employee Sponsor and the approval message has been send to the guest through email.
  - **Rejected -** The request is rejected by Administrator/Guest Operator/Employee Sponsor and the rejection message has been send to the guest through email.
- **Approver Name -** The person who approves the self-registration request.

  - **Admin-XXX -** Admin indicates the sponsor belongs to The Administrator group; XXX indicates the account for the group.
  - **EmployeeSponsor-YYY -** EmployeeSponsor indicates the sponsor belongs to the employee group; YYY indicates the employee account for the group.
  - **GuestSponsor-ZZZ -** GuestSponsor indicates the sponsor belongs to the Guest Operator group; ZZZ indicates the Guest Operator account for the group.
- **Approval Time -** The date and time when the self-registration request was approved.
- **Email -** Email address of the guest user.
- **Telephone -** Telephone number of the guest user.
- **Description -** Optional description information provided by the guest.

Note: Custom attributes will show if you configured **Custom Attributes** in Guest Access Strategy.

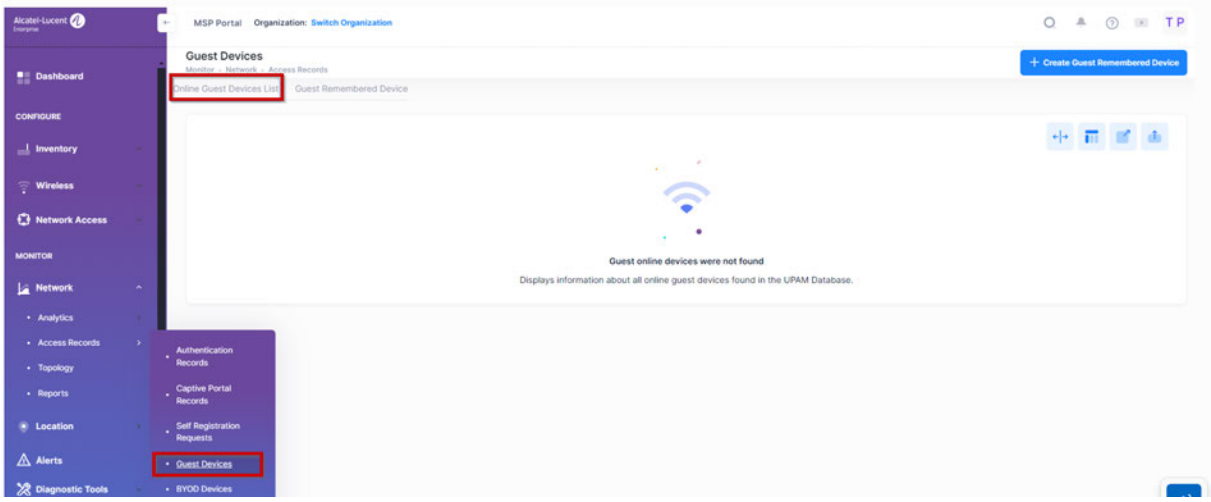
21 Oct 2025

8.1.2.4 Guest Devices

The Guest Devices screen displays all authenticated online guest devices (see page 894) as well as all guest devices that were previously on the network and are stored in UPAM (see page 895). You can also manually add the Guest Remembered device (see page 898) and Search by an attribute value (see page 899) for the Guest account from this screen. To access the Guest Devices screen, click on **Network > Access Records > Guest Devices** under the “Monitor” section of the OmniVista Terra Menu (see page 45).

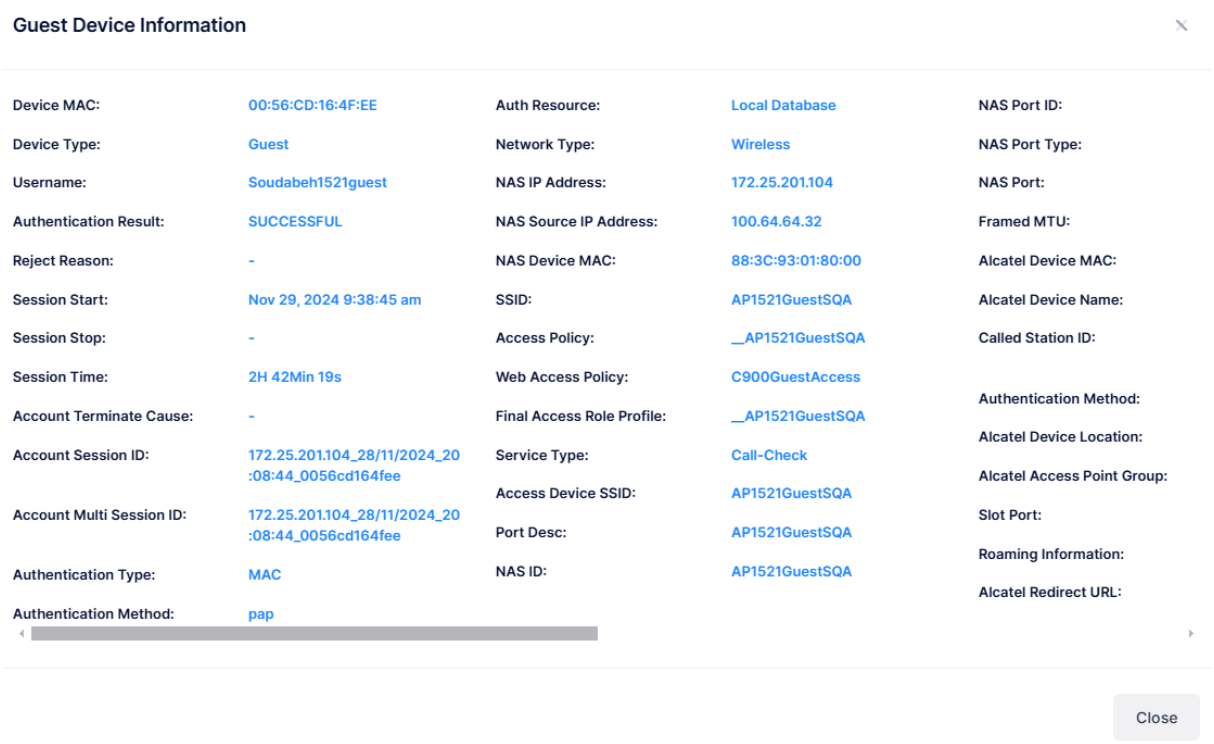
8.1.2.4.1 Online Guest Devices

By default, the Online Guest Devices List is displayed on the Guest Devices screen. This is a list of all authenticated online Guest Devices.



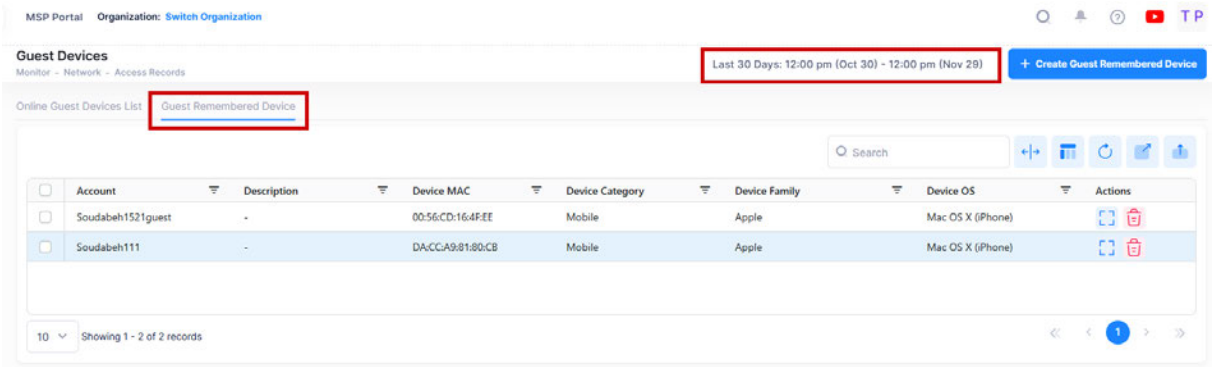
8.1.2.4.1.1 Online Guest Devices List

The Online Guest Devices List displays information for all Guest devices. Click on the Additional Information icon under the “Actions' column next to a list entry to display detailed information for a specific Guest device.



8.1.2.4.2 Guest Remembered Devices

Click on the **Guest Remembered Devices** tab to see the Guest Remembered Devices List. This is a list of all Guest devices that were previously on the network and are stored in UPAM. You can also select a specific time window range from the date range to filter the Guest Remembered Devices by starting time. For example:



8.1.2.4.2.1 Guest Remembered Devices List

The Guest Remembered Devices List displays information for all Guest devices that were previously on the network and are stored in UPAM. Click on the Additional Information icon under the “Actions' column next to a list entry to display detailed information for a specific Guest device.

The Guest Device field values provide the following information:

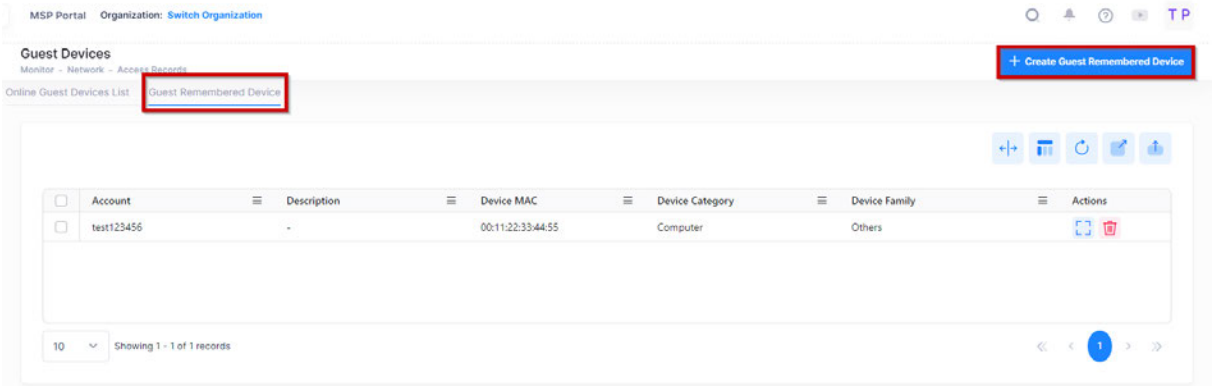
- **Account -** User name of the guest account.
  - For MAC authentication - Account name is the MAC address of the guest device.
  - For Captive Portal Authentication - Account name is user name of the guest user.
- **Description** - Description of the device.
- **Remembered method -** It indicates whether the device was manually added to the list (Static) or automatically added through Captive Portal Authentication (Auto).
- **Remembered time** - The time and date on which the online device was remembered by UPAM.
- **Device Category -** Category of the guest device:
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver
  - Others
- **Device Family -** Production vendor of the guest device:
  - Alcatel-Lucent Enterprise
  - Apple
  - Samsung
  - Huawei
  - Microsoft
  - LG
  - Lenovo
  - HP
  - IBM
  - Nokia
  - MI

  - HTC
  - Sony
  - Blackberry
  - Others
- **Device OS -** OS running on the guest device.
  - Linux
  - Windows
  - MacOS
  - Android
  - IOS
  - Others
- **Expiry time** - Indicate the expiry time of the guest device. When it is expired, the guest device will be deleted from the remembered list in UPAM.
- **Authentication Resource -** Guest account database used for authentication (None or Local Database).
- **Session Start -** The date and time when the user was online and the connection session created.
- **Access Role Profile -** Access Role Profile applied on the guest device.
- **Strategy name -** The name of the guest user.
- **Policy -** Policy List applied on the guest device.
- **Redirect URL -** Redirect URL returned to the guest device by UPAM.
- **Device MAC -** MAC address of the NAS to which the guest device is attached.
- **Time Quota** - Enable or disable a time quota for guest traffic.
- **Data Quota** - Specify the guest traffic quota, in MB, for the Service Level.
- **Used Data Quota** - Specify the traffic quota in MB, consumed by the guest.
- **Data Quota Amount** - Specify the guest traffic quota, in MB, for the Guest Access Strategy.
- **Used Time Quota** - Specify the number of hours consumed by the guest.
- **Time Quota per day** - Specify the number of hours each day that the time quota is applied to guest traffic. The quota is reset at the beginning of each day.
- **Time Quota by hours** - Specify the number of hours that guest traffic is allowed.
- **Blocked hours** - Specify the number of hours to block guest traffic once the number of hours allowed is reached. After the number of hours to block is reached, the number of hours to allow guest traffic starts up again.
- **Reduced Up Bandwidth** - Bandwidth Up is set for the Access device. It will be set for the accessing device when the device reaches the Data/Time quota limitation. The unit is kbit/s.
- **Reduced Down Bandwidth** - This is set in the registration configuration file. The Bandwidth will be set for the accessing device when the device reaches the Data/Time quota limitation. The unit is kbit/s.
- **Exhausted Data Time** - It indicates the end time of the 'Block for' on the device, 'the Block for' field is set in Registration Profile, once the device reaches the 'Allow access for', it will be blocked for the number of hours specified in the 'Block for' field.

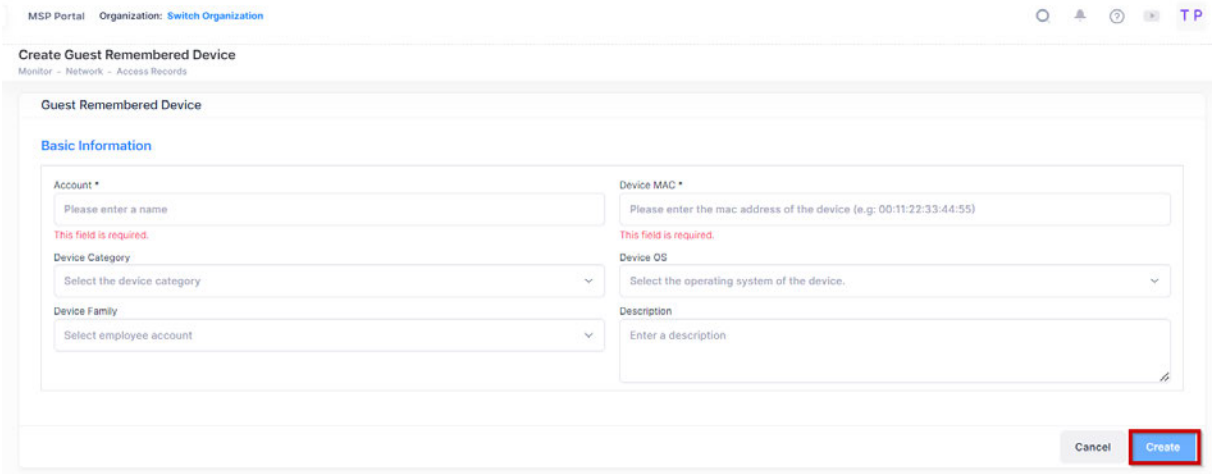
A device may still appear in the Guest Remembered Devices List for approximately 15 minutes after the Expiry Time. Once the device is cleared from this list, the Guest Account status will change to “Expired”.

8.1.2.4.2.2 Create Guest Remembered Device Manually

The user can manually add devices in the Guest Remembered Device database by using the **Create Guest Remembered Device** tab at the top right of the Guest Devices screen.



The following screen appears. Enter the required fields and click on **Create** to add a Remembered Device.

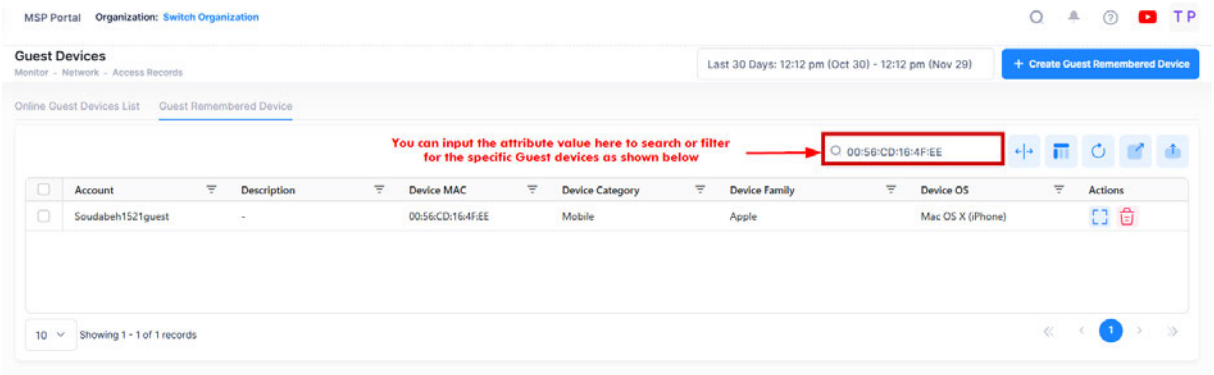


- **Account** - The Guest Account name of the device.
- **Device MAC** - The MAC address of the device.
- **Device Category** - Specify the category of the device from the drop-down list like mobile, computer, tablet etc.
- **Device OS** - Select the operating system of the device from the drop-down list. (Windows, Linux, Android etc.)
- **Device family** - Select the Employee account of the device.
- **Description** - Provide a optional short description for the account.

Note: A Guest Account is required before creating the Guest Remembered Device by Account. For more details please refer Guest Accounts. (see page 727)

8.1.2.4.2.3 Search by an Attribute Value

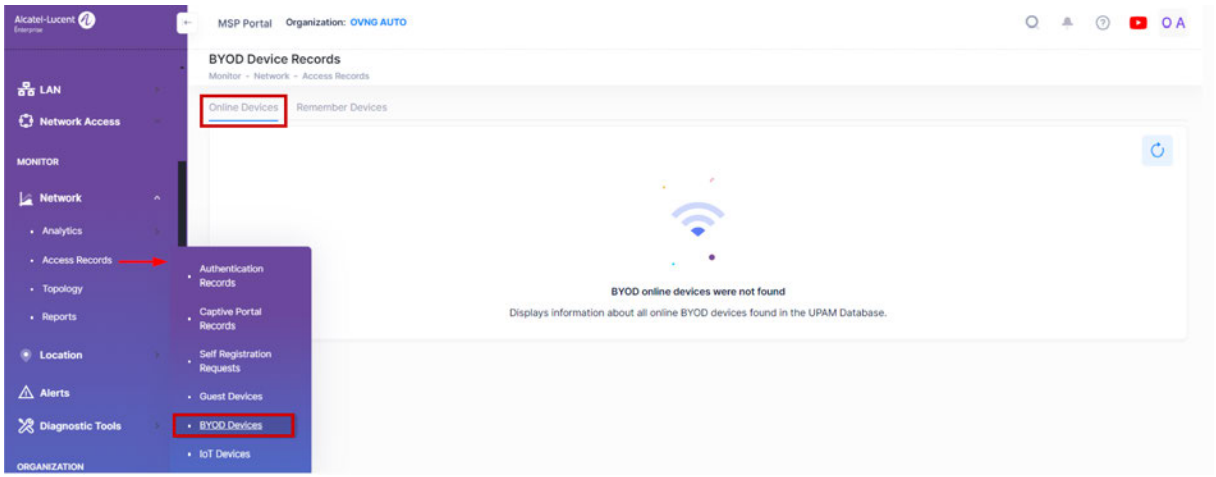
You can search for Guest Remembered devices by using the Search box option. The search results are refined based on the attribute value selected from the available list (Device MAC/Account). Only those records that contain the matching searched values are displayed in the results.



21 Oct 2025

8.1.2.5 BYOD Device Records

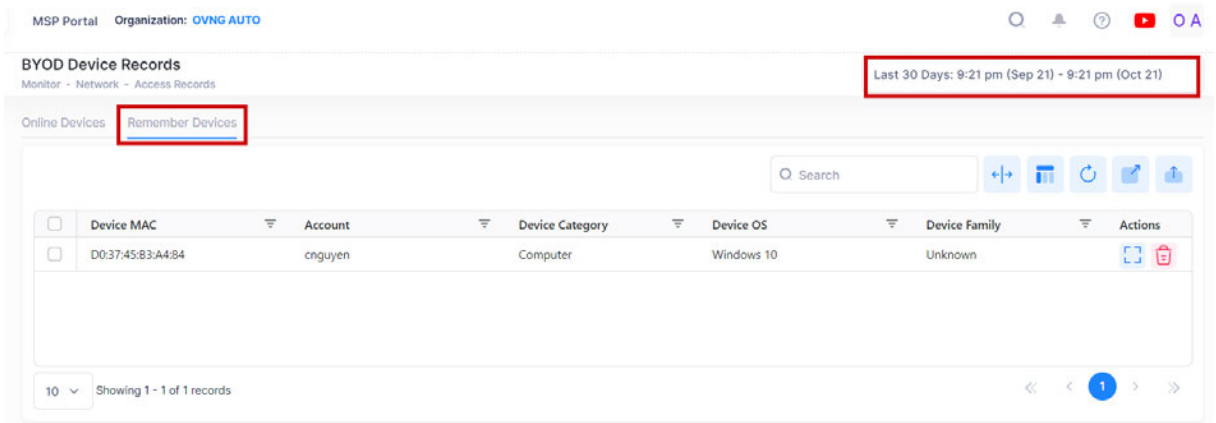
The BYOD Device Records screen displays all authenticated online BYOD devices as well as all BYOD devices that were previously on the network and are stored in UPAM. To access the BYOD Device Records screen, click on **Network > Access Records > BYOD Devices** under the “Monitor” section of the OmniVista Terra Menu (see page 45).



By default, the List of Online BYOD Device Records is displayed. This is a list of all authenticated online BYOD devices.

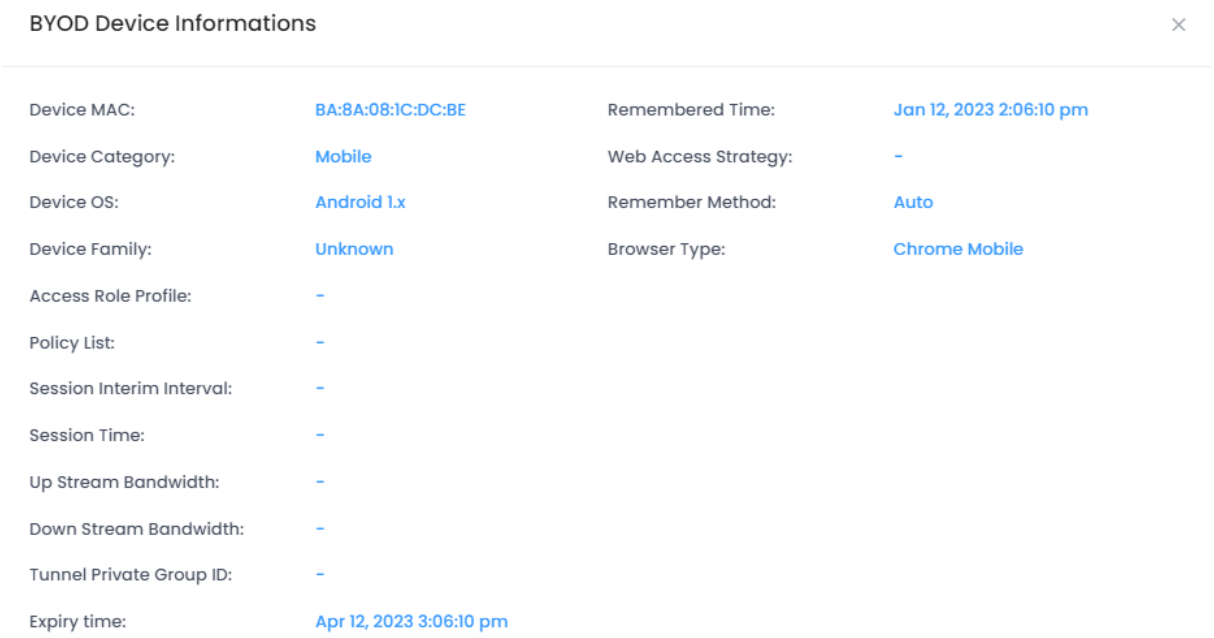
8.1.2.5.1 BYOD Remembered Devices

Click on the **Remembered Devices** tab to see all BYOD devices that were previously on the network and are stored in UPAM. You can also select a specific time window range from the date range filter the BYOD Remembered Devices by starting time. For example:



8.1.2.5.2 BYOD Devices List

The BYOD Devices List displays information for all BYOD devices. Click on the Additional Information icon under the “Actions' column next to a list entry to display detailed information for a specific BYOD device.



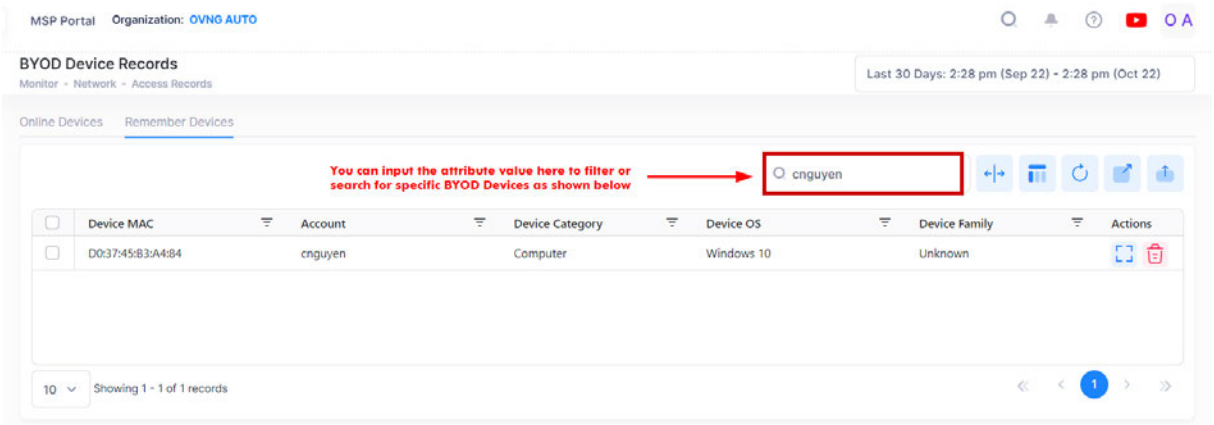
The BYOD Device Records field values provide the following information:

- **Device MAC** - The MAC address of the all authenticated BYOD devices.
- **Device Category** - Category of the BYOD device:
  - Computer
  - Mobile
  - Tablet
  - Game console
  - Digital media receiver
  - Others
- **Device Family** - Production vendor of the BYOD device:
  - Alcatel-Lucent Enterprise
  - Apple
  - Samsung
  - Huawei
  - Microsoft
  - LG
  - Lenovo
  - HP
  - IBM
  - Nokia
  - MI
  - HTC

    - Sony
    - Blackberry
    - Others
- **Device OS** - The OS running on the BYOD device.
    - Linux
    - Windows
    - MacOS
    - Android
    - IOS
    - Others
- **Access Role Profile** - Access Role Profile applied on the BYOD device.
- **Policy List** - The policy list of the BYOD device.
- **Session Interim Interval** - Number of seconds between each interim update for this specific session.
- **Session Time** - It specifies the maximum number of seconds of service provided prior to session termination.
- **Up Stream Bandwidth** - The maximum rate at which the data is sent.
- **Down Stream Bandwidth** - The maximum rate at which the data is received.
- **Tunnel Private Group ID** - Used to support the VLAN assignment from RADIUS (ID=VLAN ID).
- **Expiry Time** - Indicate the expiry time of the BYOD device. When it is expired, the BYOD device will be deleted from the remembered list in UPAM.
- **Remembered Time** - The time and date on which the BYOD device was remembered by UPAM.
- **Web Access Strategy** - The Access Strategy used for the device. One device can login through multiple BYOD Access Strategies.
- **Remember method** - It indicates whether the device was manually added to the list (Static) or automatically added through Captive Portal Authentication (Auto).
- **Browser Type** - Browser of the BYOD device.

8.1.2.5.3 Search by an Attribute Value

You can search for BYOD Remembered devices by using the Search box option. The search results are refined based on the attribute value selected from the available list (Device MAC/Account). Only those records that contain the matching searched values are displayed in the results.

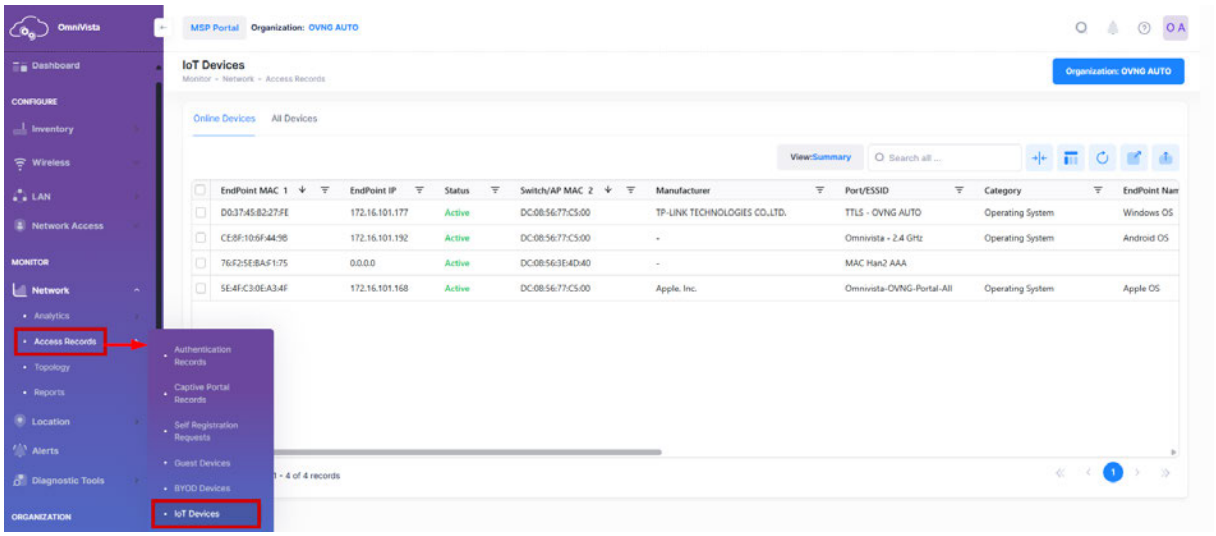

MSP Portal
Organization: OVNG AUTO
BYOD Device Records
Monitor - Network - Access Records
Last 30 Days: 2:28 pm (Sep 22) - 2:28 pm (Oct 22)
Online Devices
Remember Devices
You can input the attribute value here to filter or search for specific BYOD Devices as shown below
cnguyen
Device MAC
Account
Device Category
Device OS
Device Family
Actions
D0:37:45:B3:A4:84
cnguyen
Computer
Windows 10
Unknown
10
Showing 1 - 1 of 1 records
1

21 Oct 2025

8.1.2.6 IoT Devices

The IoT Inventory Devices Screen provides detailed information for all endpoint devices that are connected to the network (e.g., PCs, Tablets, Smartphones).

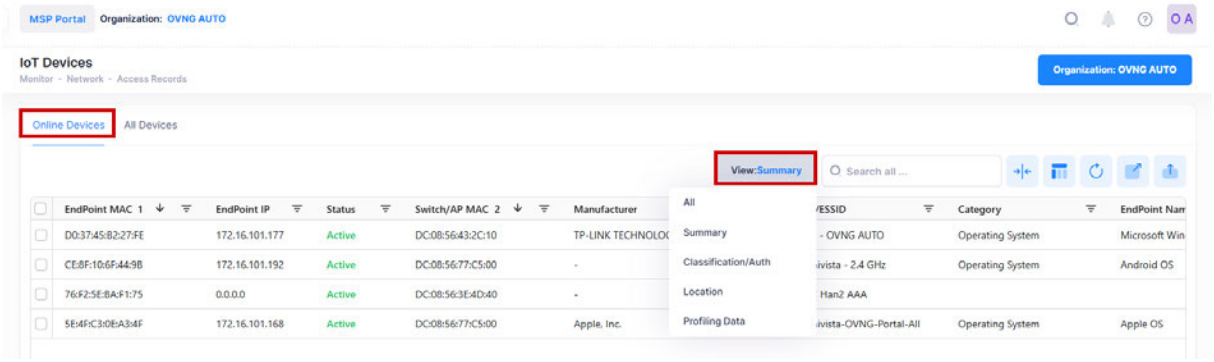
Use the IoT Devices screen to display information about all of the connected IoT Devices. To access the IoT Devices screen, click on **Network > Access Records > IoT Devices** under the “Monitor” section of the OmniVista Terra Menu (see page 45).



> **Note:** If you enable IoT on a device that already has connected clients, the clients will not show up as IoT devices until you reconnect them to the device.

The new endpoint association or disassociation (Endpoint Status) is updated in real-time (click on the **Refresh** button to display the latest information from the OmniVista Terra database). Once an endpoint is Active, any changes to the endpoint (e.g., profile change, IP address change) are updated in every 5 minutes for devices connected to Stellar Access Points.

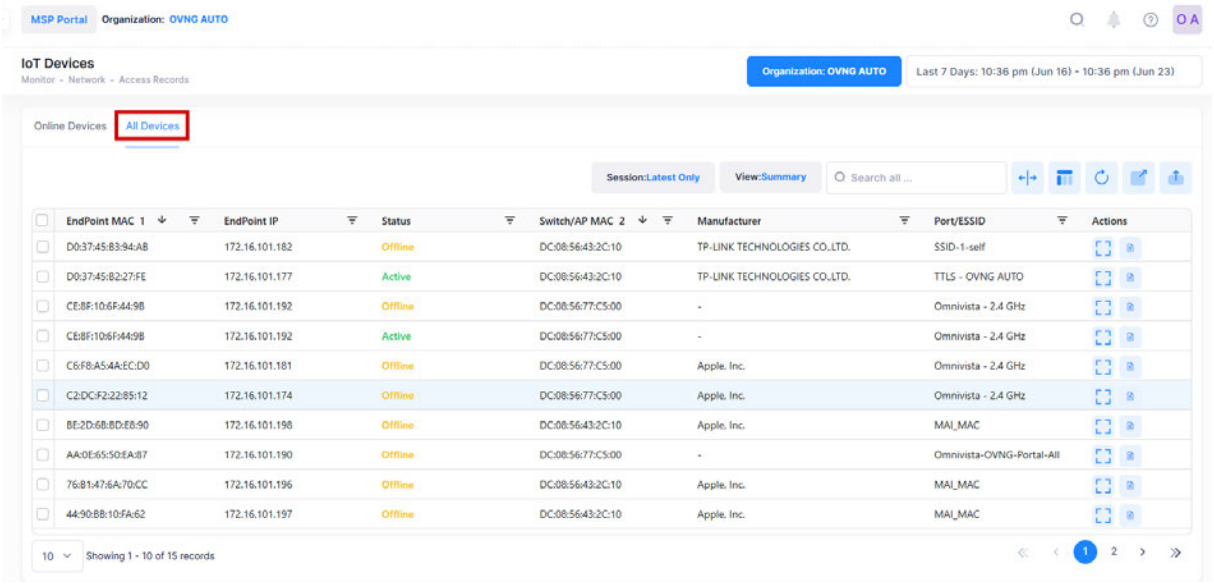
By default, the Online Devices List is displayed on the IoT Devices screen. This is a list of clients currently online. Click on the **All Devices** tab to view all available devices list. By default, only the Summary view is displayed in the IoT Online Devices List for each device; however, you can display all available information by selecting the “All” option on the filter window. For example:



8.1.2.6.1 IoT All Devices List

The IoT Devices List displays information for all IoT Devices. By default, the "Summary" view of the IoT Devices List is displayed, which gives an overview of device inventory. To display detailed information about a specific Device, click on the Additional Information icon under the “Actions” column.

Data displayed in each widget can be exported into a CSV, PDF or Excel sheet format. You can also switch the widgets to full-screen mode for a better display.



For each of the IoT Devices, the following field values are displayed:

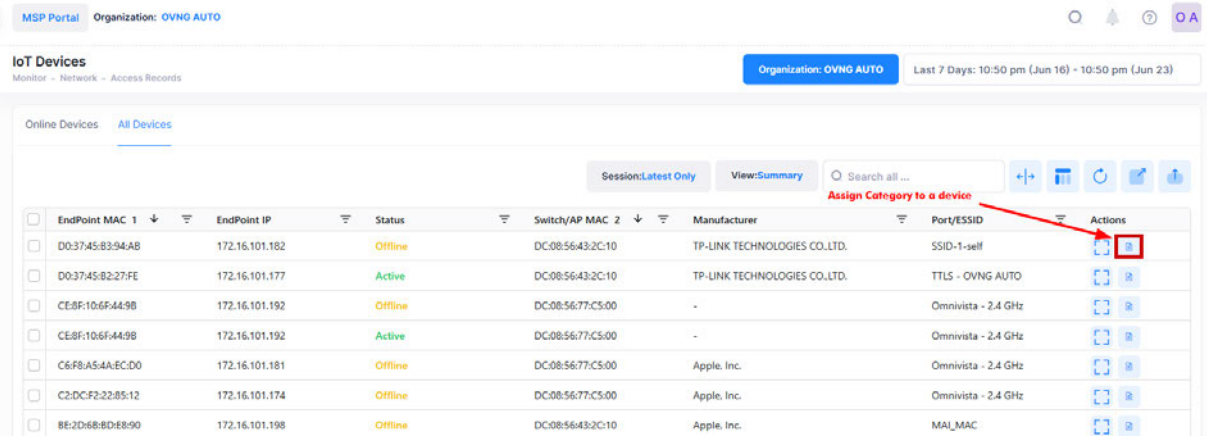
- **Endpoint MAC -** The MAC Address of the device.
- **Endpoint IP -** The IP Address of the device.
- **Status -** The operational status of the device on the network.
  - **Active -** The device was active on the network when it was last known by OmniVista. Note that if a Access Point is deleted from OmniVista or IoT is disabled on a Access Point, OmniVista will display all devices connected to that Access Point as "Offline" regardless of the device's actual status. This is because OmniVista receives no updates regarding these devices in these scenarios. If a Access Point goes down, OmniVista will not automatically change the status of the devices connected to it.

    - **Offline -** The device is not currently active on the network. Note that if IoT is disabled on a device or a device is removed from the Managed Devices List, the device remains in the Inventory List with device information "grayed out" and the last know information displayed.
    - **Error -** The device was unable to connect to the network (e.g., MAC Authentication fails).
- **Category -** The device category (e.g., Datacenter Appliance, Phone/Table/Wearable). Note that that initial Category value is not likely to be very specific. As more activity happens on the endpoint device, Access points send additional details about the endpoint, and the category description will be more specific. Also note that for some devices, this field may be empty. This generally happens when insufficient fingerprint information about the device is available. (e.g., Access Points receives only the MAC address of the endpoint and the MAC is unknown or unpopular).
- **Manufacturer -** The device manufacturer. This is derived from the MAC address of the device. The field may be empty if the device uses randomized MAC addresses.
- **Endpoint Name -** The name of the endpoint device as determined by the Device Fingerprinting Service.
- **Endpoint Version -** The endpoint device Operating system version.
- **Category Hierarchy -** The Category, Manufacturer, and Endpoint name used to categorize the device.
- **Switch/AP Name -** The IP address of the Switch/Access Point through which the device is connected to the network.
- **Switch/AP MAC -** The MAC address of the Switch/Access Point through which the device is connected to the network.
- **Port/ESSID -** The switch port or ESSID through which the device is connected to the network.
- **Port Type -** The port type through which the device is connected to the network (Wireless/ Wired/UNP).
- **Port Description -** A description of the port through which the device is connected to the network, as received from the device.
- **VLAN -** The VLAN through which the device is connected to the network.
    - **AOS Devices -** The untagged VLAN, or the tagged VLAN if traffic is tagged.
    - **Stellar APs -** The VLAN mapped to the Access Role Profile.
- **Tunnel Type -** If the endpoint is set up on tunnel, the tunnel type is displayed:
    - SPB
    - VXLAN
    - L2GRE
    - Guest Tunnel.
- **Far End IP -** The IP address of the far end tunnel termination (displayed for wireless clients only).
- **VPN ID -** The Tunnel ID that identifies a GRE Tunnel VPN (displayed for wireless clients only).
- **UNP -** The Access Role Profile assigned to the device, if applicable.
- **UNP Type -** The UNP type, if enforcement is applied:

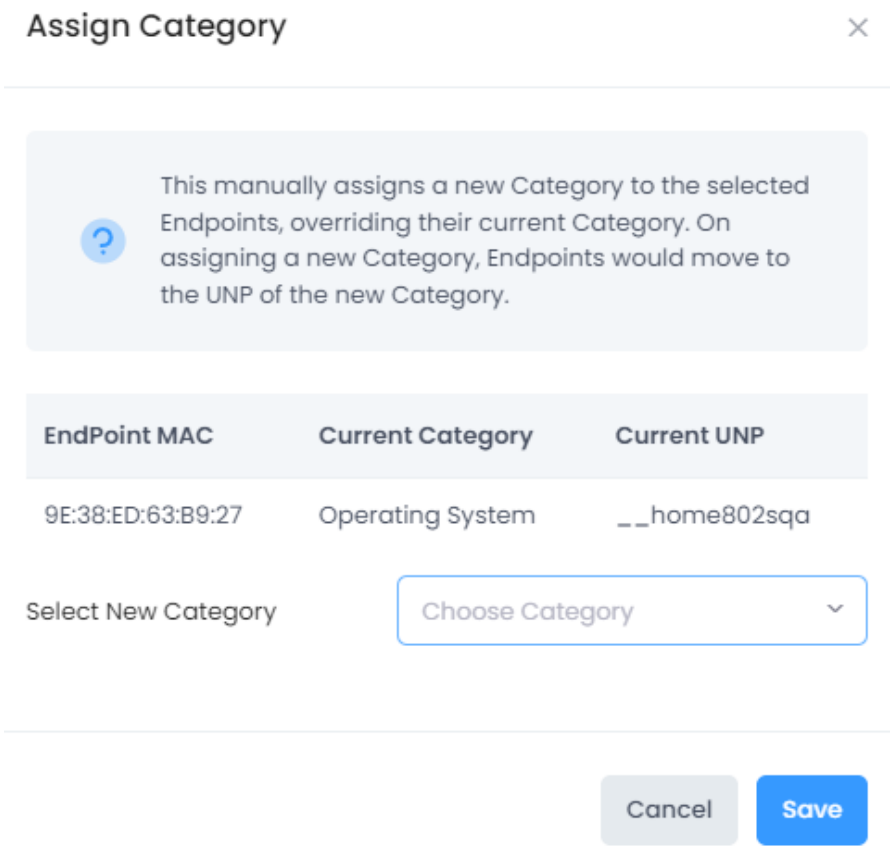
  - Default UNP
  - Pass-Alternate UNP
  - Authetication-Server Down UNP
  - UNP from Classification
  - UNP from RADIUS
  - UNP from OmniVista Enforcement.
- **Policy List -** The Policy List applied to the device, if applicable.
- **Authentication Type -** The type of authentication used for the device (e.g., MAC, 802.1X)
- **Authentication Status -** The status of device authentication, if applicable (e.g., Passed, Failed).
- **Connection Error -** The connection error if the device was unable to connect to the network, if applicable.
- **Enforcement Status -** The status of profile enforcement, if applicable:
  - Initial - Initial status.
  - Excluded - Matching by Exclusion Rules, no mapping.
  - Enforced - Successfully mapped to category.
  - Failed - SNMP enforcement failed.
  - Pending - Enforcement request was send to device/Access Point. One reason may be that ARP is not configured on the device.
  - Disabled - OmniVista is working in manual mode.
- **Start Time -** The time the device first accessed the network.
- **End Time -** The time the device disconnected from the network.
- **Last Updated -** The last time OmniVista received message from the device and the message was successfully processed.

8.1.2.6.2 Assigning a Custom Category to a Device

The user can override the Default Category assigned to a device through Fingerprinting and manually assign a Custom Category to a device. Select the device(s) in the Inventory List and click on the **Assign Category** button as shown below:



Then the Assign Category Confirmation window appears. Select a New Category from the Choose Category drop-down list and click on the **Save** button as shown below:

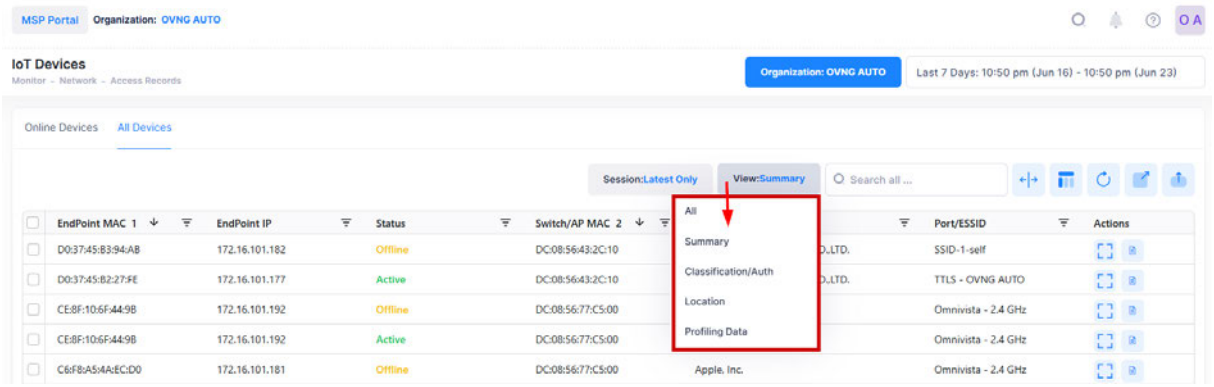


Now, the selected device(s) will appear in the IoT Device List with the new Custom Category device name.

Note : If Enforcement was configured for the assigned Category, endpoints might change their UNP mapping to the UNP that mapped with new category, or to no enforcement if the new category has no UNP mapping.

8.1.2.6.3 Customizing the Display

The user can customize the “View” of the IoT Devices list screen. By default, the “Summary” view of IoT Devices list is displayed on the screen. The display can be changed by clicking on the “View” button at the top right of the List as shown below:



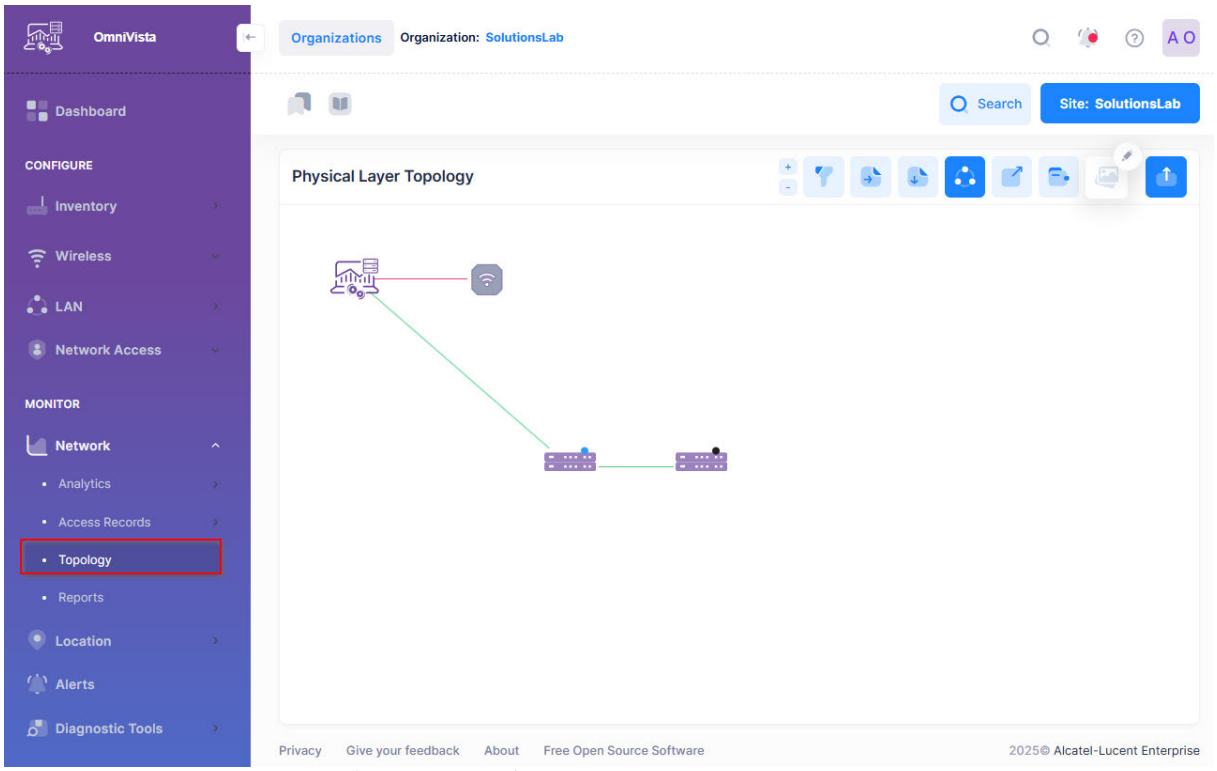
The display can be changed by clicking on any of the options available in the drop-down list. (e.g. All, Classification/Auth, Location or profiling Data). For example, if the user select the “Classification/ Auth” option from the menu list, the below revised IoT Devices List will appear on the screen.

21 Oct 2025

8.1.3 Topology

The Topology application enables you to view the topology of all managed devices in the network, view information about a specific device and perform certain actions on those devices (e.g., edit a device, telnet to a device, reboot a device). You can view devices in a topology map in various ways. For example, you can view managed devices in the Physical Layer Topology, highlight specific devices or links, and re-arrange devices in a map and save that new map view. The figure below provides an overview of some of the functions that can be performed in the Topology application. Specific functions available when working with maps are detailed below.

> Devices must first be added to the Device Catalog and licensed before they are displayed in Topology. See the Device Catalog (see page 170) online help for more information.



The Physical Layer Topology (shown above) is automatically created by OmniVista Terra and displays all managed network devices. Unmanaged devices may also appear in the topology if they were detected in the LLDP info of a managed device within 30 minutes or less.

8.1.3.1 Topology Maps

The Topology application not only provides an overview of the network, it can also be used to perform many functions that you can use to view and configure network devices. These functions are detailed in the following sections:

- Working with Topology Maps (see page 911)
  - Viewing Map Information (see page 911)

- Customizing Maps (see page 914)
- Creating/Restoring Map Snapshots (see page 916)
- Importing/Exporting Maps (see page 918)

- Working with Network Devices (see page 919)
  - Viewing Device Information (see page 919)
  - Displaying Clients Connected to a Device (see page 921)
  - Performing Device Actions (see page 921)

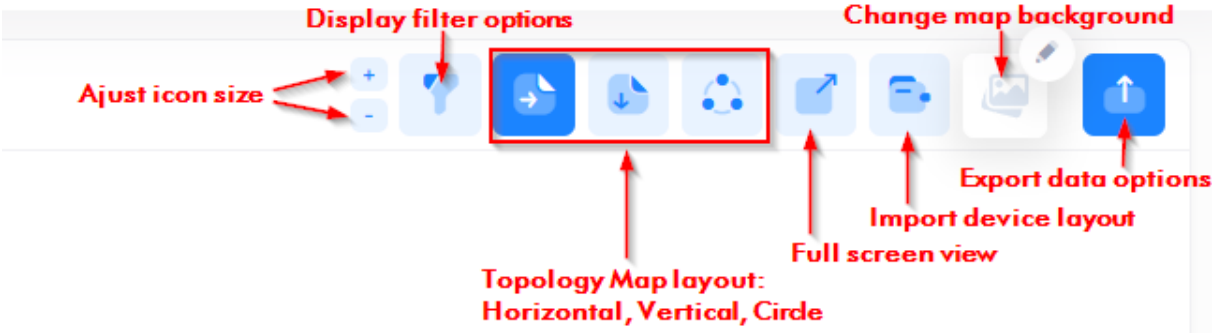
8.1.3.1.1 Working with Topology Maps

This section details the Topology Map view. In this view, you can view device and link information, customize the map background image, change the map layout, and perform device actions.

8.1.3.1.1.1 Viewing Map Information

Topology Maps provide a visual representation of the network. The administrative status of the device or link is indicated by color, and detailed information can be displayed by clicking on a device or link.

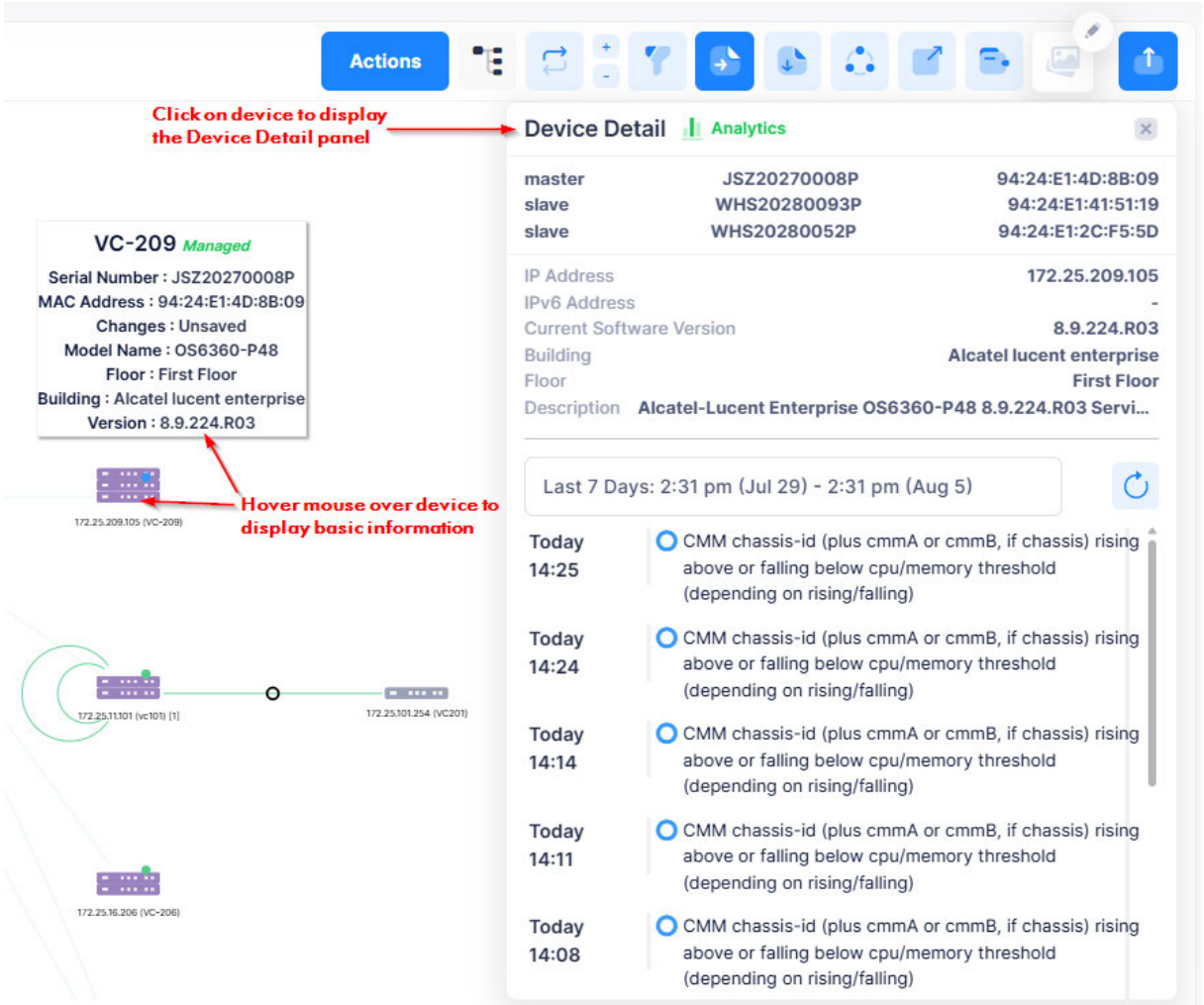
You can change the Topology Map view, layout, background, and import or export Map information using the following icons located at the top-right corner of the screen.



To save a Topology Map view, you can take a snapshot and/or export the Map layout to a text (.txt) or .svg file.

Devices

Each device type is displayed with an icon. Hover the mouse over a device to display basic information. Click on a device to open the Device Detail panel and view detailed information about the device.



The status of a device is indicated by the following color coding of the small dot in the upper-right corner of the device icon and/or by the icon itself. The dot color to use for the device status is based on the specified color theme for trap severity levels configured in the User Preference settings for Appearance (see page 26).

- **Green** - Device connectivity is up and there are no trap notifications.
- **Orange** - Device connectivity is unknown or warning/major trap notifications received from the device.
- **Red** - Device connectivity is up with critical trap notifications received.
- **Blue** - Device connectivity is up with minor or normal trap notifications.
- **No Circle** - No management connectivity information or trap notifications received from the device.
- **Solid-Grey Device Icon** - Device connectivity is down with no trap notifications.
- **Generic Icon** - The device is unmanaged by OmniVista. You can hide unmanaged devices on the Topology Map by clicking on the Show Filter Options (see page 911) icon in the top-right corner of the screen. Click the icon again to display unmanaged devices.

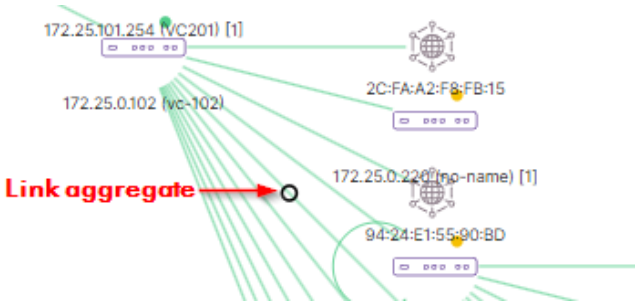
Note that the trap event notification status is only displayed if traps have been configured on the device.

Links

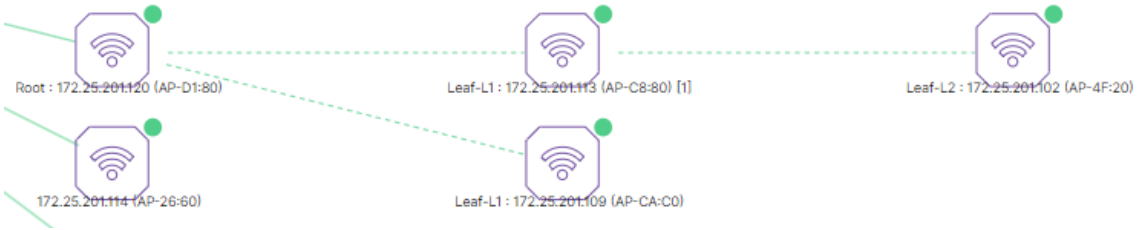
Links between devices are displayed as a single line, whether there is a single link or multiple links.

- **Green** - Link is up. If there are multiple links, Green indicates all of the links are up.
- **Red** - Link is down. If there are multiple links, Red indicates all of the links are down.

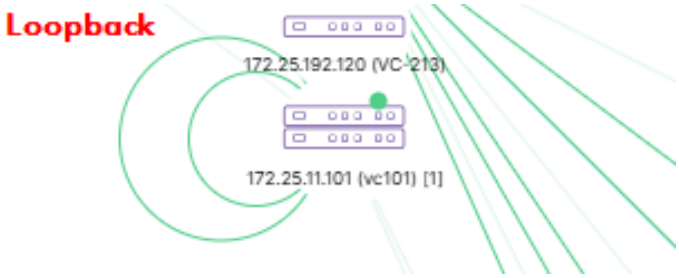
Aggregate links are displayed as a solid line with a black circle.



AP Mesh networks are displayed with a dashed line between AP Wi-Fi icons that are part of the Mesh network configuration.



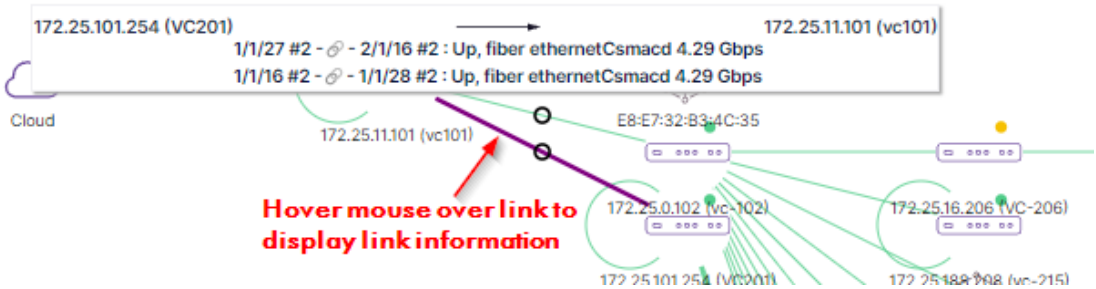
A loop next to a switch indicates a loopback port link on the switch.



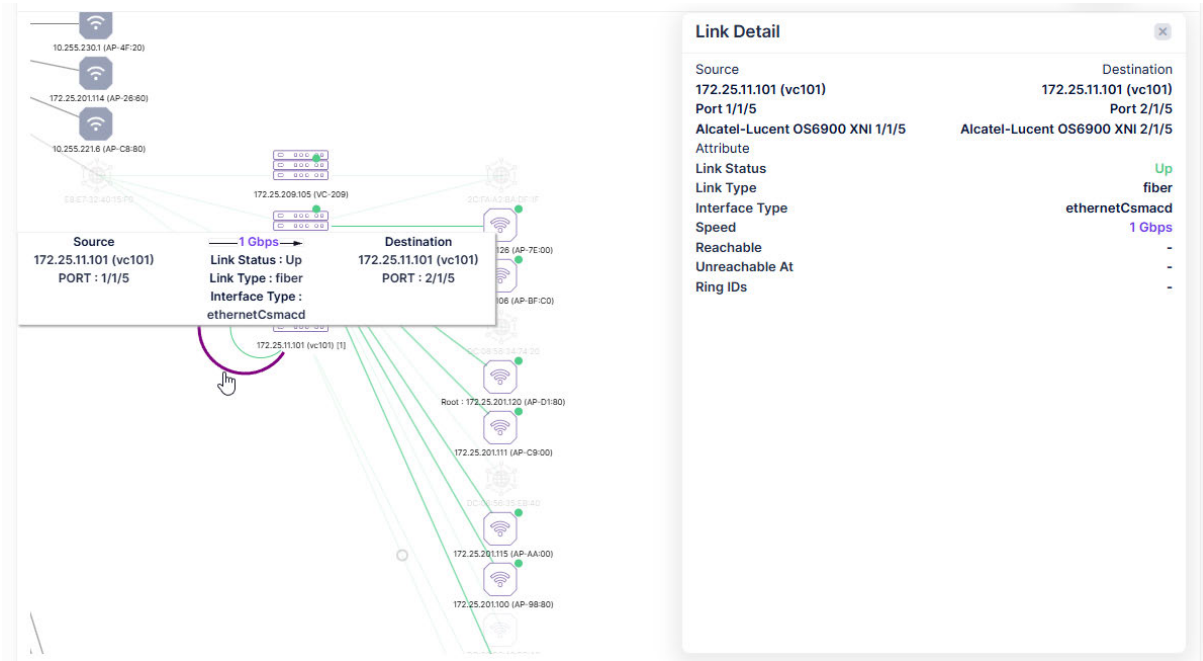
You can hide loopback links on the Topology Map by clicking on the Show Filter Options icon (see page 911) in the top-right corner of the screen. Click the icon again to display the loopback links.

Displaying Link Information

To display link information, move the mouse over the link until the pointer turns into a finger. Link information will be displayed as shown below. Information for all links is displayed.



You can also click on a link to display detailed link information. Move the mouse over the link until the pointer turns into a finger and click. The link is highlighted and link information is displayed in the Link Detail panel as shown below.



8.1.3.1.1.2 Customizing Maps

You can change the Topology Map display, layout, and background image.

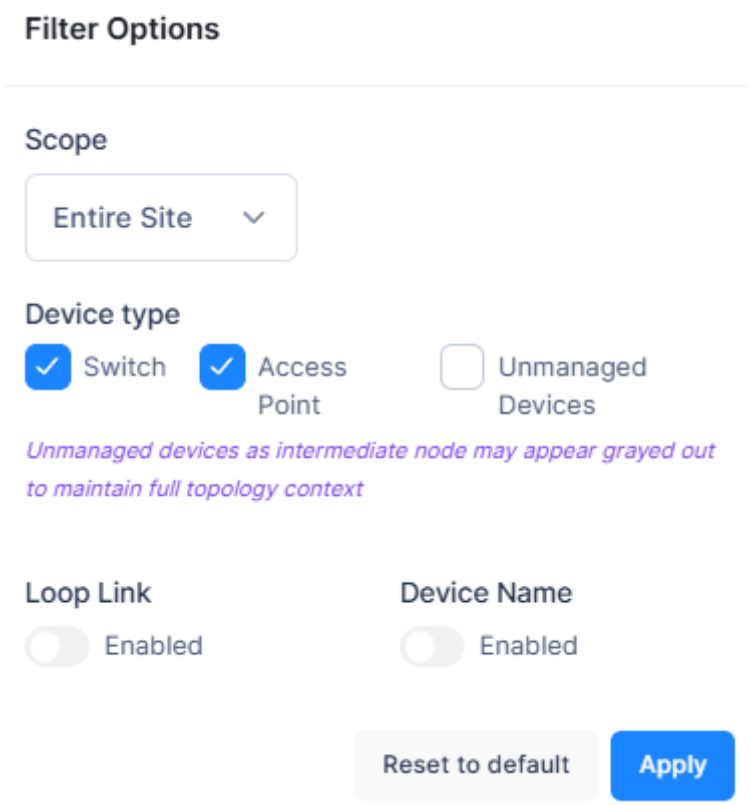
Adjusting the Size of Device Icons on the Topology Map

The size of the device icons is adjustable to make the icons smaller or larger on the Topology Map. Decreasing the size of the device icons can help to provide a clean, compact view of a large network topology.

To increase or decrease the size of device icons, click on the plus (+) or minus (-) sign (see page 911) in the top-right corner of the screen.

Filtering the Topology Map Display

You can specify which devices that you want to include in the Topology Map by clicking on the Show Filter Options (see page 911) icon in the top-right corner of the screen. Select the display options from the drop-down menu as described below.



- **Scope** - Select Entire Site (the default), Building, or Floor.
  - **Entire Site** - Displays all devices associated with the current Organization Site.
  - **Building** - Displays all devices associated with a specific Building. Select the Building to include from the “Select Entity” drop-down list.
  - **Floor** - Displays all devices associated with a specific Floor. Select the Floor to include from the “Select Entity” drop-down list.
- **Device type** - Select the type of devices that you want to include in the Topology Map (Switch, Access Point, Unmanaged Devices). Note that Unmanaged Devices are not selected by default. However, if an unmanaged device is an intermediate node, it may still appear grayed out in the Topology Map.
- **Loop Link** - Enable or disable (the default) the display of loopback link ports on the Topology Map.
- **Device Name** - Enable or disable (the default) the display of device names next to Topology Map devices.

When you are finished selecting the Filter Options for the Topology Map, click **Apply**. The Map display will change based on the options you selected.

Changing the Map Layout

To change the basic layout of the Topology Map, click on the Horizontal, Vertical, or Circle icon (see page 911) in the top-right corner of the screen.

- **Horizontal** - Displays devices in a horizontal pattern.
- **Vertical** - Displays devices in a vertical pattern.
- **Circle** - Displays devices in a spiral pattern.

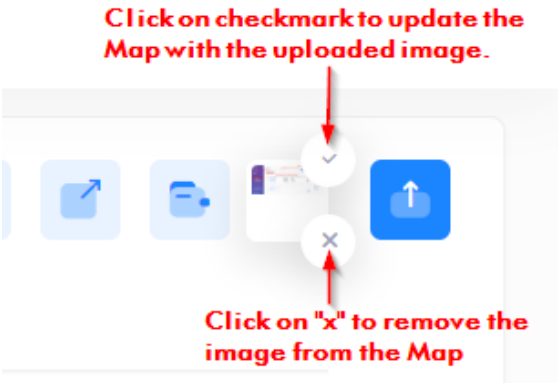
You can also change the layout of a Topology Map using any of the following methods:

- Select a device and drag it to a new location on the Map. Press **Shift** and click to select multiple devices.
- Zoom in or out on a Map using the mouse scroll wheel.
- Move an entire Map on the screen by clicking anywhere outside the map and dragging the Map to a new location on the screen.

Changing the Background Image

You can change the Topology Map background image by clicking on the Change Background icon (see page 911) in the top-right corner of the screen. When you click on this icon, you are prompted to locate and upload an image file that you want to set as the background image for your Topology Map.

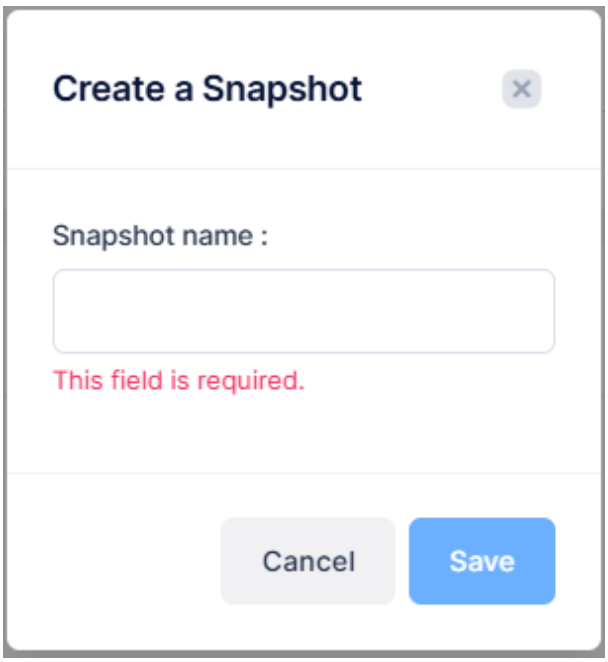
After the selected image is uploaded, click on the checkmark in the top corner of the Change Background icon to update the background of the Topology Map. The checkmark will then disappear from the icon.



To remove a background image, click on the “x” in the bottom corner of the Change Background icon.

8.1.3.1.1.3 Creating a Snapshot of the Topology Map

To create a snapshot of your Topology Map nodes, devices, and client positions, click on the Create a Snapshot icon located next in the top-left corner of the screen. A Create a Snapshot window will open. Enter a name to assign to the snapshot file, then click on **Save**.



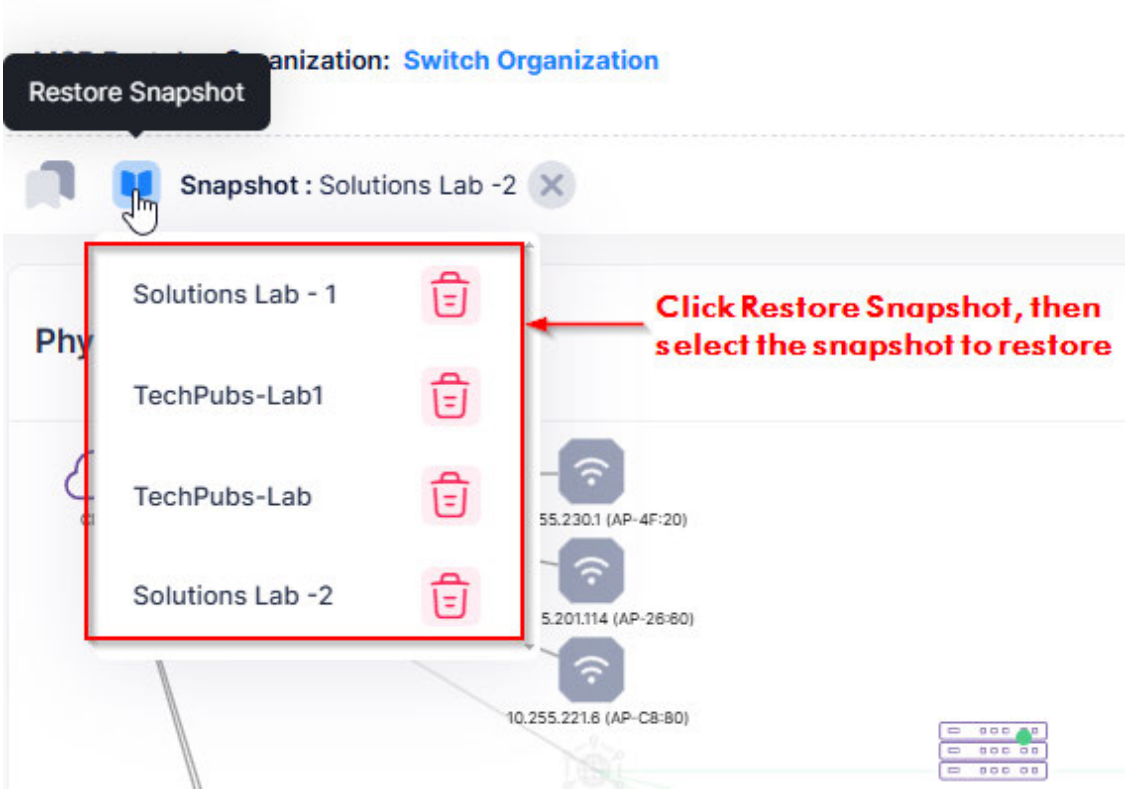
The Topology Map snapshot you created now appears next to the Restore Snapshot icon.

If you make any changes to the Topology Map layout after the snapshot is done, the changes are not automatically updated in the existing snapshot file. You have the following two options to save the changes:

- Update the current snapshot positions by clicking on the checkmark next to the snapshot name. The checkmark indicates that changes were made after the snapshot was saved.

- Create another snapshot for the updated Topology Map.

To restore a Topology Map screenshot, click on the Restore Snapshot icon, then select the snapshot file that you want to restore from the drop-down menu.



When you restore a snapshot of a Topology Map, the snapshot image does not change. For example, if you uploaded a background image (see page 916) for your Topology Map, then did a snapshot and a restore, the background image remains in place.

Importing/Exporting the Topology Map Layout

In addition to the snapshot/restore functionality, you can also import and export a Topology Map. This is particularly useful if you want to share your topology position layout with another user. For example, you can export your topology position layout to a text file (.txt) and send it to another user who can then import the position layout and save it to their own snapshot.

Importing a Topology Map

To import a Topology Map, click on the Import Device Layout icon (see page 911) in the top-right corner of the screen. You are prompted to locate and upload a Text File. The layout contained in the text file is displayed on the screen.

Exporting a Topology Map

You can export a Topology Map to a Text File or an SVG Document. To export the Map, click on the Export Data Options icon (see page 911) in the top-right corner of the screen and select “txt” or “svg” from

the drop-down menu. You are then prompted to select the location where you want to download the exported file. Select the location on your computer, then click **Save**.

8.1.3.1.2 Working with Network Devices

You can view detailed information (see page 919) about a device or perform certain actions (see page 921) on a device by clicking on the device in the map. Actions can be performed on a single device or multiple devices. After selecting a device(s), you can perform one of the actions displayed in the Actions drop-down list. Note that the actions available depend on the device type(s) selected and whether or not you select a single device or multiple devices.

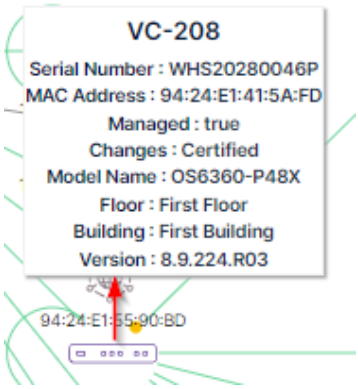
8.1.3.1.2.1 Viewing Device Information

Use the following methods for displaying device information on the Topology Map:

- Hover the mouse over a device in the Map to display basic information (see page 919).
- Click on a device in the Map to display detailed device information (see page 919) in the Device Detail panel on the right side of the screen.
- Click on a device in the Map, then on the Show/Hide Client (see page 921) icon to display clients that are connected to the device.

Displaying Basic Device Information

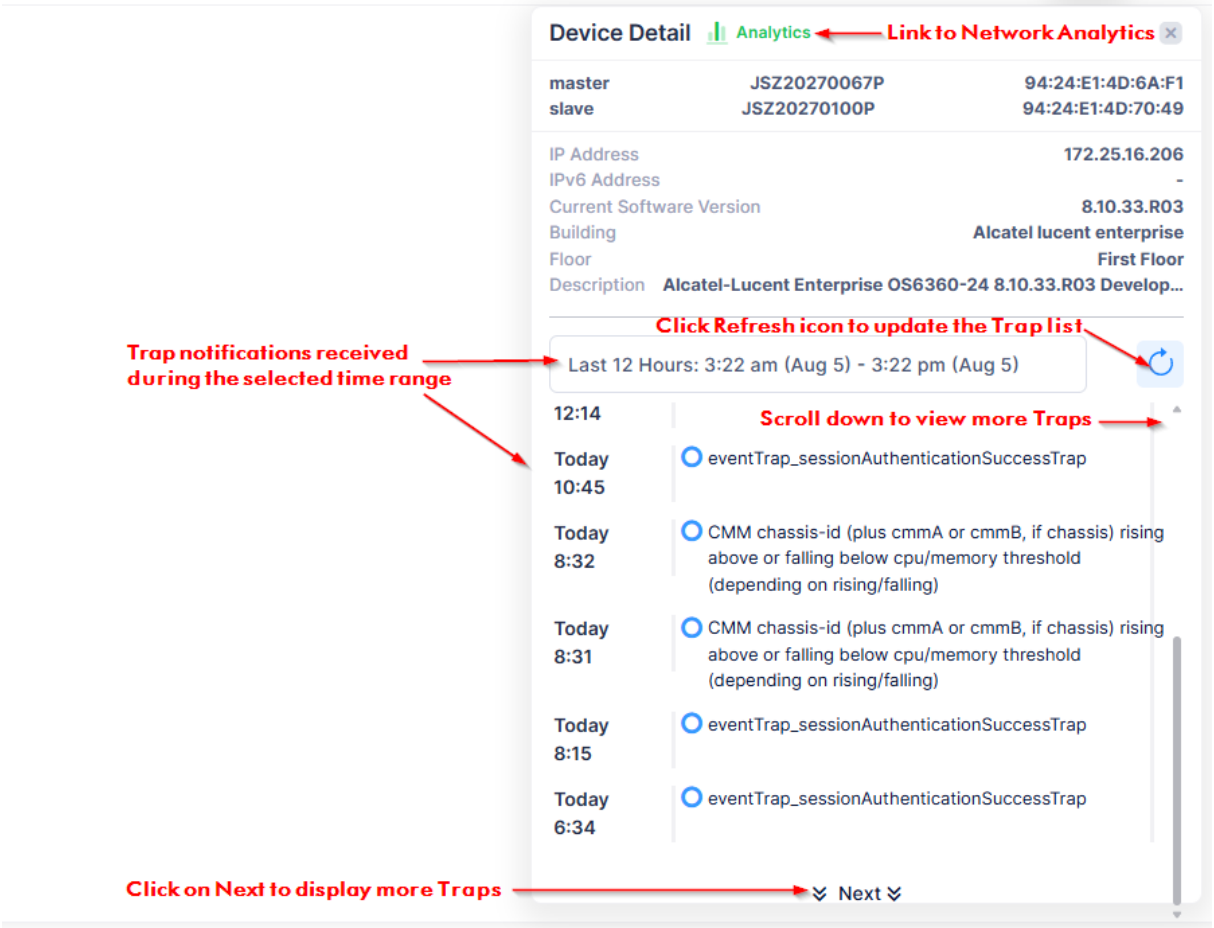
When you hover the mouse over a device in the Topology Map, the following window displays above the device showing basic information for the device:



- **Serial Number** - The serial number of the device.
- **MAC Address** - The MAC address of the device.
- **Managed** - Is the device managed by OmniVista Terra (True or False).
- **Changes (Switch Only)** - Are changes saved (Certified or Unsaved).
- **Model Name** - The model name for the device.
- **Floor** - The floor where the device is located within the Site building.
- **Building** - The building where the device is located within the Site.
- **Version** - The version of software running on the device.

Displaying Detailed Device Information

When you click on a device icon in the Topology Map, the following Device Detail window displays on the right-hand side of the screen showing additional device information:

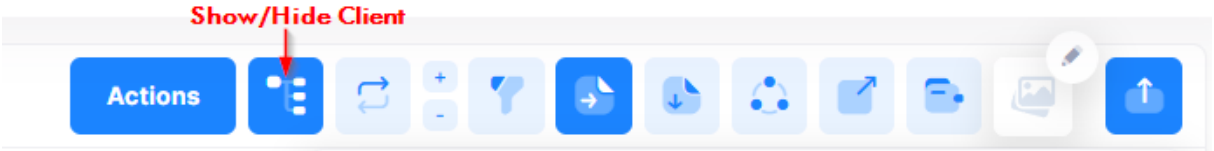


- **Analytics** - Click on this link to open the Network Analytics screen for the selected device.
- **MAC Address** - The MAC address of a standalone device. This field is not displayed for switch Virtual Chassis (VC) configurations. Instead, the serial number and MAC address of each switch in the VC is displayed.
- **IP Address** - The IP address of the device.
- **Current Software Version** - The version of software currently running on the device.
- **Serial Number** - The serial number of a standalone device. This field is not displayed for switch VC configurations. Instead, the Serial Number and MAC address of each switch in the VC is displayed.
- **Building** - The Building where the device is located within the Site.
- **Floor** - The Floor where the device is located within the Site.
- **Description** - A description of the device received when the device was added to the Device Catalog.
- **Trap Notification List** - A list of traps received from the device during the specified time range. Scroll down the list and click on Next to to view more traps. Click the refresh icon to update the display from the OmniVista Terra database.

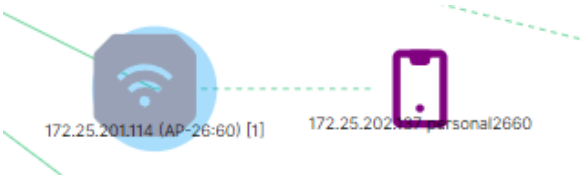
8.1.3.1.2.2 Displaying Clients Connected to a Device

By default, device clients do not show on the Topology Map. If clients are connected to a device, the number of connected clients is displayed at the end of the Friendly Name in brackets. For example, AP 172.25.201.114 [1] has one connected client.

To display the connected clients, select the device and click on the Show/Hide Client icon located in the top-right corner of the screen.



The connected client(s) appear on the Map.



Note the following about displaying connected clients:

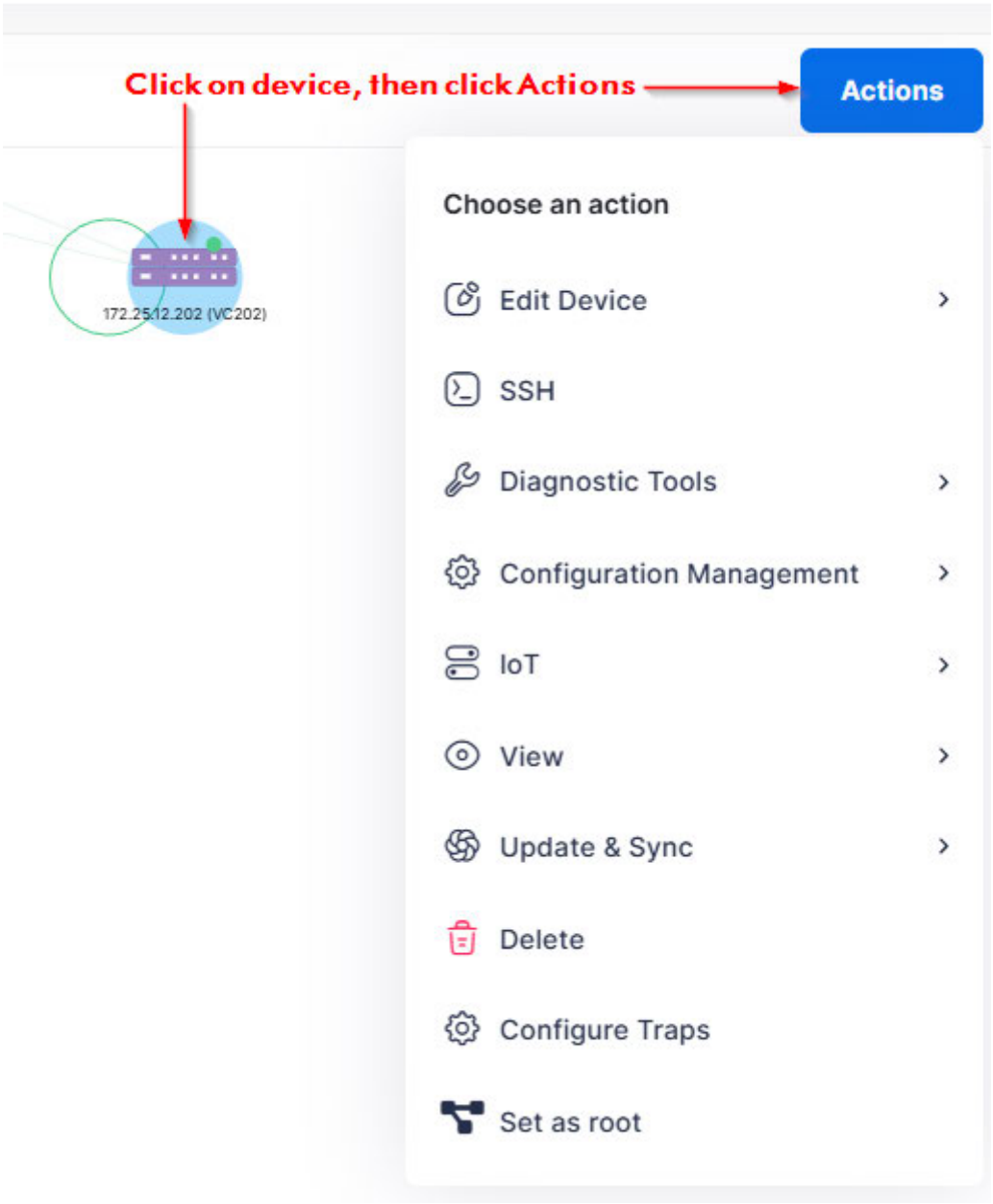
- A wired client displays with a solid link line between the client and the device.
- A wireless client displays with a dashed link line between the client and the device.
- A phone icon is displayed for clients. However, if the client device type is a computer (including tablets) a computer icon is displayed.

You can also find a client by entering the client MAC address in the search box at the top-right corner of the screen. If the client is found, the device to which the client is connected is highlighted and the client device is displayed.

To view additional information about the client, click on the connected client icon. The Client Session History (see page 833) screen for the client will open in a new tab.

8.1.3.1.2.3 Performing Device Actions

You can perform device operations by selecting a device(s) in the Topology Map, then clicking on **Actions** to select one of the operations from the drop-down menu. Note that the **Actions** button does not appear until you select a device.



Refer to the Performing Device Operations (see page 227) online help for the Device Catalog for information about the options on the Action drop-down menu. However, the Set as root (see page 923) action is specific to the Topology application.

- Not all operations are supported on all devices, and some operations can only be performed on a single device, not multiple devices. If an action is not supported for the selected device(s), it is not included in the “Actions” drop-down list.

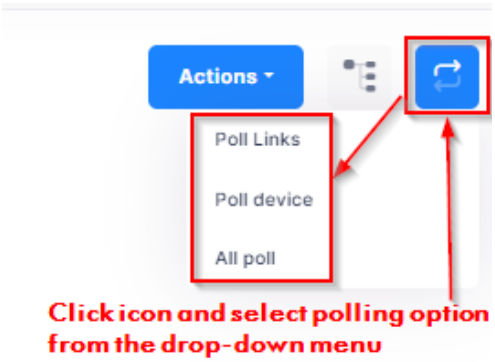
- When you Ping a device from the Topology Map (Actions > Diagnostics Tools > Ping), the connectivity dot for the device changes to green (ON). The dot stays green for approximately two minutes. If after two minutes a message is received from the device, the dot stays green. However, if no message is received, the dot color changes to orange (warning) and the device is then greyed out after three minutes if no message is received.

Setting the Root of the Topology Map

The root of the Topology Map is usually the upstream device; the device that provides Internet access. To change the root, click on the device that you want to become the root, then click on **Actions** and select the **Set as root** option. The Topology Map will automatically re-arrange devices around the new Topology root device.

Polling Devices

You can poll devices to update device/link information. Click on the device that you want to poll, then click on the Poll icon and select the polling option from the drop-down menu.



Polling is supported only for switch devices in the topology; AP polling is not supported. When switches are polled, links between switches (Switch-Switch) and links between switches and APs (Switch-AP) are detected.

- **Poll Links -** Causes an immediate poll of any links on the device(s).
- **Poll Device -** Causes an immediate poll of the selected device(s).
- **All Poll** - Causes an immediate poll of the device(s) and any links on the device(s).

21 Oct 2025

8.1.4 Analytics Reports and Custom Dashboards

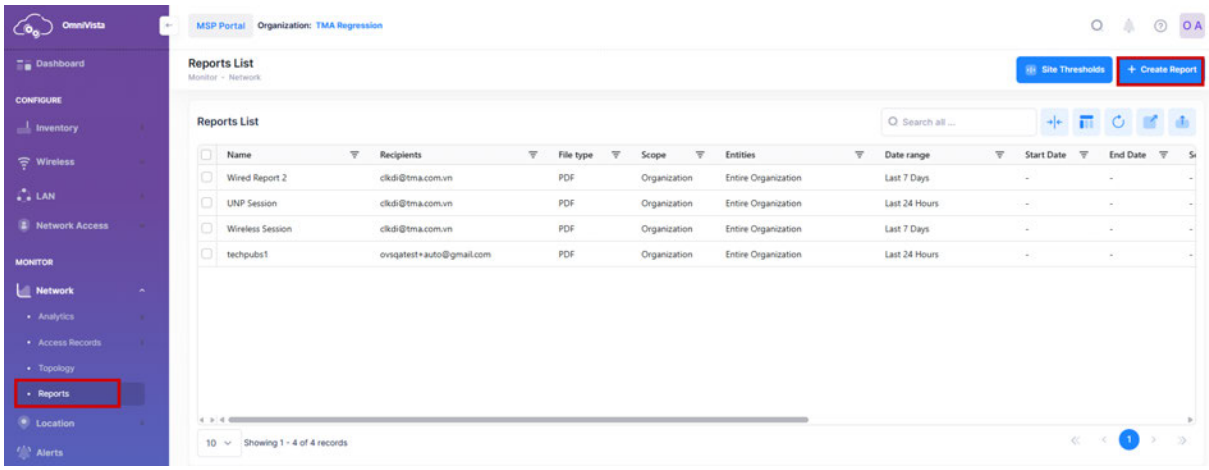
- Analytics Reports (see page 925)
- Custom Dashboards (see page 35)

21 Oct 2025

8.1.4.1 Analytics Reports

Analytics Reports provide users with a comprehensive view of network resource utilization, including information on users, devices, and applications. Reports can also provide information on usage trends, including predictive analysis of future network resource utilization.

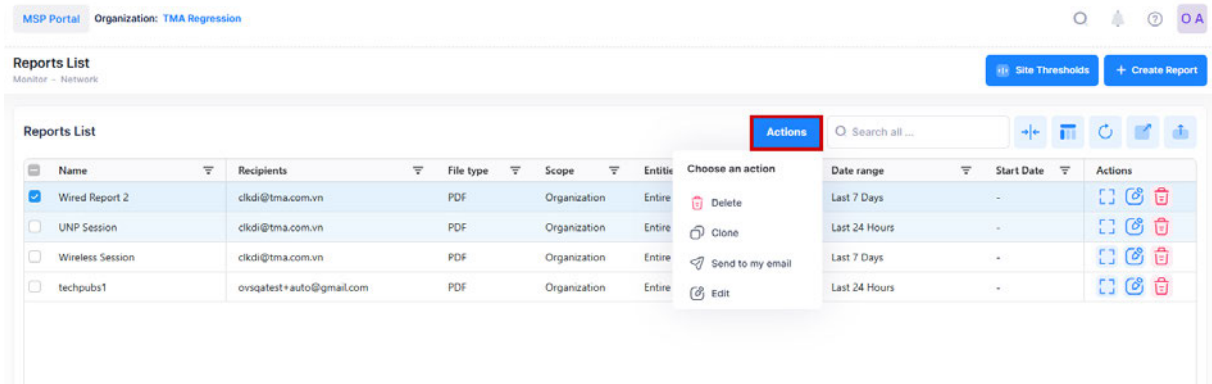
The following Reports applications are accessed by clicking on the **Reports** option under the “Monitor” section of the OmniVista Terra Menu (see page 45):



The Reports List displays the current active reports that have been configured to provide instant or scheduled reports.

8.1.4.1.1 Report Actions

Reports can be edited, cloned or deleted and also scheduled to be sent immediately by using the Action menu from the Reports home page.



Click on **Actions** to open the Actions menu. You can perform the following tasks.

Send to my email - Select “Send to my email” option to receive the report in your email instantly.

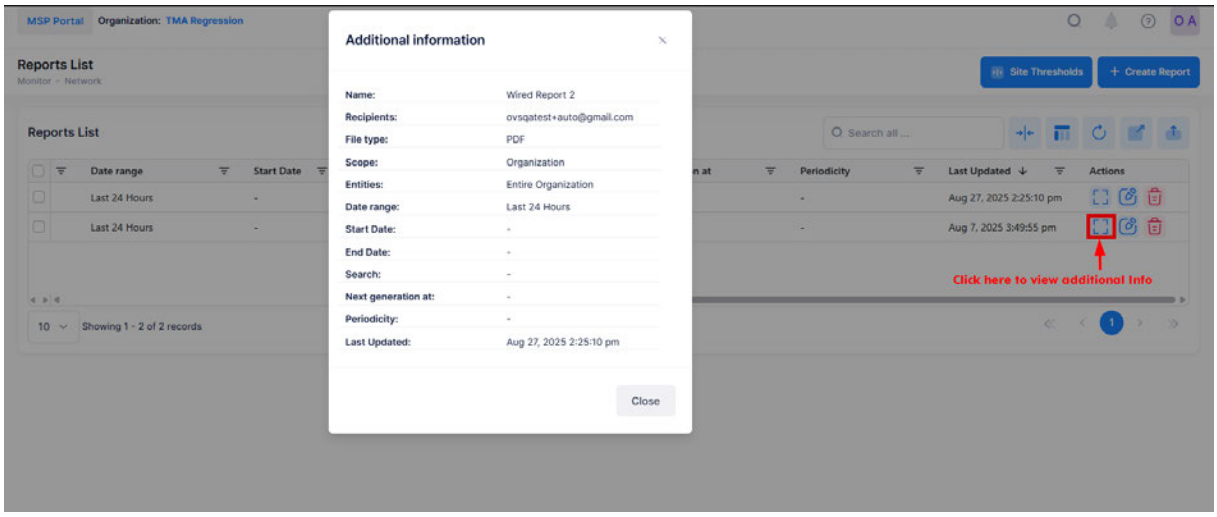
Edit - Select “Edit” option to edit the report.

Clone - Select “Clone” option to duplicate the report.

Delete - Select “Delete” option to remove the report.

8.1.4.1.1.1 Additional Information

To view more information about the created report, click on **Additional Information Details** icon.



A pop up window opens to give more details about the selected report.

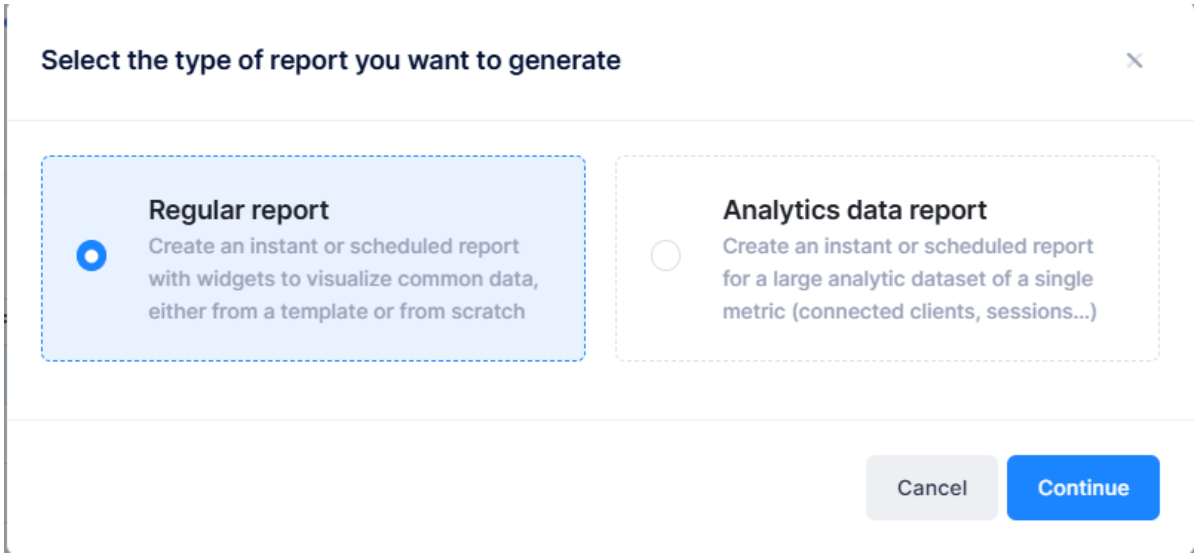
The information in this section describes how to utilize the following OmniVista Terra analytics reports to monitor and evaluate the network resource utilization:

- Create Reports (see page 927)
- Site Thresholds (see page 940)
- Custom Reports
- Report Templates (see page 933)
- Edit Reports (see page 937)

21 Oct 2025

8.1.4.1.2 Create Reports

To create a new report, click on **Create Report** on the Reports List (see page 925) screen. You will be prompted for the type of report that you want to schedule or generate.



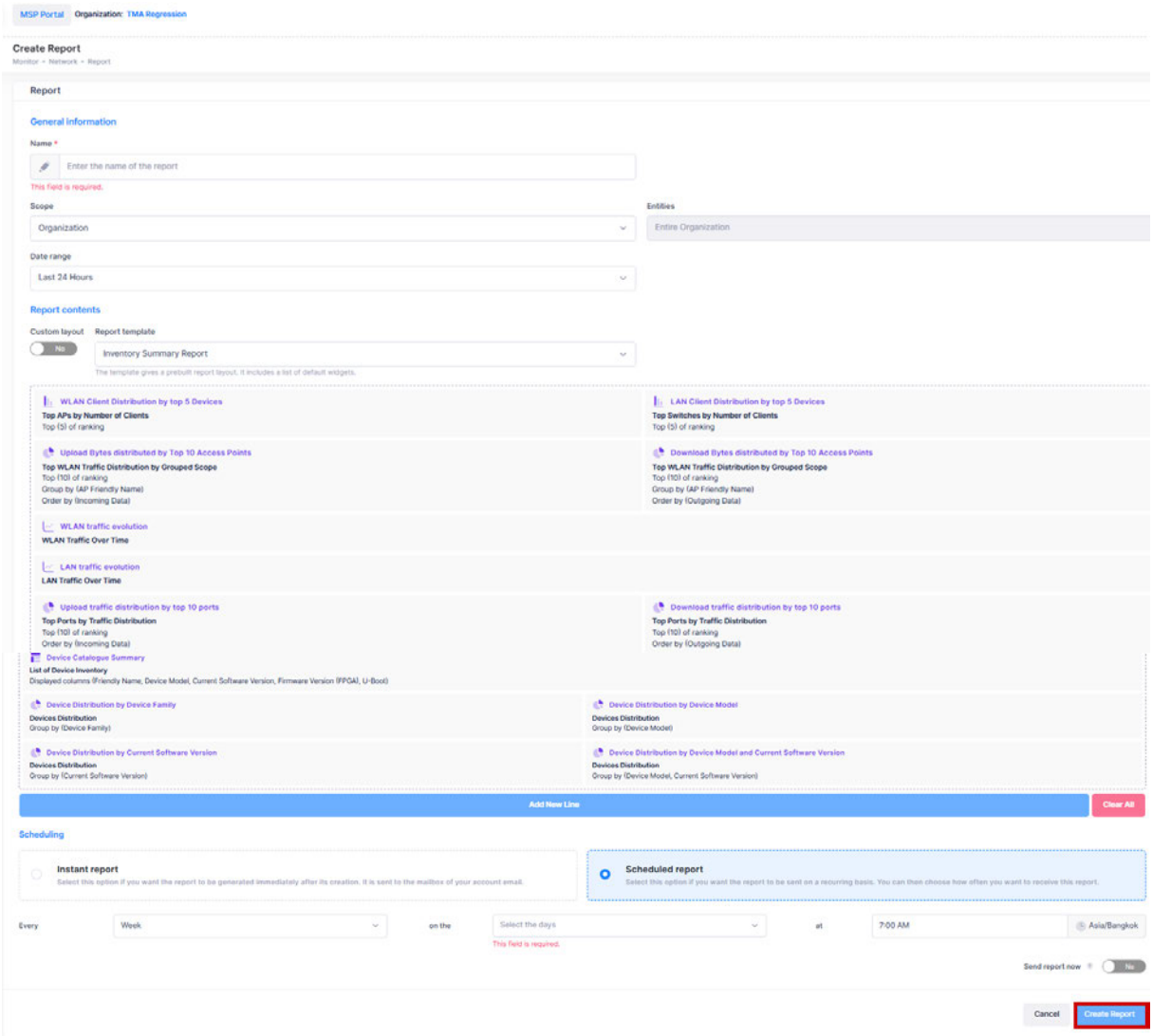
Two types of reports can be generated covering multiple Metrics, Analytics, QoE and KPIs.

- **Regular report** - Create an instant or scheduled report by selecting widgets from a set of available widgets.
- **Analytics data report** - Create a new instant or scheduled report to export a large amount of client analytic data.

Click **Continue** to open the Report Information screen.

8.1.4.1.2.1 Regular Report

When you select **Regular report** option as your choice, the following Create Report screen appears.



Enter the required Report Information to create a report.

- **Name** - Enter a logical name for the report.
- **Scope** - Select the scope from the drop-down list that will be used to filter the report results based on Organization, Site, Building, Floor, or Access Point.
- **Entities** -Select the entities from the drop-down list with reference to the scope that will be applied to this report. Note that if you selected Organization as the scope, all entities of the Organization will be included in the report.
- **Date range** - Select a relative time duration or a specific time range by using the Custom option.
- **Report Contents** - Select the template to be used for the report's content.
  - **Report template** - Select the template to be used for the report's content from the drop-down list. A template includes a list of default widgets. For more information, see Report Templates (see page 933).
  - **Custom layout** - You can custom the report layout by editing the widget. By default, this option is disabled. Click on “Yes” to enable.
- **Scheduling** - Select the type of report that needs to be generated. There are two options:

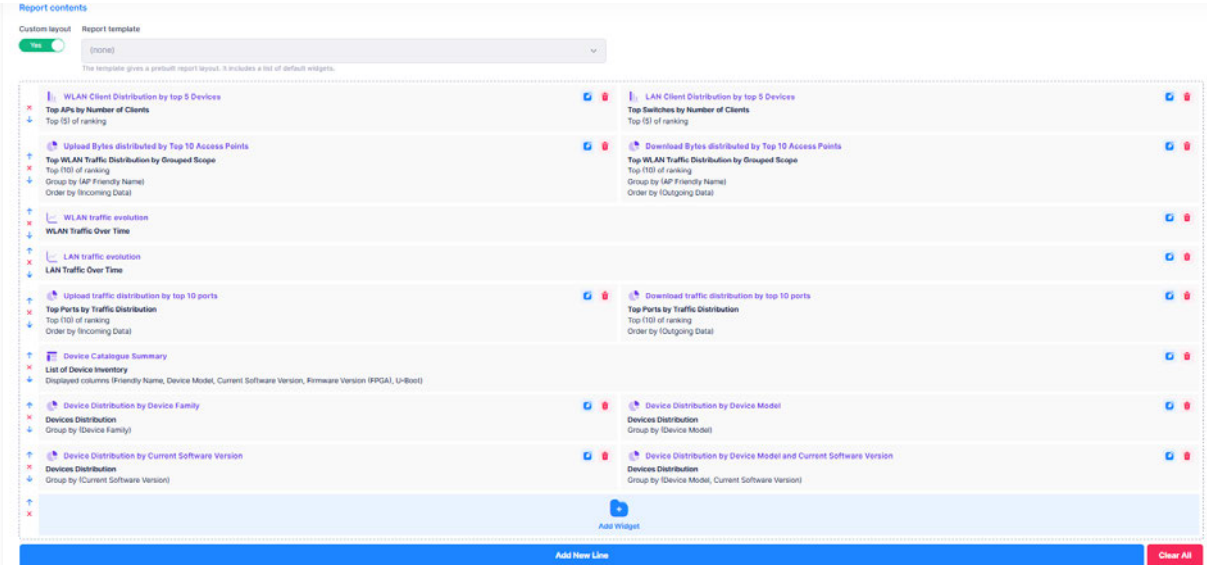
- **Instant report** - Select this option if you want the report to be generated immediately after it is created. You will receive the report within few minutes by email.
- **Scheduled report** - Select this option if you want the report to be sent on a recurring basis. You can then choose how often you want to receive this report.
  - **Send report now** - Click the slider to “On” if you want an initial report sent right after the report is created. Subsequent reports are sent based on the specified recurrence interval. This option only displays when you select “Scheduled report” as the Report Type.

Click on **Create Report**. A new report is created and is displayed on the Reports List screen.

If you have selected the Instant Report option, you will receive the report within few minutes by email.

8.1.4.1.2.2 Custom layout

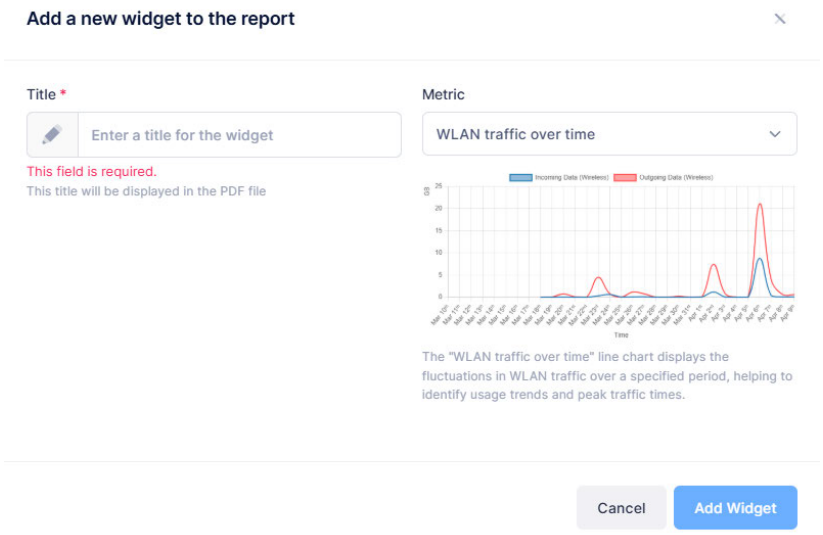
When you enable the **Custom layout** option as your choice, the following Create Report screen appears.



Enter the required information, similar to the Built-in-templates option. However, instead of selecting a template, you can add widgets and select the metrics that is required in your custom report.

Click on **Edit Widgets** to add or remove a specific metric for the widgets in the report.

You can also **Add Widgets** to add new custom widgets by clicking on **Add New Line** tab**.** The below screen appears:



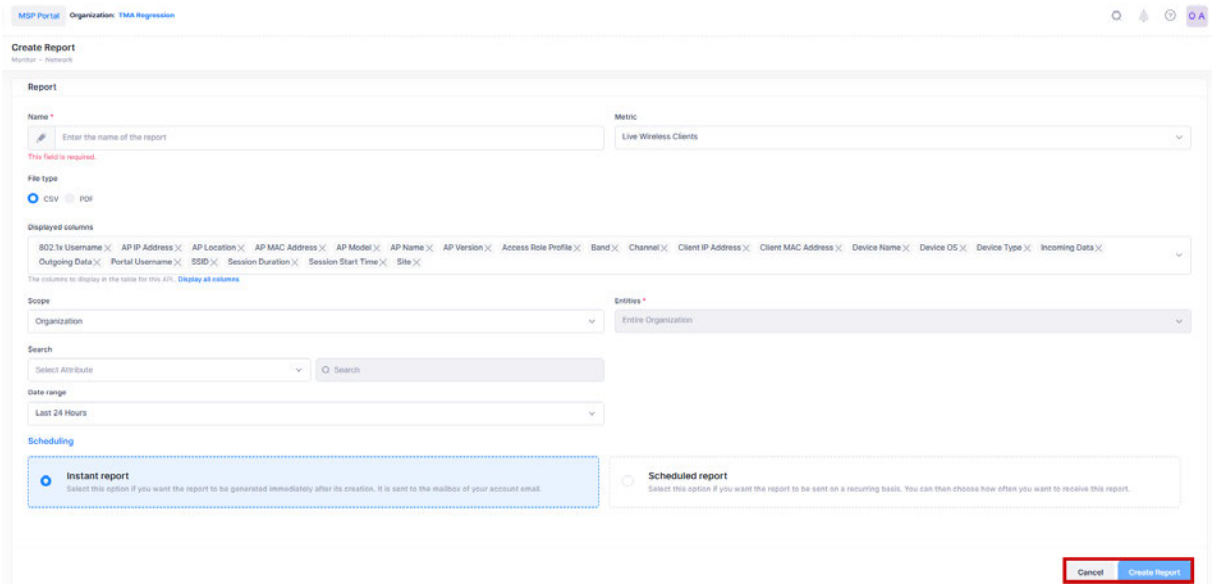
Enter the required information for the custom widgets. You can add multiple widgets with different metric details in the custom report.

Click on **Create Report**. A new report is created and is displayed on the Reports List screen.

For information on editing a report , see Edit Reports (see page 937)

8.1.4.1.2.3 Analytical Data Reports

When you select **Analytics data report** option as your choice, the following Create Report screen appears.



You can create a new instant or scheduled report tot export a large analytic data.

Enter the required Report Information to create a report.

- **Name -** Enter a logical name for the report.
- **Metric -** Select the metric that is required in your analytical report.
- **File type -** Select the file format you would like to export to: CSV or PDF.
- **Displayed Columns -** Specify which column you would like to display in the table for this API of the report.
- **Scope -** Select the scope from the drop-down list that will be used to filter the report results based on Organization, Site, Building, Floor, or Access Point.
- **Entities -** Select the entities from the drop-down list with reference to the scope that will be applied to this report. Note that if you selected Organization as the scope, all entities of the Organization will be included in the report.
- **Search** - Select the attribute value from the drop-down list and search for the specific widget.
- **Date range -** Select a relative time duration or a specific time range by using the Custom option.
- **Scheduling -** Select the type of report that needs to be generated. There are two options:
  - **Instant report** - Select this option if you want the report to be generated immediately after it is created. You will receive the report within few minutes by email.
  - **Scheduled report** - Select this option if you want the report to be sent on a recurring basis. You can then choose how often you want to receive this report.
    - **Send report now** - Click the slider to “On” if you want an initial report sent right after the report is created. Subsequent reports are sent based on the specified recurrence interval. This option only displays when you select “Scheduled report” as the Report Type.

Click on **Create Report**. A new report is created and is displayed on the Reports List screen.

If you have selected the Instant Report option, you will receive the report within few minutes by email.

21 Oct 2025

8.1.4.1.3 Report Templates

OmniVista Terra has built-in reporting features for generating standardized reports from your network data. Reports can be scheduled to either run in real time or at planned intervals to provide detailed information into the network for conformance, monitoring, or troubleshooting.

A preconfigured template can be set to generate reports with scheduling and output options. A template includes a list of default widgets. The default widgets that can be selected are:

8.1.4.1.3.1 Radio Health Reports

- Thresholds
- Top 10 sites by Best Client Health
- Trend of # of Radios with Low/High Radio Noise
- Trend of # of Radios with Low/High Radio Utilization
- Trend of # of Radios with Low/High Radio Interference

8.1.4.1.3.2 AP Health Report

- List of AP radios 2.4 GHz
- List of AP radios 5 GHz
- List of AP radios 6 GHz
- List of APs with most MIC Errors 2.4 GHz
- List of APs with most MIC Errors 5 GHz
- List of APs with most MIC Errors 6 GHz
- Top 5 sites by usage

8.1.4.1.3.3 **Building Summary Report**

- Network Distribution by Building
- Summary of Network by Building
- Client Evolution by top 5 Buildings
- WLAN traffic evolution
- LAN traffic evolution
- Session duration by top 10 Buildings
- Upload Bytes distributed by Top 10 Connection Mode
- Upload Bytes distributed by Top 10 VLAN
- Upload Bytes distributed by Top 10 Buildings
- Download Bytes distributed by Top 10 Buildings
- Download Bytes distributed by Top 10 VLAN
- Sessions by Buildings and VLAN
- Sessions by Buildings and Connection Mode
- Session distribution by VLAN

- Session distribution by Access Role Profile
- Client Distribution by Device Type
- Client Distribution by Device OS

8.1.4.1.3.4 Client Health Report

- Top 10 WLAN clients with most uploaded data
- Client Distribution by Category
- Session Distribution by SSID
- Session Distribution by Connection Mode
- Session Distribution by Device Type
- Session Distribution by Device OS
- Session Distribution by VLAN
- Session Distribution by Band
- Session Distribution by AP Model
- Session Distribution by AP Version
- Session Distribution by SSID
- Session Distribution by Channel
- Session Distribution by Health
- Top 5 WLAN Clients based on uploaded data
- Upload Bytes distributed by Top 10 VLAN
- Upload Bytes distributed by Top 10 Connection Mode
- Upload Bytes distributed by Top 10 SSID
- Download Bytes distributed by Top 10 VLAN
- Download Bytes distributed by Top 10 Connection Mode
- Download Bytes distributed by Top 10 SSID

8.1.4.1.3.5 **Client Summary Report**

- Upload Bytes distributed by Top 10 VLAN
- Upload Bytes distributed by Top 10 Connection Mode
- Upload Bytes distributed by Top 10 SSID
- Session Distribution by SSID
- Session Distribution by Connection Mode
- Session Distribution by SSID and VLAN
- Session Distribution by Connection Mode and VLAN
- Client Session Distribution by SSID, Connection Mode and VLAN
- Session Distribution by VLAN
- Session Distribution by Access Role Profile
- Upload traffic evolution in bytes by SSID

- Download traffic evolution in bytes by SSID
- Client Distribution by Device Type
- Client Distribution by Device OS
- Client Distribution by Connection Category
- Client Distribution by Device Manufacturer

8.1.4.1.3.6 **Floor Summary Report**

- Network Distribution by Floor
- Summary of Network by Floor
- Client evolution by top 5 Floors
- WLAN traffic evolution
- LAN traffic evolution
- Session duration by Top 10 Floors
- Upload Bytes distributed by Top 10 Connection Mode
- Upload Bytes distributed by Top 10 VLAN
- Upload Bytes distributed by Top 10 Floors
- Download Bytes distributed by Top 10 VLAN
- Download Bytes distributed by Top 10 Floors
- Sessions by Floor and VLAN
- Sessions by Floor and Connection Mode
- Session Distribution by VLAN
- Session Distribution by Access Role Profile
- Client Distribution by Device Type
- Client Distribution by Device OS

8.1.4.1.3.7 **Inventory Summary Report**

- WLAN Client Distribution by top 5 devices
- LAN Client Distribution by top 5 devices
- Upload Bytes distributed by Top 10 Access Points
- Download Bytes distributed by Top 10 Access Points
- WLAN traffic evolution
- LAN traffic evolution
- Upload traffic distribution by top 10 ports
- Download traffic distribution by top 10 ports
- Device Catalogue Summary
- Device Distribution by Device Family
- Device Distribution by Device Model
- Device Distribution by Current Software Version

- Device Distribution by Device Model and Current Software Version

8.1.4.1.3.8 SSID Summary Report

- Usage over time for SSID
- Clients over time for SSID
- Detailed usage for SSID

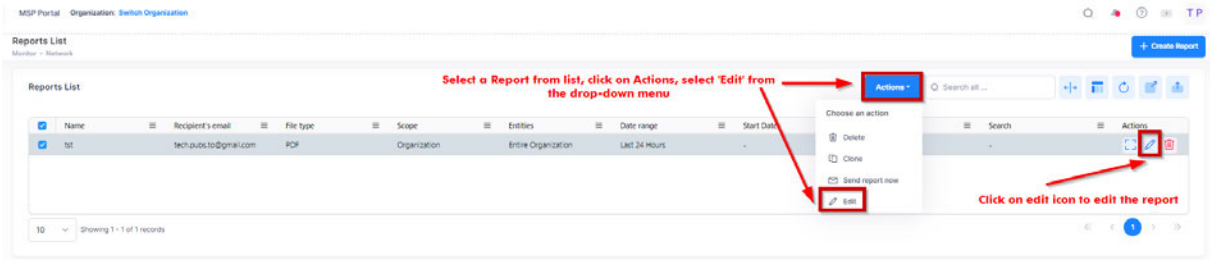
8.1.4.1.3.9 **Site Summary Report**

- Network Distribution by Site
- Summary of Network by Site
- Client evolution by top 5 Sites
- WLAN traffic evolution
- LAN traffic evolution
- Session duration by Top 10 Sites
- Upload Bytes distributed by Top 10 Connection Mode
- Upload Bytes distributed by Top 10 VLAN
- Upload Bytes distributed by Top 10 Sites
- Download Bytes distributed by Top 10 VLAN
- Download Bytes distributed by Top 10 Sites
- Sessions by Site and VLAN
- Sessions by Site and Connection Mode
- Session Distribution by VLAN
- Session Distribution by Access Role Profile
- Client Distribution by Device Type
- Client Distribution by Device OS

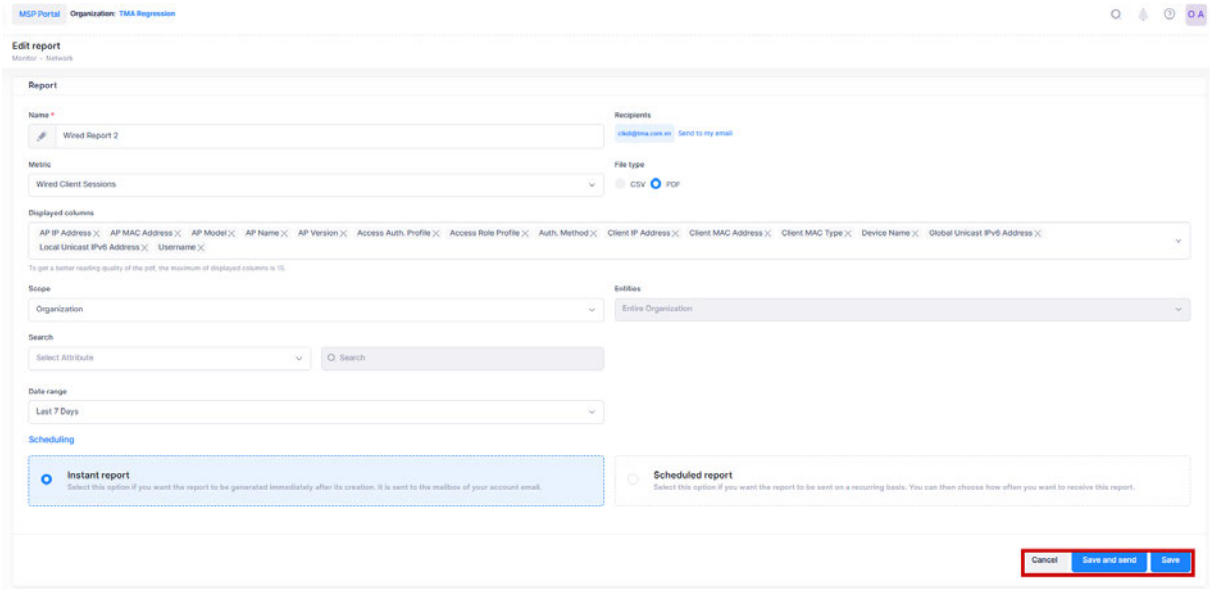
21 Oct 2025

8.1.4.1.4 Edit Reports

Reports can be edited and also scheduled to be sent immediately by using the Actions menu from the Reports home page.
Click on **Actions** to open the Actions menu. Select “Edit” option to edit the report.



When you select **Edit** option as your choice, the following Edit Report screen appears.



The Edit Report screen displays the current active data that have been configured to provide instant or scheduled reports.

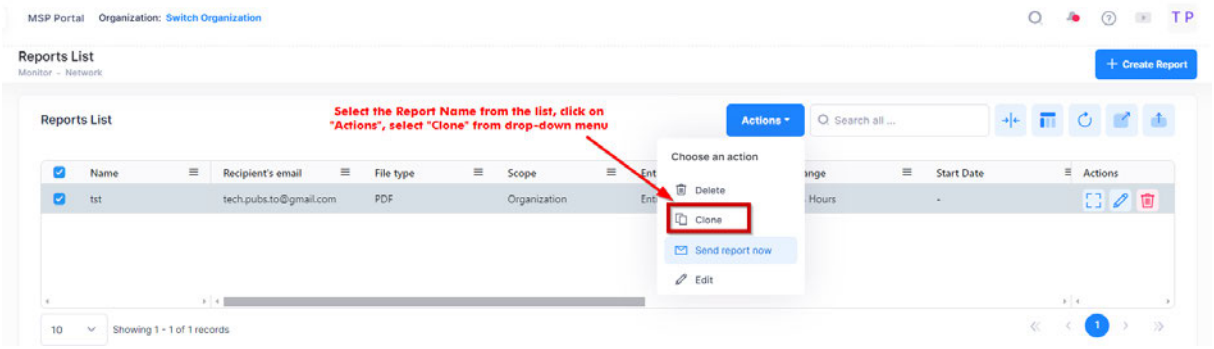
You can edit the existing data, add or delete custom widgets and save the report. You can also click on **Save and send** to sent the report immediately to your configured email id.

For information on creating a report , see Create Reports (see page 927)

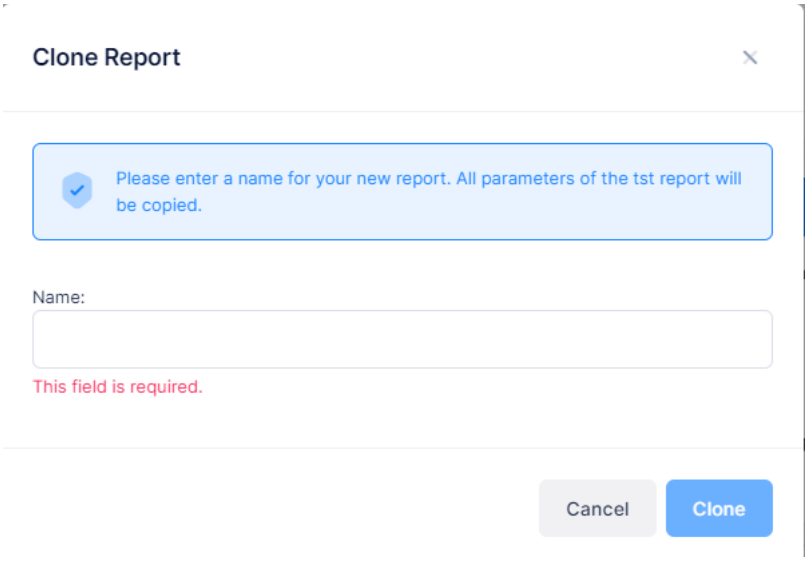
21 Oct 2025

8.1.4.1.5 Clone Reports

Reports can be cloned and also scheduled to be sent immediately by using the Actions menu from the Reports home page.
Click on **Actions** to open the Actions menu. Select “Clone” option to Clone the existing report in the list as shown below:



When you select **Clone** option as your choice, the following Edit Report screen appears.



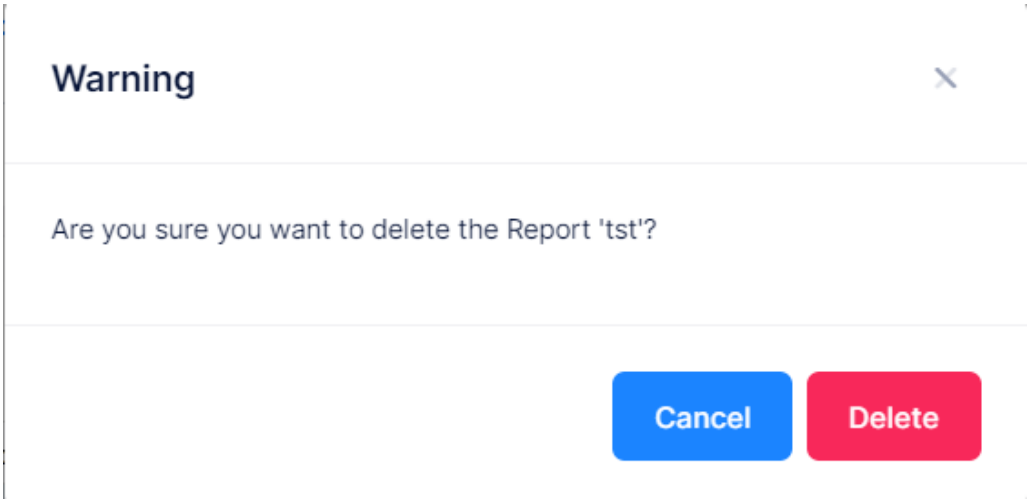
You can enter the Name for new report and all the parameters of main report file will be copied here.

Once you click on **Clone** tab, you will be directed to Create Report (see page 938) screen to complete the fields of report information.

21 Oct 2025

8.1.4.1.6 Delete Reports

Select a Report from the Reports list and click on the Delete icon under the “Actions” column or click on the **Actions** button and select Delete from the drop-down menu. When the following confirmation prompt appears, click on **Delete** to delete the Report.



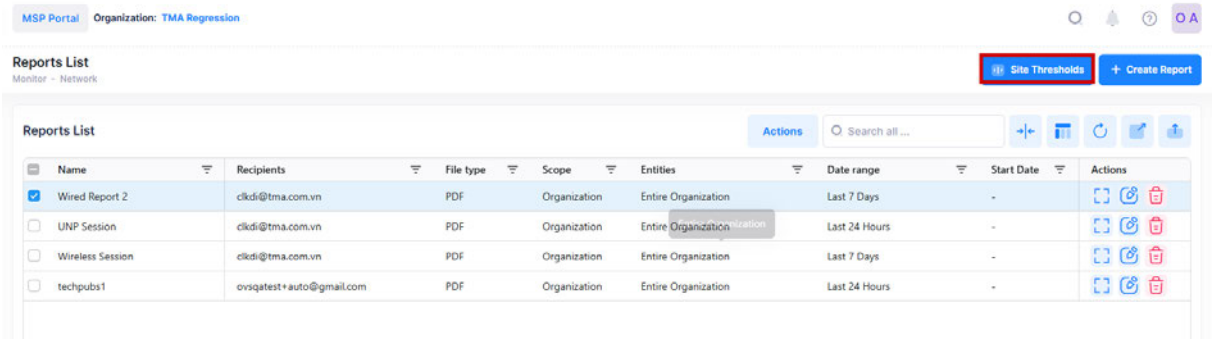
Click on **Delete** to confirm that you want to delete the Report from the List .

21 Oct 2025

8.1.4.1.7 Site Thresholds

The Client Health analytics can also be computed based on Site threshold values of the devices. The Site Thresholds button appears next to the Create Report button when you are looking at a specific Site to view the Device Health.

The following Site Thresholds screen can be accessed by clicking on the **Reports** option under the "Monitor" section of the OmniVista Terra Menu (see page 45).



To set a Site threshold value for a specific Site, click on the **Site Thresholds** button. The following screen appears from which you can edit the following threshold values for the Access Points:

Client Health (2.4 GHz) threshold (%): Defaults to 60% usage.

Client Health (5 GHz) threshold (%): Defaults to 60% usage.

Client Health (6 GHz) threshold (%): Defaults to 60% usage.

Client SNR (2.4 GHz) threshold (%): Defaults to 15% usage.

Client SNR (5 GHz) threshold (dbm): Defaults to 15% of usage.

Client SNR (6 GHz) threshold (dbm): Defaults to 15% of usage.

Radio Noise (2.4 GHz) threshold (dbm): Defaults to -92% of usage.

Radio Noise (5 GHz) threshold (%): Defaults to -92% of usage.

Radio Noise (6 GHz) threshold (%): Defaults to -92% of usage.

Radio Utilization (2.4 GHz) threshold (%): Defaults to 50% of usage.

Radio Utilization (5 GHz) threshold (%): Defaults to 50% of usage.

Radio Utilization (6 GHz) threshold (%): Defaults to 50% of usage.

Radio Interference (2.4 GHz) threshold (%): Defaults to 25% of usage.

Radio Interference (5 GHz) threshold (%): Defaults to 25% of usage.

Radio Interference (6 GHz) threshold (%): Defaults to 25% of usage.

Retransmissions threshold (%): Defaults to 10% of usage.

Errors threshold (%): Defaults to 5% of usage.

Configure thresholds for site Site-6685
Client Health (2.4 GHz) threshold (%)
60
0
100
Client Health (5 GHz) threshold (%)
60
0
100
Client Health (6 GHz) threshold (%)
60
0
100
Client SNR (2.4 GHz) threshold (%)
15
0
100
Client SNR (5 GHz) threshold (dbm)
15
0
100
Client SNR (6 GHz) threshold (dbm)
15
0
100
Radio Noise (2.4 GHz) threshold (dbm)
-92
-110
0
Radio Noise (5 GHz) threshold (%)
-92
-110
0
Radio Noise (6 GHz) threshold (%)
-92
-110
0
Radio Utilization (2.4 GHz) threshold (%)
0
100
Radio Utilization (5 GHz) threshold (%)
50
0
100
Radio Utilization (6 GHz) threshold (%)
50
0
100
Radio Interference (2.4 GHz) threshold (%)
25
0
100
Radio Interference (5 GHz) threshold (%)
25
0
100
Radio Interference (6 GHz) threshold (%)
25
0
100
Retransmissions Threshold (%)
10
0
50
Errors Threshold (%)
5
0
50
Reset to default
Cancel
Save

After changing any of the threshold values, click the **Save** button. To revert thresholds to their default values, click the **Reset to default** button.

- The Site health threshold is a global threshold that applies to all the devices belonging to that Site. It can be overridden by the device health threshold which is configured with the Device Thresholds option.
- OmniVista Terra sends the commands to configure the Thresholds on OV managed devices.
- You can select only one device at a time to configure the Thresholds values

21 Oct 2025

8.2 Location

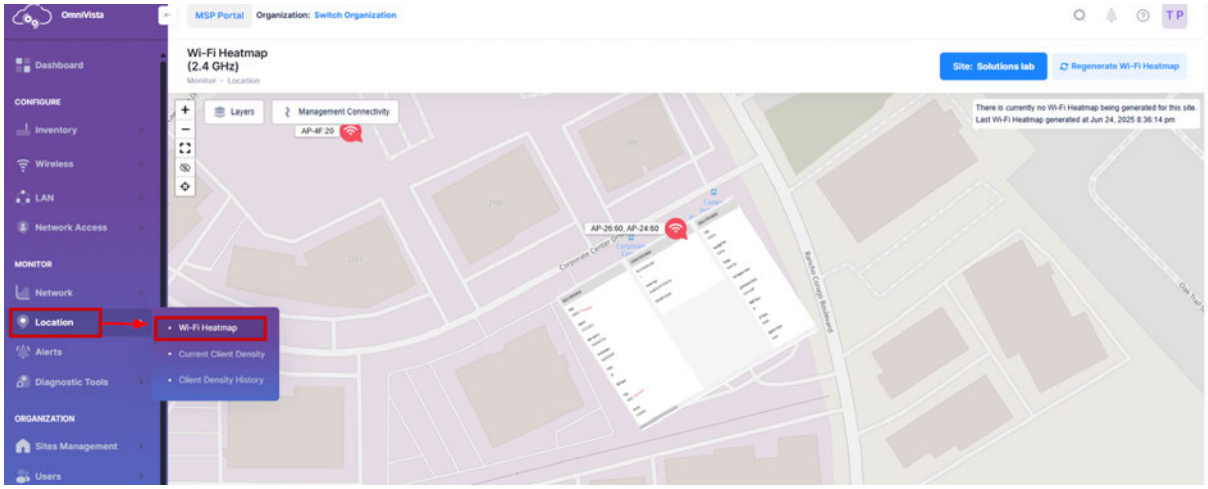
The following group of Wi-Fi Heatmap applications are accessed by clicking on the **Location** option under the “Monitor” section of the OmniVista Terra Menu (see page 45):

- Wi-Fi Heatmap (see page 943)
- Current Client Density (see page 946)
- Client Density History (see page 946)

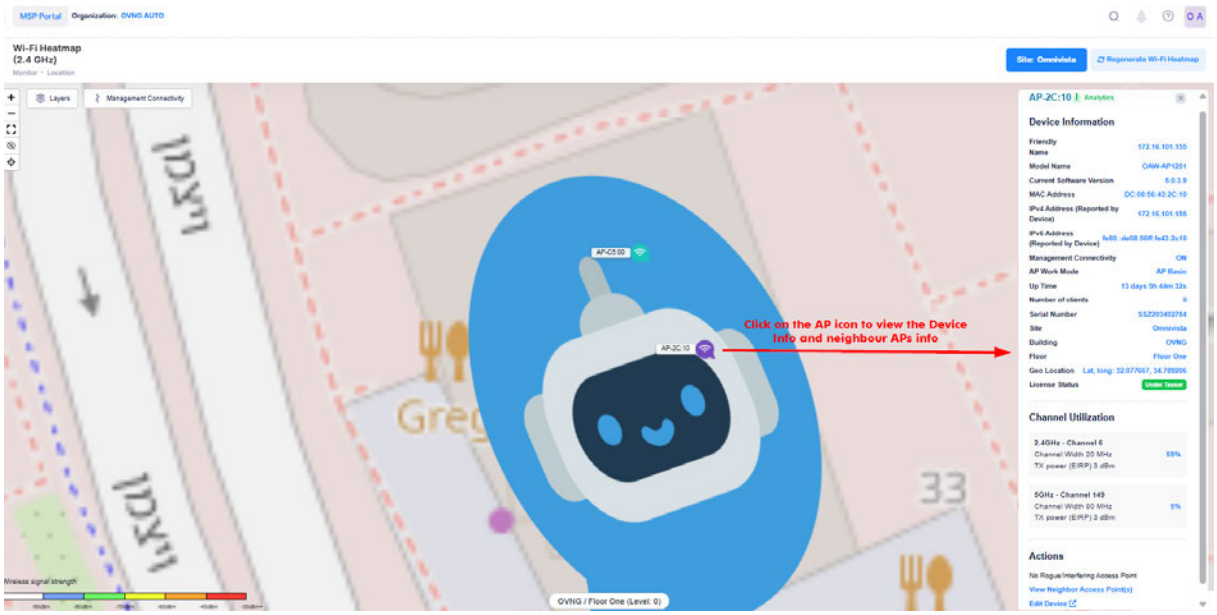
> Note that creating an OmniVista Terra WiFi RTLS Location Engine (see page 405) profile is a pre-requisite for using the Wi-Fi Heatmap applications. The Location Engine server profile must also be assigned to the Provisioning Configuration (see page 313) that is associated with the AP Group to which the AP is a member.

8.2.1 Wi-Fi Heatmap

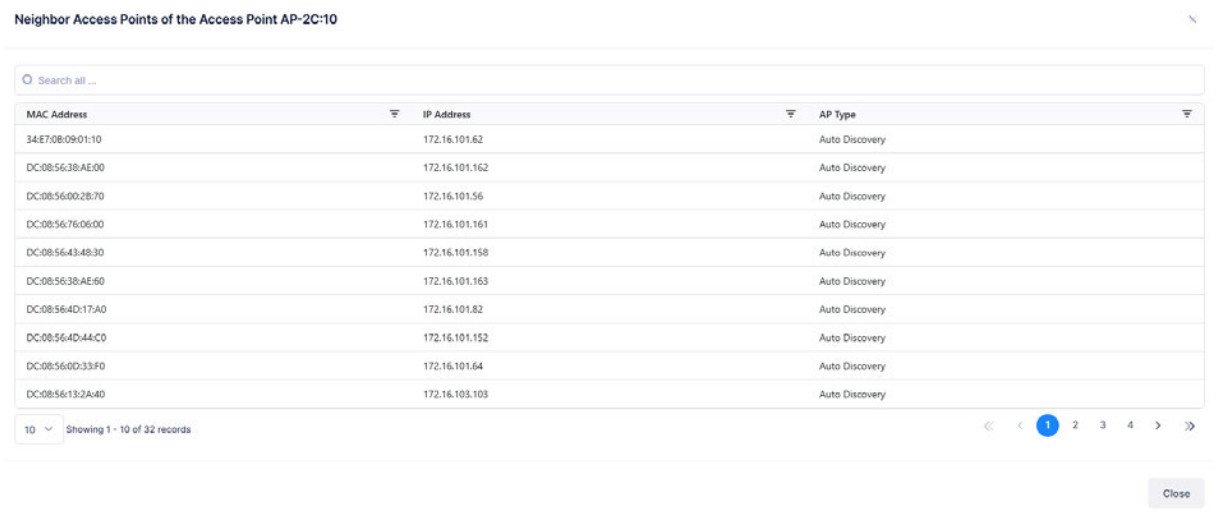
Wi-Fi heatmap is a visual representation of the wireless signal coverage and strength of Access Points connected to the network. Creating a Wi-Fi heat map allows network administrators to visualize the real signal strengths of their wireless infrastructure, and more quickly understand which AP clients have limited or missing Wi-Fi connections.



The wireless devices are displayed as Wi-Fi logos. Click on any of the wireless device logos to view the detailed summary of that device as shown below.



Click on the **View Neighbor Access Point(s)** link under the Actions section to view a list of neighboring Access Points detected for the specific device.



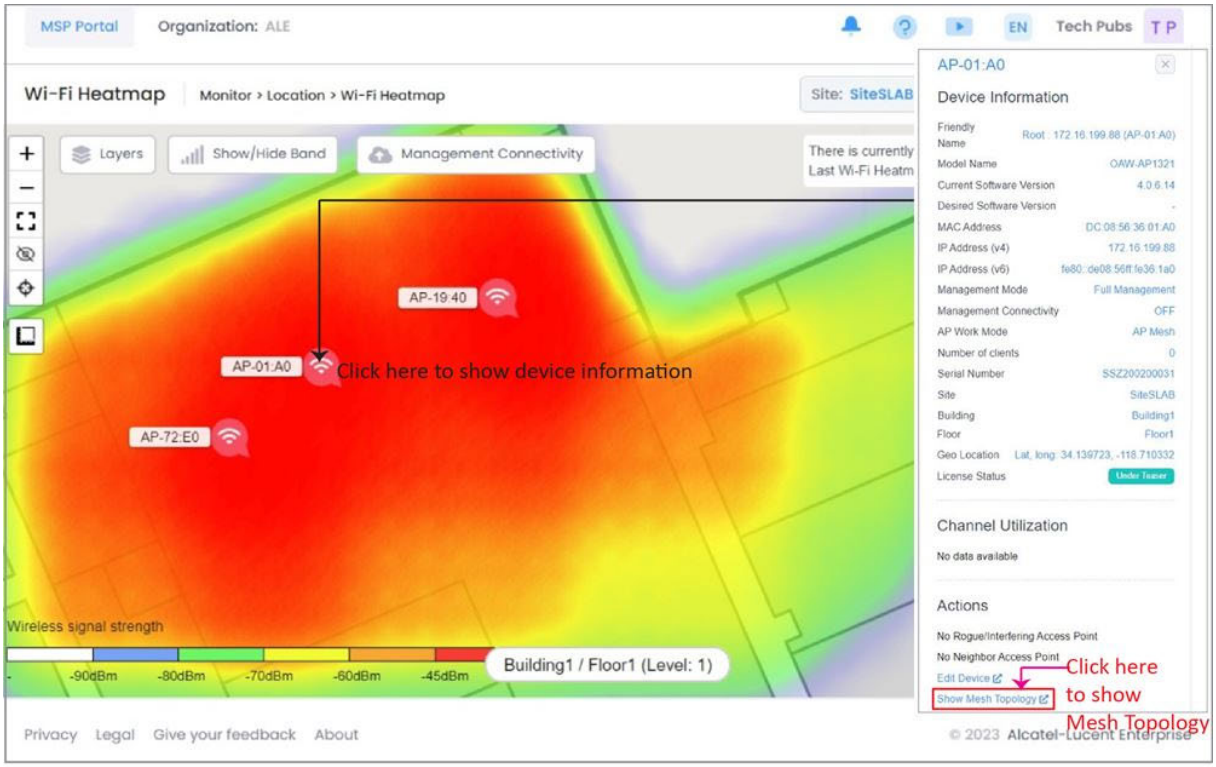
Note: 1. The 2.4GHz label on the Wi-Fi Heatmap indicates the heatmap for the 2.4GHz frequency.

2. The Wi-Fi Heatmap is calculated with the position of APs, for the 2.4 GHz and with 6 dBm Tx Power.

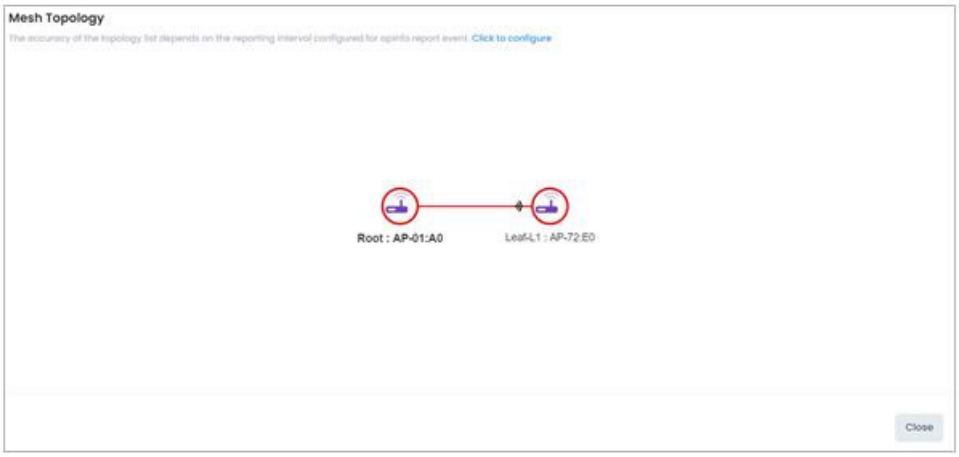
8.2.2 Show Mesh Topology

The graph depicting the mesh topology is presented within a modal window that can be accessed through the Wi-Fi heatmap. The wireless devices are displayed as Wi-Fi logos.

Select a device from the Heatmap. If the device is part of any Mesh network, the “Show Mesh Topology” link is displayed under the “Actions” section.



Click on **Show Mesh Topology** to launch the modal that displays topology in graphical format as shown below.



The format for the node label is 'Level: Name'.

The topology graph displays all devices that are part of the Mesh network, regardless of whether they are on the selected floor of the Heatmap or not. This means that the graph may show devices that are not included in the Heatmap from which it is launched.

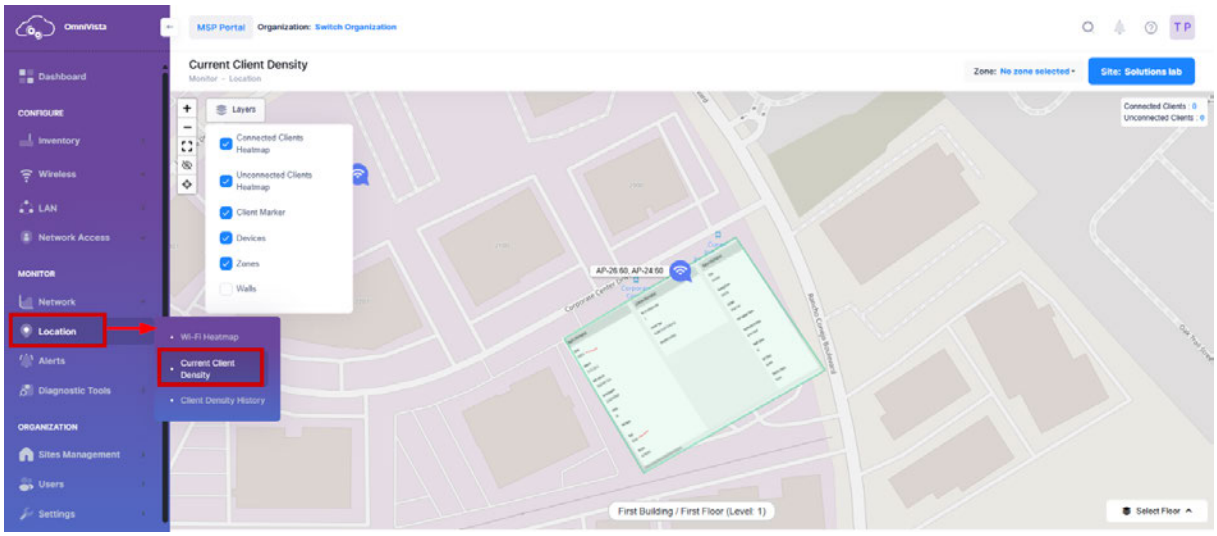
Note: The Mesh links between the APs are displayed only when they exists.

8.2.3 Current Client Density

The heatmap is based on density of clients. (If the density is high, it is shown red, medium density yellow, low density green, etc.)

The heatmaps are calculated using the number of devices detected at any time. The colors represent the areas on the map where there is the most "presence." The intensity is based on how many devices were detected during the time period. Areas may be dark red because there were lots of devices detected.

The Current Client Density can be accessed by clicking **Current Client Density** on the **Location** option under the “Monitor” section of the OmniVista Terra Menu (see page 45).



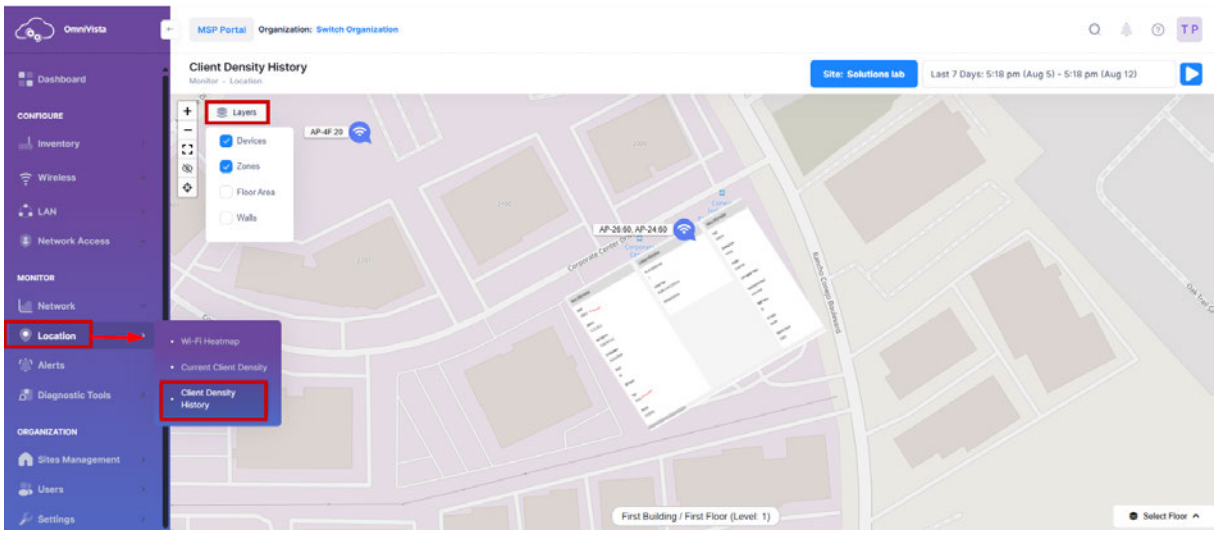
You can filter the view of the Current Clients Heatmaps by selecting or unselecting the following layers:

- Connected Clients Heatmaps
- Unconnected Clients Heatmap
- Client Marker
- Devices
- Zones
- Walls

8.2.4 Client Density History

In Client History page, Total Dwell time can be calculated for each client that has connected to at least 1 AP presented in the zone, within the selected time period. When you click on a particular zone, the trend view of the client density in this zone will be displayed (using the time range selected).

The Client Density History can be accessed by clicking **Client Density History** on the **Location** option under the “Monitor” section of the OmniVista Terra Menu (see page 45).



You can filter the view of the Current Density History by selecting or unselecting the following layers:

- Devices
- Zones
- Floor Area
- Walls

> For more information on monitoring network components and device activity, see Monitoring Network Device Activity (see page 773).

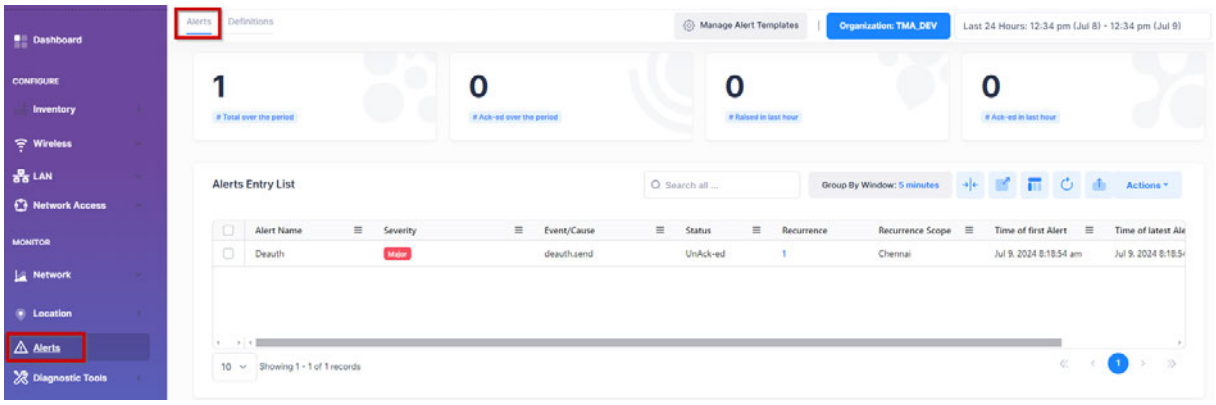
21 Oct 2025

8.3 Alerts

OmniVista Terra can generate alerts based on the network device events and user configuration failure. Similar to the Events notification (see page 981) screen, the Alerts screen provides a list of alerts received and basic alert information (for example, severity, date/time received). You can also manage alerts and configure alert templates to identify specific alerts that you want OmniVista Terra to report.

There are two ways to access the Alerts screen from the Organization Dashboard (see page 71):

- Click on the **Alerts** panel heading in the lower-right of the dashboard.
- Click on the **Alerts** option under the “Monitor” section of the OmniVista Terra menu (see page 45).

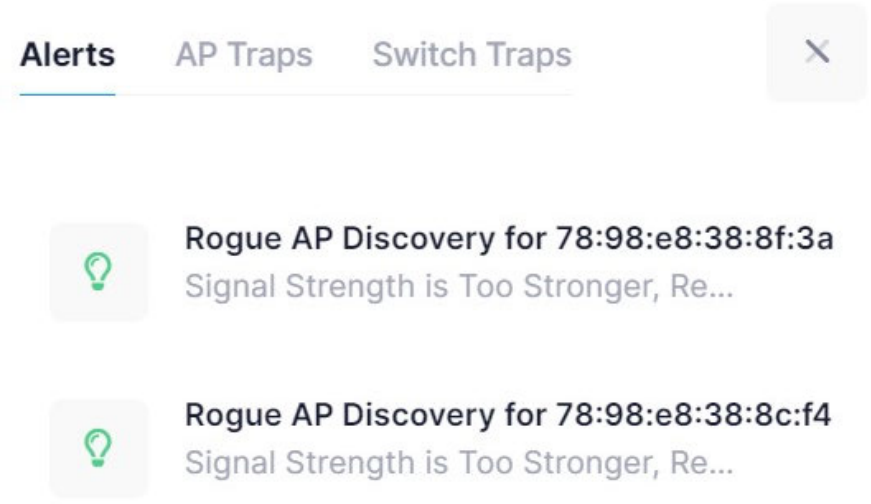


The top section of the Alerts screen provides a summary of alert activity during the specified time range. The bottom section of the screen is the Alerts Entry List, which displays the alerts (see page 948) generated based on the network device events and user configuration failure within the specified time range. You can also use the Alerts screen to acknowledge alerts (see page 953), delete alerts (see page 954), export alerts (see page 955), and manage alert templates (see page 958).

8.3.1 Viewing the Alerts Entry List

All Alerts from all devices within the Organization scope and specified timeframe are displayed and updated in real-time. New Alerts received are also indicated when a red blinking dot appears to the top of the bell icon on the Organization banner. For example:

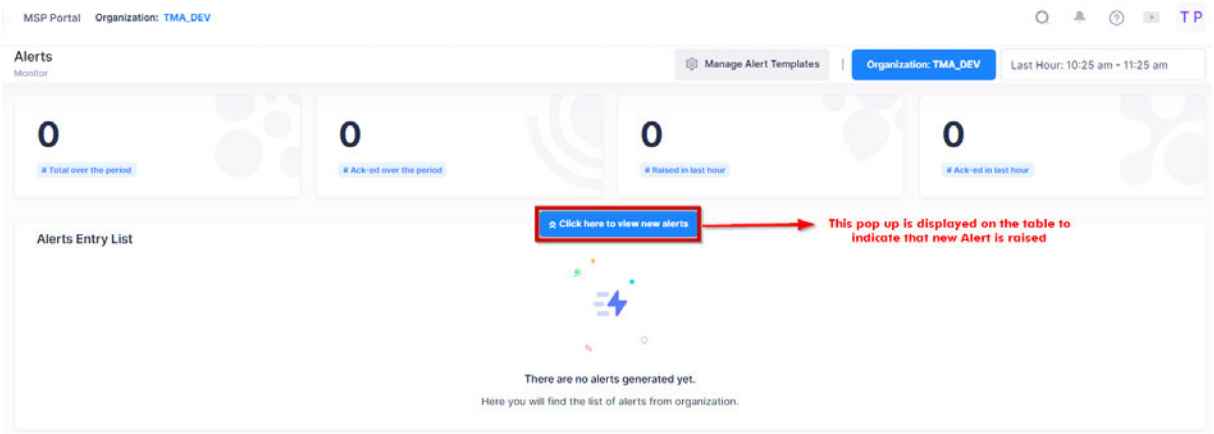
The bell icon provides a list of recent 10 new traps and Alerts received. To view the list of traps, click on the bell icon, then on **AP Traps** or **Switch Traps**. A drop-down window displays the list of new Traps and Alerts.



The dialog box will display only the recent 10 records of the Alerts. To view all the records or entries, you have to click on **See All** at the bottom of the drop-down list, then all Alerts are displayed on the screen.

8.3.1.1 View New Alerts Notification

When a new alert or trap is received, you will get a pop-up which is displayed on the top of the “Alerts Entry List” table to indicate that the new alert has been raised as shown below:



The above pop-up is displayed only when matching one of the below criteria:

- When received alert matches the column filters.
- When received alert matches the search filter.
- When received alert falls under the selected scope entity.
- When the time filter is selected other than the custom range. (for example, last hour, last 6 hours, etc.)

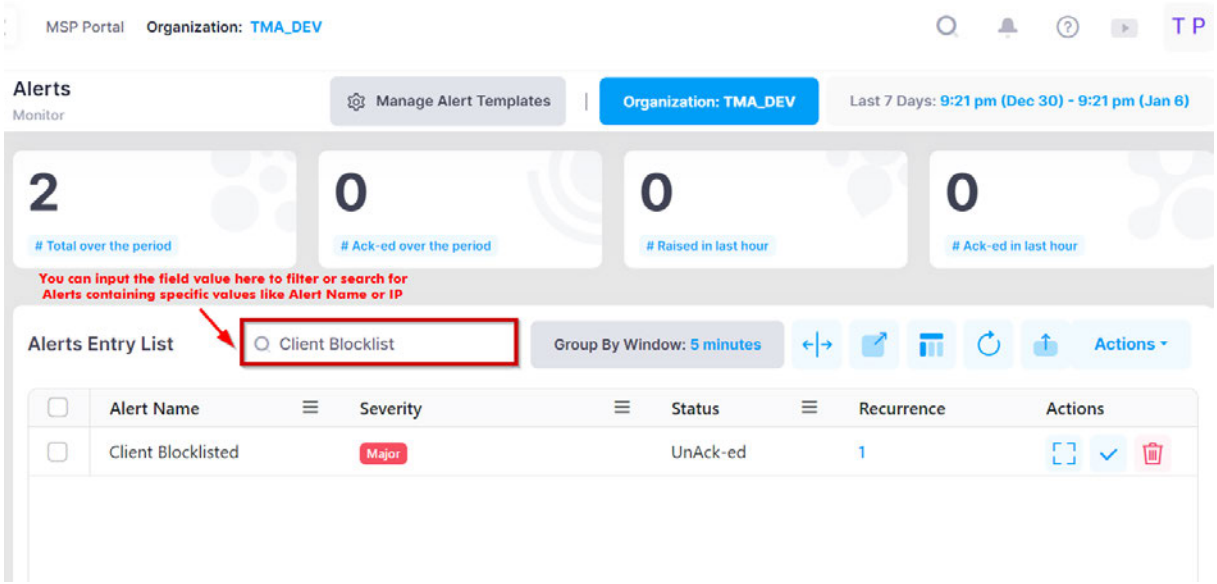
Note: The red blinking on the top of the bell icon is always displayed whenever a new alert or trap is received, irrespective of the mentioned criteria.

8.3.1.2 Alerts Entry List Information

The Alerts Entry List provides the following information for each alert received:

- **Alert Name** - The name assigned to the alert.
- **Severity** - The severity level (Minor/Major/Critical) of the alert.
- **Event/Cause** - The specific alert generated based on which events (source) or which cause.
- **Status** - Whether the alert is un-acknowledged (**UnAck-ed**) or acknowledged (**Ack-ed**).
- **Recurrence** - The number of alerts received for a specific alert type, from the selected Recurrence Scope (see page 950), within the selected Group by Window (see page 951) range, and Acknowledged status. Click on the number in this field to view details for each recurrence of the alert type.
- **Recurrence Scope** - Displays alerts from all devices in the Organization, Site, Building, Floor, or from a specific device. Use the display filter at the top of the Alerts screen to select which one of these entities to view.
- **Time of first alert**- The date and time the alert was initially received.
- **Time of latest alert** - The date and time the alert was last received.

Tooltip: Use the Search box option to view the Alerts containing a specific Alert Name, severity, recurrence scope, IP address, reason, code, version, VAP, SSID, STAMAC or Client MAC. Usually, the Client MAC doesn't appear in the Alerts List Table, but the search result will display all such Alerts containing a specific Client MAC as shown below:



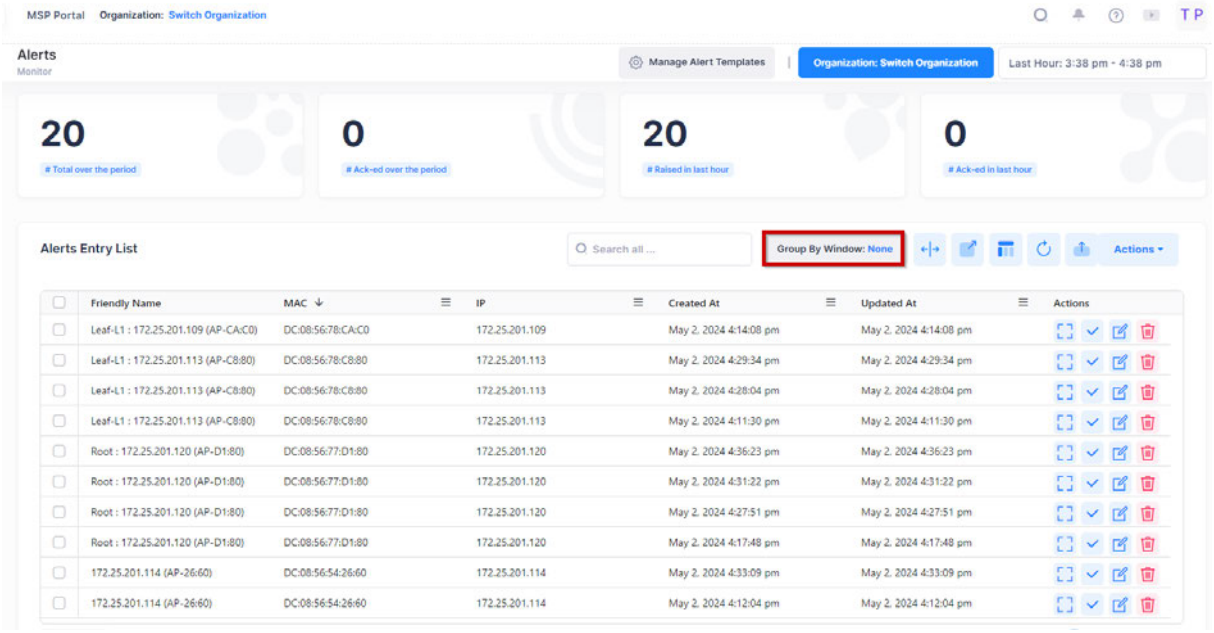
8.3.1.3 Group by Window

The Group by Window display option allows you to select a range of time during which each type of alert received is counted. To select the time range for the Group by Window, click on **Group by Window** and select from 5 minutes (the default) up to 24 hours from the drop-down menu.

The total number of a specific alert type received within the Group by Window range is used to calculate the value reported in the “Recurrence” field. Value reported in the “Recurrence” field is based on Alert Name, Status, Recurrence Scope and Group by Window.

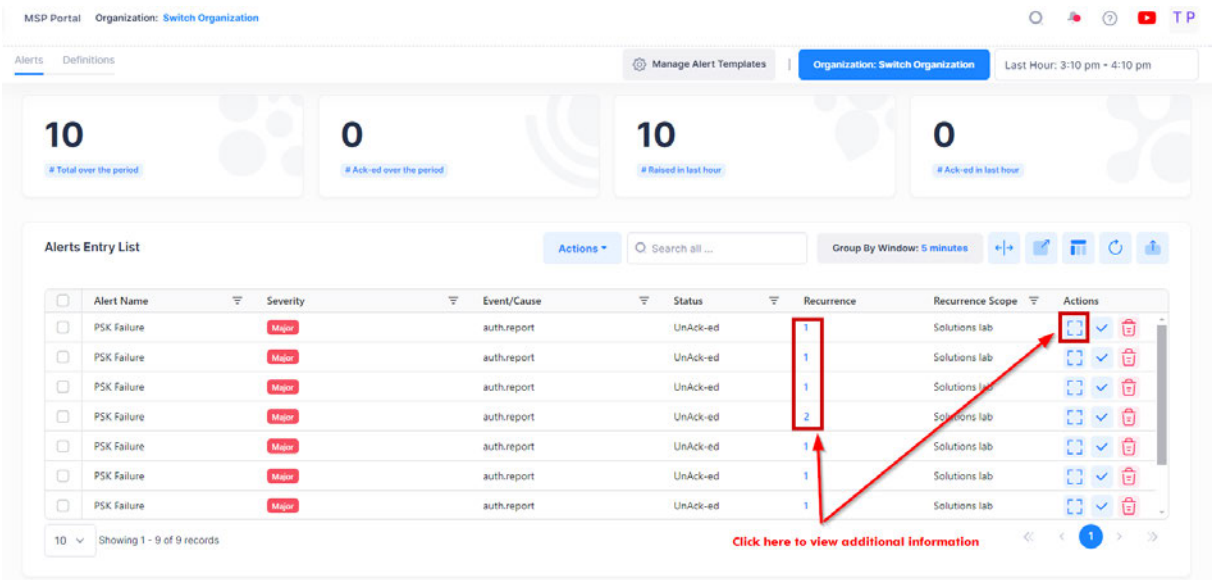
For example, if the Group by Window range is set to 24 hours and the Recurrence number for alert type “Port Auth Failure” is 12, then a “Port Auth Failure” alert was received 12 times during the 24-hour Group by Window range.

If you select the “None” option from the **Group by Window** drop-down menu, then it displays the detail view of the Alerts Entry List without any grouping of time range as shown below:

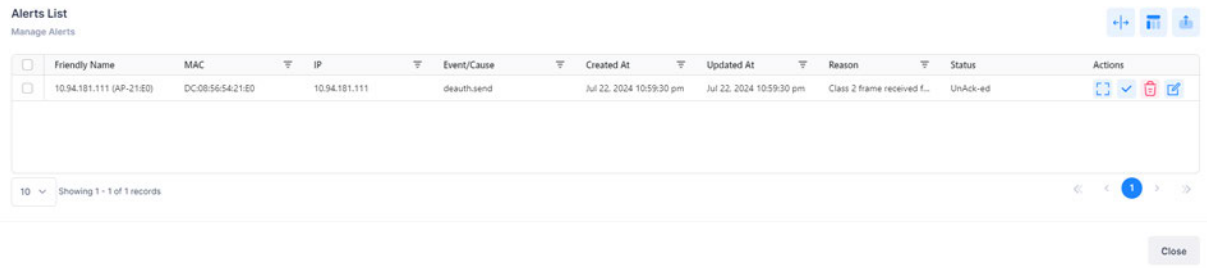


8.3.2 Display Additional Alerts Information

The Alerts Entry List displays entries grouped according to recurrence within the specified Group by Window time range. If you want to see a list of alert entries detail page, click on **Recurrence** column or **Additional Information** on “Actions” column next to a list entry to display detailed information for a specific Alert Entry.



The following screen appears:

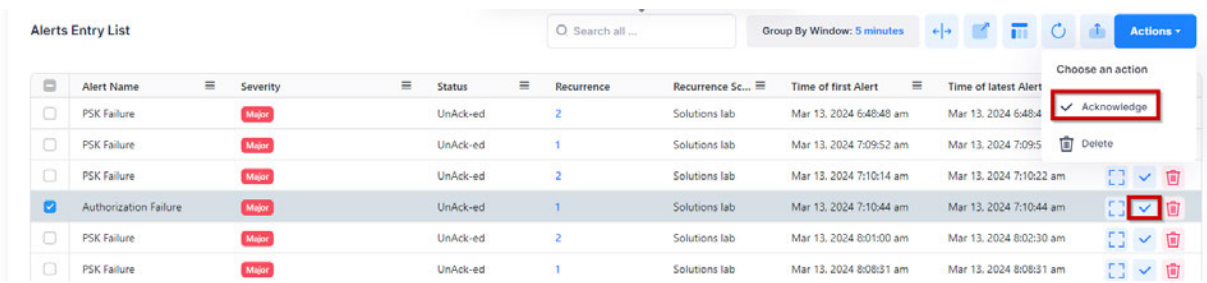


The following information for each alert is received:

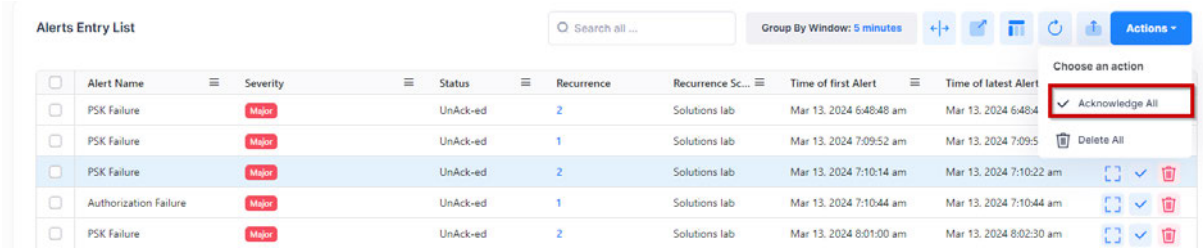
- **Friendly Name** - The name assigned to the device is derived from the Preferred Device Naming convention specified in the user preference settings (see page 26). By default, the Friendly Name is set to IP Address (System Name).
- **MAC** - The Access Point or Switch MAC address.
- **IP** - The IP address of the AP or Switch device.
- **Created At** - The date and time on which the alert was initially received.
- **Updated At** - The date and time on which the alert was updated by the user.
- **Reason** - The reason for the Alert.
- **Event/Cause** - The specific alert generated based on which events (source) or which cause.
- **Status** - Whether the alert is un-acknowledged (**UnAck-ed**) or acknowledged (**Ack-ed**).
- **STAMAC** - The MAC address of the connected Client.
- **SSID** - The name of the WLAN SSID.
- **VAP** - The name of the WLAN interface.
- **Alert Name** - The name assigned to the alert.
- **Severity** - The severity level (Minor/Major/Critical) of the alert.
- **Code** - The response status code of 802.11.
- **Notes** - The notes for the alerts. (Notes can be updated by you through edit button in Actions column).
- **Version** - The version of Access Point or Switch Interface.

8.3.3 Acknowledging Alerts

To acknowledge specific alerts, select one or more alerts in the Alerts Entry List, then select **Acknowledge** from the drop-down “Actions” menu or click on the checkmark next to the alert under the “Actions” column.

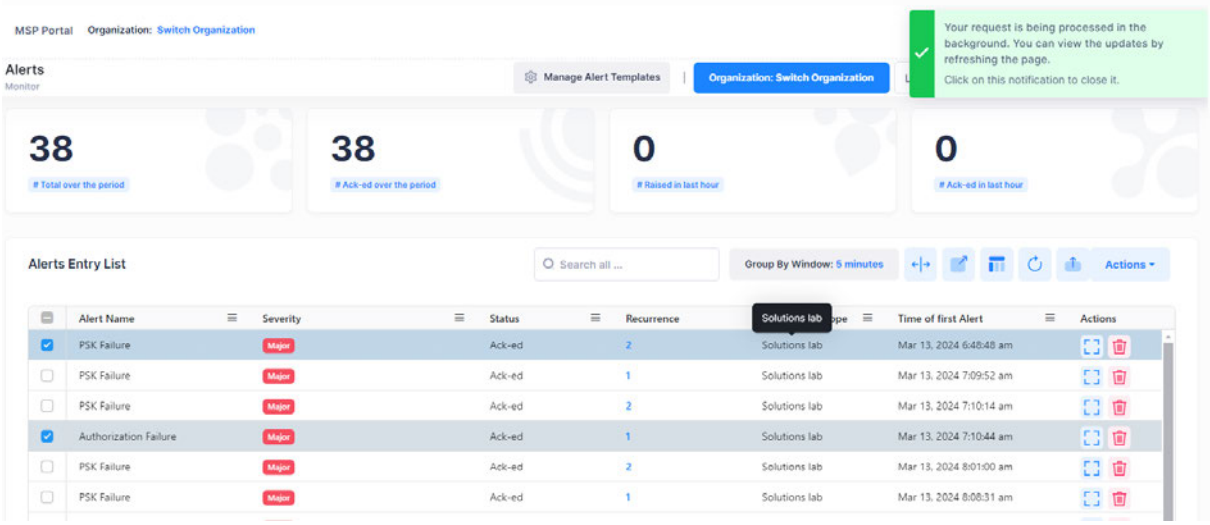


To quickly acknowledge all alerts, select **Acknowledge All** from the “Actions” drop-down menu. Note that this option is available only when there are no specific alerts selected within the list.



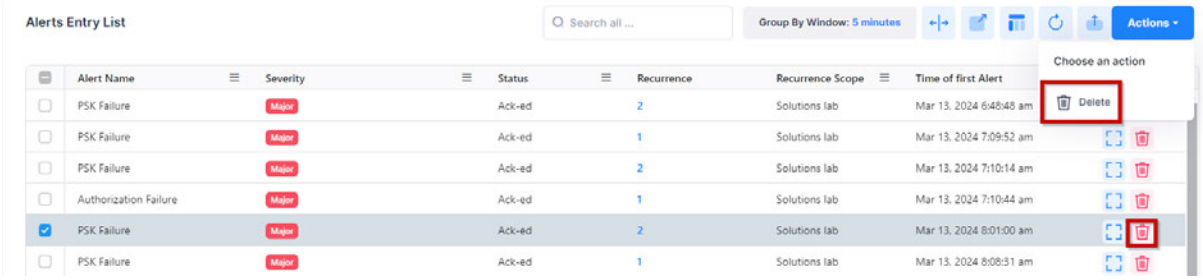
After you acknowledge an alert(s), the status for the alert(s) changes to **Ack-ed**.

> **Note:** The acknowledge Alerts operation is done in the background. You can view the updated results by clicking on the refresh button at certain time intervals as shown below.

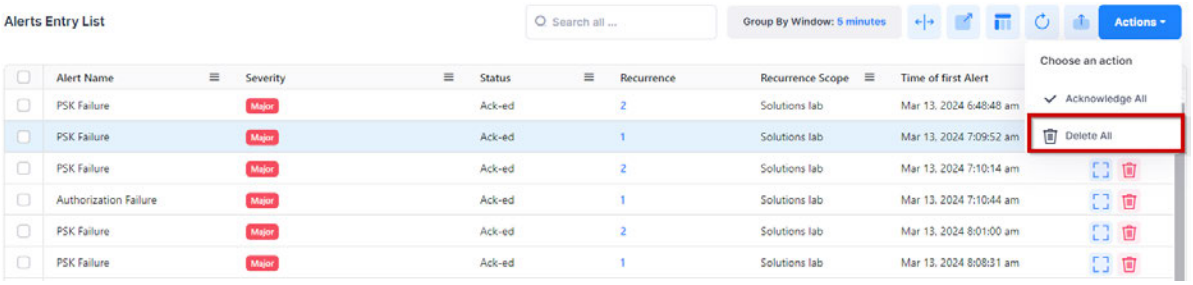


8.3.4 Deleting Alerts

To clear specific alerts from the Alerts Entry List, select one or more alerts, then select **Delete** from the “Actions” drop-down menu or click on the Delete icon next to the alert under the “Actions” column.



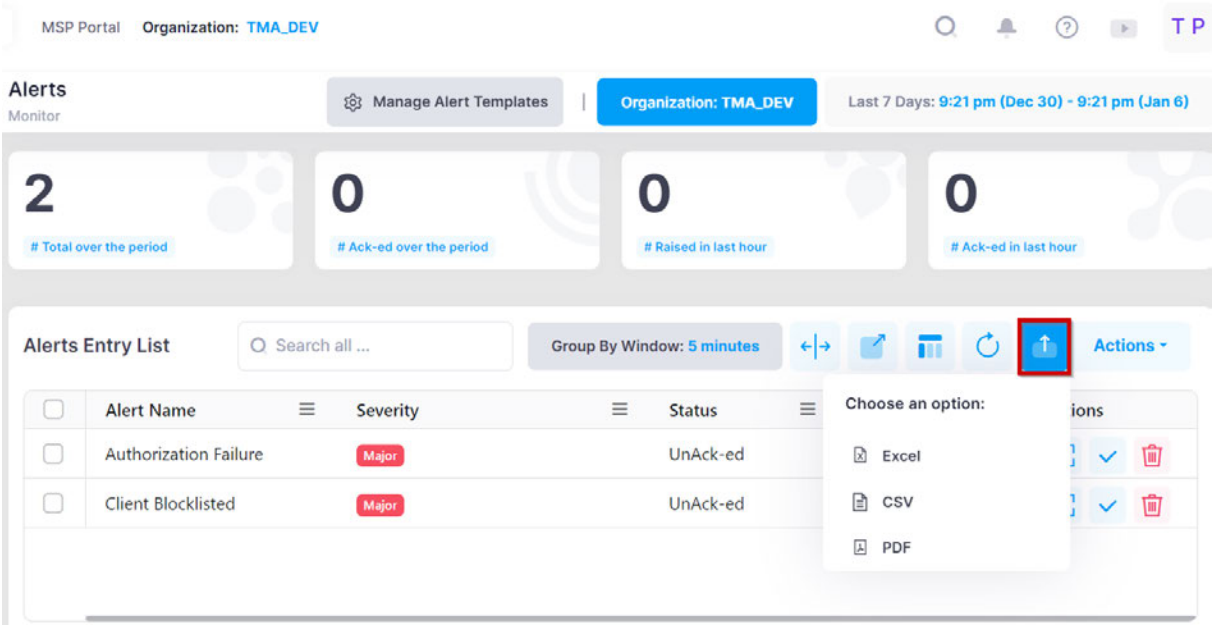
To clear all alerts from the Alerts Entry List, select **Delete All** from the “Actions” drop-down menu. Note that this option is available only when there are no specific alerts selected within the list.



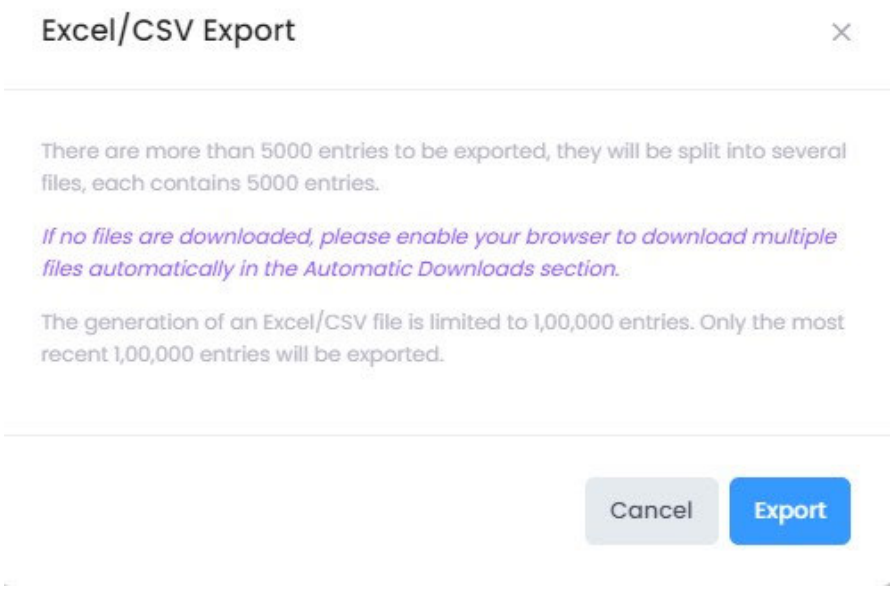
Note: The delete Alerts operation is done in the background. You can view the updated results by clicking on the refresh button at certain time intervals.

8.3.5 Export Alerts

To export multiple Alerts from an existing Alerts Entry List, click on the **Export** tab and select one of the available options to export the data in an Excel, CSV or PDF file format as shown below.



You will then be prompted to a dialog box that displays the notification that if there are more than 5000 entries to be exported, then the data will be split into multiple files, each containing 5000 entries. Also there is a limitation on the browser level to export only the latest 1,00,000 data entries for a chosen scope and time.



8.3.6 Alert Event Source List

The following table displays the list of Alerts with the Event or Cause related to that specific Alert. You can view the Event/Cause for the specific Alert on the summary and detail page of the Alert Entry List (see page 952).

Alerts Name	Event Source
DHCP Failure	dhcp.nack
DHCP Declined	dhcp.decline
EAP/802.1x Failure	auth.response
	auth.report
MAC Auth Failure	mac-auth.response
	mac-auth.timeout
	auth.report
PSK Failure	auth.report
Association Failure	assoc.response

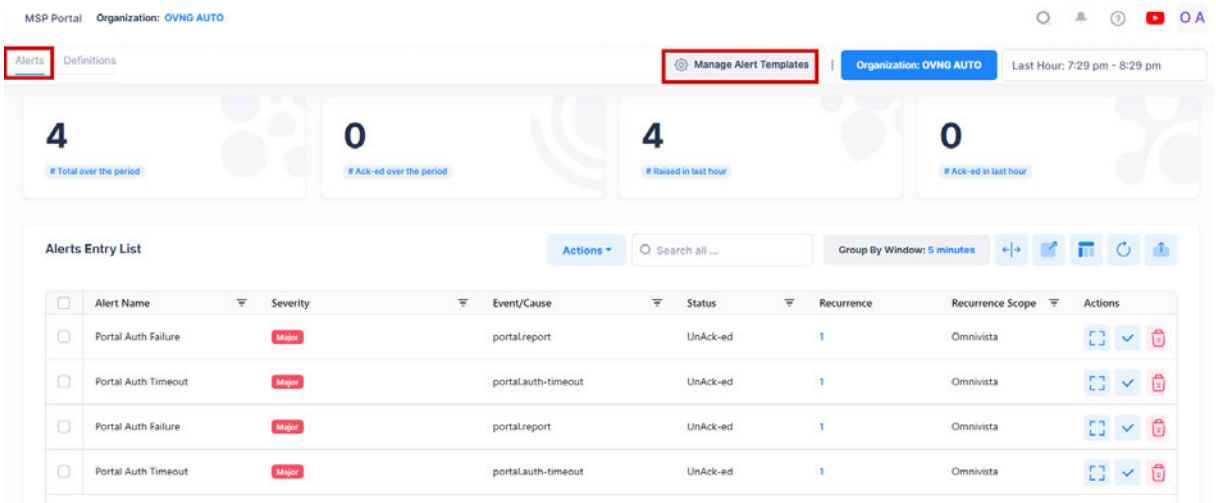
Alerts Name	Event Source
	auth.report
Deauth	deauth.send
	deauth.recv
DisAssoc	disassoc.send
	disassoc.recv
Reassoc Failure	reassoc.response
Roaming Failure	roam.report
Portal Auth Failure	portal.report
Portal Session Timeout	portal.session-timeout
Portal Auth Timeout	portal.auth-timeout
Portal Idle Timeout	portal.idle-timeout
Authorization Failure	auth.response
	auth.report
Rogue AP Discovery	aprogueinfo.report
Rogue AP Cleared	aprogueinfo.report
Client Blocklisted	aprogueclient.report
AP License Installed Alert	apLicenseInstalledAlert
AP License Mode Changed Alert	apLicenseModeChangedAlert
AP License No Connectivity Alert	apLicenseNoConnectivityAlert

Alerts Name	Event Source
AP Naas Expiry Day Alert	apNaasExpiryDayAlert
AP Naas Degraded State Alert	apNaasDegradedStateAlert
Apply configuration to AP/Switch Failure	Different cause based on module
Configuration backup failed	backup
Configuration backup partial failure	backup
Golden configuration setup failed	audit
Golden configuration drift detected	audit
Failed to perform golden configuration audit	audit

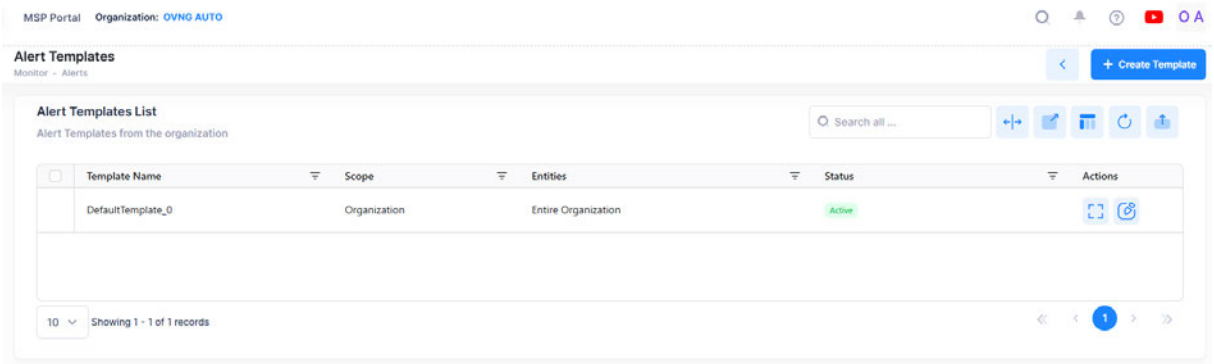
8.3.7 Managing Alert Templates

OmniVista Terra initially uses a default alert template (“DefaultTemplate_0) to determine which alerts to report on the Alerts Entry List. The default template is configured to report on all the selected alert types received from devices within all Sites of an Organization. You cannot delete the “DefaultTemplate_0” template but you can edit the default template attributes (for example, name, scope, and alert types) or define a new template (see page 959) to override the default template.

To view the active alert template, click on **Manage Alert Templates** at the top of the Alerts screen as shown below:



The **Alert Templates List** screen opens.

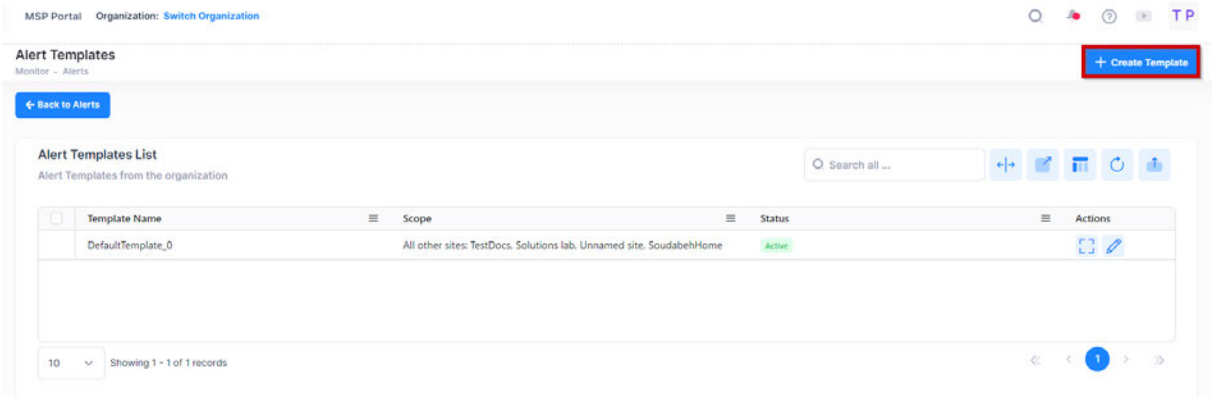


The following information is provided for the template:

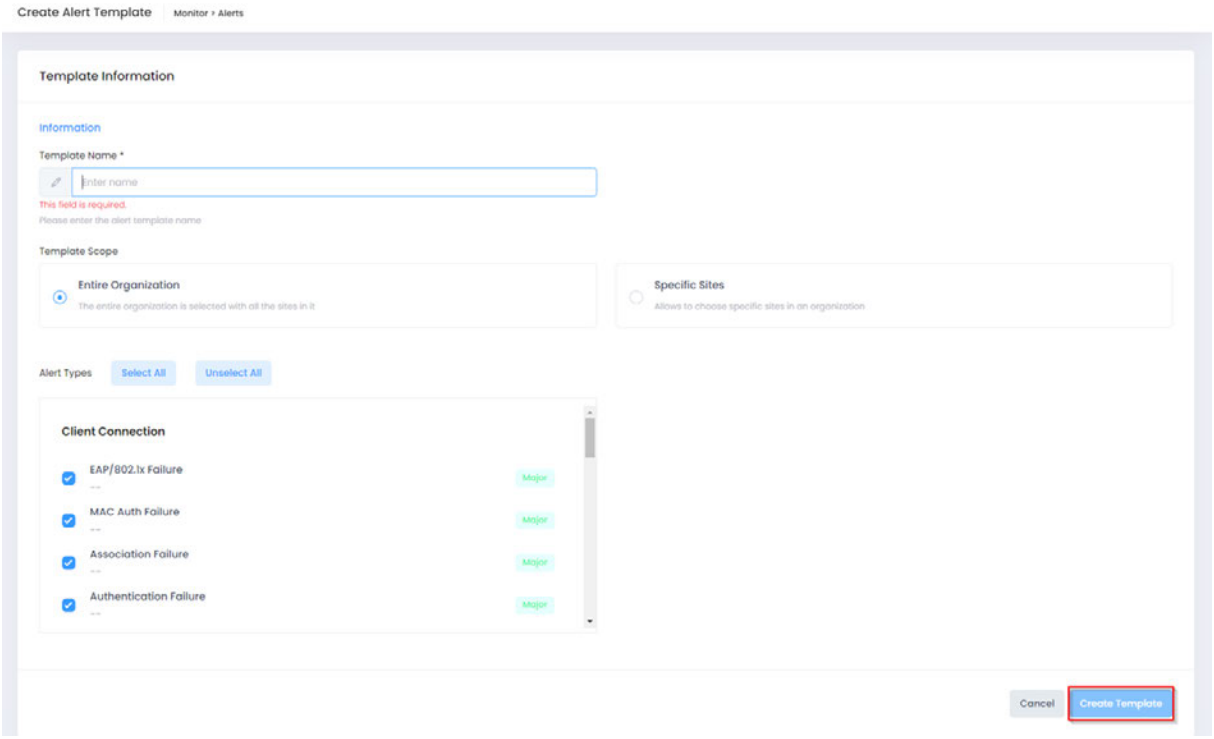
- **Template Name** - The name assigned to identify the alert template.
- **Scope** - Report the selected alerts received from all Sites within the Organization or only from specific Sites within the Organization.
- **Status** - Whether the template is active or inactive.

8.3.7.1 Create a New Template

To create a new template, go to **Monitor > Alerts > Manage Alert Templates** and click on **Create Template** on the Alert Templates List screen.



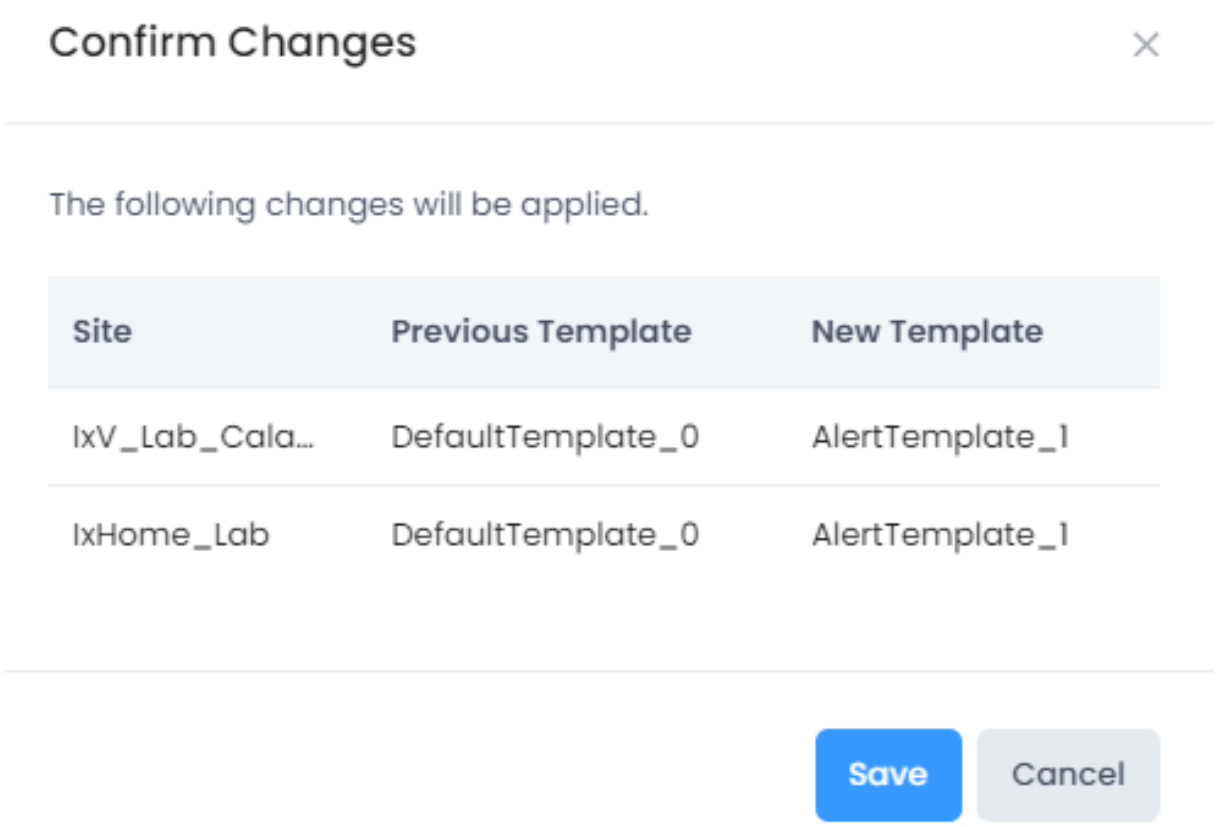
The Create Alert Template screen opens.



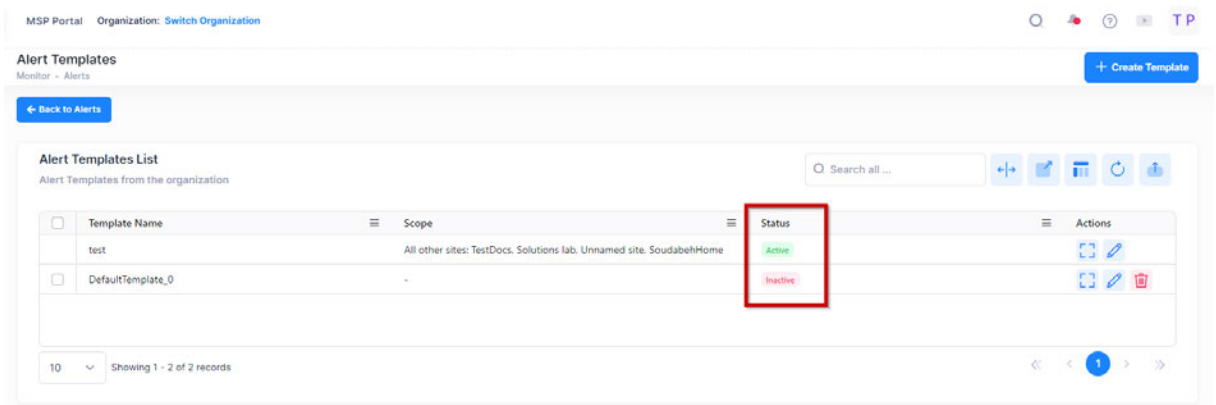
Complete the following fields as described:

- **Template Name** - Enter a name to assign to the new template.
- **Template Scope** - Select Entire Organization (the default) or Specific Sites.
- **Alert Types** - Select the alert types (see page 962) that you want to view on the Alerts Entry List. By default, all alerts are selected.

After you have finished configuring the new template, click **Create Template**. You are then prompted to confirm overriding the existing template with the new template.



Click **Save** to confirm. The new template becomes the only “active” template and the old template is “inactive”.



When a new template is created, you are prompted to confirm that the new template settings will override the existing active template settings within the same time scope. There can only be one active template at a given time for a specific time scope.

For the “Alert Templates”, follow the following use cases:

- You can not delete the template with Entire Organization.
- If a site is configured with a specific template, it will use the site template.
- If a site does not have a template, it will follow the Entire Organization template.

Note: You can view the updated new severity levels of Alerts in the Manage Alert Templates list by navigating to following screen, **Monitor > Alerts > Manage Alert Templates > Actions > Edit**.

8.3.7.2 Alert Types

The following alert types are available for you to select when creating or editing an alert template:

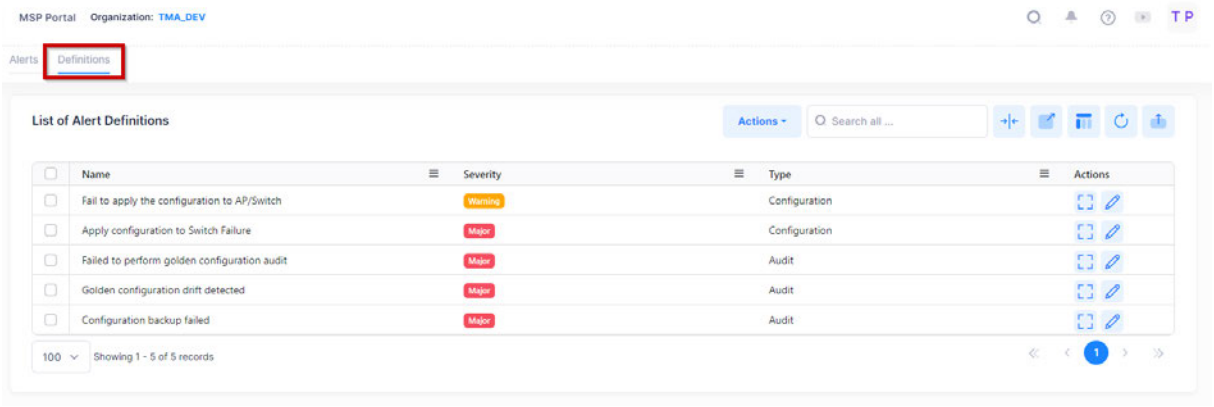
Client Connection	WIPS	NaaS	Audit	Backup	Configuration
EAP/802.1X Failure (Major) MAC Auth Failure (Major) Association Failure (Major) Authentication Failure (Major) Deauth Failure (Major) Disassoc Failure (Major) Reassoc Failure (Major) Roaming Failure (Major) Portal Auth Failure (Major) Portal Session Timeout (Major) Portal Auth Timeout (Major) Portal Idle Timeout (Major) PSK Failure (Major) Authorization Failure (Major) DHCP Failure (Major) DHCP Declined (Major)	Rogue AP Discovery (Minor) WIDS Event (Minor) Rouge AP Cleared (Minor) Client Blocklisted (Major)	AP License Installed Alert (Major) AP License Mode Changed Alert (Major) AP License No Connectivity Alert (Critical) AP NaaS Expiry Day Alert (Critical) AP NaaS Degraded State Alert (Major)	Failed to perform golden configuration audit (Major) Golden configuration setup failed (Major) Golden configuration drift detected (Major)	Configuration backup partial failure (Minor) Configuration backup failed (Major)	Fail to apply the configuration to AP/Switch (Major)

Note: Sites-based Alert templates will have a higher precedence than Organization-based Alerts templates.

21 Oct 2025

8.3.8 Alert Definitions

The Alert Definitions screen displays a list of all supported alerts and provides a brief description of each alert. You can also edit (see page 965) the severity level for an alert. To access the Alert Definitions screen, click on **Alerts** and select **Definitions** tab under the “Monitor” section of the OmniVista Terra Menu (see page 45).



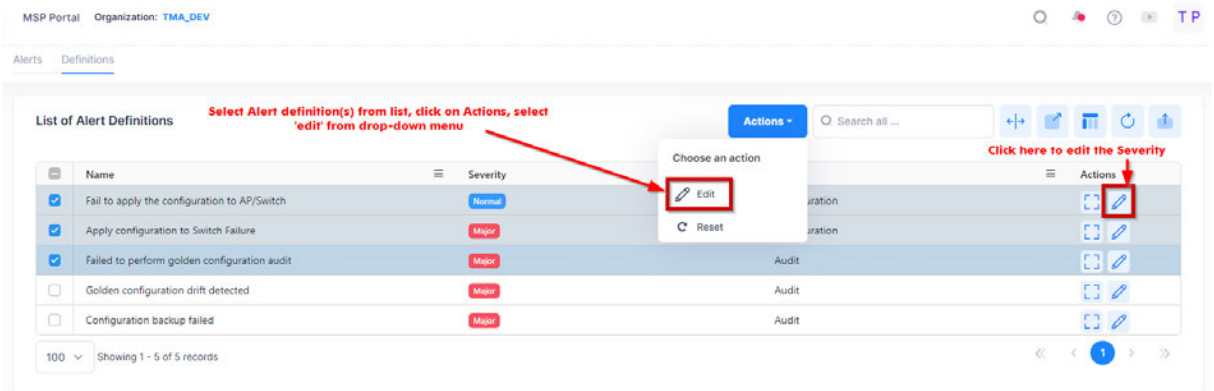
The Alert Definitions screen provides a List of Alert Definitions that displays basic (see page 965) alert information (for example, name, type, severity level). You can search for alerts by entering a search criteria (for example, Name, type, Severity) in the "Search" field. Only those alerts matching the search criteria are displayed. You can also export the alert definitions list to an Excel sheet, CSV, or PDF file.

8.3.8.1 Basic Alert Definition Information

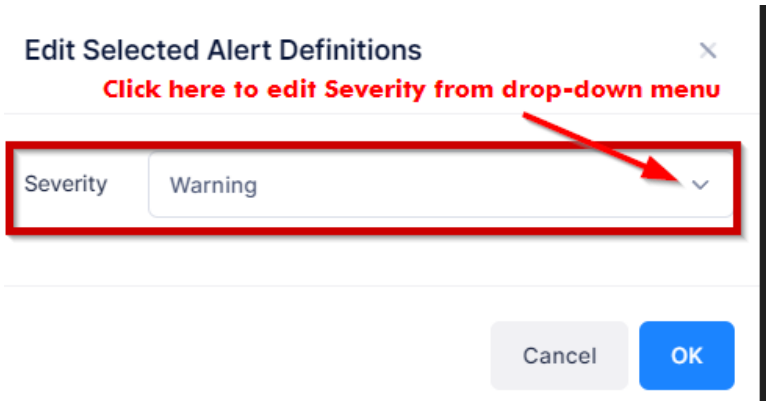
- **Name -** The name assigned to the alert.
- **Type** - A description of the alert type. QoE (see page 986)
- **Severity -** The severity level of the Alert. (Normal/Warning/Minor/Major/Critical).

8.3.8.2 Editing an Alert Definition

Note that you can only edit the Severity field for Alert Definitions. To edit the severity level for an alert or multiple alerts, select the alert in the Alert Definitions list and click on the Edit icon under the “Actions” column.

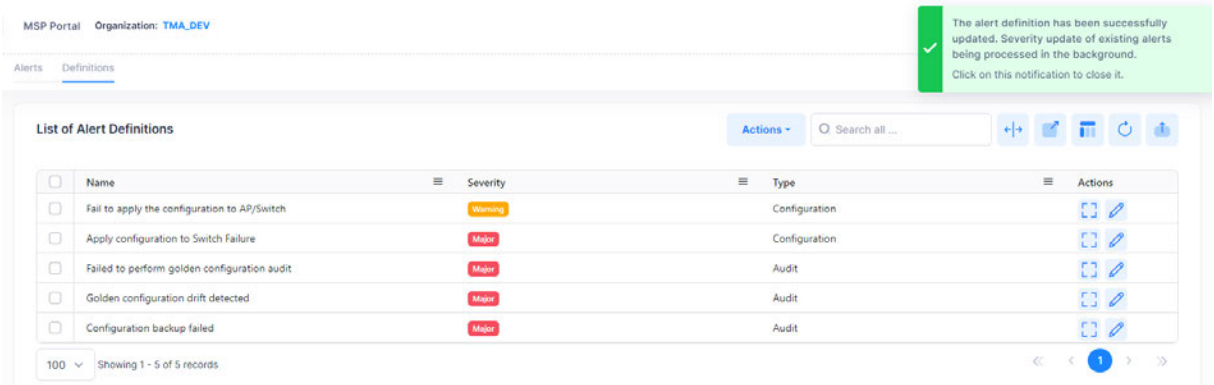


The following screen will appears.

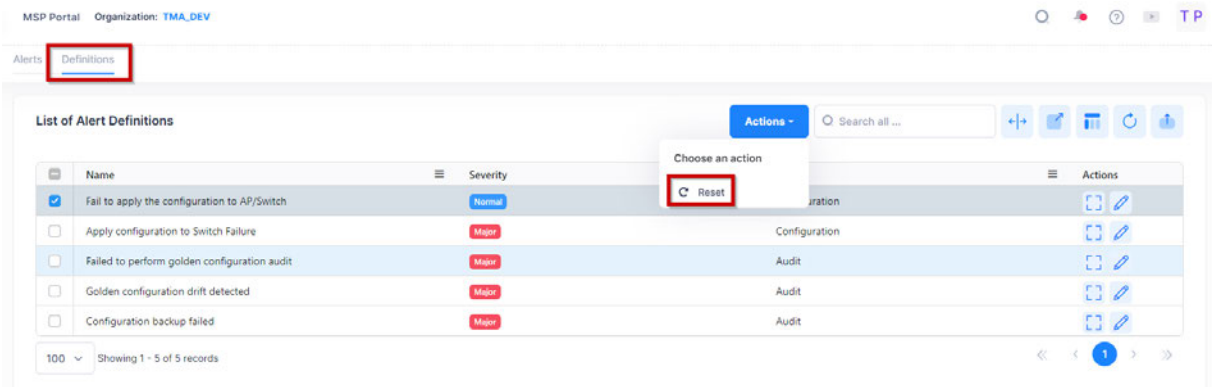


When you are done making changes, click **OK** to retain your updates and return to the Alert Definitions screen.

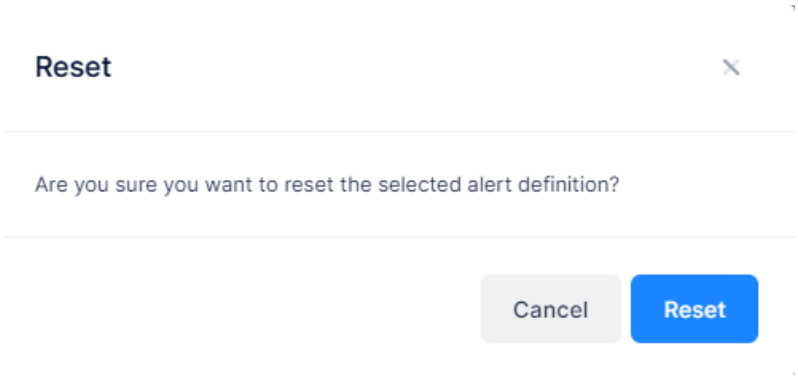
> **Note:** During editing of Alert Definitions, the Severity Alerts update operation is done in the background. You can view the updated results by clicking on the refresh button at certain time intervals as shown below.



To restore the default settings for the Severity field, select the alert in the Alert Definitions list and click on **Actions**, then click on **Reset**.



The following confirmation prompt will appears.



Click on **Reset** to make changes and return to the Alert Definitions screen.

To view the updated severity changes for the Alerts, you can navigate to **Monitor > Alerts > Definitions**. You can also navigate to Alerts summary and details page to view the severity updates.

21 Oct 2025

8.3.9 Alerts - FAQs/Troubleshooting

8.3.9.1 I can’t select a longer time period in the data filter on the Alerts screen.

The time range options that you can select on the Alerts screen are based on the data persistency values set in Basic Settings for the Organization.

- Check the values set for Alerts in the data persistency section of the Basic Settings (see page 127) screen (**Organization** > **Settings > Basic Settings).**
- Limit for the Alerts is minimum 7 days to maximum 30 days.

8.3.9.2 I don’t see the specific type of Alerts in the summary section of the Alerts screen.

The type of Alerts displayed is based on the Scope/Alert type selected in the Alert template. Check that the correct Scope and Time period is selected.

- Click on **Manage Alert Templates** on the Alerts screen.
- An Alert template is applied to the selected Scope. Select the Active template of the desired Scope and click on the Edit icon under the “Actions” column.
- Select the missing Alert Type and save the changes.

Note that the Site Scope is always preferred over the Organization Scope.

8.3.9.3 I don’t see the live notifications in the real time.

- Live notification are displayed at the interval of one minute.
- The Notification Panel displays only the latest 10 (approximately) records. To see all records, click on **see all** at the bottom of the panel.

21 Oct 2025

8.4 Diagnostic Tools

The OmniVista Terra Diagnostic Tools are accessed by clicking on **Diagnostic Tools** under the “Monitor” section of the OmniVista Terra Menu (see page 45). When you click on the Diagnostic Tools menu option, the following list of applications is provided to assist you with analyzing and troubleshooting your network:

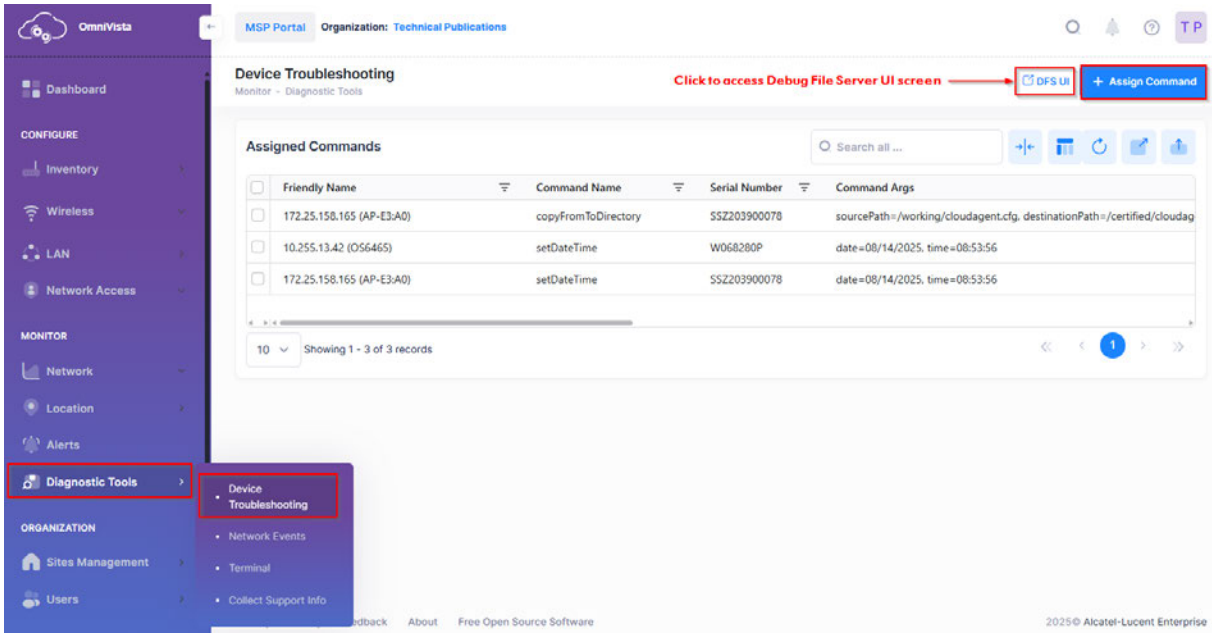
- Device Troubleshooting (see page 970) - Used to send commands to network devices to troubleshoot and resolve device problems.
- Network Events (see page 981) - Monitor notification events and configure event management tasks.
- Terminal (see page 1015)- Establish a basic CLI/Scripting session with a device.
- Collect Support Information (see page 1018) - Collect log files from a network device that you can send to Alcatel-Lucent Enterprise (ALE) to troubleshoot problems.

21 Oct 2025

8.4.1 Device Troubleshooting

The Device Troubleshooting screen is used to send commands to network devices to troubleshoot and resolve device problems. A list of commands is provided. You can use these commands as is, or edit them for your specific situation. Commands previously issued to network devices are displayed in the Assigned Commands Table and can be used to access troubleshooting logs.

To access the Device Troubleshooting screen, click on **Diagnostic Tools > Device Troubleshooting** under the “Monitor” section of the OmniVista Terra Menu (see page 45).

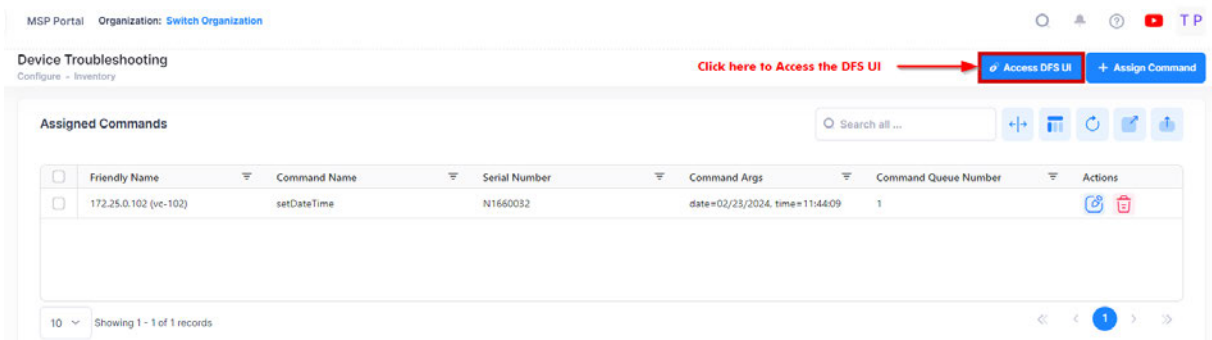


Use the Device Troubleshooting screen to view a list of assigned commands previously issued to network devices, create troubleshooting commands to issue to network devices, edit and delete assigned commands.

8.4.1.1 Accessing the Debug File Server User Interface

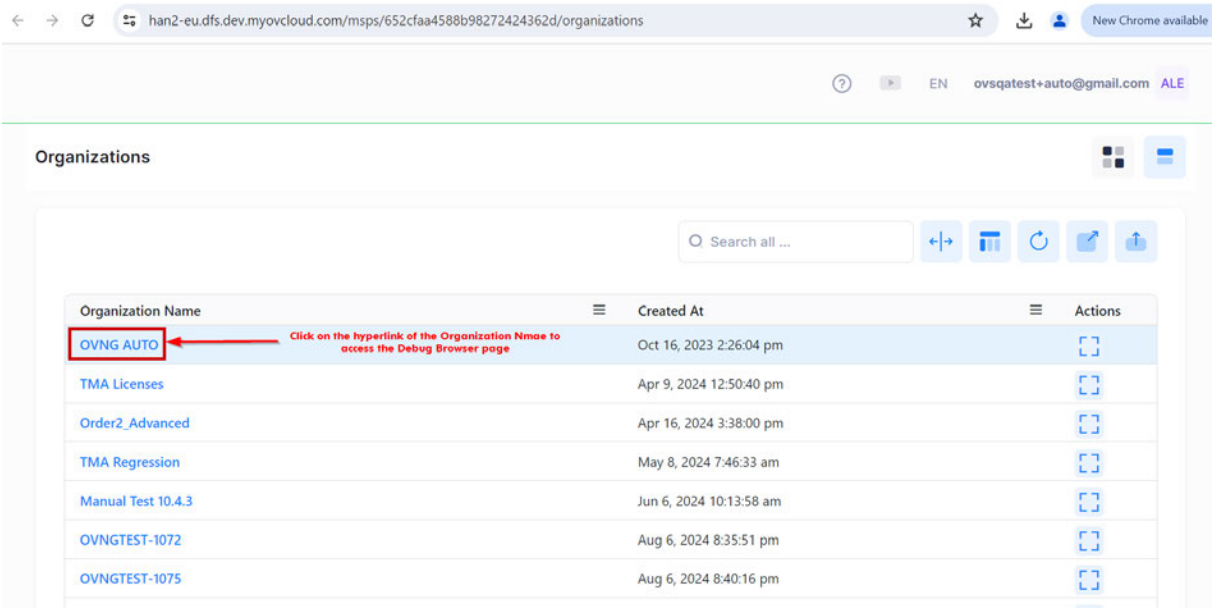
By accessing the DFS UI screen, you can execute a command on multiple devices at once within an Organization user ID.

To access the DFS UI, click on the **Access DFS UI** tab on Device Troubleshooting screen as shown below:

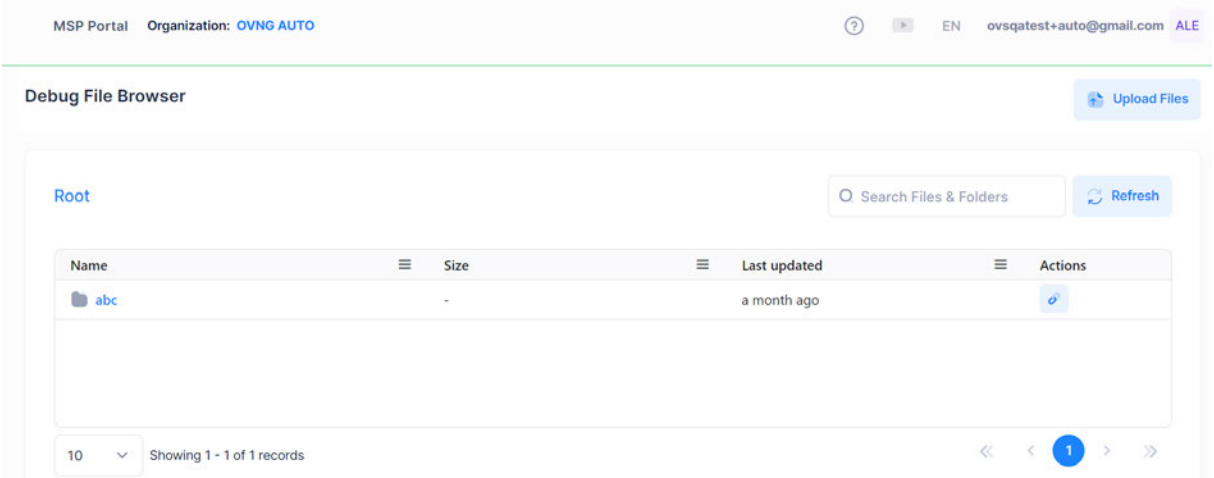


The following screen will display all the Organizations that the current account can access as shown below:

- You don't need to create a different account to access the Debug File Server UI, although you can log in successfully by using the credentials of your existing account.



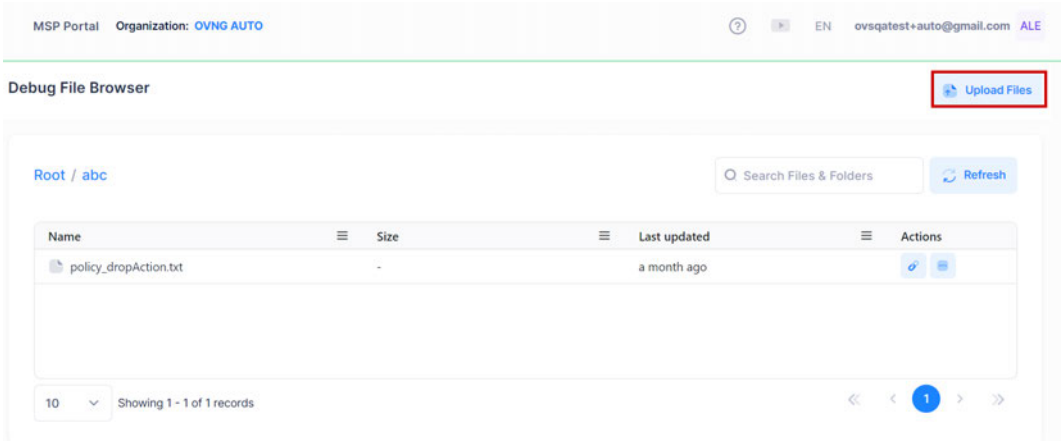
Click on the hyperlink in the Organization name column and it redirects you to the **Debug File Browser** page as shown below:



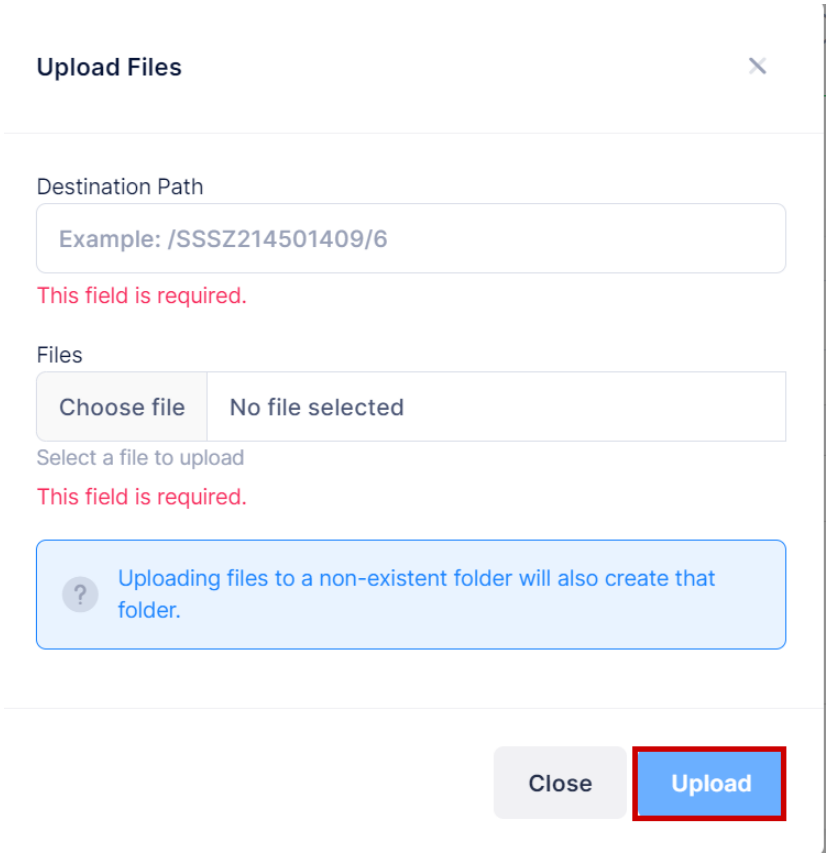
You can view the list of files or directories in the system and the files are grouped by organizations. You can perform different operations like move files/folder (see page 974), download file (see page 973), upload file (see page 972), delete file/directory (see page 975) or retrieve directory listing (see page 973) by using the Actions button.

8.4.1.1.1 Upload Device File

You can click on the **Upload Files** button on the right hand side of the screen to upload files or directories to the destination path on the server.



The following window opens:



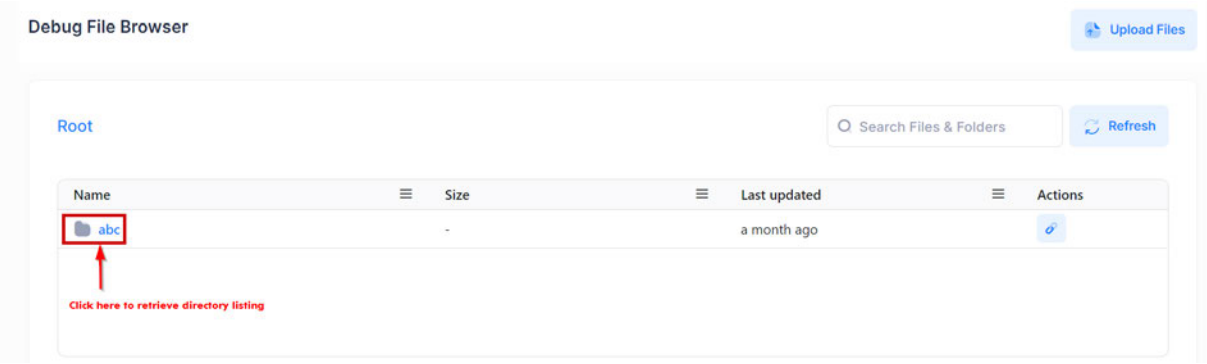
Complete the following field value and click on **Upload**. The files will be uploaded to the destination directory.

- **Destination Path** - Enter the destination path to which you need to upload the file/folder.
- **Files** - Select a file to upload from your computer.

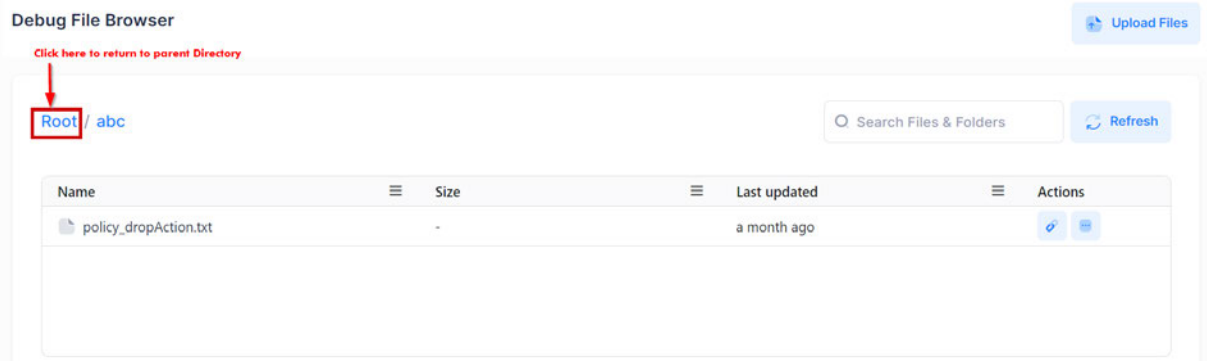
Note: While uploading a file, the file will automatically be overwritten if the file already exists on that path.

8.4.1.1.2 Retrieve Directory Listing

You can click on a **directory** name to retrieve the list of child files or child directory.



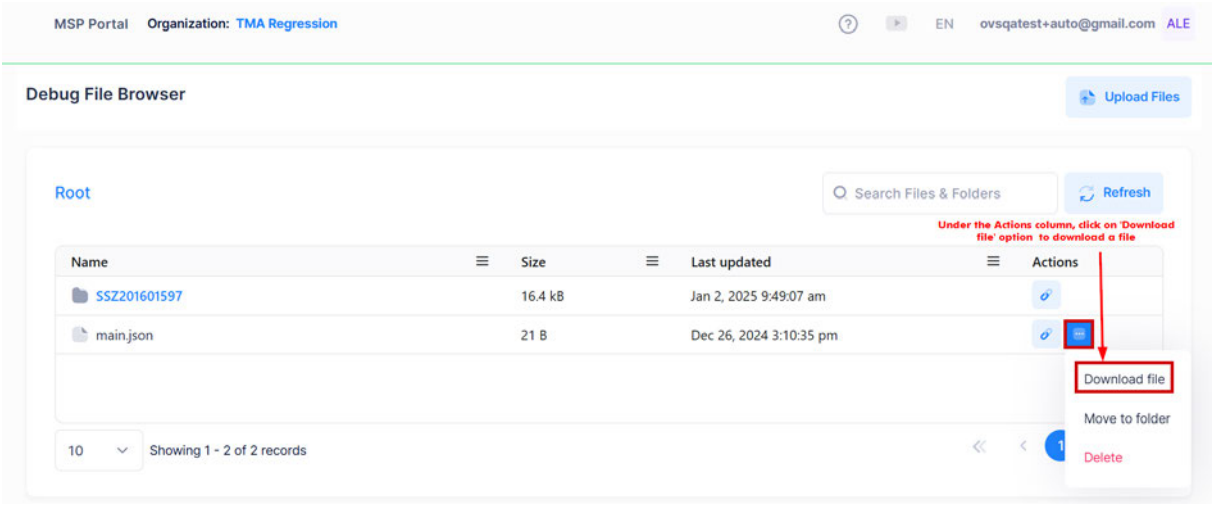
The table will then change and display the contents in that directory as shown below:



Click on the top left of the table to go back to the parent directory.

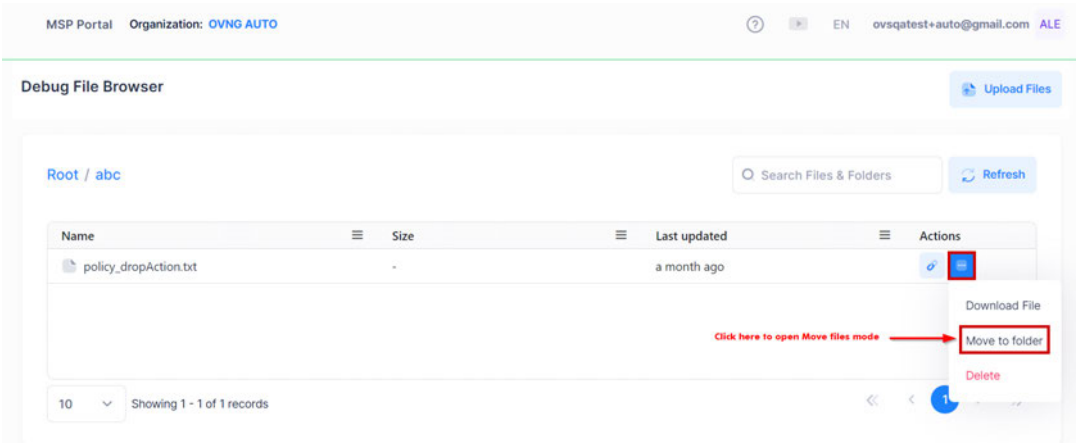
8.4.1.1.3 Download Device File

To download the device file from the server, go to the Actions column, and click on the Download File option from the drop-down menu then the file will be downloaded.

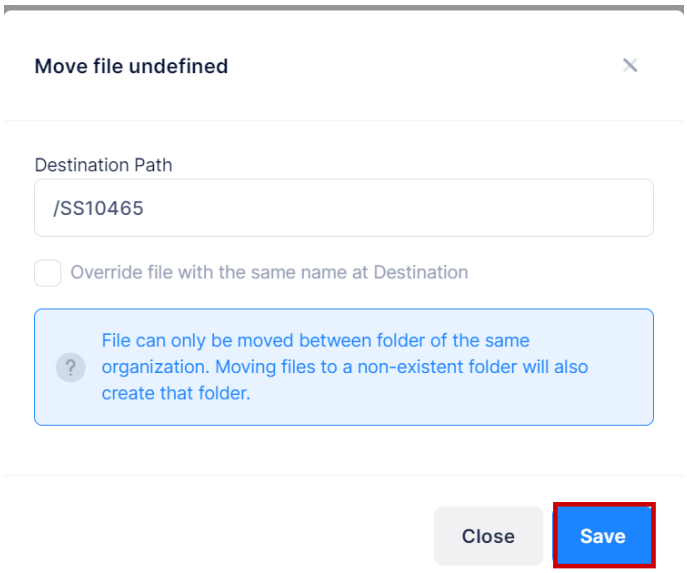


8.4.1.1.4 Move Device Files

To move the Device files within the Organization, go to Actions column and click on **Move to Folder** from the drop-down list.



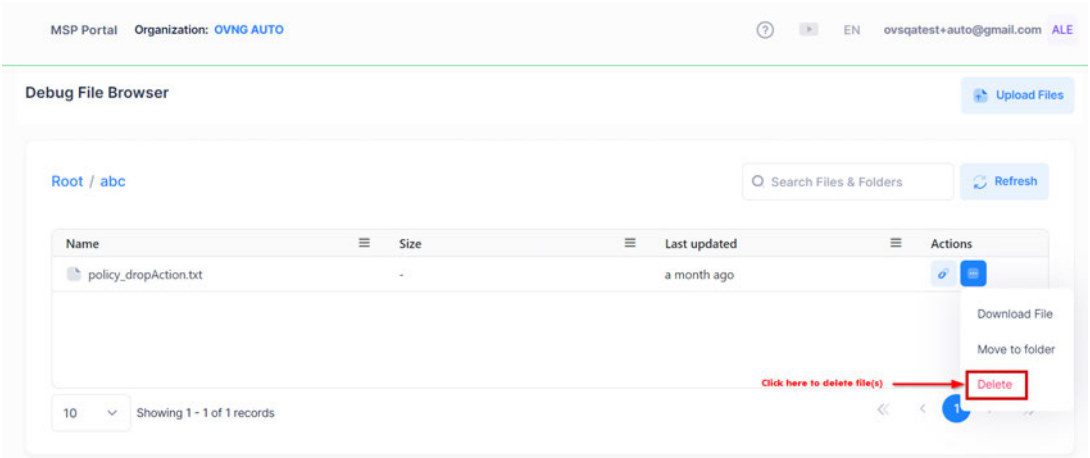
It will open the move files mode as below:



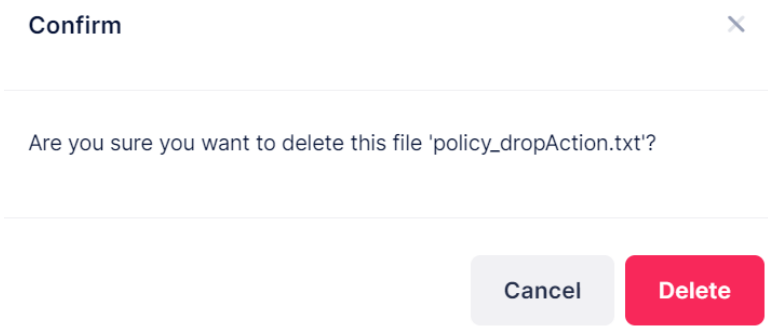
Enter the Destination path to move a file, and if there is a file with the same name at the Destination, you should check in the Override checkbox. The files can only be moved between folders of the same Organization, the Destination path should start with the direct children folder of the Organization. Click on **Save** button to save changes.

8.4.1.1.5 Delete Device File

You can delete the Device Directory or File by clicking on the **Delete** button in the Actions column of each File/Directory.



The confirmation window appears, click on **Delete** to permanent delete a File. All the contents of the child File(s) or child Directory will also be deleted by using this action.



8.4.1.2 Troubleshooting a Device

To issue a troubleshooting command to one or more network devices, click on **Assign Command** in the top-right corner of the Device Troubleshooting screen. The Assign Command screen provides the following step-by-step process to create and issue a troubleshooting command to a network device(s):

Step 1. Device Selection (see page 976) **-** Select the device(s) to which the troubleshooting command will be issued.

Step 2. Command Selection (see page 977) - Select the command to be issued to the selected network device(s).

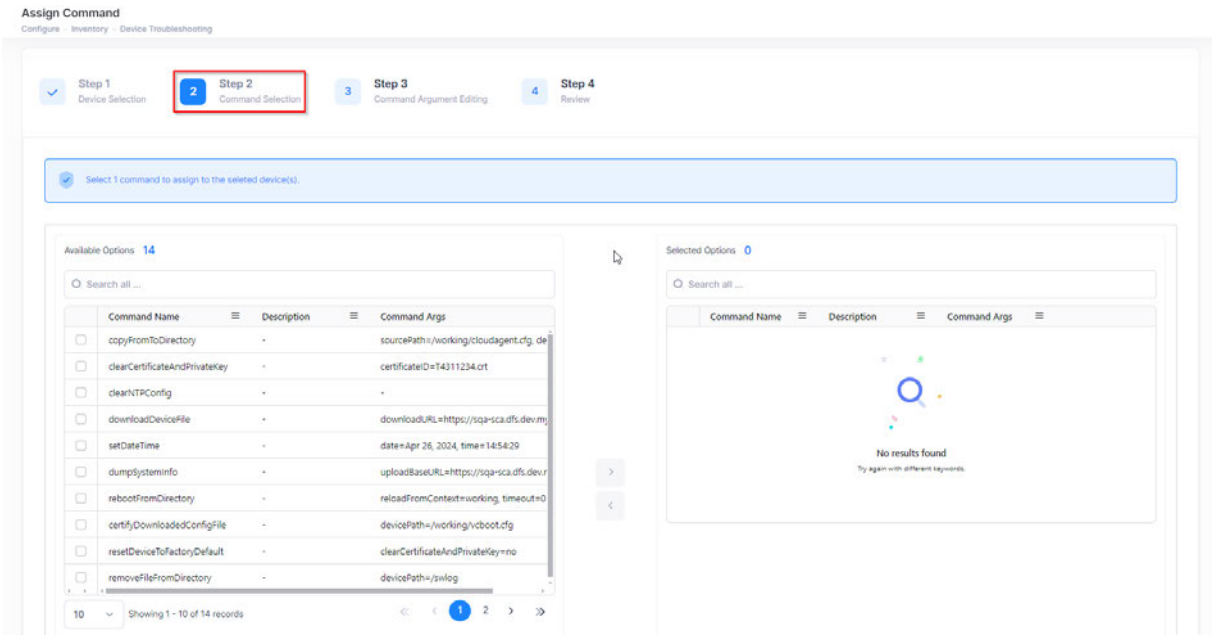
Step 3. Command Argument Editing (see page 977) - Edit the default command argument, if necessary.

Step 4. Review (see page 978)- Review command details and assign the command to the selected network device(s).

8.4.1.2.1 Step 1. Device Selection

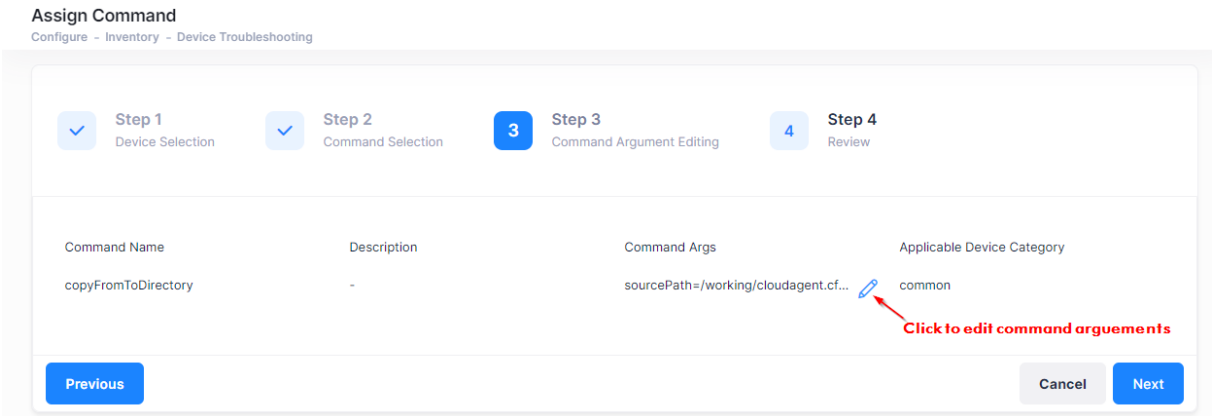
Select one or more devices from the list to which you will issue a troubleshooting command, then click **Next** to move to the next tab (Step 2). You can also apply filters to search for a specific device selection.

8.4.1.2.2 Step 2. Command Selection

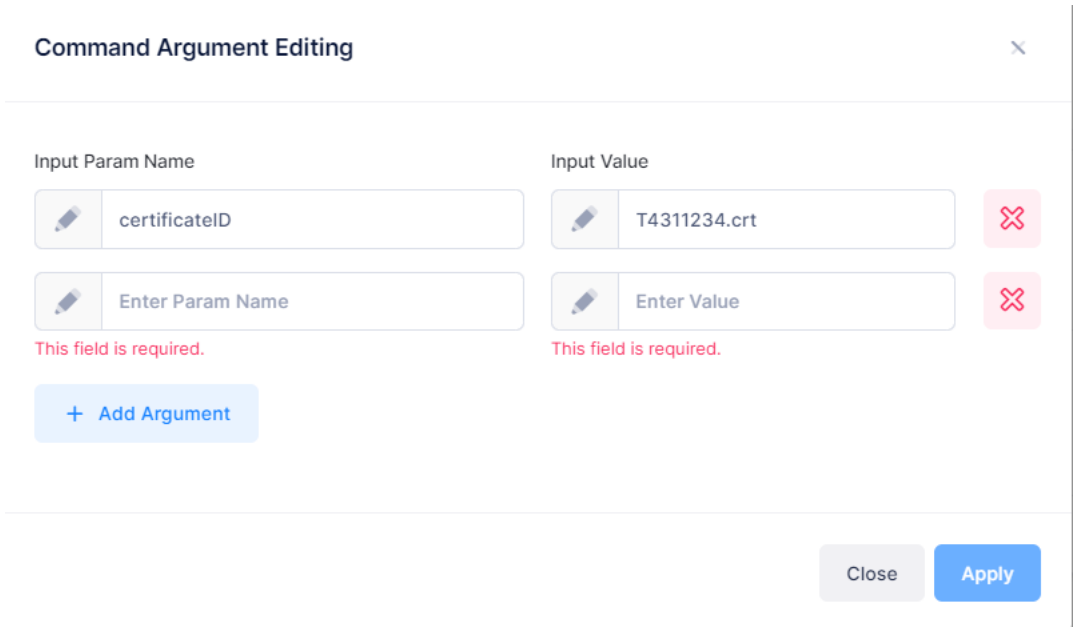


Select the command that you will issue to the selected device(s), then click **Next** to move to the next tab (Step 3). You can only select one command at a time. Click here (see page 979)for an overview of the available troubleshooting commands.

8.4.1.2.3 Step 3. Command Argument Editing



Troubleshooting commands contain default arguments, which are sufficient in most situations. If you do not want to make any changes to the argument, click **Next** to move to the next tab (Step 4). If you want to edit the command argument, click on the pencil icon next to the command argument. The following Command Argument Editing window opens:

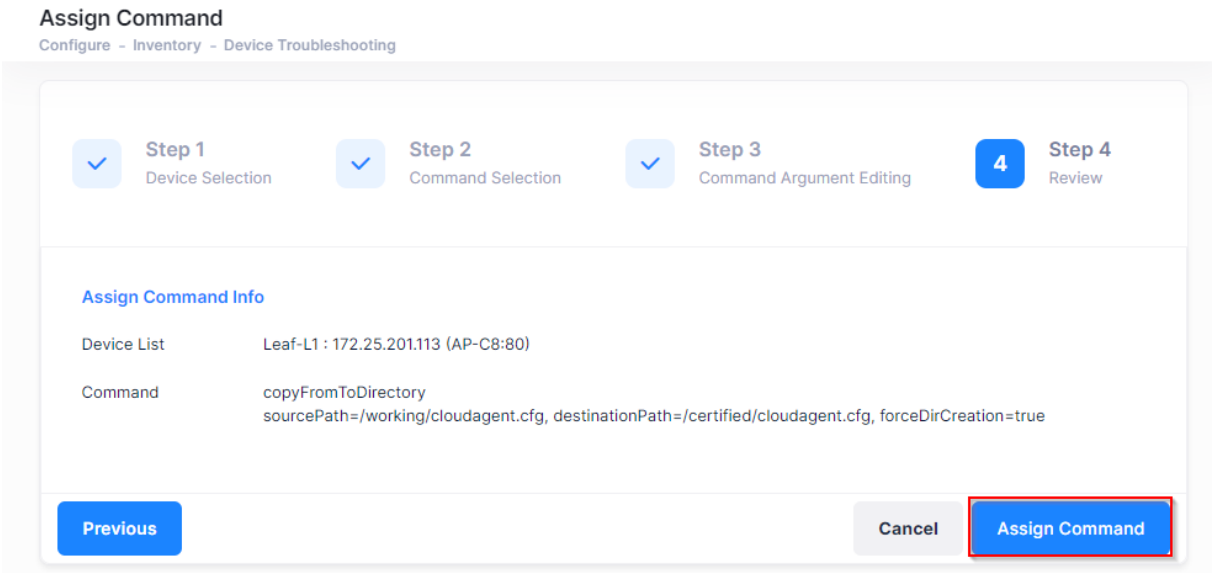


On the Command Argument Editing window, you can do any of the following:

- Click in the "Input Value" field to edit the argument.
- Click on the Delete icon to delete an argument from the command.
- Click on **Add Argument** to define an input parameter name and input value for a new argument.

When you are done editing and/or adding command arguments, click on **Apply** to save your changes.

8.4.1.2.4 4. Review



Review the command details. Click **Previous** to return to a previous step to make changes. Click on **Assign Command** to complete the troubleshooting command assignment. The command will be issued the next time the device calls home.

8.4.1.3 Troubleshooting Commands

The following list of commands can be used to troubleshoot/resolve device problems.

uploadCertificateAndPrivateKey	Upload both the certificate and the private key to the device. This command can be used to backup the certificate and the private key. Each of the arguments are expected to use Json String Escape (https://www.freeformatter.com/json-escape.html#ad-output) to replace newline to '\n' and carriage return to '\r'.
resetDeviceToFactoryDefault	Reset a device to factory default settings. This will remove all the existing configurations on the device.
forceLoadNewCertificateAndPrivateKey	Push a new certificate and private key to a device. This is useful if a certificate has expired or otherwise disappeared from a device. The certificate and private key will be updated on the next "call home". *This command is expected to be used in very rare cases.*
clearCertificateAndPrivateKey	Remove both the certificate and key with the associated base name from a device. This command can be used if the certificate and key on a device have expired or are invalid. This command removes them and updates them on the next "call home". *This command is expected to be used in very rare cases.*
dumpSystemInfo	Generate device information logs that can be used to troubleshoot a device. For example, output information to DFS.
uploadDeviceFile	Upload a device file that can be used for troubleshooting. For example, upload a file from the device to DFS.
copyFromToDirectory	Copy a file from one directory to another directory. This command can be used to backup important files to another folder (e.g., vcboot.cfg, private key, public key).
removeFileFromDirectory	Remove a file(s) from the device. This command can be used to remove large, unnecessary files to free up space on the device (e.g., image.bak file, log file).

clearNTPConfig	Removes all NTP configuration values from the running config and then writes memory. The date is part of the device validation process. This command removes the current NTP and updates the device with a new NTP server.
setDateTime	Force date and time update on the device. The date is part of the device validation process. This command can be used to update date and time on the device.
downloadDeviceFile	Downloads a file from DFS to the device.
rebootFromDirectory	Reboot the device from a specific directory.
certifyDownloadedConfigFile	Certifies the configuration file that was downloaded to the device.
reboot	Reboots the device.

21 Oct 2025

8.4.2 Network Events

The Network Events application provides the following screens to monitor network events and configure event management tasks:

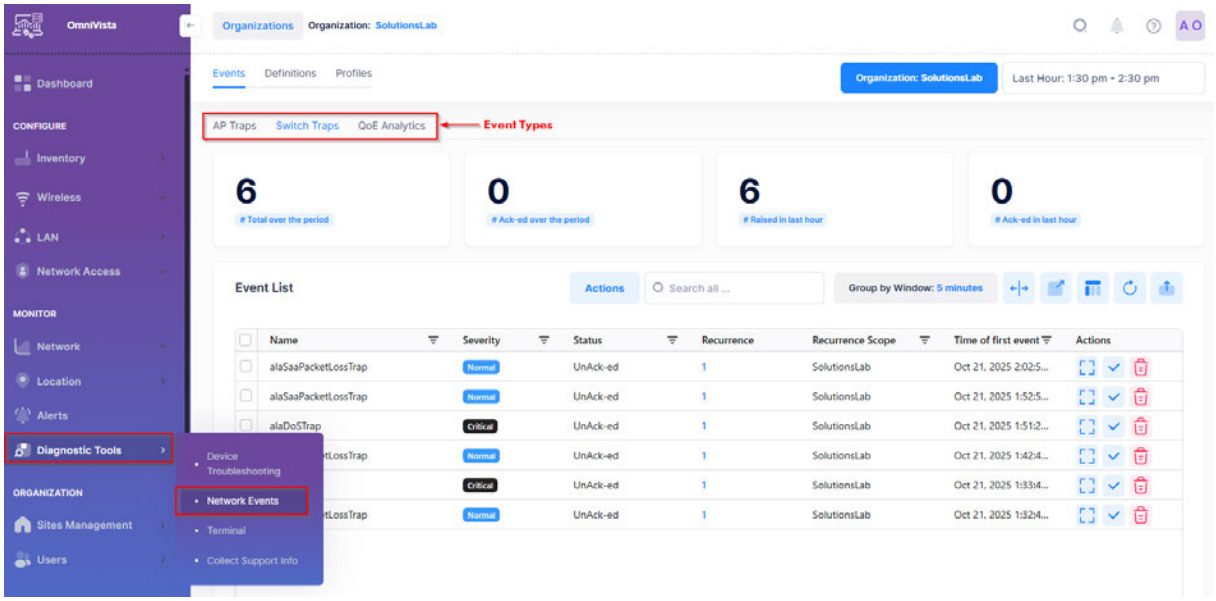
- **Events** (see page 982)- Displays a list of events received over a specific period of time. Can filter the list based on whether to include analytics events (see page 775) (for example, QoE Analytics) or only trap notifications from network devices.
- **Event Definitions** (see page 993) - Provides definitions for supported events received from network devices.
- **Event Responder Profiles** (see page 996)- Used to configure the response (if any) that you want OmniVista Terra to take when a specified event is received. The event can be specified by severity level or through the use of filters. The response can take the form of an e-mail sent to a user-specified address and/or an auto-acknowledgement (auto-ack) of the event.
- **Event Configuration** (see page 1004) - Used to configure network devices to send events to OmniVista Terra. Until you configure events on the network devices, you will not be able to receive or view any event notifications on the Events screen.

21 Oct 2025

8.4.2.1 Using the Network Events Display

The Network Events screen displays configured events received from network devices and provides basic event information (for example, severity, date/time received).

To access the Network Events screen, click on **Diagnostic Tools > Network Events** and select the **Events** tab under the “Monitor” section of the OmniVista Terra Menu (see page 45).



The top section of the Network Events screen provides a summary of event activity during the specified time range based on type of Events. The bottom section of the screen is the Events List, which displays the events (see page 982) received within the specified time range. You can also use the Events list to acknowledge (see page 989) or delete (see page 990) events.

8.4.2.1.1 Viewing the Events List

All event notifications from all devices within the Organization scope and specified timeframe are displayed and updated in real-time. As you scroll the the list of events and a new event is received, a “Click here to view new events” message will appear. Click on the message to return to the top of the list to view the new events.

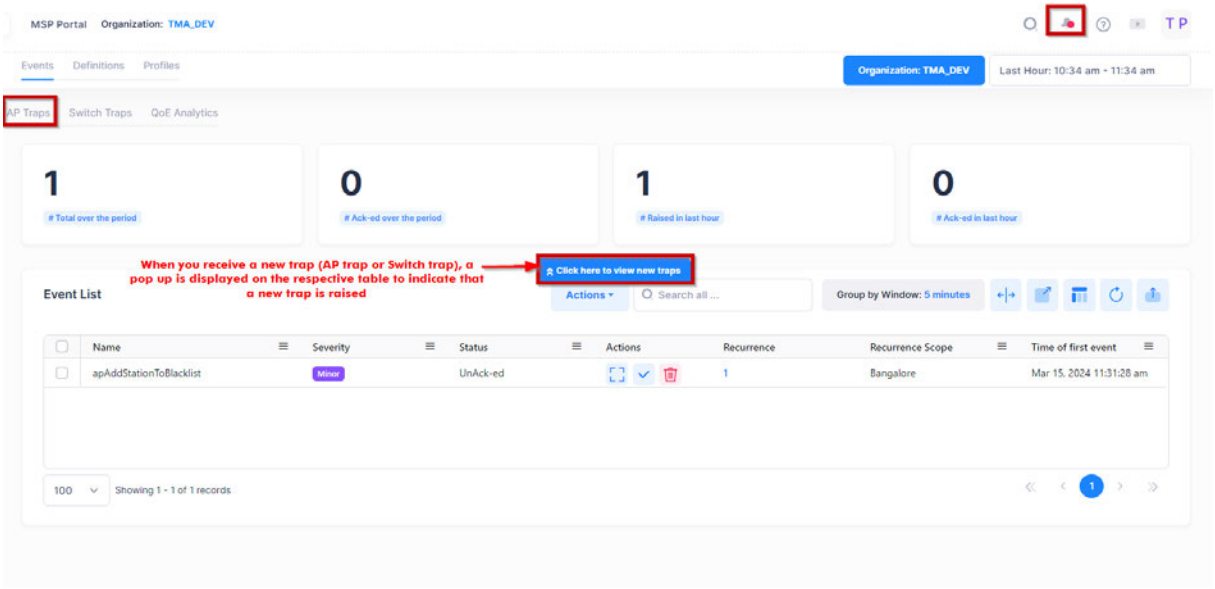
New events received are also indicated when a red blinking dot appears to the top of the bell icon on the Organization banner. For example:

The bell icon provides a list of recent 10 new traps and alerts received. To view the list of traps, click on the bell icon, then on **AP Traps**. A drop-down window displays the list of new Traps and Alerts.

If you click on **See All** at the bottom of the drop-down list, the Network Events screen is displayed.

8.4.2.1.1.1 View New Events Notification

When a new event is received, you will get a pop-up which is displayed on the top of the Event List table to indicate that the new trap (AP trap or Switch trap) has been raised as shown below:



The above pop-up displays only when one of the below criteria is matched:

- Received trap matches the column filters.
- Received trap matches the search filter.
- Received trap falls under the selected scope entity.
- The time filter is selected other than the custom range. (for example, last hour, last 6 hours, etc.)

Note: The red blinking dot on the top of the bell icon displays whenever a new trap is received, irrespective of the mentioned criteria.

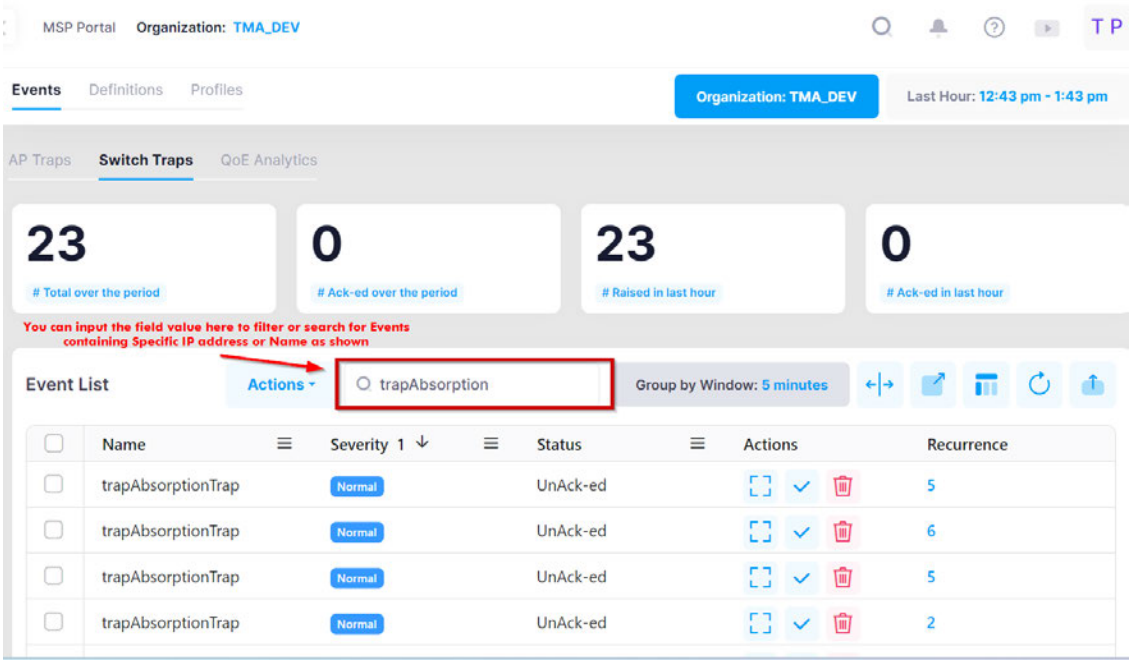
8.4.2.1.1.2 Events List Information

The Events List provides the following information for each event received:

- **Name** - The name of the trap as defined in the respective MIB.
- **Severity** - The severity level (Normal/Warning/Minor/Major/Critical) assigned to the event, as shown on the Events Definitions (see page 993) screen . Note that you can edit the severity level of an event using the Events Definitions screen.
- **Status** - Whether the event is un-acknowledged (**UnAck-ed**) or acknowledged (**Ack-ed**).
- **Recurrence** - The number of times the event was received, from the selected Recurrence Scope, in the selected Group by Window (see page 988) range within the specified time frame. Click on the number in this field to view details for each recurrence of the event type.
- **Recurrence Scope** - Displays events from all devices in the Organization, Site, Building, Floor, or from a specific device. Use the display filter at the top of the Network Events screen to select which one of these entities to view.
- **OID** - The trap object identifier number.
- **Time of first event** - The date and time the event was initially received.

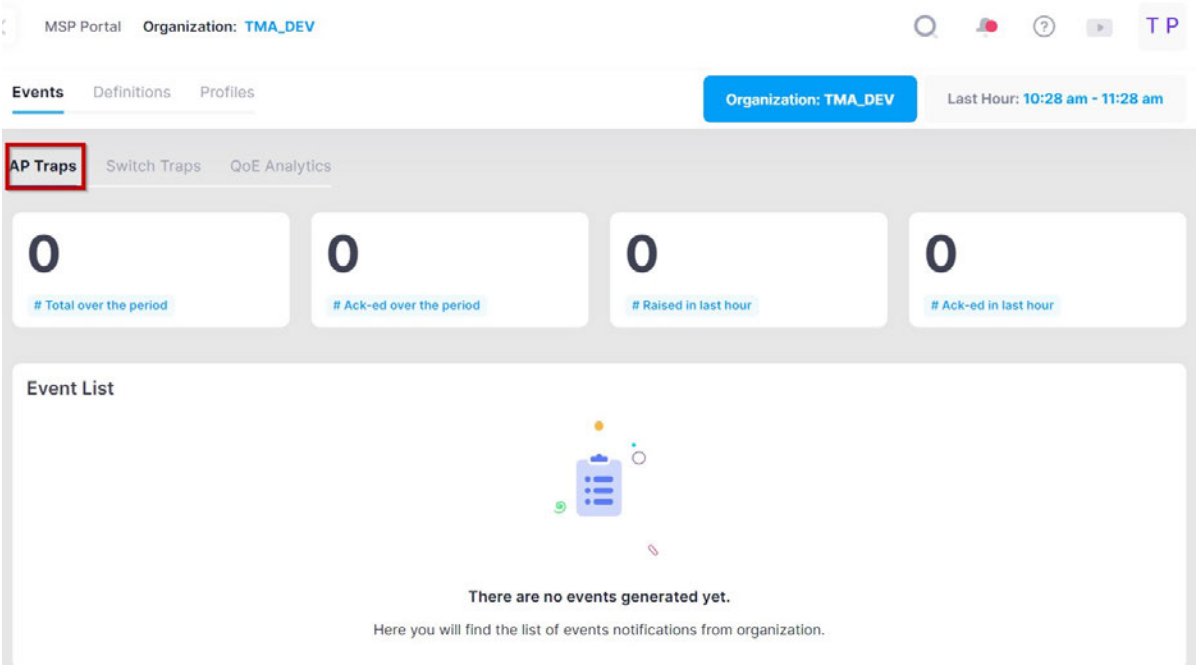
- **Time of latest event** - The date and time the event was last received.

ToolTip : Use the Search box option to view the Events containing a specific Name, Severity, type, Recurrence scope, source IP, synopsis or Client MAC. Usually, the Client MAC doesn't appear in the Event List Table, but the search result will display all such Events containing a specific Client MAC or Source IP as shown below:



8.4.2.1.2 Types of Event Notifications

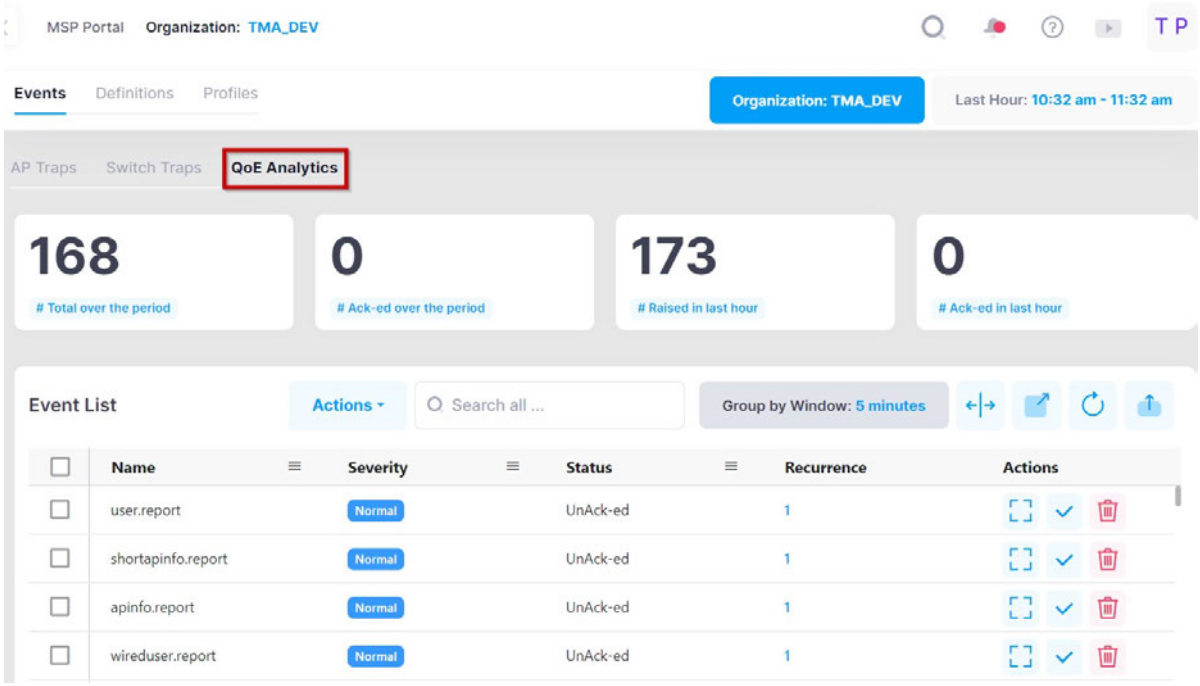
AP Traps - The AP Traps are the notification events from the devices. To access the AP Traps screen, go to **Network Events > Events** and click on **AP Traps** as shown below.



The top section of the **AP Traps** screen provides a summary of Traps activity during the specified time range based on type of Events. The bottom section of the screen is the Events List, which displays the events (see page 982) received within the specified time range.

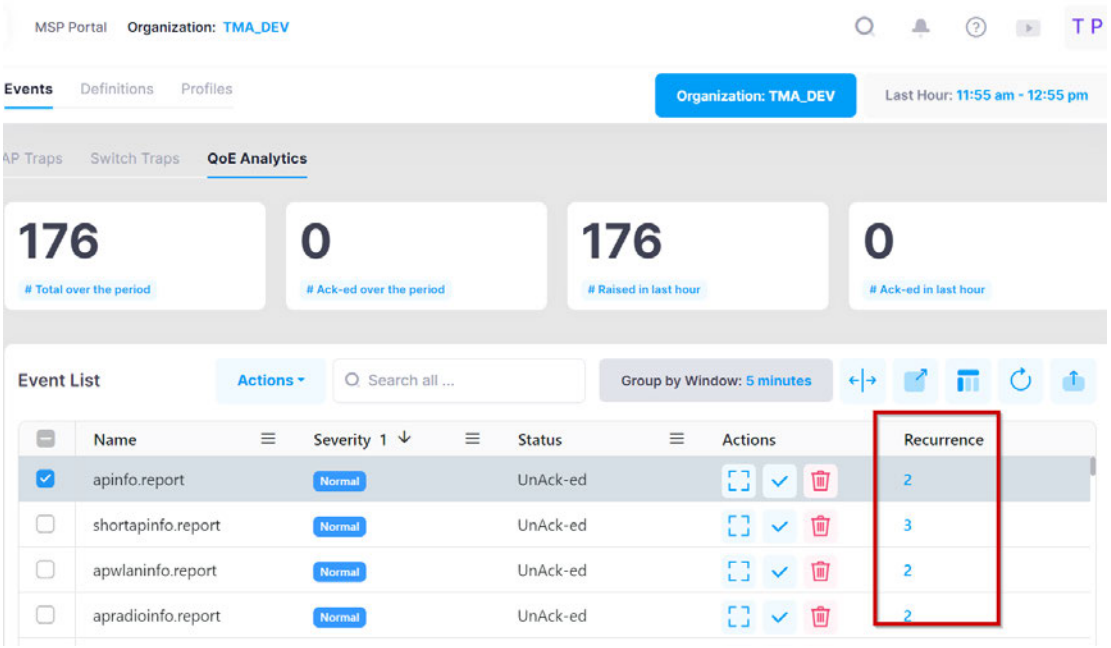
Note: For AP Traps, the maximum time range that you can specify to view Event Notifications is 15 days. You cannot use the custom range option to view Traps metrics for more than 15 days.

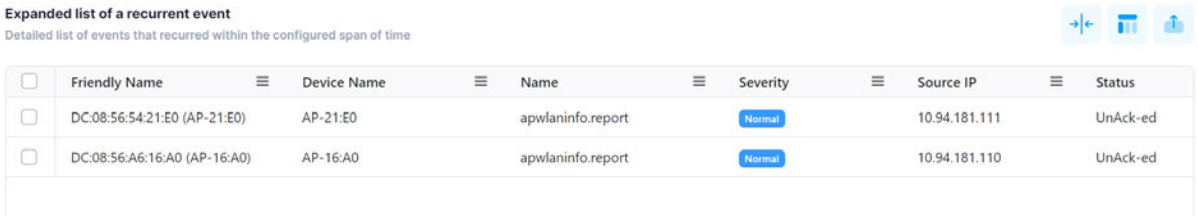
QoE Analytics - The QoE Analytics events are the events from devices that are sent to OmniVista Terra for monitoring and analysis. To access the **QoE Analytics** screen, go to **Network Events** > **Events** and click on **QoE Analytics** as shown below.



The top section of the QoE Analytics screen provides a summary of QoE Analytics activity during the specified time range based on type of Events. The bottom section of the screen is the Events List, which displays the events (see page 982) received within the specified time range.

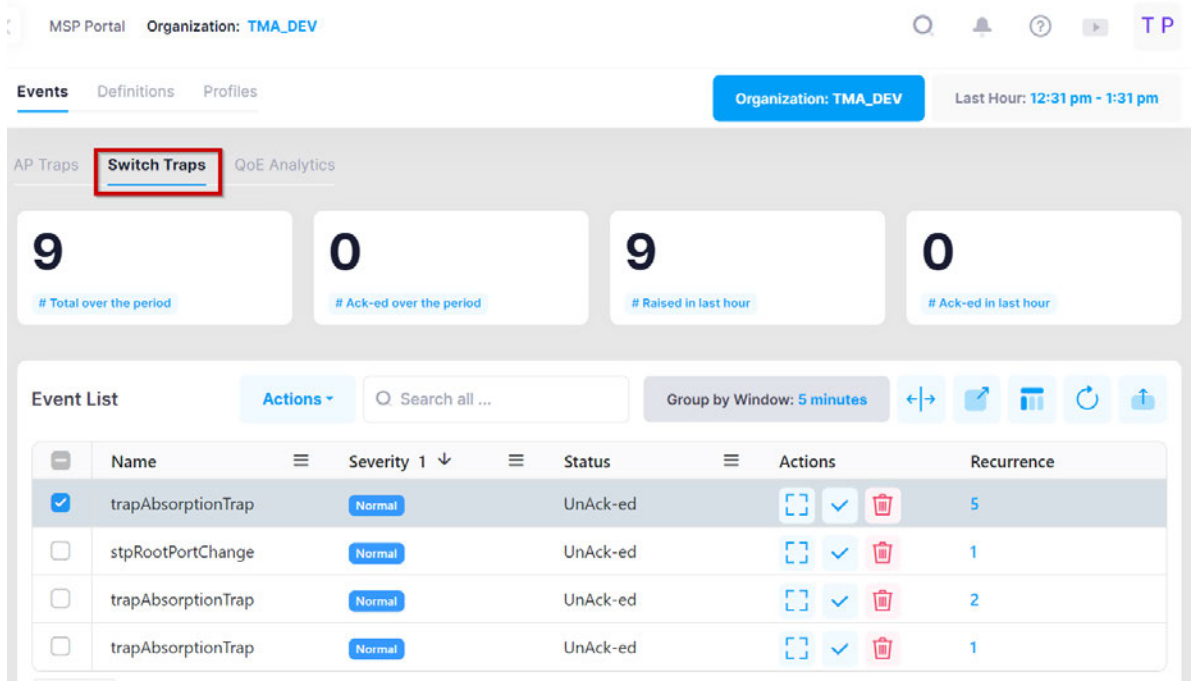
If you want to view the all the occurrences for the Events, then click on the **Recurrence** column and it will redirect you to the detailed list of events that recurred within the configured span of time as shown below.





Note: For QoE Analytics Events, the maximum time period that can be selected in date filter to view Event Notifications is 24 hours.

Switch Traps - The Switch Traps are the notification events from the switches To access the **Switch Traps** screen, go to **Network Events > Events** and click on **Switch Traps** as shown below.



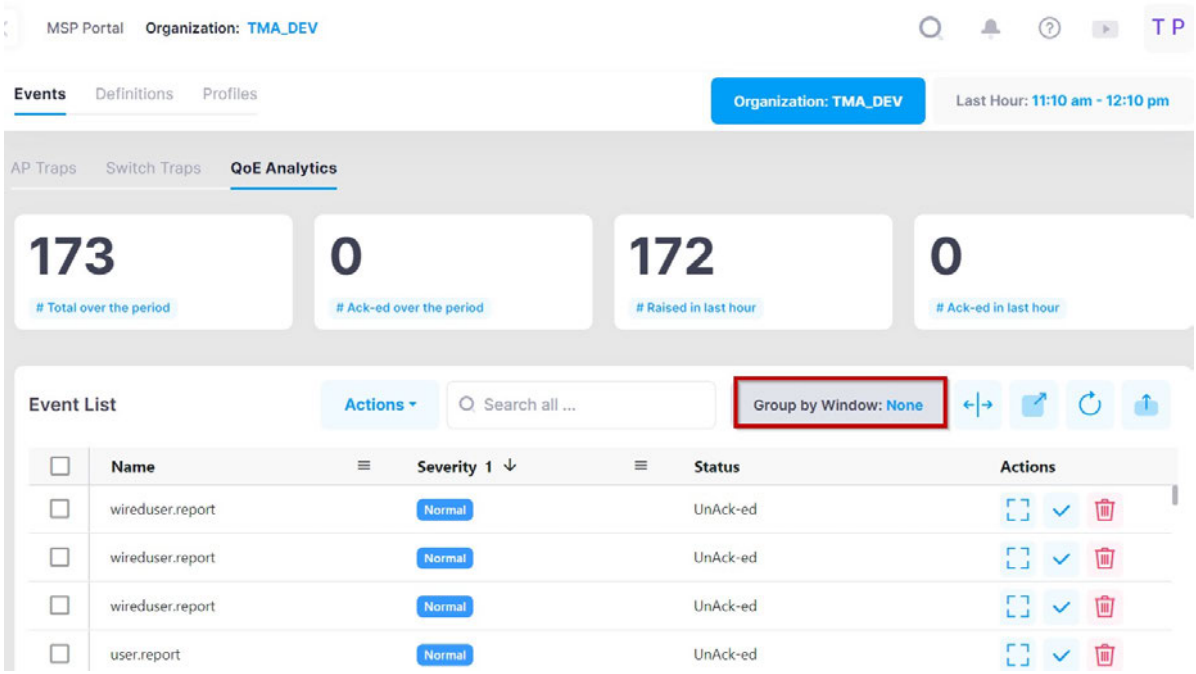
The top section of the Switch Traps screen provides a summary of Traps activity during the specified time range based on type of Events. The bottom section of the screen is the Events List, which displays the events (see page 982) received within the specified time range.

8.4.2.1.2.1 Group by Window

The Group by Window display option allows you to select a range of time during which each type of event received is counted. To select the time range for the Group by Window, click on **Group by Window** and select from 5 minutes (the default) up to 24 hours from the drop-down menu.

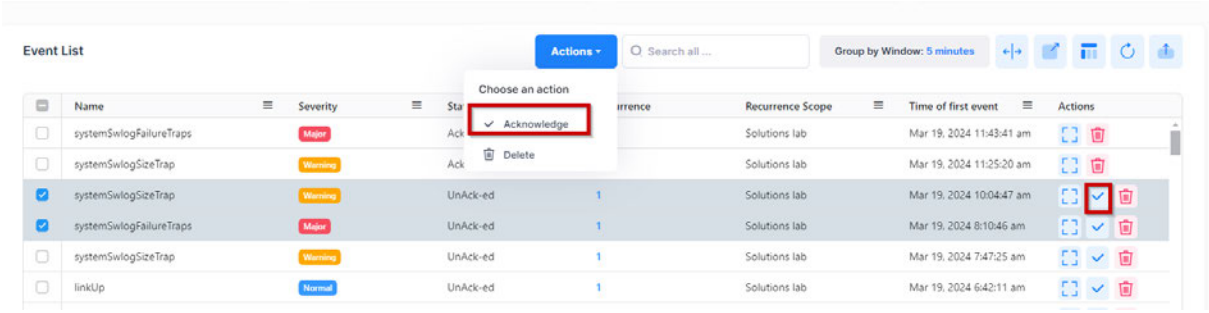
The total number of a specific event type received within the Group by Window range is used to calculate the value reported in the “Recurrence” field. For example, if the Group by Window range is set to 24 hours and the Recurrence number for alert type “Port Auth Failure” is 12, then a “Port Auth Failure” alert was received 12 times during the 24-hour Group by Window range.

If you select the “None” option from the **Group by Window** drop-down menu, then it displays the detail view of the Event List without any grouping of time range as shown below:

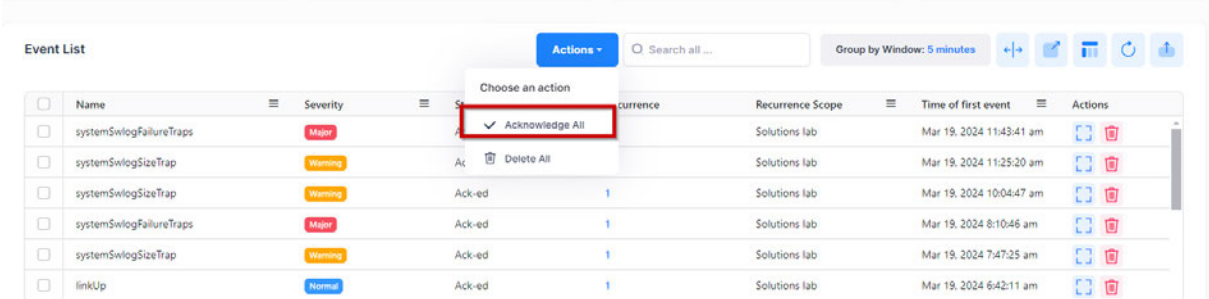


8.4.2.1.3 Acknowledging Events

To acknowledge specific events, select one or more events, then select **Acknowledge** from the drop-down “Actions” menu or click on the checkmark next to the event under the “Actions” column.

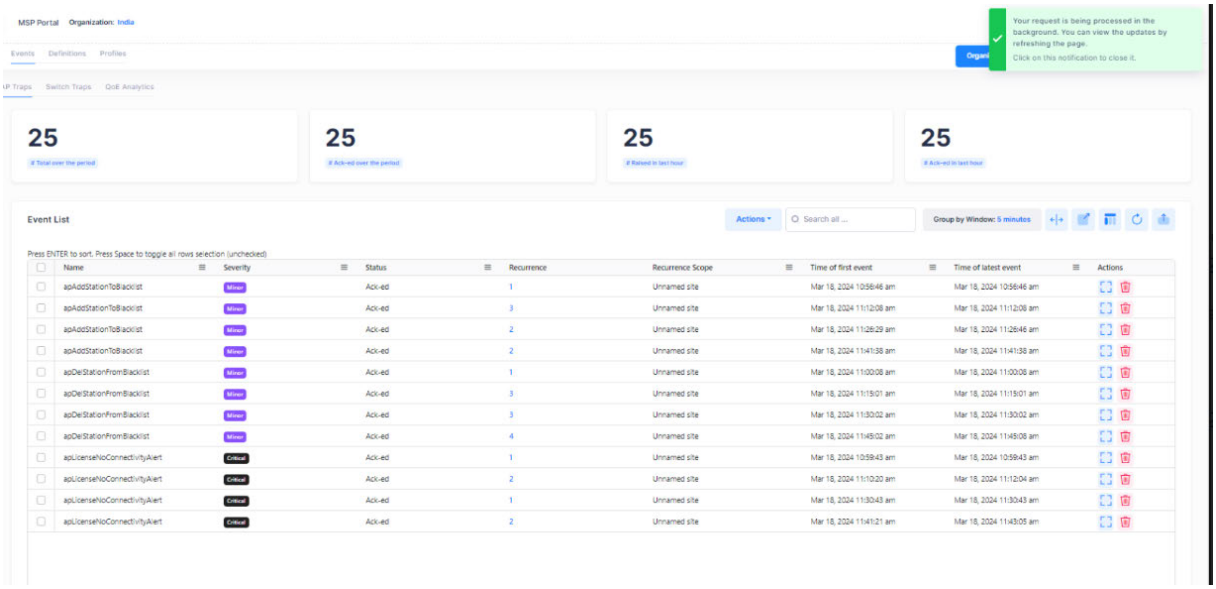


To quickly acknowledge all events, select **Acknowledge All** from the “Actions” drop-down menu. Note that this option is available only when there are no specific events selected within the list.



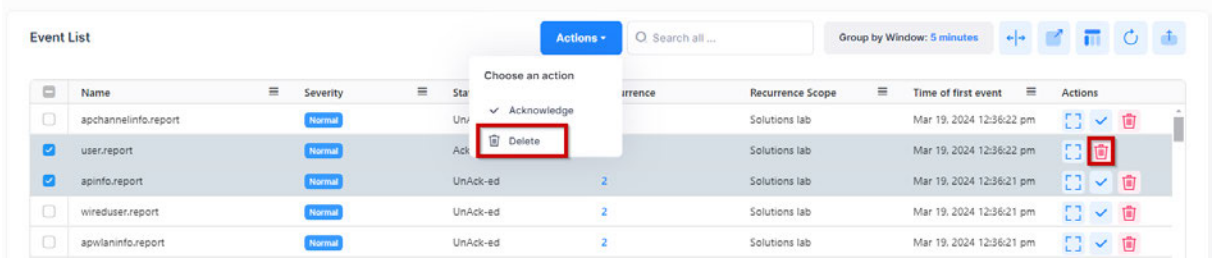
After you acknowledge an event(s), the status for the event(s) changes to **Ack-ed**.

Note: During acknowledge all events, the acknowledge events operation is done in the background. You can view the updated results by clicking on the refresh button at certain time intervals as shown below.

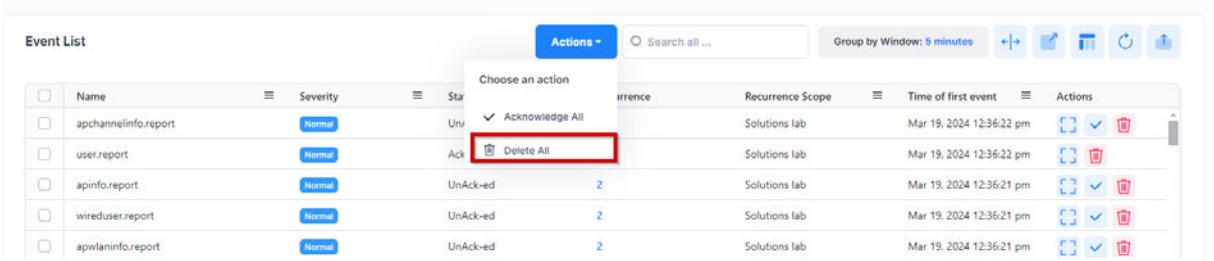


8.4.2.1.4 Deleting Events

To clear specific events from the Events List, select one or more events, then select **Delete** from the “Actions” drop-down menu or click on the Delete icon next to the event under the “Actions” column.



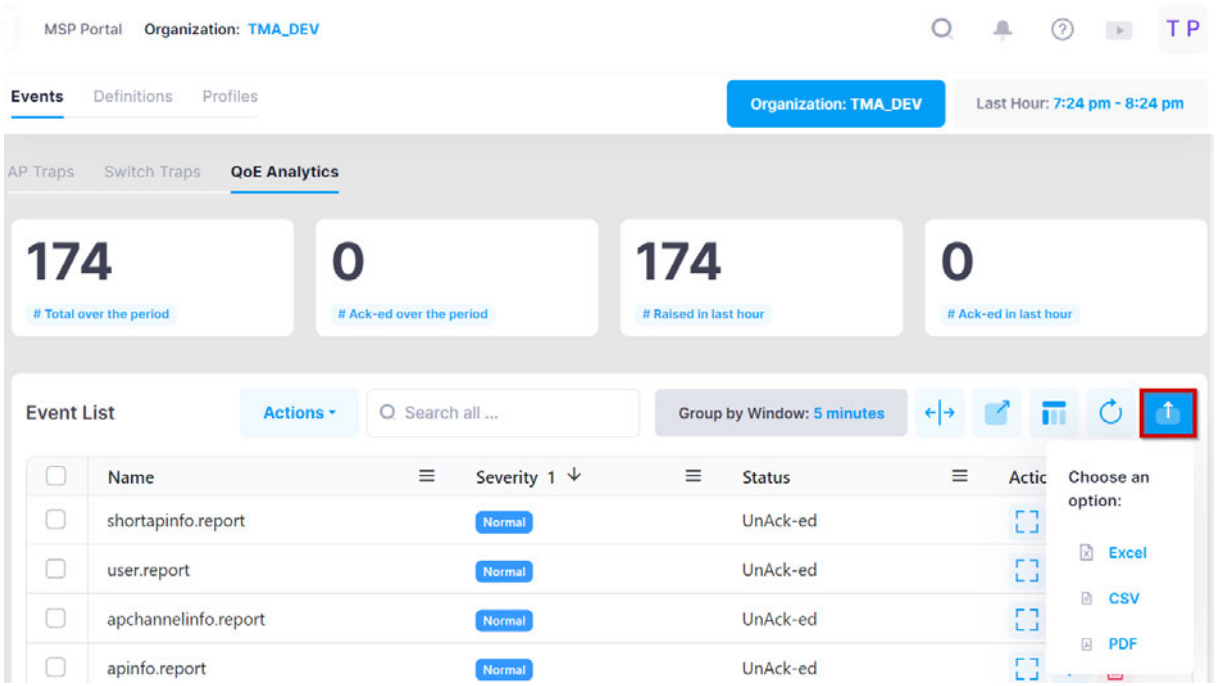
To clear all events from the Events List, select **Delete All** from the “Actions” drop-down menu. Note that this option is available only when there are no specific events selected within the list.



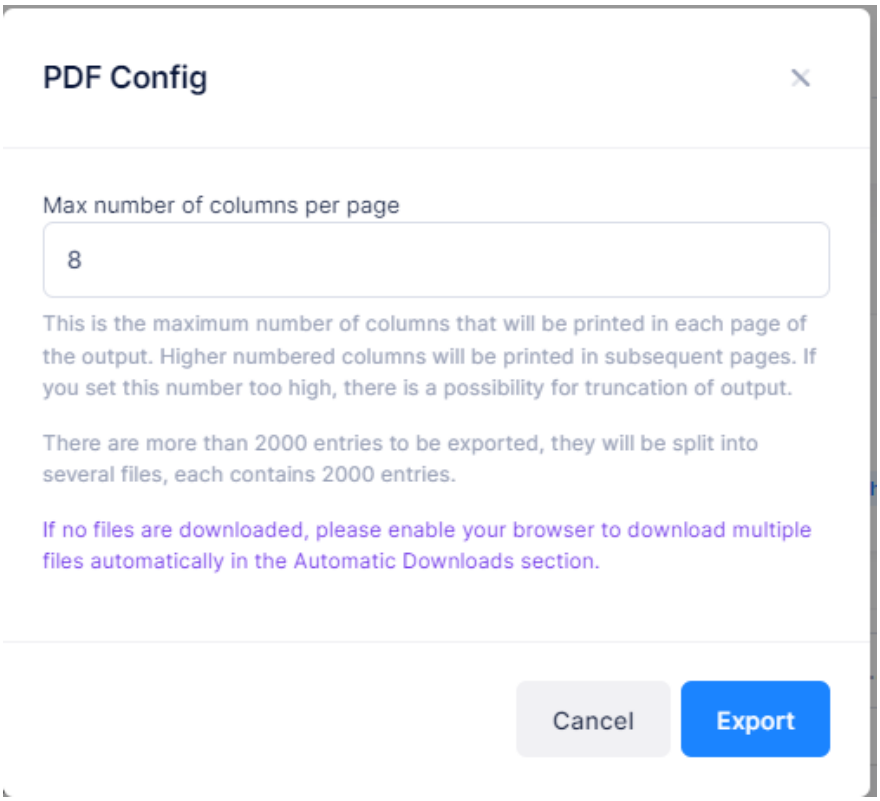
Note: During delete all events, the delete events operation is done in the background. You can view the updated results by clicking on the refresh button at certain time intervals.

8.4.2.1.5 Export Events

To export multiple Events from an existing List, click on the **Export** button and select one of the available options to export the data in an Excel, CSV or PDF file format as shown below.



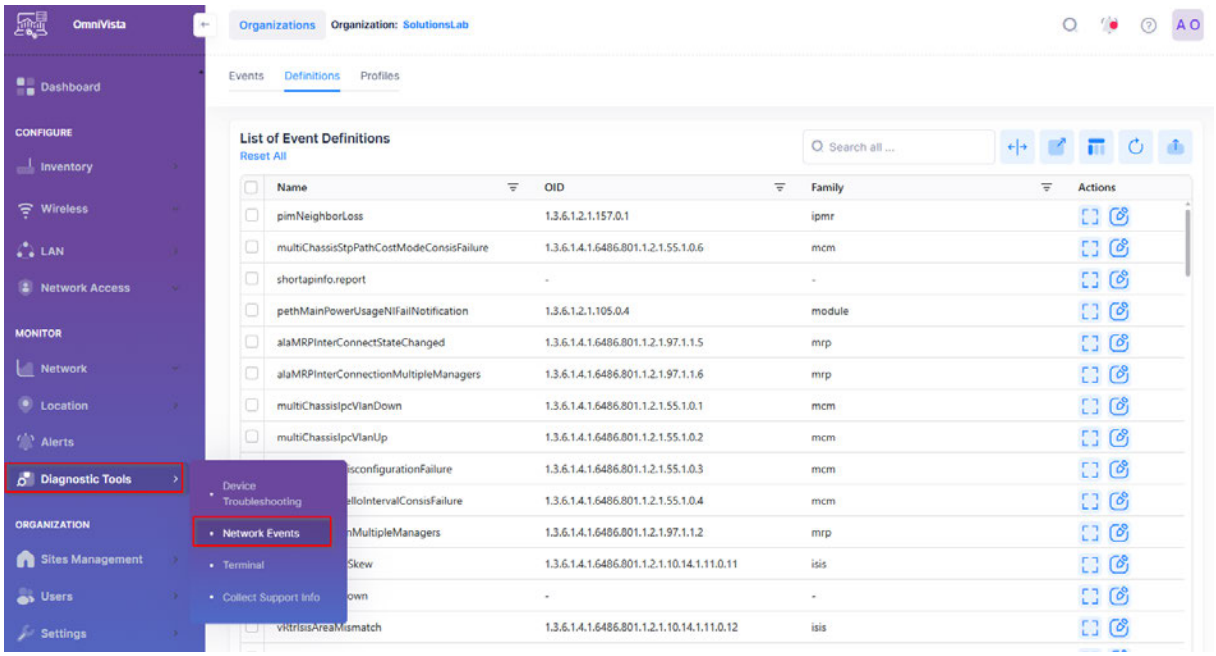
You will then be prompted to a dialog box that displays the notification that if there are more than 2000 entries to be exported, then the data will be split into multiple files, each containing 2000 entries. Also, there is a limitation on the browser level to export only the latest 15,000 data entries for a chosen scope and time.


PDF Config
Max number of columns per page
8
This is the maximum number of columns that will be printed in each page of the output. Higher numbered columns will be printed in subsequent pages. If you set this number too high, there is a possibility for truncation of output.
There are more than 2000 entries to be exported, they will be split into several files, each contains 2000 entries.
If no files are downloaded, please enable your browser to download multiple files automatically in the Automatic Downloads section.
Cancel
Export

21 Oct 2025

8.4.2.2 Event Definitions

The Event Definitions screen displays a list of all supported events and provides a brief description of each event. You can also edit (see page 994)the severity level and trap synopsis for an event. To access the Event Definitions screen, click on **Diagnostic Tools > Network Events** and select **Definitions** tab under the “Monitor” section of the OmniVista Terra Menu (see page 45).



The Event Definitions screen provides a List of Event Definitions that displays basic (see page 993) event information (for example, name, severity level). You can modify the columns displayed in the list by clicking on the Settings icon and adding/removing columns to/from the display. Click on the Additional Information icon under the “Actions” column to display detailed (see page 994) event information. You can also search for events by entering a search criteria (for example, Name, Severity) in the "Search" field. Only those events matching the search criteria are displayed. You can also export the events list to an Excel sheet, CSV, or PDF file. The order of precedence of the Event Definitions are Device, Access Point Group, Site and Organization.

8.4.2.2.1 Basic Event Information

- **Name -** The name of the event.
- **Description** - A description of the event as it appears in the analytics event or trap notification.
- **Severity -** The severity level assigned to the trap in the Notifications Application's Trap Definitions Window (Normal/Warning/Minor/Major/Critical).
- **OID** - It is the trap object identifier number.
- **Type** - The type of event notification:
  - **AP Traps** - Notification events from devices.
  - **QoE Analytics** - Device analytics events sent to OmniVista Terra for monitoring and analysis.
  - **Switch Traps -** Notification events from the Switches.

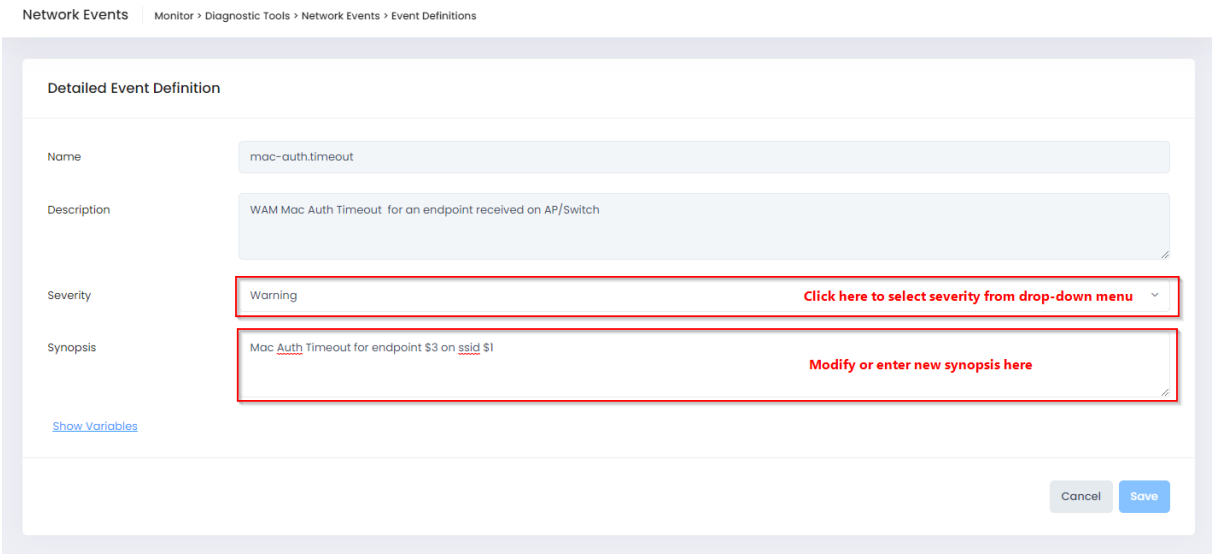
8.4.2.2.2 Additional Information

- **Name -** The name of the event.
- **Description** - A description of the event as it appears in the analytics event or trap notification.
- **Severity -** The severity level assigned to the trap in the Notifications Application's Trap Definitions Window (Normal/Warning/Minor/Major/Critical).
- **Type** - The type of event notification:
  - **AP Traps** - Notification events from devices.
  - **QoE Analytics** - Device analytics events sent to OmniVista Terra for monitoring and analysis.
  - **Switch Traps -** Notification events from the Switches.
- **Definition -** Indicates whether the event is a "Default" event or "Custom" event.
- **Family -** It represents the type of family in which the Switch Traps are classified and divided into functional families.
- **Synopsis** - A brief description of the event. When an event has variables associated with it, the values of some or all of the variables may appear in the synopsis. For example, in the event synopsis "Mac Auth Timeout for endpoint $3 on ssid $1", the $3 and $1 are variable values for the "mac-auth.timeout" event.

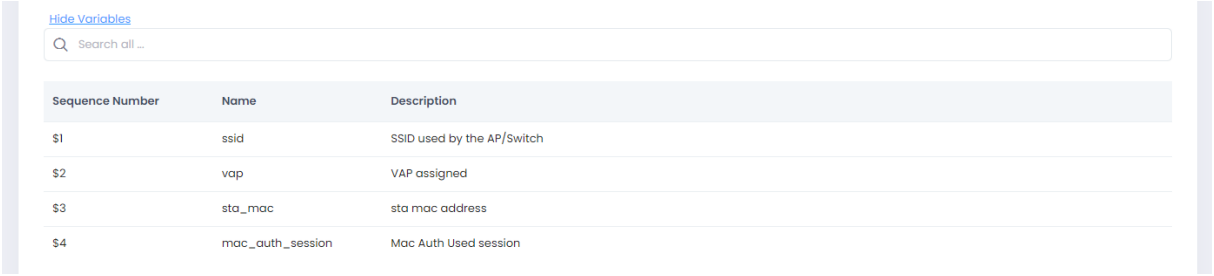
The "Family" column will have empty values for AP Traps and QoE Analytics Events.

8.4.2.2.3 Editing an Event Definition

Note that you can only edit the Severity and Synopsis fields. To edit these field values for an event, select the event in the Event Definition list and click on the Edit icon under the "Actions" column. The Detailed Event Definition screen displays.

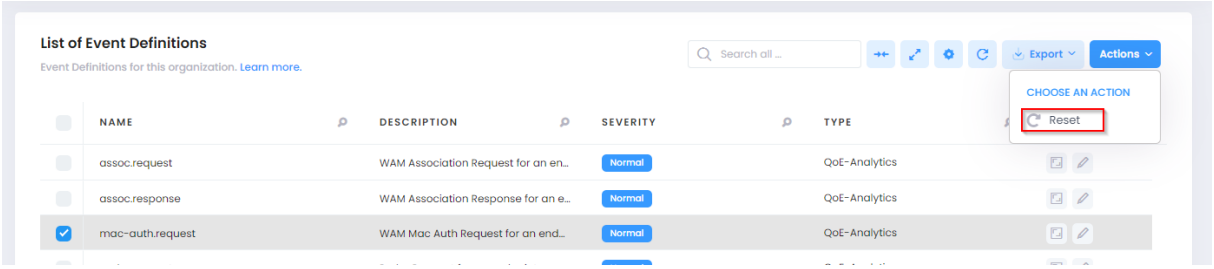


If you want to view the variable definitions for the synopsis, click on **Show Variables**. The Detailed Event Definition screen expands to show the variables.



When you are done making changes, click **Save** to retain your updates and return to the Event Definitions screen.

To restore the default settings for the Severity and Synopsis fields, select the event in the Event Definitions list and click on **Actions**, then click on **Reset**.



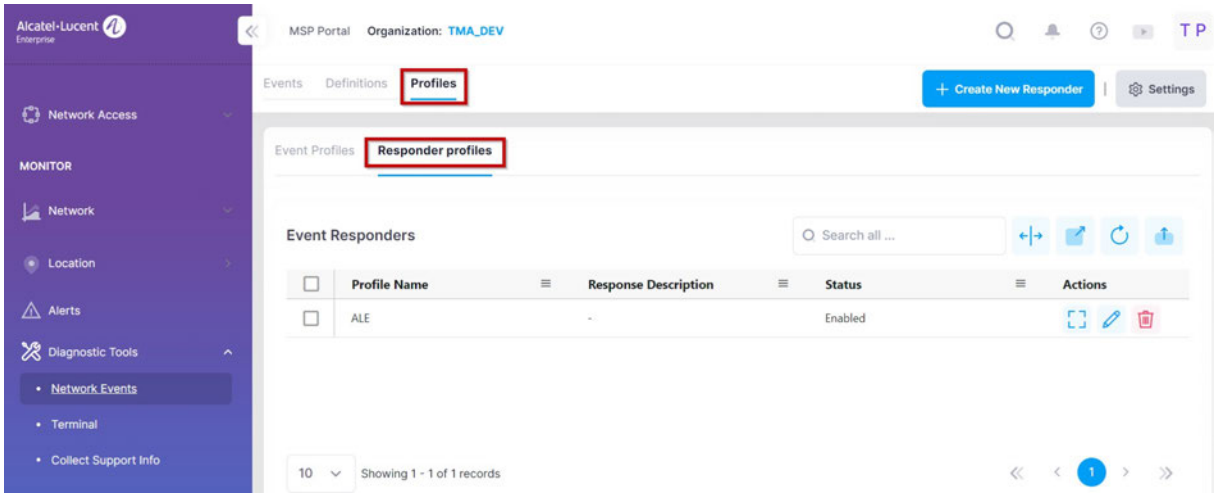
21 Oct 2025

8.4.2.3 Event Responder Profiles

An Event Responder Profile enables you to specify a response (if any) that you want OmniVista Terra to take when specified events are received by OmniVista Terra. You can specify the events to which OmniVista Terra will respond by severity level or with a custom filter. OmniVista Terra can make the following responses to receipt of a specified event:

- OmniVista can send an e-mail to any address you specify. The e-mail can include the information you want in the email through the use of variables. Variables exist for information such as the event name, synopsis, description, etc..
- Automatically acknowledge the traps.

To access the Event Responder profiles screen, click on **Diagnostic Tools > Network Events** and select **Profiles > Responder profiles** tab under the “Monitor” section of the OmniVista Terra Menu (see page 45).



The Event Responders screen displays all configured event responders, and is used to create (see page 996), edit, or delete Event Responder.

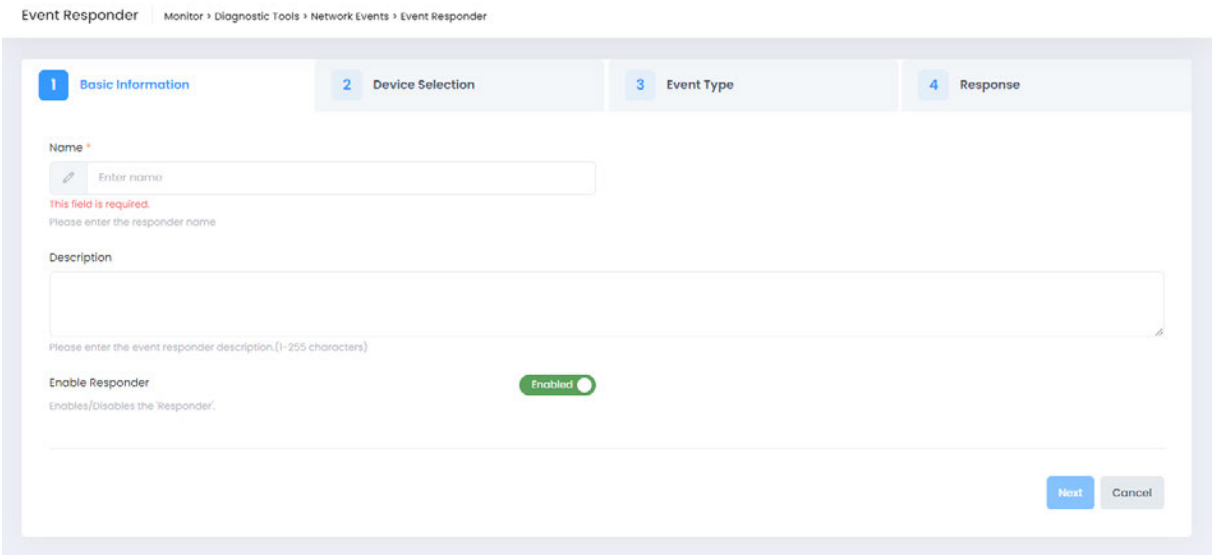
8.4.2.3.1 Creating an Event Responder

To configure an Event Responder, click **Create Event Responder** on the Event Responder screen. An Event Responder Wizard opens to walk you through the following configuration steps:

1. **Basic Information** (see page 997) - Enter a name, an optional description, and enable/disable the Responder.
2. **Device Selection** (see page 997) - Select the devices (AP or Switch) for the Responder configuration. The Responder will respond only if events are received from these devices.
3. **Event Type** (see page 998) - Specify the events to which OmniVista Terra will respond by severity level or by selected custom filters.
4. **Response** (see page 1000)- Select one or both of the following actions that the Responder will take when an event matching the Responder criteria is received:
    a. Send an e-mail response to a specified recipient.

b. Automatically acknowledge the events.

8.4.2.3.1.1 1. Basic Information

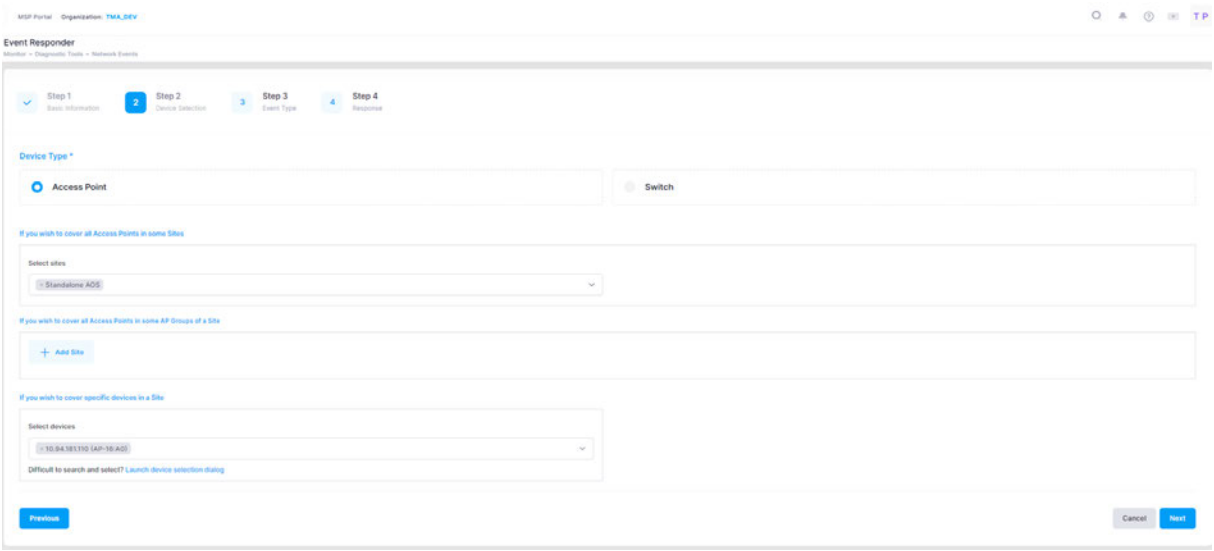


Complete the fields as described below, then click **Next** to move to Step 2:

- **Name** - The name to assign to the Responder.
- **Description** - An optional description.
- **Event Responder** - Enable (the default) or disable the Responder action. If Responder is disabled, no response action is taken.

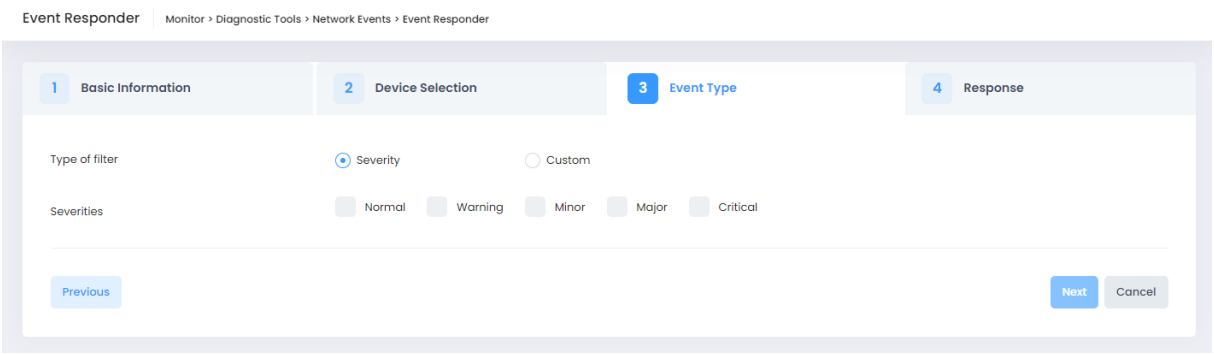
> Note: Only 8 responders can be enabled for an Organization.

8.4.2.3.1.2 2. Device Selection



Select the Switch or Access Point Groups to which a response is sent. If the user want to cover all the Access Points or Devices, then select the sites from the drop-down menu list. The Responder will only send a response to device events sent from the selected devices. To pick devices from a list of devices, click on “Launch device selection dialog”. A Device Selection window opens from which you can select the devices for upgrade. Once devices are selected, click on **Next** to move to Step 3.

8.4.2.3.1.3 3. Event Type

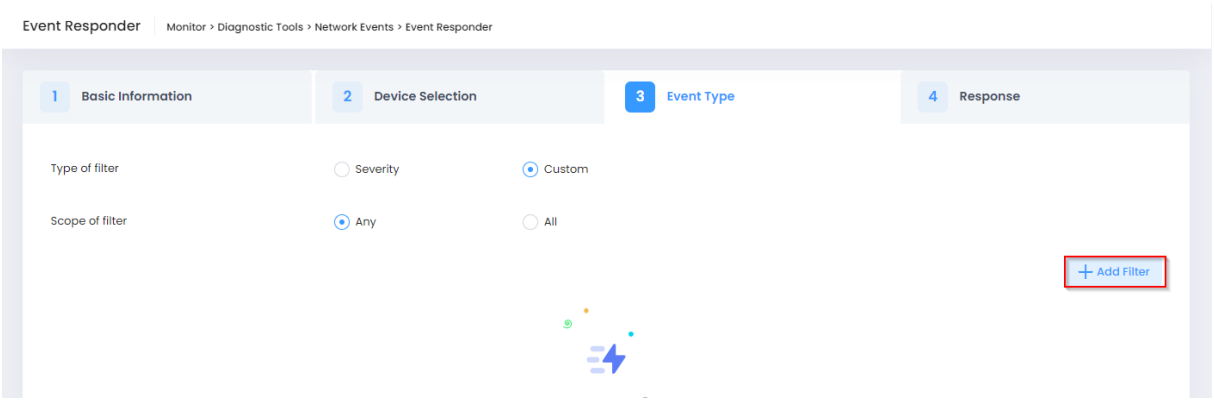


Specify the type of events to respond to by selecting one of the following two filter options:

- **Severity** - Respond only to events that match the selected severity levels.
- **Custom** - Define a custom filter to specify the event criteria that will trigger a response.

Creating a Custom Filter

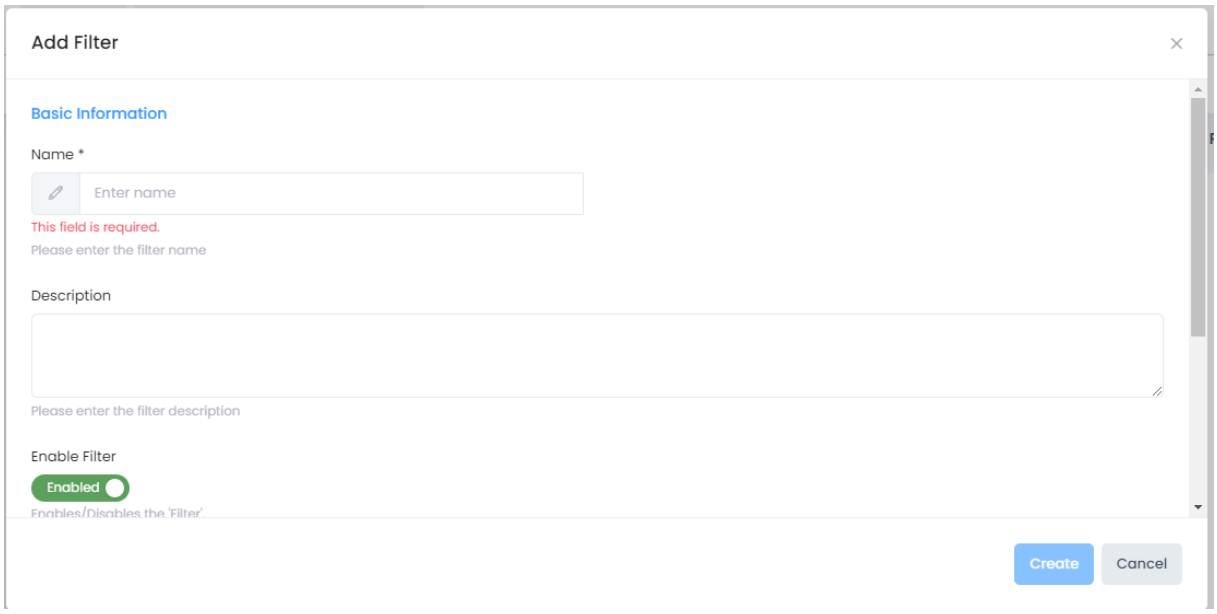
When you select **Custom** for the Type of Filter, the Event Type screen prompts you to select the scope of the filter and provides an **Add Filter** button to define a custom filter.



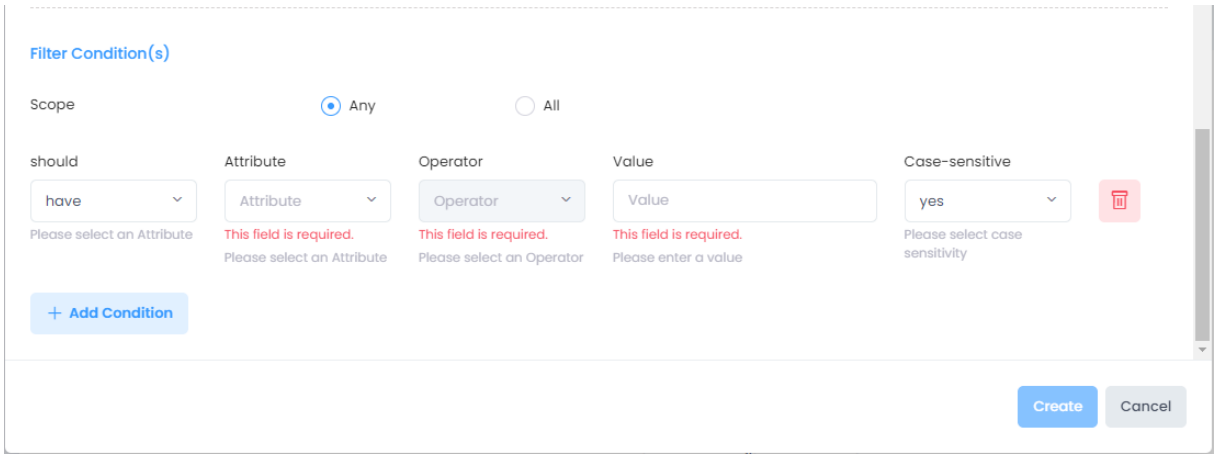
Select the filter scope by clicking on **Any** or **All**:

- **Any** - Respond to any event received from the specified devices that matches *any* of the custom filters.
- **All** - Respond to any event received from the specified devices that matches *all* of the custom filters.

Click on **Add Filter** to open the Add Filter form, which consists of a Basic Information section and a Filter Condition(s) section.



In the Basic Information section, enter a name for the custom filter and an optional description. You can also change the status of the filter (enabled by default) by clicking on the Enable Filter slider.

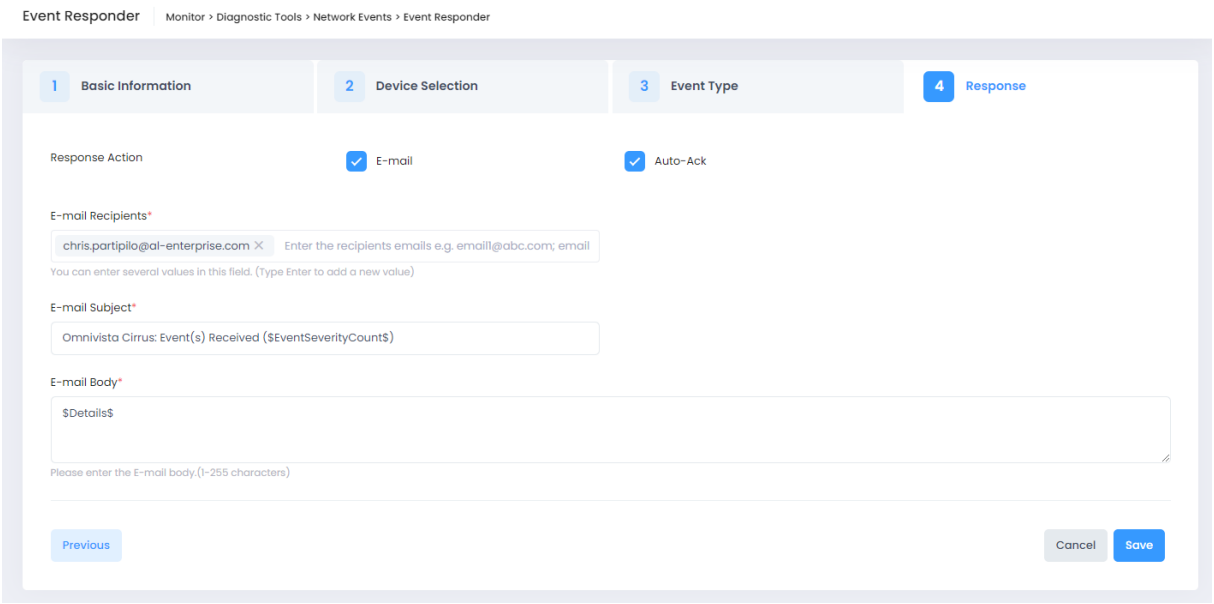


In the Filter Condition(S) section, complete the following tasks:

- Select the Scope (**Any** or **All**) then click on **Add Condition**.
- Define the condition using the fields provided. If you want to define another condition, click on **Add Condition again.**

When you are done defining all the filter conditions that you want, click **Create**. The Add Filter form closes and your custom filters are displayed on the Event Type tab. Click **Next** to move to Step 4.

8.4.2.3.1.4 4. Response



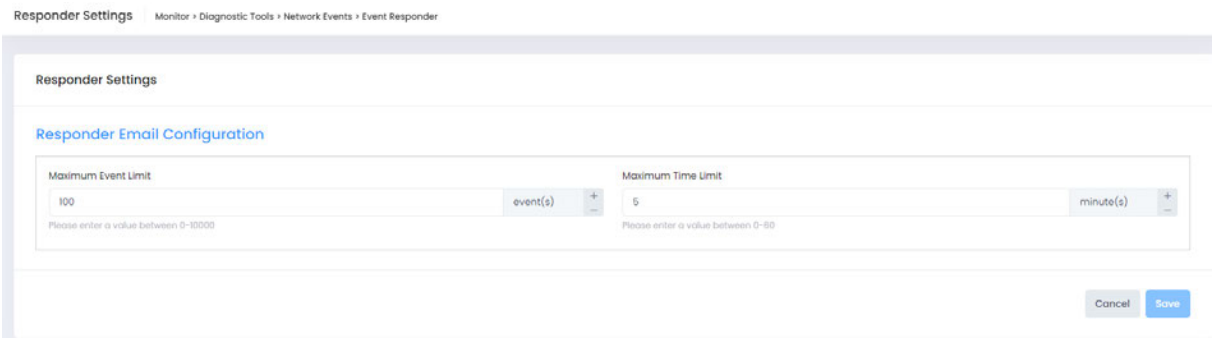
Response Action - Select one or both of the following options to configure the response to events matching the specified criteria:

- **E-mail** - The Event Responder will automatically send an e-mail. The configurable Responder Settings (see page 1000) determine when the email response is sent. When this option is selected, you are prompted to complete the following e-mail parameters:
  - **E-mail Recipients** - Enter an e-mail address(es). Multiple e-mail addresses must be separated by a semi-colon (e.g., john.smith@al-enterprise.com; jane.sullivan@al-enterprise.com).
  - **E-mail Subject** - By default, the following is included in the E-Mail Subject Line: "OmniVista: Trap(s) Received $TrapSeverityCount$" (explained in the Event Variables (see page 1001) section). You can also enter any additional information you want to include in the subject line.
  - **E-mail Body** - By default the variable $Details$ (explained in the Event Variables (see page 1001) section) is included in the body of the e-mail. The variable automatically includes event details in the body of the e-mail. You can also enter any additional information you want to include in the e-mail.
- **Auto-Ack** - The Event Responder will automatically acknowledge the events.

When you are finished, click **Save** to return to the Event Responder screen. The Event Responder you just created will appear in the Event Responder List.

Responder Settings

If you want to adjust when an email response is sent, click on **Settings** on the Event Responder screen to open the Responder Settings screen.



By default, the maximum event limit is set to 100 events and the maximum time limit is set to 5 minutes. This means that 5 minutes after the first event is sent, OmniVista Terra will send an email response if no other response was sent during that time or 100 events were received before the 5 minutes is up.

Change the Maximum Event Limit and/or the Maximum Time Limit, if necessary, then click **Save** to retain the changes. Note that the event and time limit values are maintained at the Organization level.

Event Variables

You can use the following variables when you configure an automatic event responder. There are two types of variables: generic variables and event-specific variables

Generic Variables

$Details$
For events, this variable is equivalent to the following combination of text and event-specific variables (event-specific variables are described in the following section):

Event Received: $EventName$
Type: $EventType$
Severity: $Event Severity$
Synopsis: $EventSynopsis$

Output Example:
Event Received: wireduser report
Type: QoE-Analytics
Severity: Normal
Synopsis: Wired User Report

Type
The value of type will be based on events type.

For QoE events, Type = QoE-Analytics.

For traps, Type = traps.

$Synopsis$
For events, this variable is equivalent to the event-specific variable $EventSynopsis$ which is a brief description of the event.

Event Specific Variables

$EventCount$
Total count of events that match the responder conditions/filters.

Output Example: **75**

$EventSeverityCount$
A summary of the trap severity counts.

Output Example: **3 Major, 1 Minor, 8 Warnings.**

$EventName$
The name of the Event (as defined in the Event definition).

Output Example: **apAddStationToBlacklist**

$EventSynopsis$
A brief description of the event.

Output Example: **A station (apStaMAC: XX:XX:XX:XX:XX:XX) has been added to Blacklist.**

$EventSeverity$
The severity level assigned to the event in the Network Events application's Event Definitions page. The severity level can be Normal, Warning, Minor, Major, or Critical.

Output Example: **Minor**

$EventType$
It is based on type of event. Type can be QoE-Analytics, Traps.

Output Example: **QoE Analytics**

$EventDeviceSiteName$
The name of the site that device configured.

Output Example: **Calabases**

$EventDeviceMacAddress$
The Mac Address of the device that generated the event

Output Example: **XX:XX:XX:XX:XX:XX**

$EventDeviceIP$
The IP address of the device that generated the event.

Output Example: **127.0.0.1**

$EventDeviceIPV6$
The v6 address of the device that generated event.

Output Example: **2001:db8:3333:4444:5555:6666:7777:8888**

$EventDeviceUploadTime$
The time of the event that generated by the device.

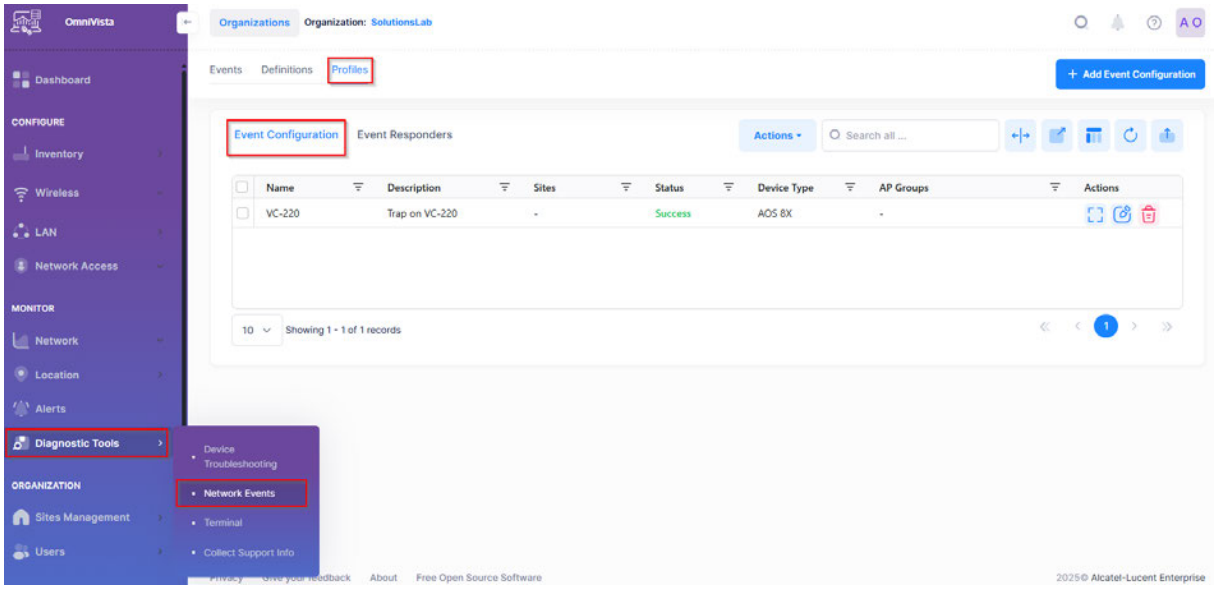
Output Example: **2023-02-28T07:39:26.597Z**

21 Oct 2025

8.4.2.4 Event Configuration

The Event Configuration screen is used to configure network devices to send events to OmniVista Terra and displays a list of existing event configurations. Note that until you configure events on network devices, you will not be able to receive or view any event notifications on the Events (see page 981)screen.

To access the Event Configuration screen, click on **Diagnostic Tools > Network Events** and select **Profiles > Event Profiles** tab under the “Monitor” section of the OmniVista Terra Menu (see page 45).



8.4.2.4.1 Create an Event Configuration

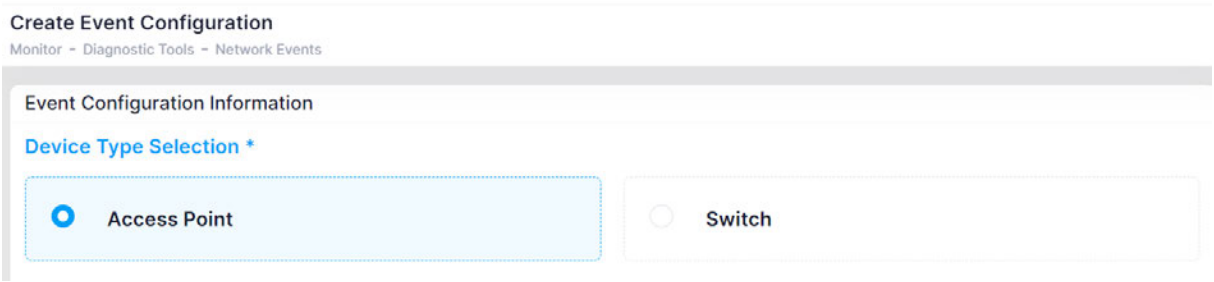
Creating an event configuration is a two-part process: first you select the devices (see page 1006) for which you want to configure events, then you specify the events (see page 1006) you want to be sent to the OmniVista Terra. At the end of the process, the event configuration is then pushed to a device after the devices reboots.

> Configuring events is supported only on devices that are fully managed (see page 170) by OmniVista Terra.

To create an event configuration, click on **Add Event Configuration** on the Event Configuration screen. The Create Event Configuration screen opens from which you can enter the device type selection (see page 1005). Use one of the following procedures for configuring events based on the type of device selected (Access Point or Switch):

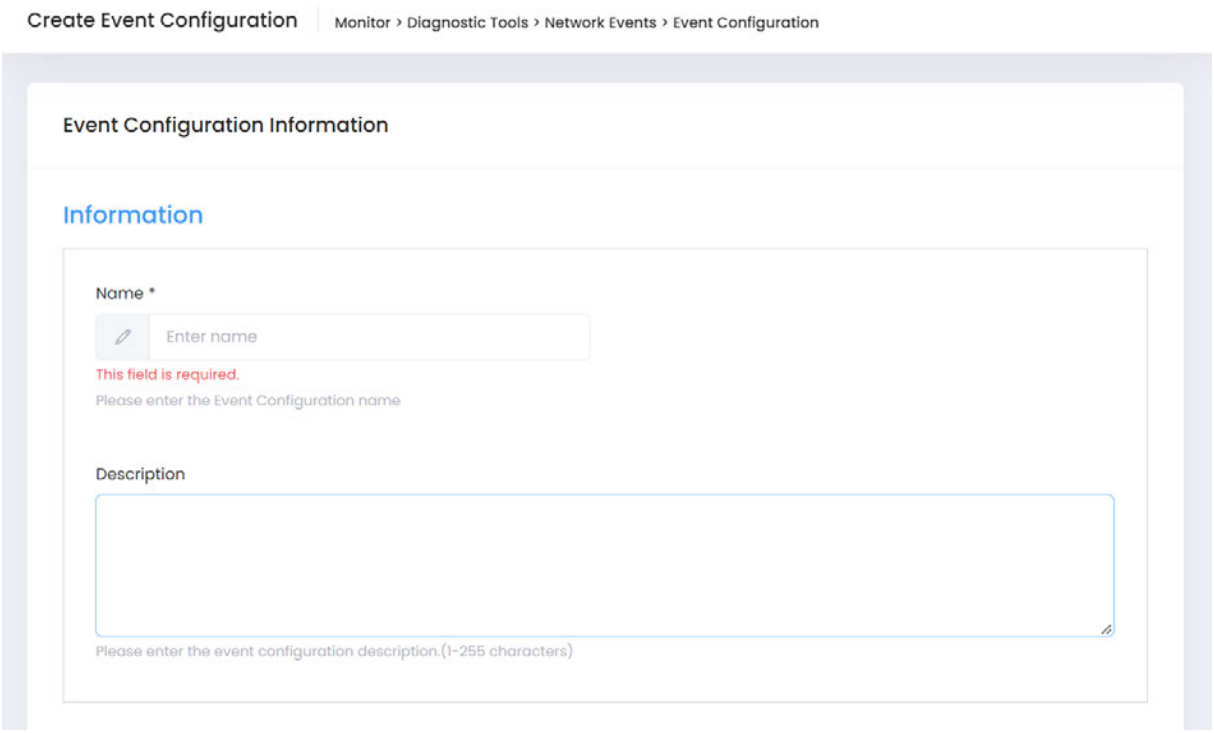
- **Access Point** - follow identifying information (see page 1005), select devices (see page 1006), and select events (see page 1006) to complete the Event Configuration on the devices.
- **Switch -** follow identifying information (see page 1005), switch selection (see page 1008), and configure traps (see page 1004) to complete the Event Configuration.

8.4.2.4.1.1 Step 1. Device Type Selection



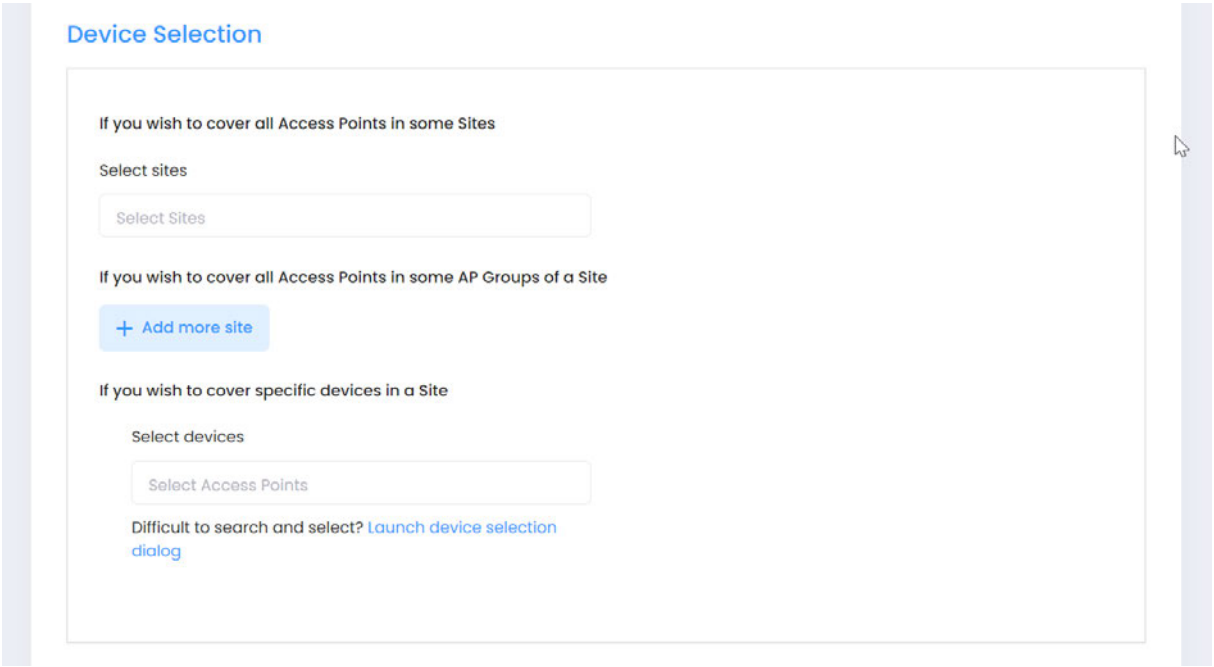
Select the Device type from the above (**Access Point** or **Switch**) for which you want to create a profile.

8.4.2.4.1.2 Step 2. Information



Enter a name to assign to the event configuration and an optional description.

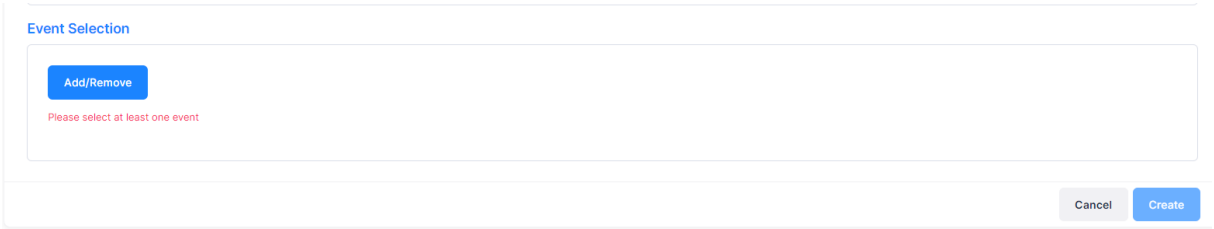
8.4.2.4.1.3 Step 3. Device Selection



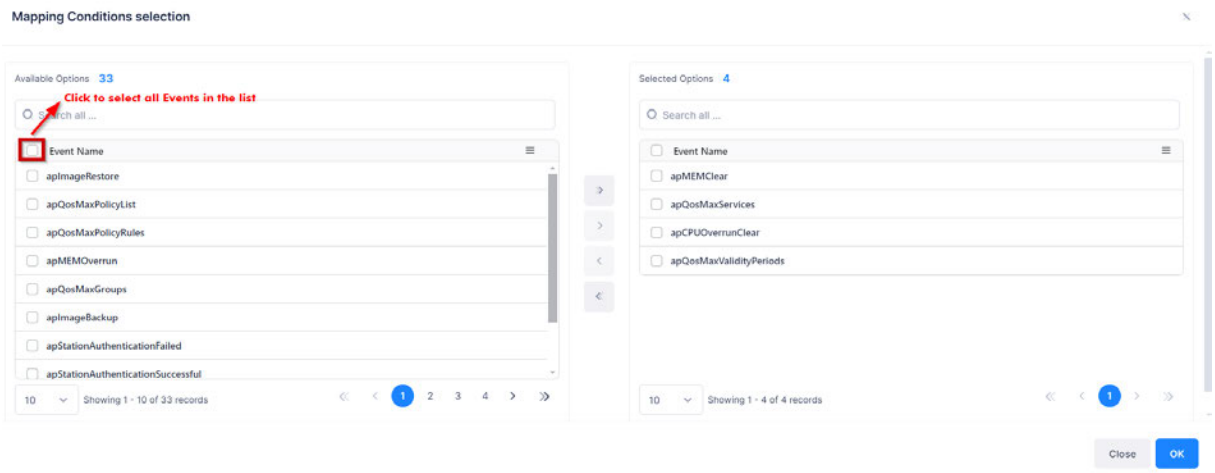
Select devices for which you want to configure events using one or more of the following methods:

- **Select sites** - Click on this field to display a list of Sites for the Organization. Select the desired Site from the drop-down menu. The event configuration will be applied to all Access Points in all AP Groups associated with the Site.
- **Select some AP Groups** - Click on **Add more site** to select some AP Groups from a specific Site. The event configuration is applied only to the Access Points in the selected AP Groups from the selected Site.
- **Select devices** - Click on this field to display a list of devices. Select the device from the drop-down menu. Repeat this action for each device you want to select. To pick devices from a list of devices, click on “Launch device selection dialog”. A Device Selection window opens from which you can select devices.

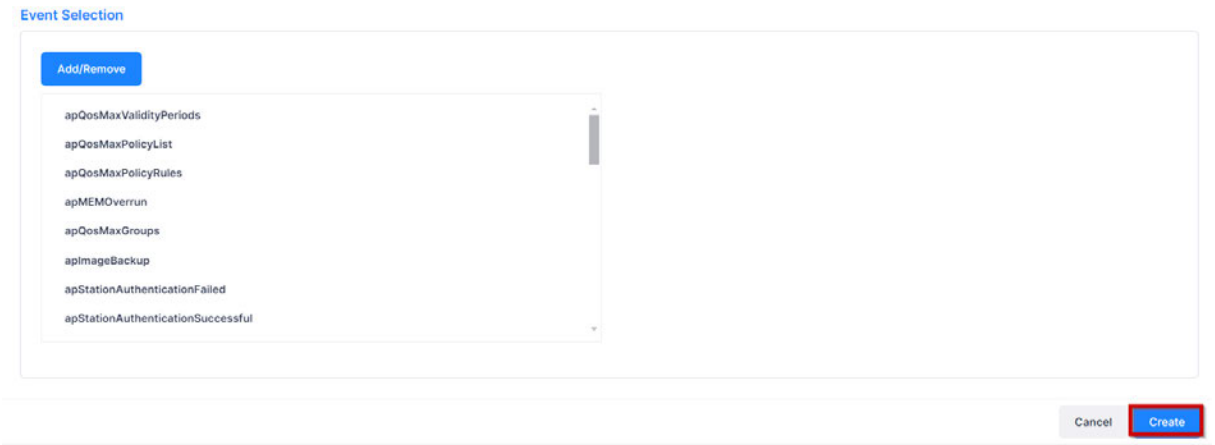
8.4.2.4.1.4 Step 4. Event Selection



Click on **Add/Remove** to open the events selection window.



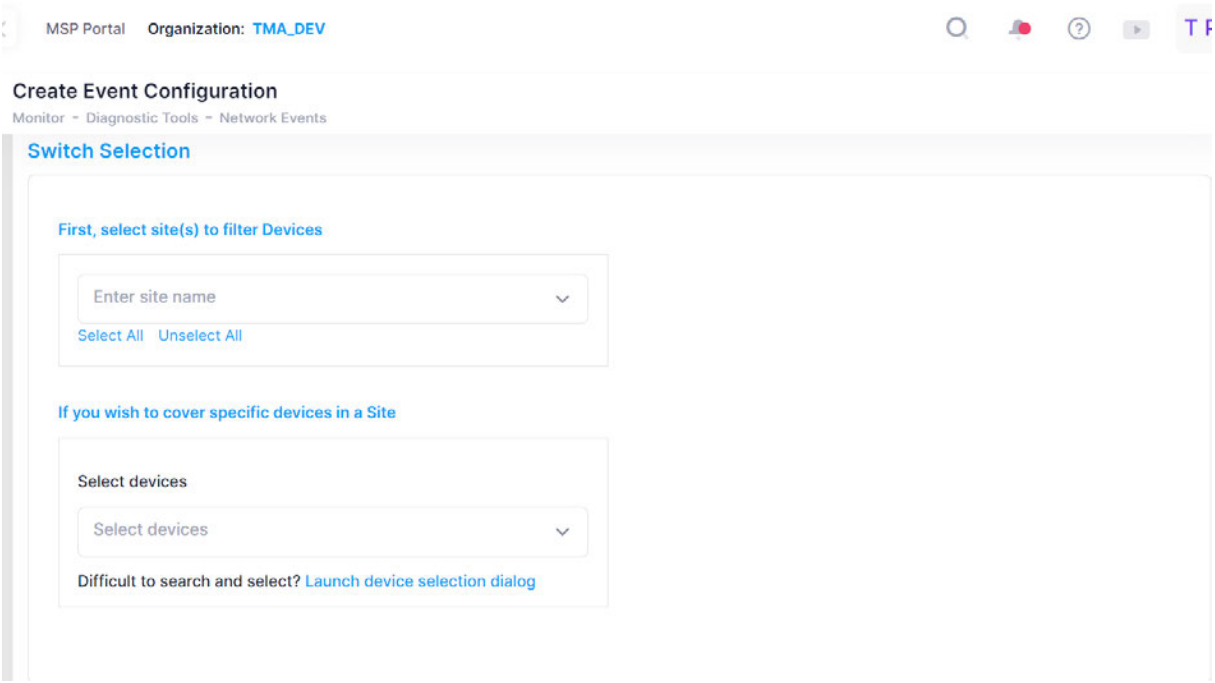
Select the events that you want to configure on the selected devices, then click **OK**. The event selection window closes and a list of the events you selected is displayed.



When you are done defining the event information, device selection, and event selection, click **Create**. The event configuration will be pushed to the selected devices with name of “trap.conf” (tmp/config/trap.conf).

Note: For Access Points Event Configuration, the below-mentioned scope priority is followed: **Device level > AP group level > Event configuration selected in Provisioning Configuration > Site level**

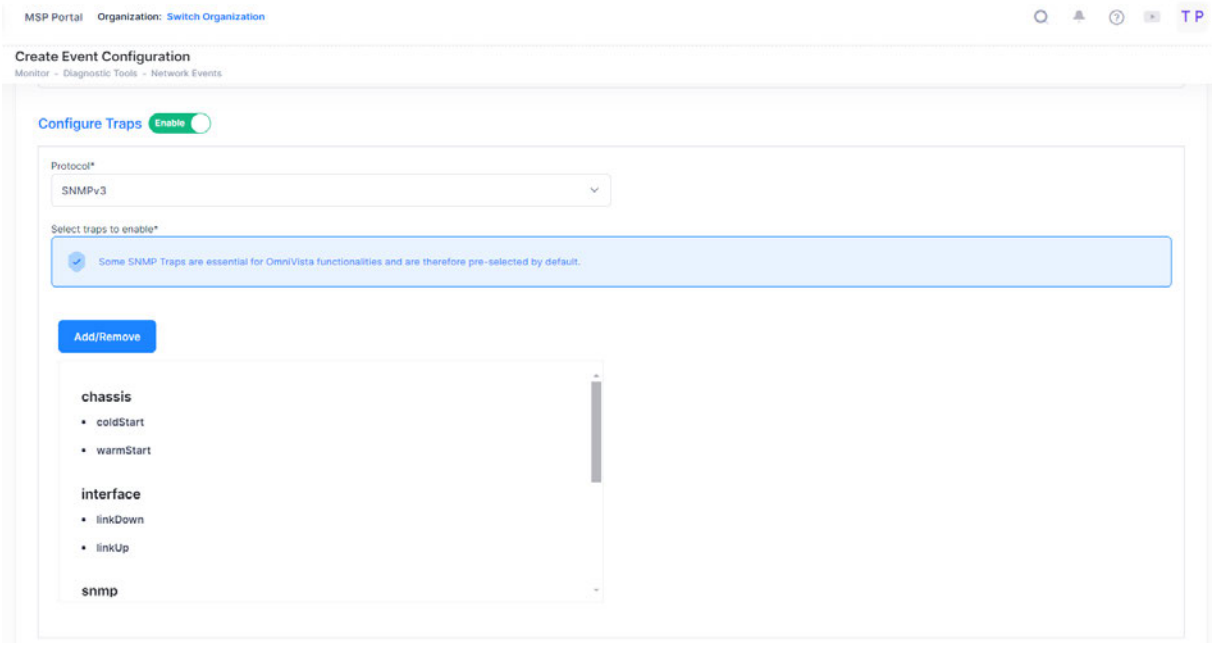
8.4.2.4.1.5 Step 5. Switch Selection



Select devices for which you want to configure events using one or more of the following methods:

- **Select sites** - Click on this field to display a list of Sites for the Organization. Select the desired Site from the drop-down menu.
- **Select devices** - Click on this field to display a list of devices. Select the device from the drop-down menu. Repeat this action for each device you want to select. To pick devices from a list of devices, click on “Launch device selection dialog”. A Device Selection window opens from which you can select devices.

8.4.2.4.1.6 Step 6. Configure Traps

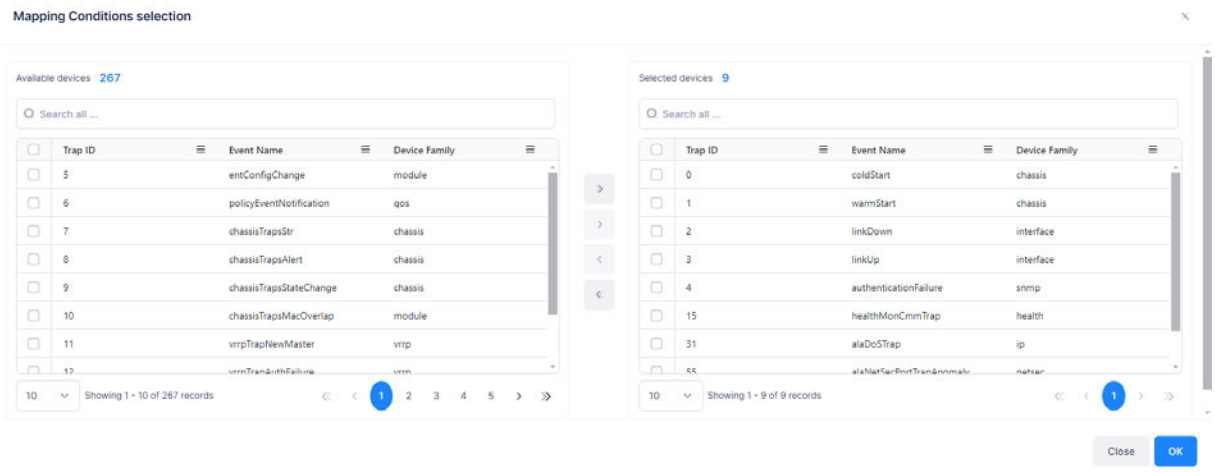


- **Configure Traps**
  - **Enable -** The OmniVista Terra Server will be notified about traps (Default).
  - **Disable -** The OmniVista Terra Server will not be notified about traps.
- **Protocol -** Select the protocol used to send traps to the server (SNMPv2 or SNMPv3). The Default is SNMPv3.
- **Select traps to enable** - There are some SNMP Traps that are essential for OmniVista functionalities and are therefore pre-selected by default. The following Traps are automatically configured on Switches through pre-provisioning when they are added to OmniVista Terra.
  - LinkUp
  - LinkDown
  - coldstart
  - warmstart
  - cpu/memory/temperature threshold crossing
  - alaDoSTrap
  - alaLldpTrustViolation
  - alaNetSecPortTrapAnomaly
  - authenticationFailure
  - healthMonCmmTrap

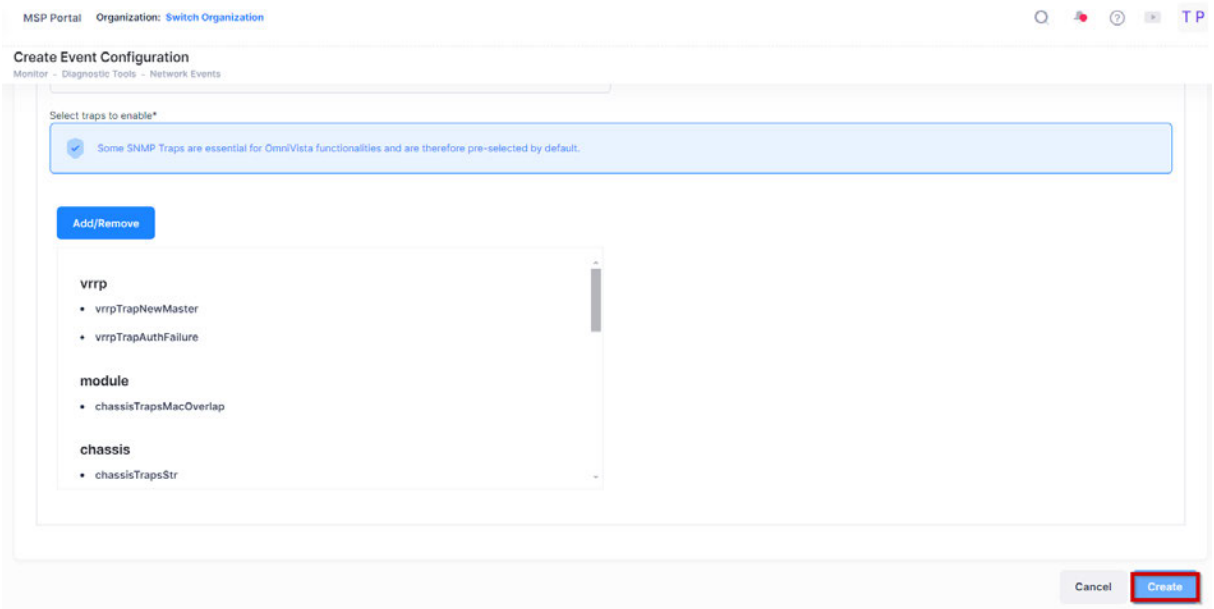
The SNMPv3 user is automatically created and configured on Switches through pre-provisioning to send the above default configured SNMP traps. The command executed on the Switch is shown below:

```
user ovngv3_sha_aes password "*************" read-only all SHA384+AES
allow-ssh disable
aaa authentication snmp local
snmp authentication-trap enable
snmp station XXX.XXX.X.X XXXXX ovngv3_sha_aes v3 enable
```

Click on **Add/Remove** to open the events selection window.



Select the events that you want to configure on the selected devices, then click **OK**. The event selection window closes and a list of the events you selected with the default traps are displayed.

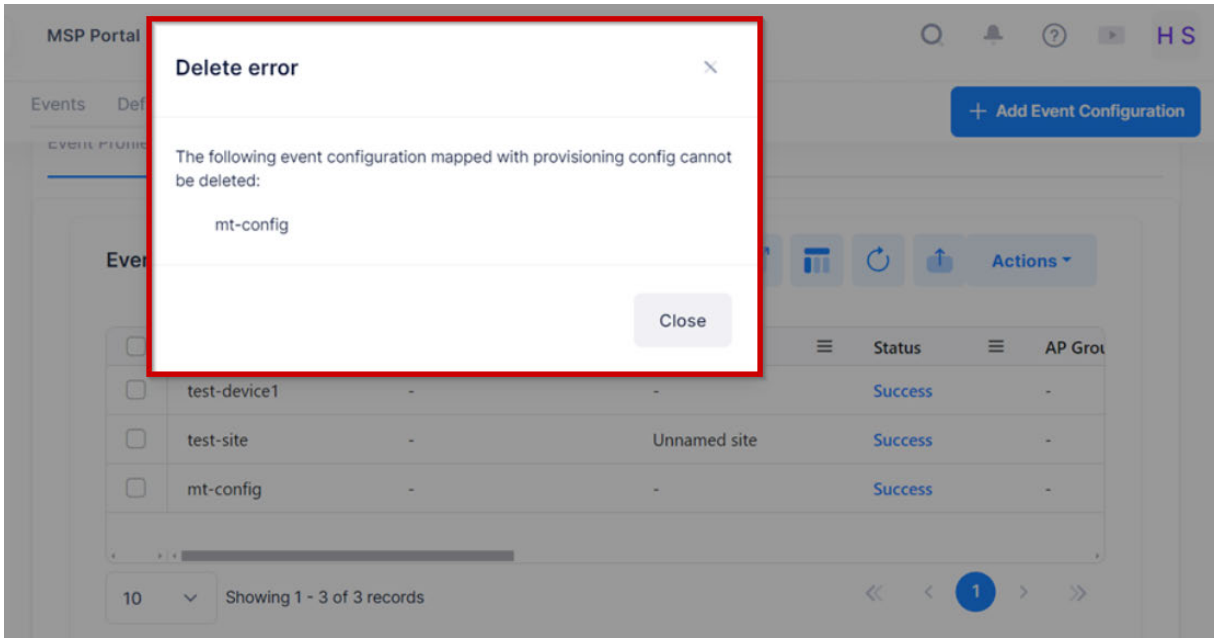


When you are done defining the event information, device selection, and event selection, click **Create**. The event configuration will be pushed to the selected devices with name of “trap.conf” (tmp/config/trap.conf).

Configure Traps is not valid if you choose “Access Point” for **Device type Selection**.

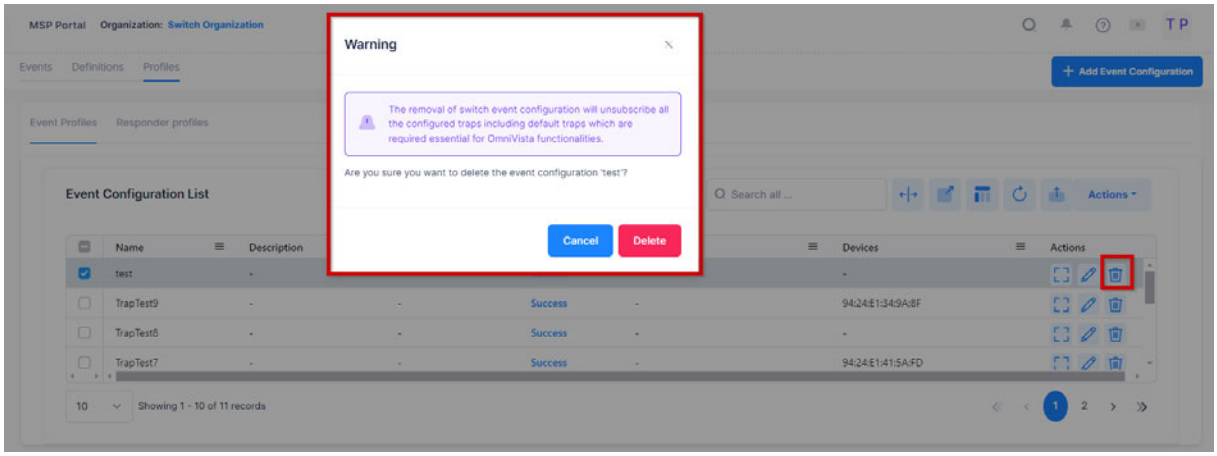
8.4.2.4.1.7 Access Point Event Configuration Deletion Policy

When you select to delete an AP Event configuration associated with a Provisioning Configuration from the **Event Configuration** list, OmniVista Terra will display the warning message as shown below.



8.4.2.4.1.8 Switch Event Configuration Deletion Policy

When you select to delete a Switch Event configuration from the **Event Configuration** list, OmniVista Terra will display the warning message as shown below.



Note: The removal of switch event configuration will unsubscribe all the configured traps including default traps which are required essential to OmniVista Terra functionalities.

21 Oct 2025

8.4.2.5 Events - FAQs/Troubleshooting

8.4.2.5.1 From Event Application, I can't select the larger period in the data filter.

The time range which can be selected in Event application is based on the data persistency values set in the Basic Settings (see page 127).

For **Traps**,

- Check the time period selected for **'Event Traps'** in Basic Settings (see page 127).
- Limit for the Traps is minimum 7 days to maximum 30 days.

For **QoE Analytics**,

- Limit is set to 5 days by default and maximum time span can be selected is 24 hours.
- This is default settings and can't be modified.

8.4.2.5.2 I don't see Live Notifications in the Real Time.

- Live Notification is displayed at the interval of one minute.
- Notification panel displays only the latest 10 (approx.) records and to see all notifications you can Click on **'see all'** option at bottom.

8.4.2.5.3 I don't see the specific type of Traps in the Event Application.

Traps are received from Access points depending upon the Event Type selected in the Event Configuration.

- Check the correct Scope and Time period is selected.
- Go to **Network Events > Event Configuration.** (see page 1004)
- Configuration is applied to Access Point as per device selection in the Event Configuration.
- Edit the configuration, Select the missing Event type and save the changes.
- Then you will start receiving selected Traps.

8.4.2.5.4 I don't see the QoE Events updated in the Event Application.

QoE Events are received as per the configuration done in the external engines.

- First check, correct Scope and Time period is selected.
- Go to **Wireless > Advanced > External Engines.**
- Select the engine with type **OmniVista Terra Advanced Analytics**.
- Check the missing type is selected in QoE Events.
- If No, select the type and set the Interval.
- If Yes, please check the interval configured, the event is received as per the interval. Please check Event Application after the configured Interval Time period.

8.4.2.5.5 How can I modify the Severity for the Event?

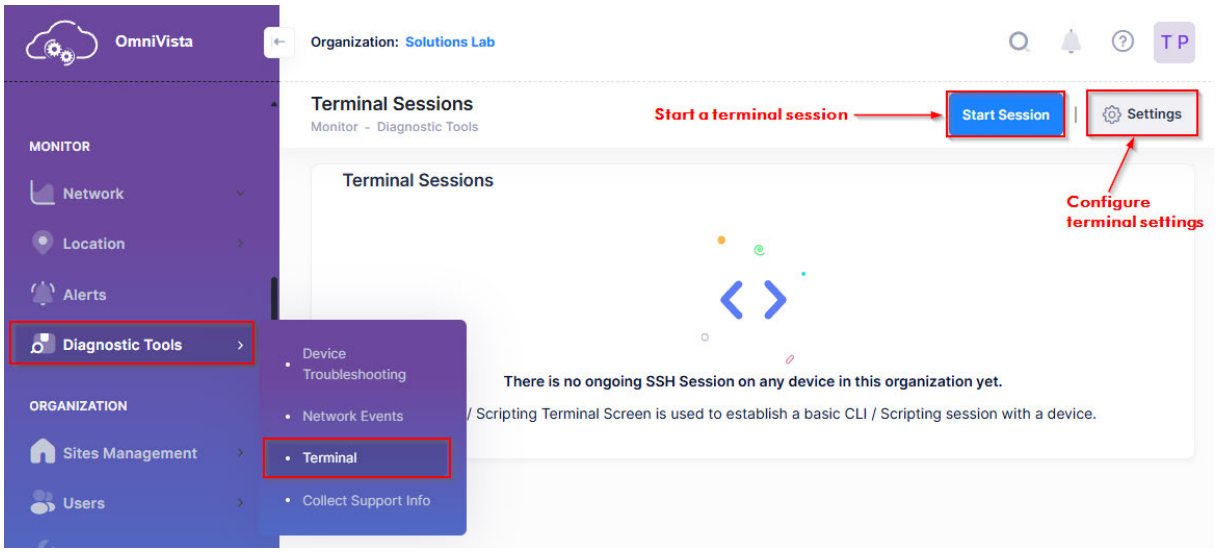
Event Severity depends upon the settings done in the Event Definition.

- Go to **Network Events >Event Definitions** (see page 993).
- Select the event type and click on **Edit.**
- Can update the Severity and the Synopsis and click on save button.
- The existing Events and new Events will have the modified Severity.

21 Oct 2025

8.4.3 Terminal

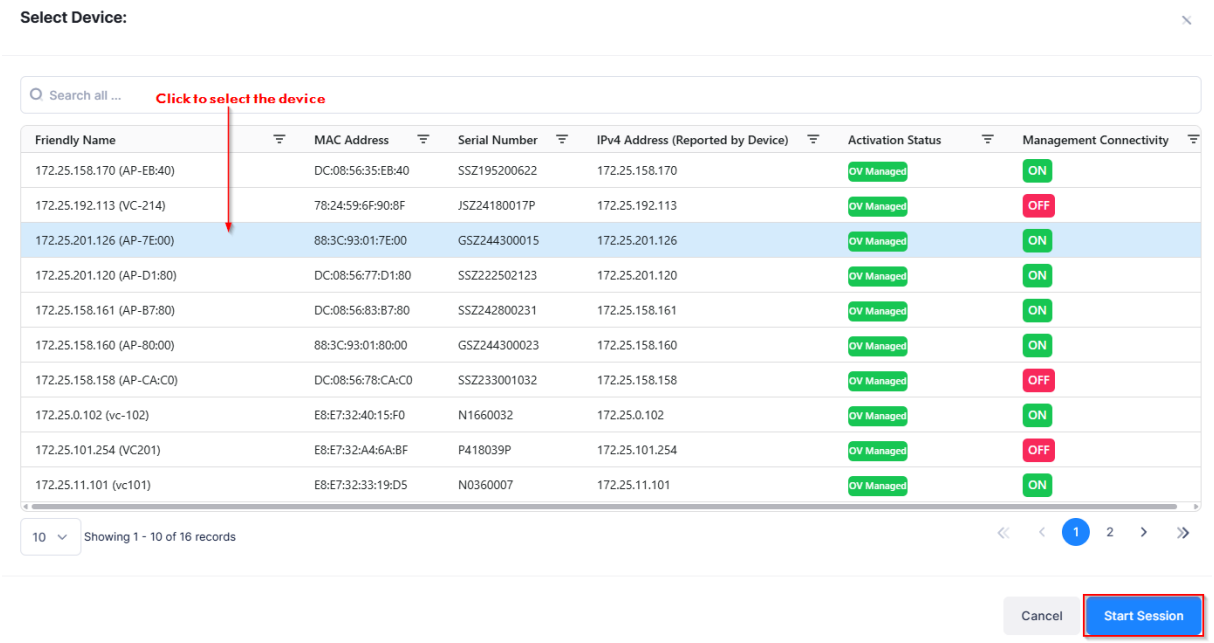
The Terminal application allows you to establish a basic CLI/Scripting session with a device in the Organization. To initiate a terminal session, click on **Diagnostic Tools > Terminal** under the “Monitor” section of the OmniVista Terra Menu (see page 45). The Terminal Sessions screen displays.



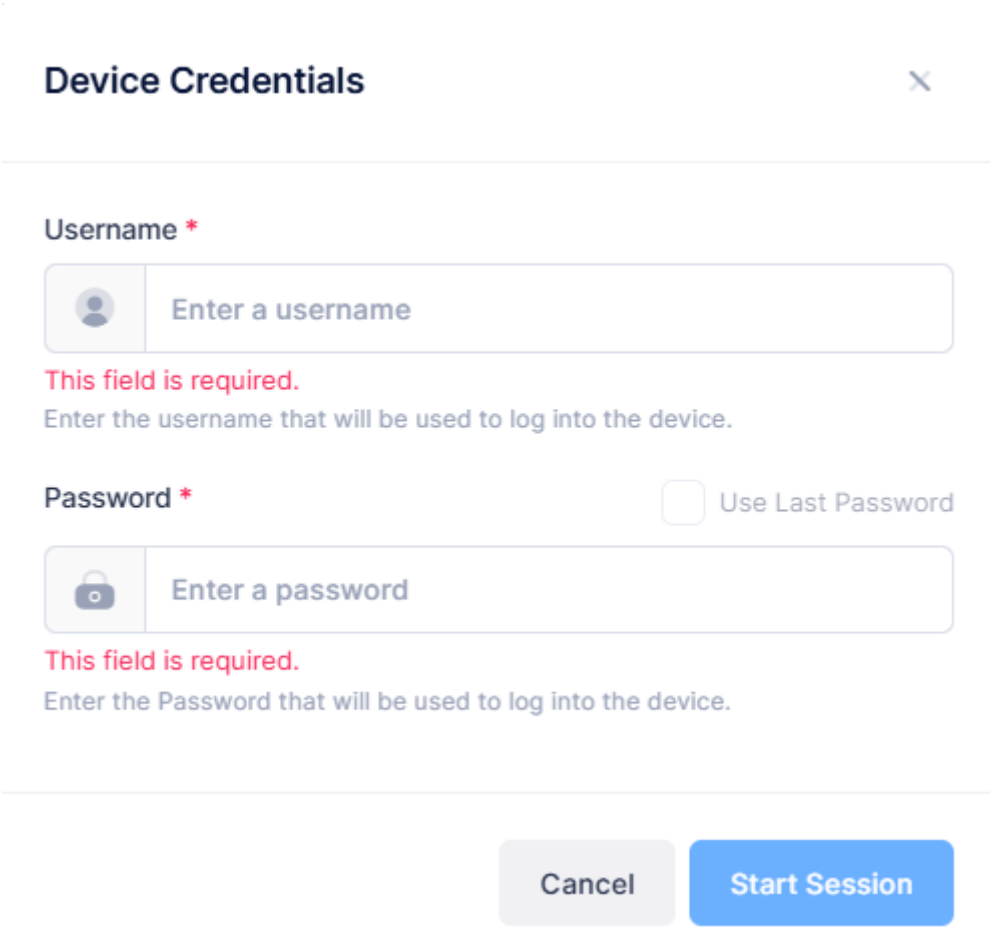
The Terminal Sessions screen displays a list of any open sessions with devices that belong to the current Organization. Use this screen to start a new session (see page 1015) and configure format settings (see page 1017) for the terminal session.

8.4.3.1 Connecting to a Device

To connect to a device, click on **Start Session**. The following Select Device screen opens and displays only devices that are fully managed (“Management Connectivity” set to “On”) and the “Activation Status” is set to “OV Managed”. Connecting to a device that is not “OV Managed” is not supported.



On the Select Device screen, click on the device entry to select the device for the terminal session. After selecting the device, click on **Start Session**. You are then prompted to enter the Username and Password required to log into the device.

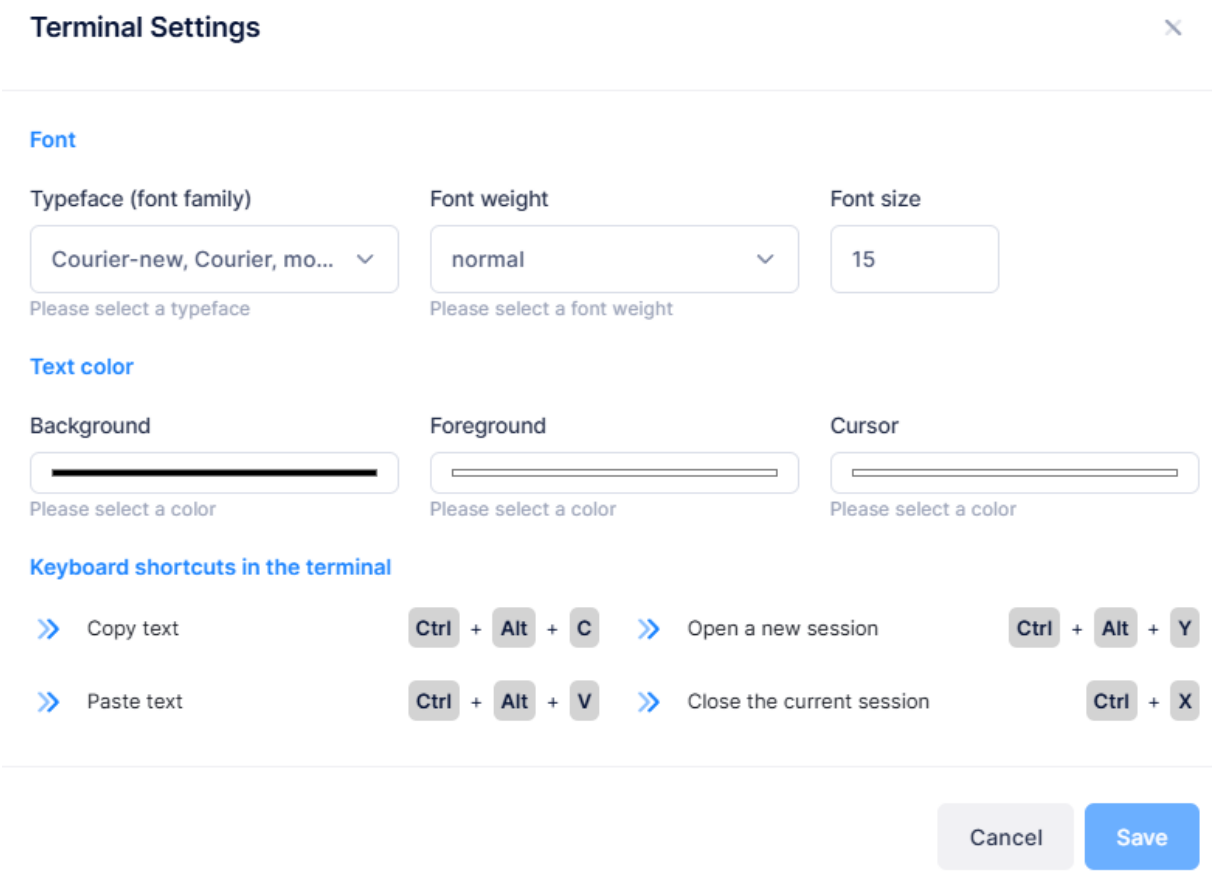


Enter the Username and Password, then click on **Start Session** to open an SSH (Secure Shell) connection to the selected device.

> Make sure that the SSH Login option is enabled in the Provisioning Configuration (see page 313) associated with the AP Group (see page 309) to which the device belongs. If it is not enabled, connecting to the device will fail.

8.4.3.2 Session Preferences

To configure the appearance of a terminal session (for example, font, text color), click **Settings** on the Terminal Sessions screen. The following Terminal Settings screen opens.



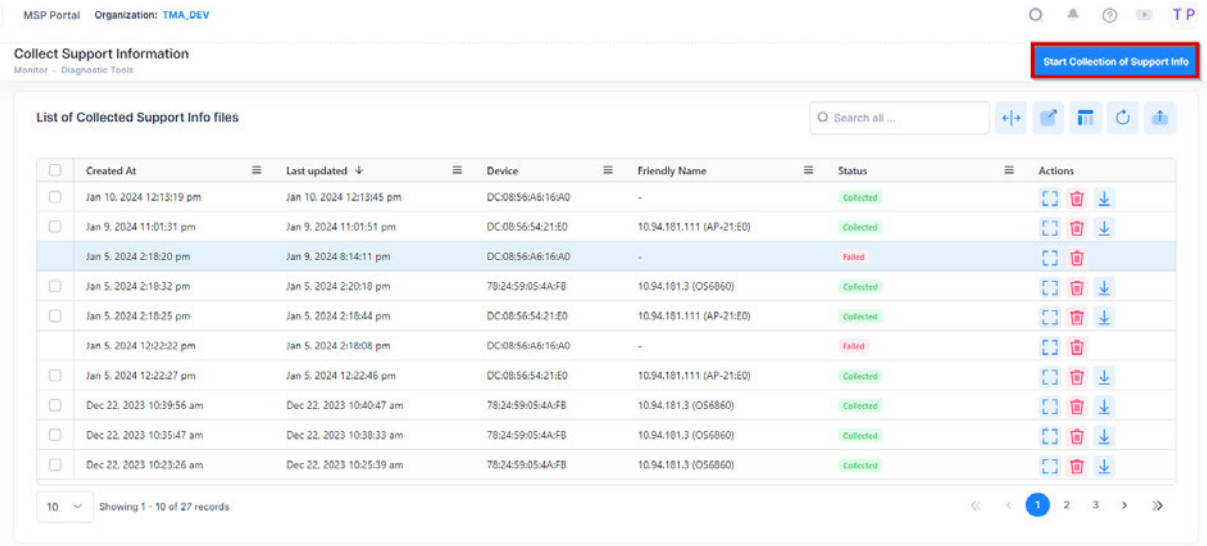
The Terminal Settings screen displays the current font and text color settings and also shows the keyboard shortcuts that are available within a terminal session. Modify the Font and Text Color, as desired, then click on **Save** to apply your changes. The next terminal session will reflect your font and text color changes.

21 Oct 2025

8.4.4 Collect Support Information

The Collect Support Information application allows you to collect log information from network devices that you can send to the Alcatel-Lucent Enterprise (ALE) team to troubleshoot problems. The log files can be downloaded to a compressed file (tar.gz for Access Point devices and Switches).

To access the Collect Support Information screen, click on **Diagnostic Tools > Collect Support Info** under the “Monitor” section of the OmniVista Terra Menu (see page 45).



The Collect Support Information screen displays a list of requests to collect log files from devices and is used to initiate log file collection and download collected log files (see page 1019).

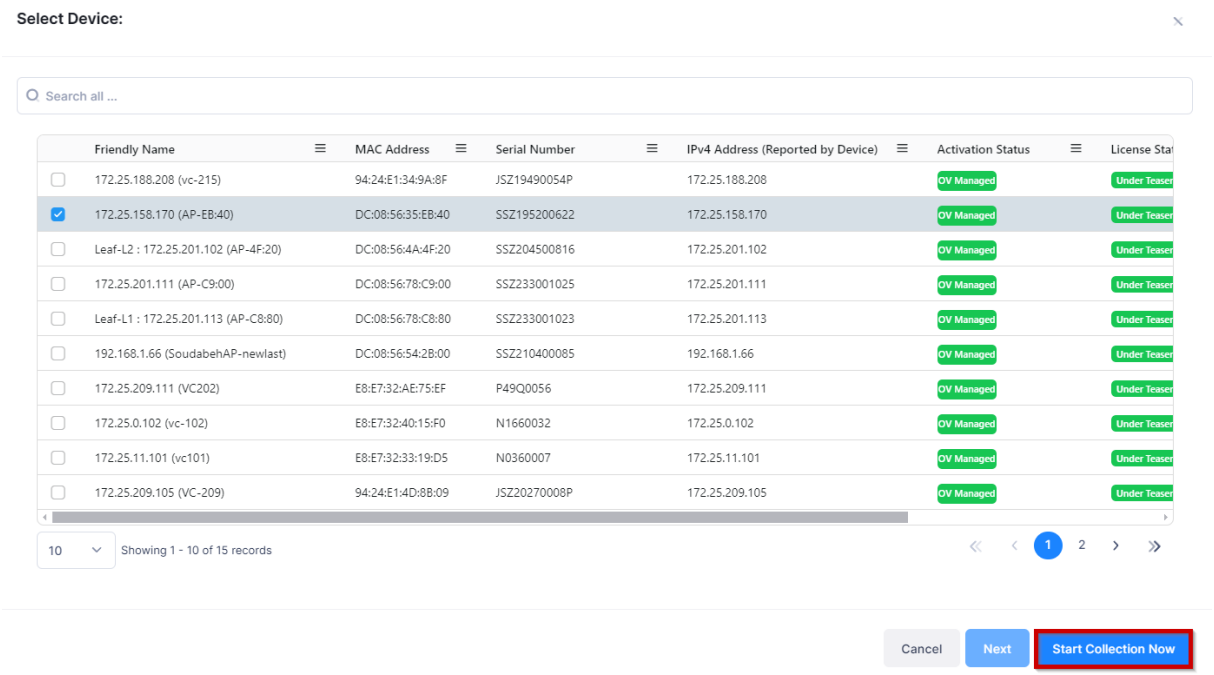
The following information is provided for each log file request entry:

- **Created At** - The date and time the request to collect log information was initiated.
- **Last Updated** - The date and time the log collection finished.
- **Device** - The MAC address of the device from which the log information was collected.
- **Friendly Name** - The user-specified friendly name for the device from which log information was collected.
- **Status** - The log file collection status:
  - **Collecting** - OmniVista is in the process of collecting the log file information from the device.
  - **Collected** - The log file information was successfully collected from the device and is ready to download.
  - **Failed** - OmniVista was unable to retrieve the log file information from the device.
  - **Uploading File** - The log file is created and it is uploading to the network Cloud.
- **File Name** - The name of the compressed log file to download. Displays only when the request is successfully completed (Status is “Collected”).

To remove a log file request entry, click on the delete icon under the “Actions” column.

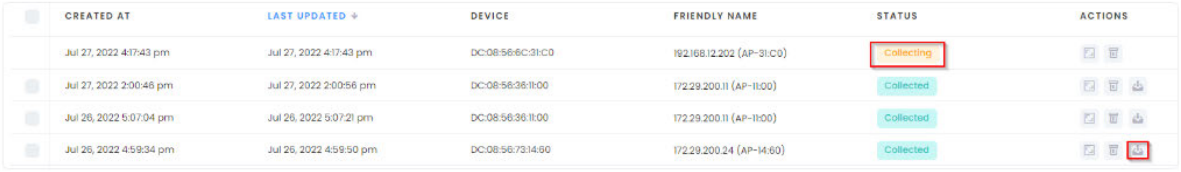
8.4.4.1 Collecting Log Files for Access Point Devices

To initiate a log file collection for a specific device, click on **Start Collection of Support Info**. The Select Device screen opens and displays only devices that are fully managed (see page 195) (“Management Connectivity” set to “On” or “Off”) and the “Activation Status” is set to “OV Managed”. Collecting log file information is not supported on Analytics Only (see page 195) devices or on Full Management devices that are not “OV Managed”.



On the Select Device screen, click on the checkbox next to the device from which you want to collect log file information. After selecting the device, click on **Start Collection Now**. Note that you can only collect log files from one device at a time. Repeat this process to collect logs for additional devices.

The List of Collected Support Files screen displays and shows the request that you just initiated in the list with a status of “Collecting”. At this stage, OmniVista has sent a request to the device to collect all logs.

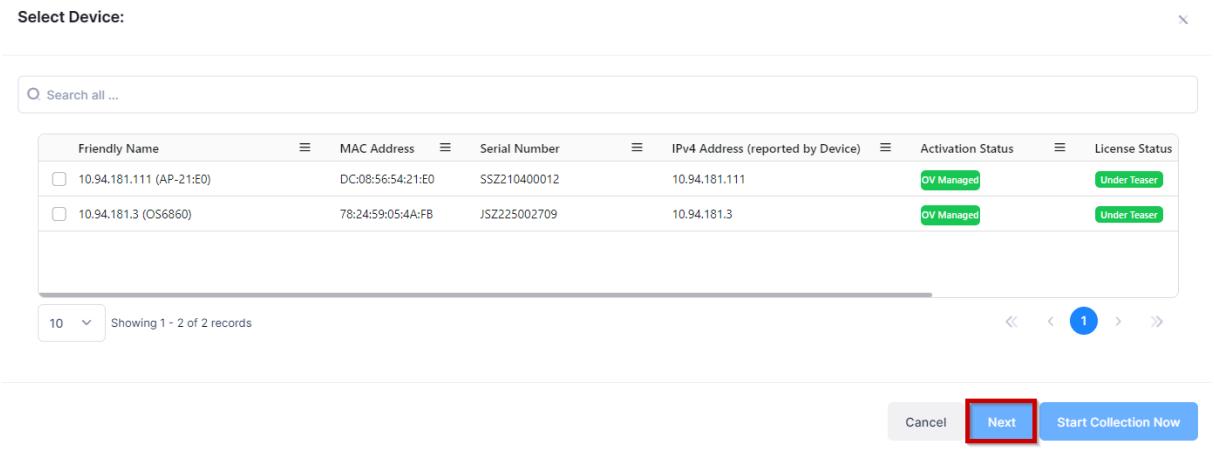


When the AP provides the log file (in tar.gz format) to OmniVista, the request status changes to “Collected” and a download icon appears next to the request under the “Actions” column. The user needs to click on the **Refresh** button to get the updated data in the table after applying any changes to view the latest status of the files. You can now click on the download icon to the save the log file to a local folder.

Note: If the request status of collecting the log file information is more than 15 minutes of duration, the request will be automatically rejected and the status will change to “Failed”.

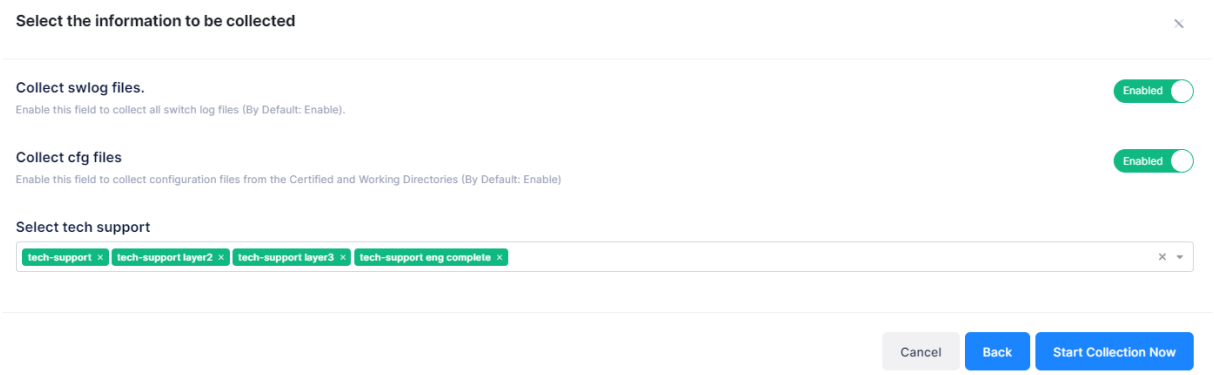
8.4.4.2 Collecting Log Files for Switches

To initiate a log file collection for a specific switch, click on **Start Collection of Support Info**. The Select Device screen opens and displays only switches that are fully managed (“Management Connectivity” set to “On” or “Off”) and the “Activation Status” is set to “OV Managed”. Collecting log file information is not supported on Analytics Only devices or on Full Management devices that are not “OV Managed”.



On the Select Device screen, click on the checkbox next to the device from which you want to collect log file information. After selecting the Switch, click on **Next**. Note that you can only collect log files from one device at a time. Repeat this process to collect logs for additional devices.

The following screen appears:

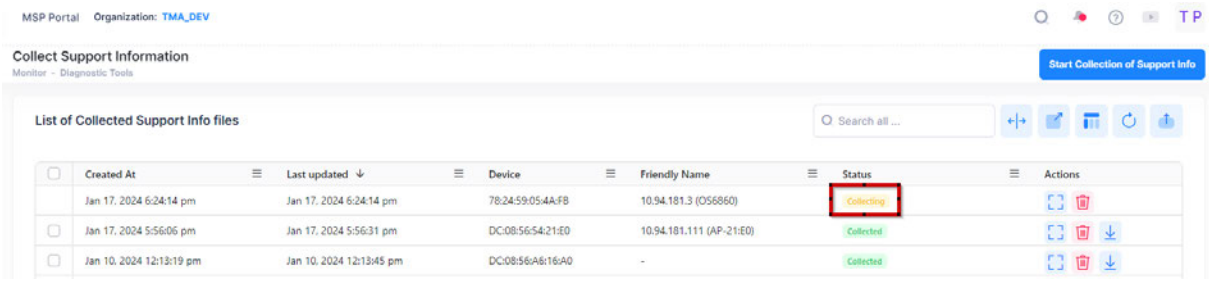


Select the information to be collected as described below, then click on the **Start Collection Now** button to download the specified log files.

- **Collect swlog Files** - Enable to collect all switch log files (Default = On).
- **Collect cfg Files** - Enable to collect configuration files (e.g., boot.cfg, vcboot.cfg) from the Certified and Working Directories (Default = On).

- **Select Tech Support Collection Level** - Select the types of Tech Support log files you want to download. By default, all file types are selected, however, you can select one or more specific type of files.
  - **Tech Support** - It includes all Configuration, Switch Log Files and Tech Support log file information like device hardware and firmware information.
  - **Tech Support Layer 2** - It includes all Configuration, Switch Log Files and Layer 2 log file information such as Layer 2 interface information.
  - **Tech Support Layer 3** - It includes all Configuration, Switch Log Files and Layer 3 log file information such as Layer 3 IP information.
  - **Tech Support Engineering Complete** - It includes all Configuration, Switch Log Files and Engineering log file information (Virtual Chassis information).

The List of Collected Support Files screen displays and shows the request that you just initiated in the list with a status of “Collecting”. At this stage, OmniVista has sent a request to the switch to collect all logs.



When the Switch provides the log file (in tar.gz format) to OmniVista, the request status changes to “Collected” and a download icon appears next to the request under the “Actions” column. The user needs to click on the **Refresh** button to get the updated data in the table after applying any changes to view the latest status of the files. You can now click on the download icon to the save the log file to a local folder.

21 Oct 2025

9 Automation with APIs

OmniVista Terra provides a set of REST APIs that can be used to configure or monitor your network. Use the REST APIs to integrate in any system, such as a Mobile application, a chatbot, or a Web application.

9.1 What you'll find here

The **Quick Start Guide** (see page 1023) provides information about how to use REST APIs offered by our service. It gives the list of prerequisites that you will need before you make your first REST API call. Finally, this section also describes globally the URL format used in our platform and the reasons why we offering this set of APIs.

In the **Authentication** (see page 1035)section, we present the authentication mechanism used to authenticate your HTTP requests. We explain in detail how to get a token and how to use it to authenticate your next requests.

Lastly, the **API Reference** (see page 1042) section gives you access to the whole list of APIs available in our service. You will be able to access a list of APIs per data model and see some examples of how to make your first API call successfully.

9.2 Quick links

- API References:
  - EU: https://eu.manage.ovcirrus.com/apidoc/apidoc.html
  - Americas: https://us.manage.ovcirrus.com/apidoc/apidoc.html
- OmniAccess Stellar Products
- Alcatel-Lucent Enterprise

21 Oct 2025

9.3 Quick Start Guide

The Quick Start Guide provides the following information that you need to know to start interacting with the OmniVista Terra APIs:

- Preamble (see page 1024)
- REST APIs Prerequisites (see page 1025)
- REST APIs Entities
- URL Design (see page 1028)
- The Application Concept (see page 1030)
- Create a First Application (see page 1031)

21 Oct 2025

9.3.1 Preamble

Welcome to the **Alcatel-Lucent Enterprise OmniVista Terra** REST APIs documentation section.

The Alcatel-Lucent Enterprise (ALE) OmniVista Terra **REST APIs** is a set of APIs based on HTTP methods which makes it easy for developers to write applications that connect to OmniVista Terra Service.

This tutorial helps you start with these REST APIs by explaining what you can do and how to use them.

9.3.1.1 What's a REST API, anyway?

An API is an application programming interface. In short, it's a set of rules that lets programs talk to each other, exposing data and functionality across the internet in a consistent format.

REST stands for `Representational State Transfer`. This is an architectural pattern that describes how distributed systems can expose a consistent interface. When people use the term 'REST API,' they are generally referring to an API accessed via HTTP protocol at a predefined set of URLs.

These URLs represent various resources, information, or content accessed at that location, which can be returned as JSON, HTML, audio files, or images. Our API only manages JSON content and images.

Often, resources have one or more methods that can be performed on them over HTTP, like `GET`, `POST`, `PUT` and `DELETE`.

9.3.1.2 Useful links

- REST API
- RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
- RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage

21 Oct 2025

9.3.2 REST APIs Prerequisites

Before making your first REST API call, you need to be familiar with the REST API schema. You also need to install an API testing tool to make it easier to test your API calls.

9.3.2.1 REST API Testing Tools

The following Testing tools can be installed on your machine:

- Insomnia (Available on Mac, Windows, and Linux)
- Postman (Available on Mac, Windows, and Linux)
- Advanced REST Client (Available on Mac, Windows, and Linux)
- HTTPie (Available on Mac, Windows, and Linux)
- Restlet Client (Chrome Extension)

When developing your applications, you can call REST APIs from any kind of programming language like JavaScript, Java, Swift, C#, Curl, PHP...

21 Oct 2025

9.3.3 REST APIs Entities

Here is the list of entities that you can access using our APIs:

Entity	Description
`Application`	These APIs authenticate your application and manage the application token.
`User`	These APIs are used to manage authenticated user.
`Usersettings`	These APIs are used to manage authenticated user's settings.
`Useractivity`	These APIs are used to manage the activities of authenticated user.
`Organization`	These APIs are used to manage organizations of authenticated user's.
`Loginhistory`	These APIs are used to get the authenticated user login's history.
`Site`	These APIs allow to manage site configuration.
`Building`	These APIs are dedicated to manage buildings inside a site.
`Floor`	These APIs are used to manage different floors inside a building.
`Device`	These APIs are used to manage devices inside building's floor.
`Subscription`	These APIs are used to manage subscription of organizations.
`Invitee`	These APIs are used to manage organizations invitations.
`Qoe`	These APIs are used to manage QoE thresholds of authenticated user's site.
`WallType`	These APIs are used to fetch wall type.
`Wall`	These APIs are used to manage walls of authenticated user's floor.

Entity	Description
`Wlananalytics`	These APIs are used to retrieve WLAN Analytics data.

21 Oct 2025

9.3.4 URL Design

9.3.4.1 API resource URL

All resources can be accessed over HTTPS from the `https://{your_region}.myovterra.myovcloud.com/api/ov` domain:

```
https://{your_region}.myovterra.myovcloud.com/api/ov
```

9.3.4.2 API Headers

The following header must be provided in all `POST` and `PUT` requests:

Header name	Value	Description
Content-Type	**application/json**	Used to indicate the media type of the resource.

If this header is missing or invalid, the API will return a `406 Not Acceptable` with the following JSON response:

```
{
    "errorCode": 406,
    "errorMsg": "The 'Content-Type' header is missing or invalid. You should use
'Content-Type: application/json'.",
    "errorDetailsCode": "invalid_header"
}
```

9.3.4.3 API Endpoints

All URLs are built in the same way.

They are composed of a **prefix** (/api/ov), an API **version number,** and a **suffix** which refers to the **collection of entities** that are addressed by the API:

```
https://{your_region}.myovterra.myovcloud.com/api/ov/{version}/{resourceName}
```

For example, a collection of entities of type `sites` will have the following URL:

```
https://{your_region}.myovterra.myovcloud.com/api/ov/v1/sites
```

If we want to address a specific `site` entity, we will have to indicate the id of the `site` in the URL:

```
https://{your_region}.myovterra.myovcloud.com/api/ov/v1/sites/{siteId}
```

Multiple entities could be added as a suffix. Here is an URL example used to fetch `buildings` of a given `site` :

```
https://{your_region}.myovterra.myovcloud.com/api/ov/v1/sites/5d7f92389990373eb098909/
buildings
```

9.3.4.4 Response

Most entities will return data in JSON format, and exceptions to this rule are indicated accordingly in our API Reference.

21 Oct 2025

9.3.5 The Application Concept

Before making your first API call, you will need to register an **Application**.

An Application can be created from the OmniVista Terra web page once the user is logged in. An authenticated user can create many applications.

> If you want to create a mobile application and a chatbot, we recommend creating two separate applications to uniquely identify each application.

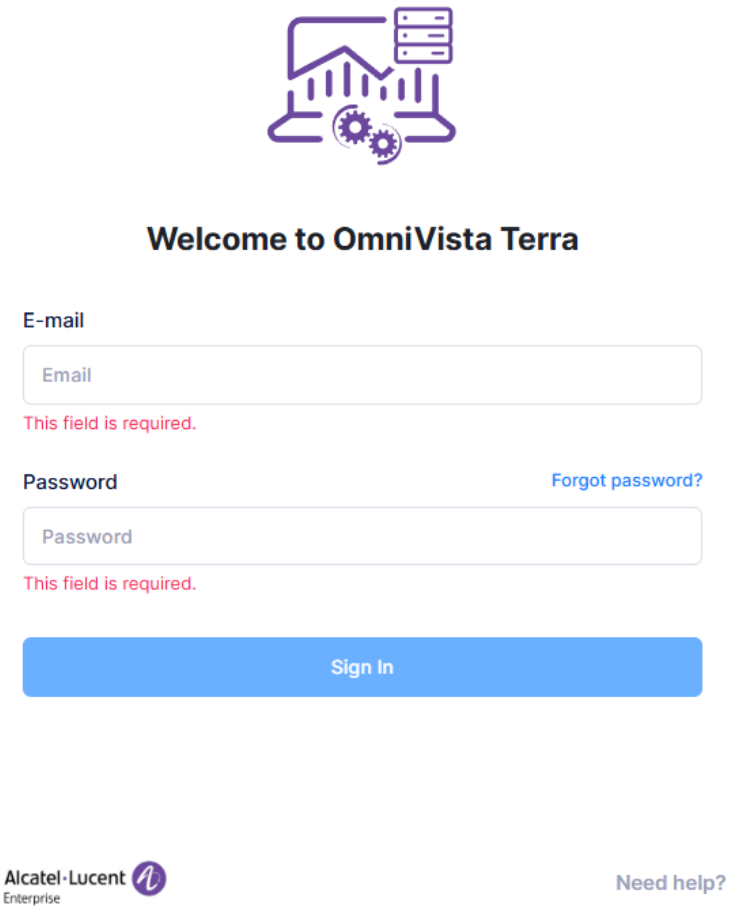
Every registered Application is assigned a unique App ID and App Secret. The App Secret should not be shared! That includes checking the string into your repository.

21 Oct 2025

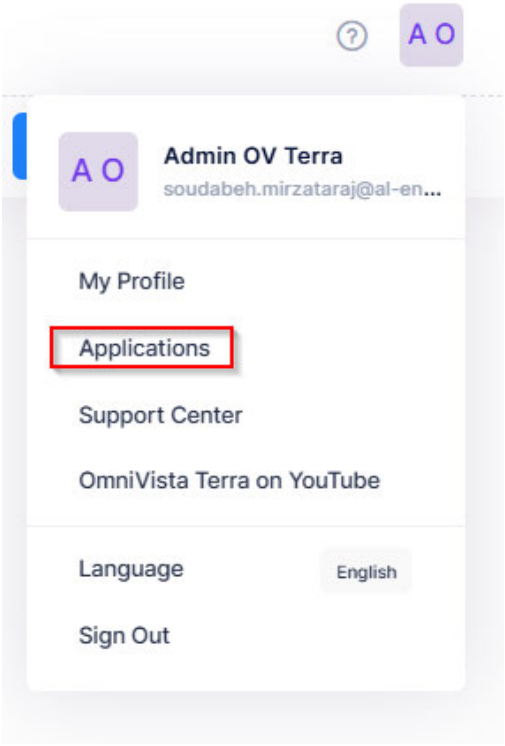
9.3.6 Create a First Application

Before making your first API call, you need to create an Application.

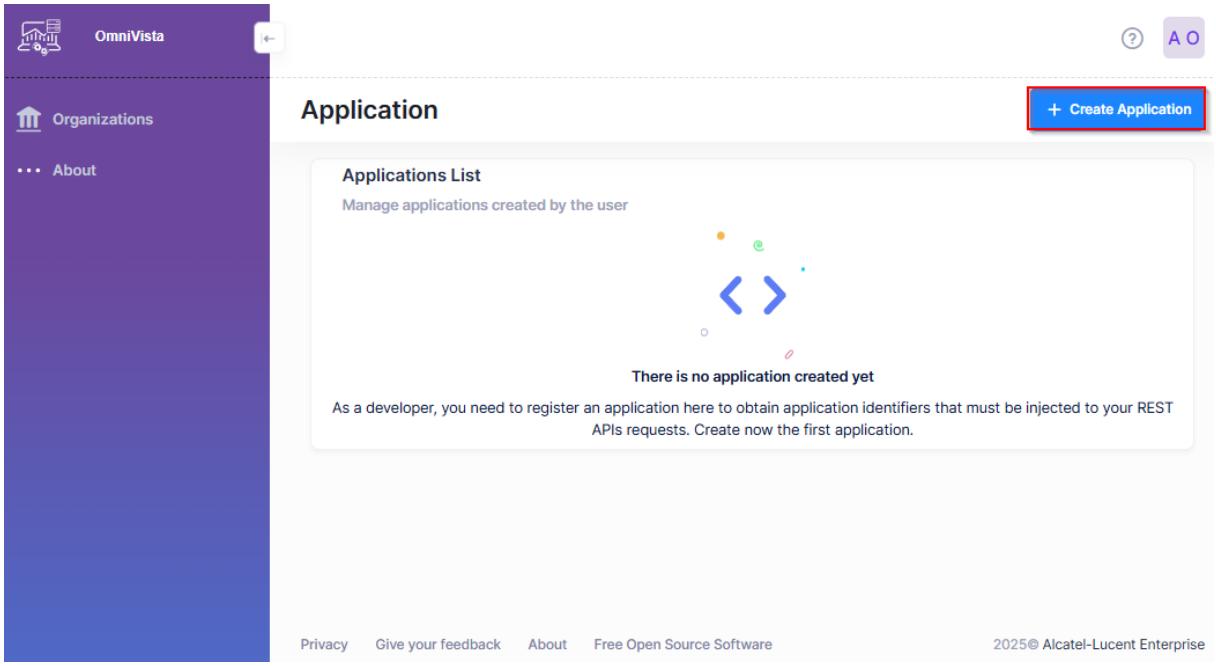
1. Sign In to the OmniVista Terra application with your user account.



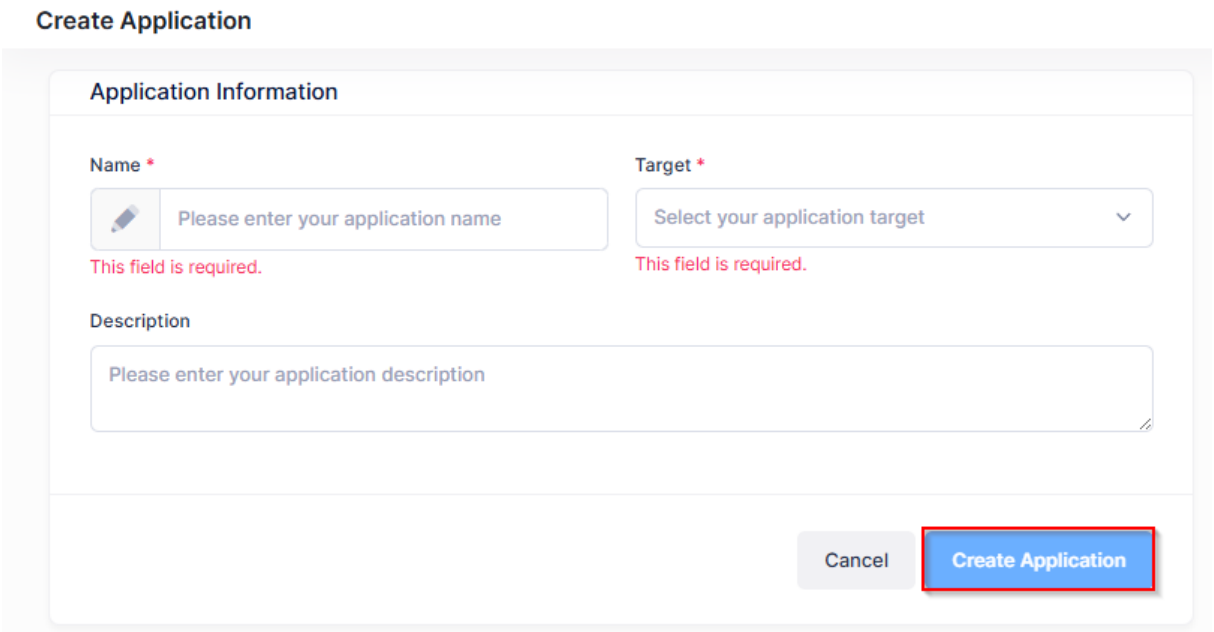
2. Click on your user icon on the top right corner and select the **Applications** item:



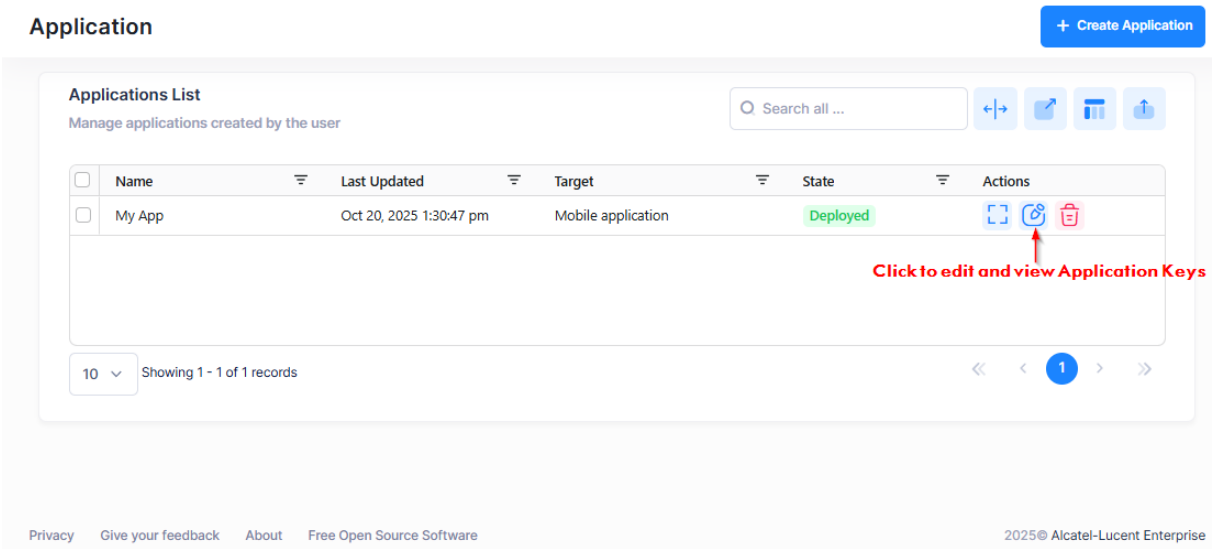
3. You are redirected to the Applications page. Click on **Create Application**.



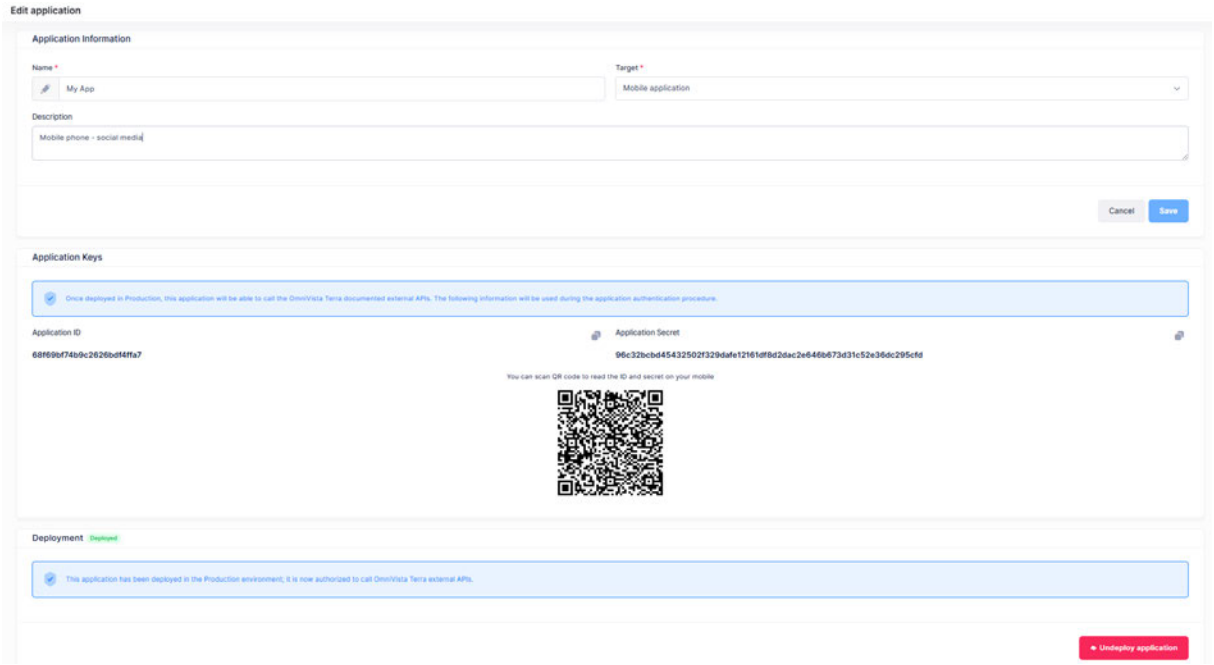
4. Fill in the new application form and click on **Create Application**.



5. The application is created and appears on your **Applications** page. Click on the **Edit** application icon to access the application keys.



6. The Application Keys section of the screen displays your generated Application ID and Application Secret. These two keys are unique and identify your application. Use these keys to make your API calls.



7. You are now ready to make your first API call!

> Tip: When a new application is created, its status is automatically set to Deployed. When an application is Deployed, its API calls are authorized on the OmniVista solution with an Application ID/Application Secret associated with the application. If you want to suspend for a time the usage of these identifiers, you can Un-deploy the application. The status will change to Undeployed and the usage of the Application ID/Application Secret identifiers are suspended.

21 Oct 2025

9.4 Authentication

This section provides insights related to the Authentication process used to identify users and their applications to access OmniVista Terra APIs:

- Authentication Principle (see page 1036)
- Authentication API (see page 1037)
- Sending Next Requests (see page 1038)
- Status Codes (see page 1040)

21 Oct 2025

9.4.1 Authentication Principle

In this section, we're going to focus on the basics of authentication.

In our platform, we are using an authentication mechanism based on **JSON Web Token**.

9.4.1.1 What is JSON Web Token?

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

It means that before making your API requests, you need first to authenticate your user and your application on the platform.

Once authenticated, you will obtain a token that must be provided in the next requests.

21 Oct 2025

9.4.2 Authentication API

OmniVista Terra Service offers an API to authenticate your application:

```
POST https://{your_region}.myovterra.myovcloud.com/api/ov/v1/applications/authenticate
```

The request body is a JSON object that should contains the following information:

- `email` : The user login email
- `password` : The user password
- `appId` : The application Id
- `appSecret` : The application secret

You can try to authenticate your application using the following Curl Snippet. Simply add your user and application credentials before making the request.

```
curl \
  "https://{your_region}.myovterra.myovcloud.com/api/ov/v1/applications/authenticate"
  -X "POST" \
  -H 'Content-Type: application/json; charset=utf-8' \
  -d $'{"email": "YOUR_EMAIL", "password": "YOUR_PASSWORD", "appId": "APP_ID",
"appSecret": "APP_SECRET"}'
```

If your request is successful, you will get a `200 OK` HTTP Response with a JSON body containing the following keys:

- `access_token` : The generated token that must be used in the next requests.
- `expires_in` : The number of seconds during which the token is valid. (15 days by default)
- `token_type` : The type of token generated. Always Bearer in our platform.

```
HTTP Response: 200 OK

{
  "access_token": "eyJhbGciOiJIU...plaVi7K04EqcjnkhPE8",
  "expires_in": 1296000,
  "token_type": "Bearer"
}
```

21 Oct 2025

9.4.3 Sending Next Requests

Once you have a valid Bearer token, you can now call the next APIs by setting the `Authorization` request header field. The valid syntax is the following:

```
Content-Type: application/json; charset=utf-8
Authorization: Bearer <access_token>
```

9.4.3.1 Example

In the following example, we'll try to fetch all sites created by the authenticated user.

```
GET https://{your_region}.myovterra.myovcloud.com/api/ov/v1/organizations/{orgId}/sites
```

Request Headers:

```
Authorization: Bearer eyJhbGciOiJIU...plaVi7K04EqcjnkhPE8
```

Response Body:


```
{
  "status": 200,
  "message": "Sites have been successfully fetched.",
  "data": [
        {
            "createdAt": "2020-07-20T07:34:48.629Z",
            "updatedAt": "2020-07-20T07:34:48.629Z",
            "id": "5f154918d0f89d17dc18c4b9",
            "name": "ALE USA",
            "countryCode": "US",
            "isDefault" :true,
            "timezone": "US/Michigan",
            "address": "",
            "location": null,
            "zoom": 19,
            "imageUrl": "",
            "organization": "5f104b94b245362fe4ccfc90"
        },
        {
            "createdAt": "2020-07-20T07:34:48.629Z",
            "updatedAt": "2020-07-20T07:34:48.629Z",
            "id": "5f154918d0f89d17dc18c4b8",
            "name": "ALE Colombes",
            "countryCode": "FR",
            "isDefault" :false,
            "timezone": "Europe/Istanbul",
```

```
            "address": "",
            "location": null,
            "zoom": 19,
            "imageUrl": "images/brest.png",
            "organization": "5f104b94b245362fe4ccfc90"
        },
        ...
    ]
}
```


21 Oct 2025

9.4.4 Status Codes

Our API uses conventional HTTP response codes to indicate the success or failure of an API request.

In general: Codes in the `2xx` range indicate success. Codes in the `4xx` range indicate an error that failed given the information provided (e.g., a required parameter was omitted, a charge failed, etc.). Codes in the `5xx` range indicate an error with our servers.

The following success and error codes are managed by our APIs:

9.4.4.1 Success

Status code	HTTP Message	Description
200	OK	Everything worked as expected.
201	Created	Resource has been created successfully
204	No Content	Server has successfully handled the request and that there is no additional content to send in the response

9.4.4.2 Error

Status code	HTTP Message	Description
400	Bad Request	The request was unacceptable, often due to missing a required parameter.
401	Unauthorized	No valid Authentication provided.
403	Forbidden	You don't have permissions to perform the request.
404	Not Found	The requested resource doesn't exist.
406	Not Acceptable	Provided content-type header is invalid

Status code	HTTP Message	Description
409	Conflict	The request conflicts with another request (perhaps due to using the same idempotent key).
429	Too Many Requests	Too many requests hit the API too quickly.
500, **502**, **503**, **504**	Server Errors	Something went wrong on our API server.

You can find more about HTTP protocol in the RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content document.

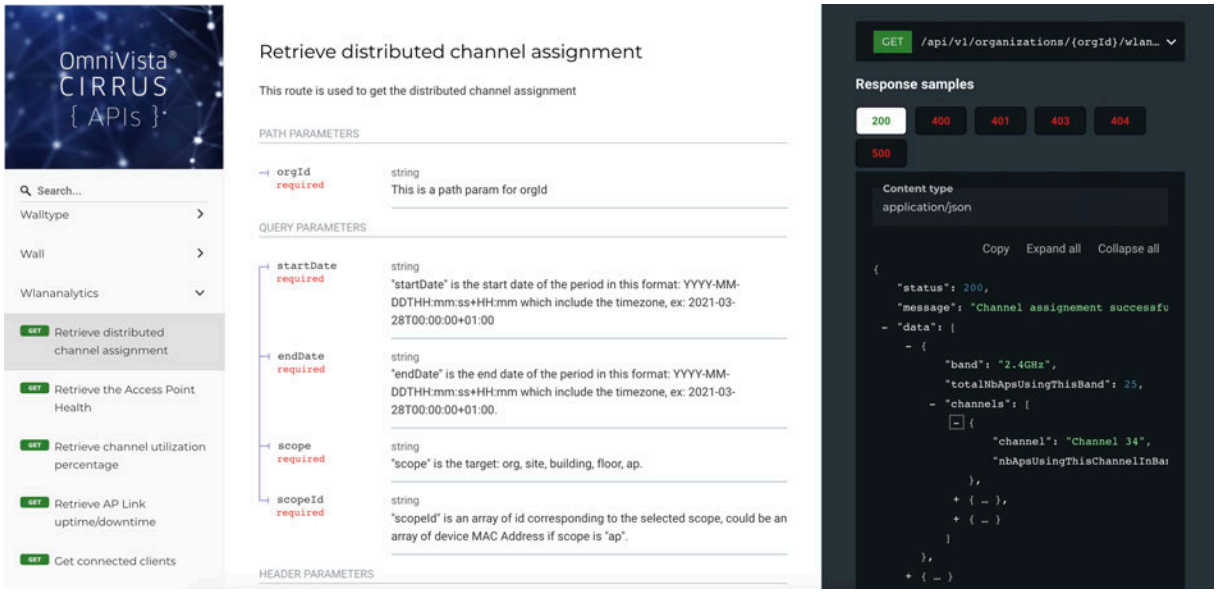
21 Oct 2025

9.5 API Reference

The complete API Reference is accessible from the following URLs depending on your region:

- EU: https://eu.manage.ovcirrus.com/apidoc/apidoc.html
- US: https://us.manage.ovcirrus.com/apidoc/apidoc.html

> The API Reference is based on the OpenAPI specification version 3.0.0.



21 The API Reference page

21 Oct 2025

10 Troubleshooting

The information provided on this page applies to general troubleshooting questions and actions when using OmniVista Terra. You can also find troubleshooting information embedded within the following features:

- Device Onboarding (see page 13)
- NaaS Device License Management (see page 262)
- AP Mesh (see page 238)
- IoT Devices (see page 904)
- Application Visibility (see page 862)
- Alerts (see page 948)
- Events (see page 981)

10.1 Troubleshooting Switch Management Problems (Management Connectivity, Configuration/Statistics Updates, Configuration Not Delivered)

If the version of the OmniVista Terra Agent is old (for example, switch was onboarded in a previous release) or the agent is stuck (not sending updates or accepting requests from OmniVista Terra), you may encounter the following switch management problems:

- Management connectivity turns on and off.
- Switch configuration and statistics are not updated in some of the UI screens.
- Configuration is not delivered to the switch.

If you do encounter any of the above switch management problems, consider the following troubleshooting tips:

- Check the OmniVista Terra Agent version, status, and supported actions here: https://docs.ovcirrus.com/ovtx/omnivista-cirrus-agent
- Update the OmniVista Terra Agent version by setting the Force Provisioning Flag (see page 453) (Device Catalog > CLI Based Provisioning > Results > Select a switch > Actions). Once this flag is set, OmniVista Terra will automatically update the version the next time the switch calls home. It can take approximately 5-10 minutes to update. To check if the switch has called home and the call home sequence has completed, check the timestamps in the Activation Server log (see page 969) (Device Catalog > Devices List > Select Switch > Diagnostic Tools > View Activation log).
- Ping the switch from the Device Catalog List (see page 169) (Device Catalog > Devices List > Select Switch > Actions > Diagnostic Tools > Ping). This can bring back the Management Connectivity in about 10-15 seconds.
- If management connectivity is “On”, you can Collect Switch Logs (see page 1018) (Monitor > Diagnostic Tools > Collect Support Info). In the tar file and inside techsupport archive, you will see ovng-monitoring and ovng-config logs. Check for any errors.

Tip: You can search a UI page quickly by using the Search bar at the top right of any page, near your Profile icon, left of Bell icon.

- If OmniVista Terra cannot reach the switch and you have access to the switch, try the following:
  Use the **show pkmgr** CLI command to verify the Agent was successfully downloaded and installed on the switch.

```
LabSwitch-> show pkgmgr
Legend: (+) indicates package is not saved across reboot
(*) indicates packages will be installed or removed after reload
Name              Version               Status             Install
Script
--------------+--------------------+-----------------
+--------------------------------
  ams             default               installed          default
  ams-apps        default               installed          default
  ovng-agent      3.5                   installed          /flash/
working/pkg/ovng-agent/install.sh
```

  Use the **show appmgr** CLI command to verify the two components of the Agent package (Config Agent and Monitoring Agent) were started.

```
LabSwitch-> show appmgr
Legend: (+) indicates application is not saved across reboot
 Application      Status    Package Name        User
Status Time Stamp
----------------+---------+-------------------+----------------------
+-------------------------
config-agent     started    ovng-agent          snmpRW
Fri Nov 22 02:25:37 2024
monitoring-agent started    ovng-agent          snmpRW
Fri Nov 22 02:25:45 2024
```

  Use the **appmgr start/restart** commands if the status is stopped. For example:

```
LabSwitch-> appmgr start ovng-agent config-agent
LabSwitch-> appmgr start ovng-agent monitoring-agent
```

- Check if the switch is connected to OmniVista Terra. The following command should report status as Connected:

```
debug ams show
```

- Check ovng-agent log files for errors:

```
LabSwitch-> ls -ltr /flash/ovng*
```

10.2 I signed up for a new account (or an invited account), but I can't find the verification email to activate my account

You can try to reconnect after 10 minutes; then OmniVista Terra will send a new verification email. If still no email is received, give the email address associated with the account to the OmniVista Terra 10 Super Admin. The Super Admin will provide you with the confirmation URL to verify your account.

10.3 My account has been successfully created but I don’t see any data in OmniVista Terra

To see data in the OmniVista Terra UI, please check that the following main steps have been completed:

- Access Points are upgraded to the supported build number. More information.
- The correct Ports in your Firewall are open and devices are not behind a proxy. More information.
- Devices are declared in your organization. More information.
- The date set in your Access Points is correctly configured for your Timezone.

10.4 From the OmniVista Terra UI, how do I know if my Access Points are connected to the platform?

When your Access Points are correctly configured and connected to the OmniVista Terra platform, you can see the date on which they issued data for the last time in the **Last Seen** column of the Device Catalog screen.

If you don’t see any date in this column, it means that the configuration of your Access Points has not been done properly. Please check this page for further details.

10.5 One of the three open browser tabs running OmniVista Terra is not responding

The problem may be caused by a compliment proxy or firewall tool (Endpoint). Please contact your IT department to verify.

10.6 I want to update a configuration object, but I can't click on the Save button. It is disabled (grayed out)

Try one of the following options to enable the Save button:

- Check to see if there are any fields on the screen that are required but they weren’t configured. If so, configure the required fields.

- Try changing another attribute/field with a current value or change a check box selection, then change it back.
- Try to refresh the updated page.

10.7 When I edit a configuration and click on “Launch … in a new browser tab” to open another screen to edit a related configuration, when I return to the main screen, the Save button is disabled (grayed out)

To enable the **Save** button on the main screen, complete other edits on that screen. When you only make changes to the related configuration screen in a new browser tab, the main screen does not reflect that any edits were made. For example, if you wanted to edit an Access Policy related to an SSID from the Customize SSID screen, you would click Edit and select "Edit Access Policy Page in a new browser tab". The Edit Access Policy screen will then open in another browser tab. After you make any changes in the Edit Access Policy screen, if you have not made any other changes in the Customize SSID screen, the Save button for the Customize SSID screen is disabled.

10.8 I open an SSH Terminal session after entering login credentials, but there is no message in the Terminal window console

There is a delay to open a connection to the device shell, as the console is waiting for the device's message. If it takes more than one minute and there is still nothing, please check the Internet connection, then close the console and restart a new SSH session.

10.9 The Access Point Health Threshold data doesn’t reflect the changes done even after saving the changes and getting the success notification message.

If the data doesn't reflect the changes after seeing the success notification message, click on the refresh button in the table or refresh the page to get the updated data.

10.10 The Device Health color and counter aren't updated after the threshold was saved and getting the success notification message.

1. Make sure the Access Point or OmniSwitch is running the minimum software required.
    a. AWOS 5.0.3 for an Access Point.
    b. 8.9R1 minimum (8.9R4 recommended) for an OmniSwitch.
2. Wait 1 to 2 minutes for the device to reflect the new threshold value.

10.11 I am not able to customize the WiFi4EU captive portal template for SSID and got error 500 when deploy changes to Access Point with layout type WiFi4EU.

To customize the WiFi4EU captive portal template, you have to upload another photo for the template’s banner as there is no button to edit the default template. However, you can edit the Login Background color and Login Button.

10.12 In Configuration Backup table, I got timeout message after waiting for 1 minute "Can not connect to the server, the request has been timeout. Please try again later."

There is an SSH connection issue between OmniVista Terra and the Switches. Please verify that SSH is enabled through the Switch CLI before performing an instant backup or scheduling a backup for the switch.

10.13 When I click on Full screen mode to put table in full screen mode, the top toolbar buttons disappear.

Try to zoom out to have larger screen resolution.

10.14 When I open an OmniVista Terra page, I wait for more than 15 seconds for the Loading the screen.

Try to refresh the page. If the error still persists, please inform the Tech Support team.

10.15 For the Guest Access code or Guest Account screen, I cannot find the Service level or Registration Profile selection when creating or updating a Guest Account or Guest Access code.

Try to refresh the page.

10.16 When I access the Wi-Fi Heatmap screen, the Device icon disappears upon selecting the Channel utilization option from the Device Layers drop-down list.

Go to the Device layers drop-down list. First, check the Channel Utilization option, then uncheck the Devices option and check it again. Now, both the Channel Utilization and Devices icons will display together.

10.17 When I try to copy the Golden Configuration content to the clipboard in the ‘Device Detail’ section on the left side of the screen (Monitor > Network > Analytics > Network Analytics), it does not work.

You can manually copy the Golden configuration content from the screen and use another user interface to duplicate it.

21 Oct 2025

11 OmniVista Terra Installation

The following information is covered in this section.

- Installation Introduction (see page 1050)
- Prerequisites (see page 1051)
- Deploying OmniVista Terra on VMware ESXi (see page 1052)
- OmniVista Admin Center (see page 1064)
- Configuring DNS for OmniVista Terra (see page 1075)
- How to Onboard an AP and Switch (see page 1076)
- License Management Overview (see page 1078)
- Uploading AOS/AWOS Images (see page 1080)
- Guidelines and FAQs (see page 1082)

11.1 Installation Introduction

This document details the OmniVista Terra 10.5.1 installation procedure. OmniVista Terra 10.5.1 can be installed as a fresh installation from a downloaded file available on the Customer Support website. OmniVista Terra is distributed as a Virtual Appliance only. There are no other standalone installers (e.g., Windows/Linux). It is installed as a Virtual Appliance, and can be deployed on the system and hypervisors defined in the Prerequisites section.

11.1.1 Deployment and Installation Overview

Below is an overview of the steps required to deploy and configure OmniVista Terra.

1. Deploy OmniVista Terra on VMware ESXi virtual machine.
2. Configure OmniVista Terra using the OmniVista Admin Center.
3. Configure Windows DNS settings.
4. Obtain and import licenses using the Subscription Manager.
5. Begin onboarding devices.

11.2 Prerequisites

Please read the following prerequisites and deployment information prior to installing OmniVista Terra 10.5.1.

Pre-requisites:

1. Download the OVTX OVA file and Build release file (.7z file) from the MyPortal website.
2. Have a VMware ESXi server with version 8.

The information below provides required minimum hypervisor configurations for the OmniVista Terra VM. You will need to install 3 nodes for OV Terra each with the below mentioned requirements. Check hardware availability on the server before installation.

- Supported Virtualization Platform: VMware
- Number of Virtual Machines Required: 3
- Minimum ESXi Version: 8

Hardware Requirements per Virtual Machine:

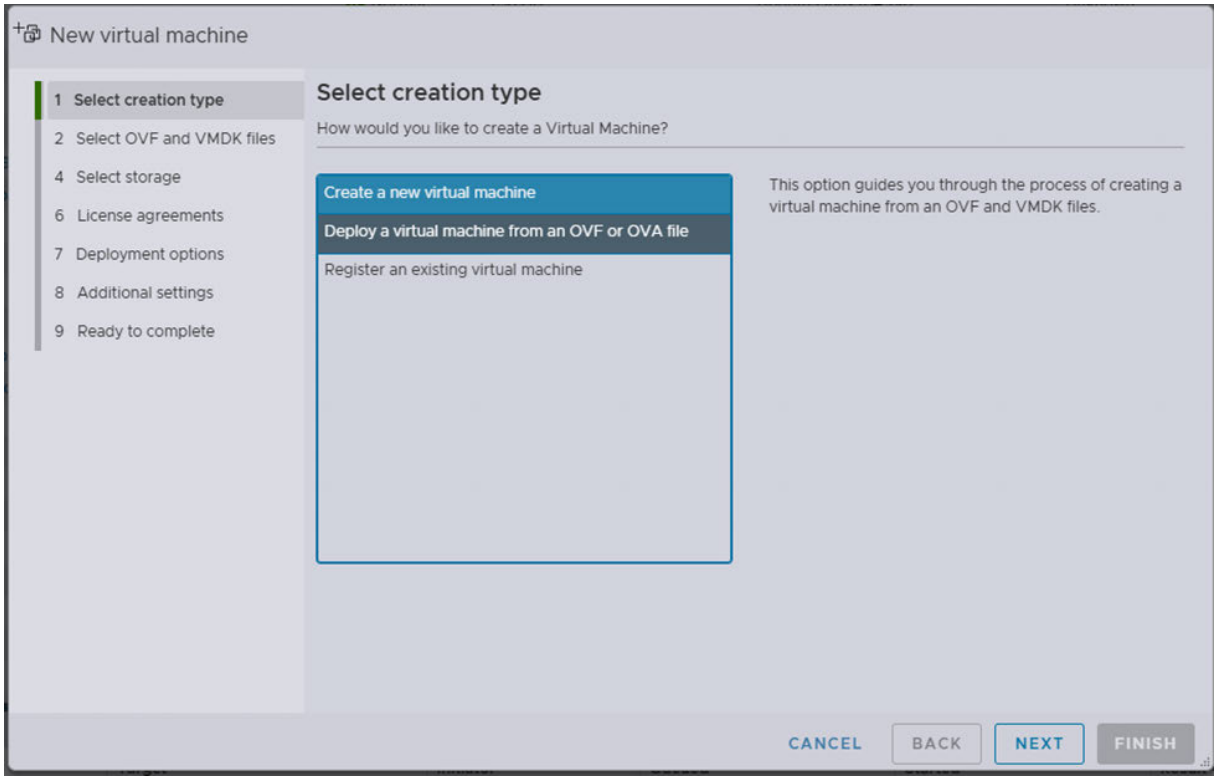
- Processors: 8 vCPU @ 3Ghz Minimum
- CPU Must Support AVX/AVX2 Instructions - In a vCenter cluster configuration, it is required to enable EVC mode with the CPU baseline set to **“Ice Lake”** (3rd Gen Xeon) or later. This ensures support for advanced CPU instruction sets such as AVX and AVX2. As a minimum requirement, the **“Broadwell”** baseline may be used
- RAM: 32 GB
- Disk Type: SSD (Minimum 50 MB/s read/write speed)
- System Disk: 200 GB
- Data Disk Size: 3 TB

Note: The HA L2 cluster supports a 3-node setup ONLY in version OVTx 10.5.1.

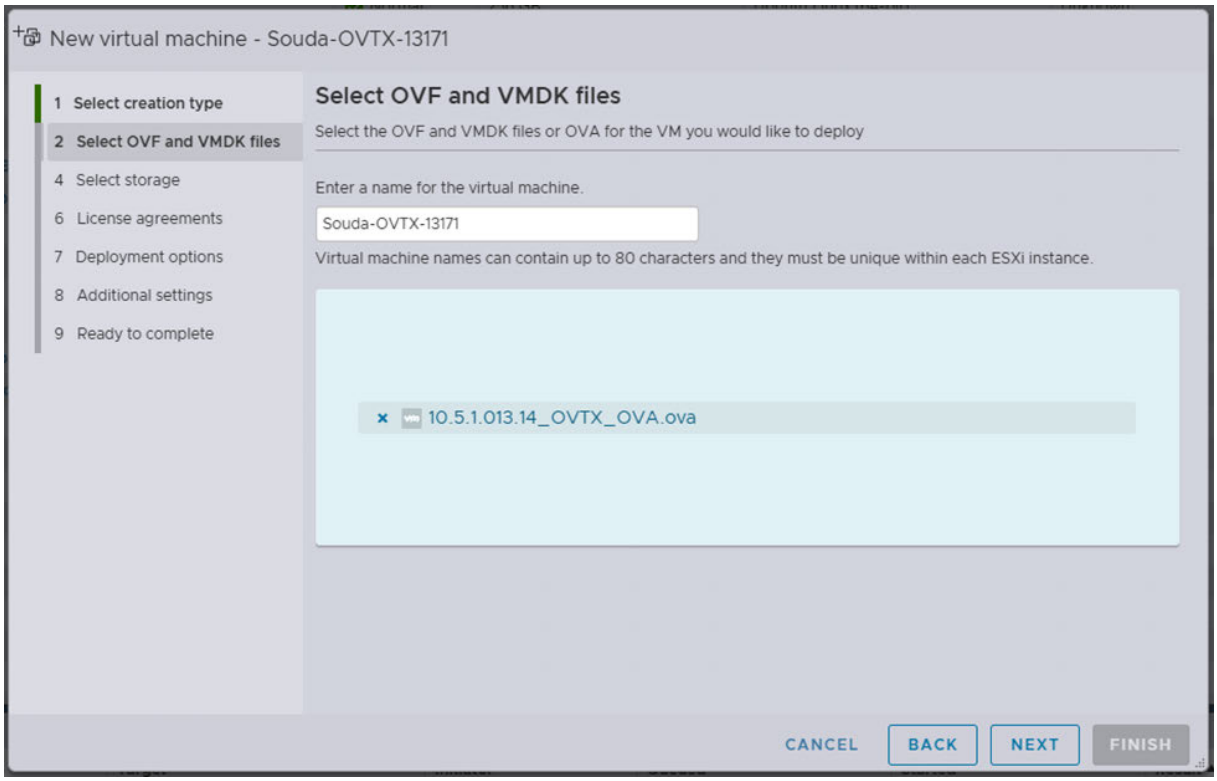
The content of this installation guide is intended for example purposes only. Configuration details should be customized to align with the specific requirements of each individual installation.

11.3 Deploying OmniVista Terra on VMware ESXi

1. Login to ESXI server and click on **Create / Register VM** button.
2. Select **Deploy a virtual machine from an OVF or OVA file** option and click on **Next** button.

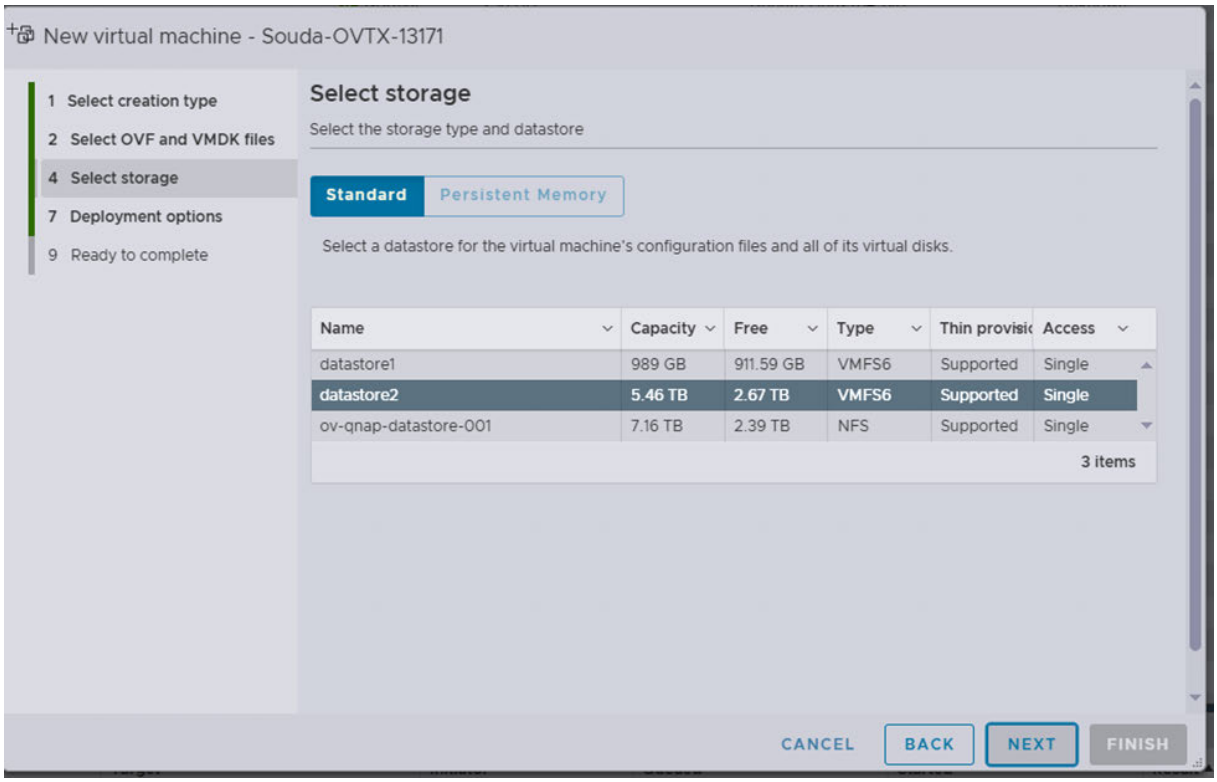


3. Enter the Name (ex: ovtx-13171) and click on **Click to select files or drag/drop** option and select the downloaded OVA file.

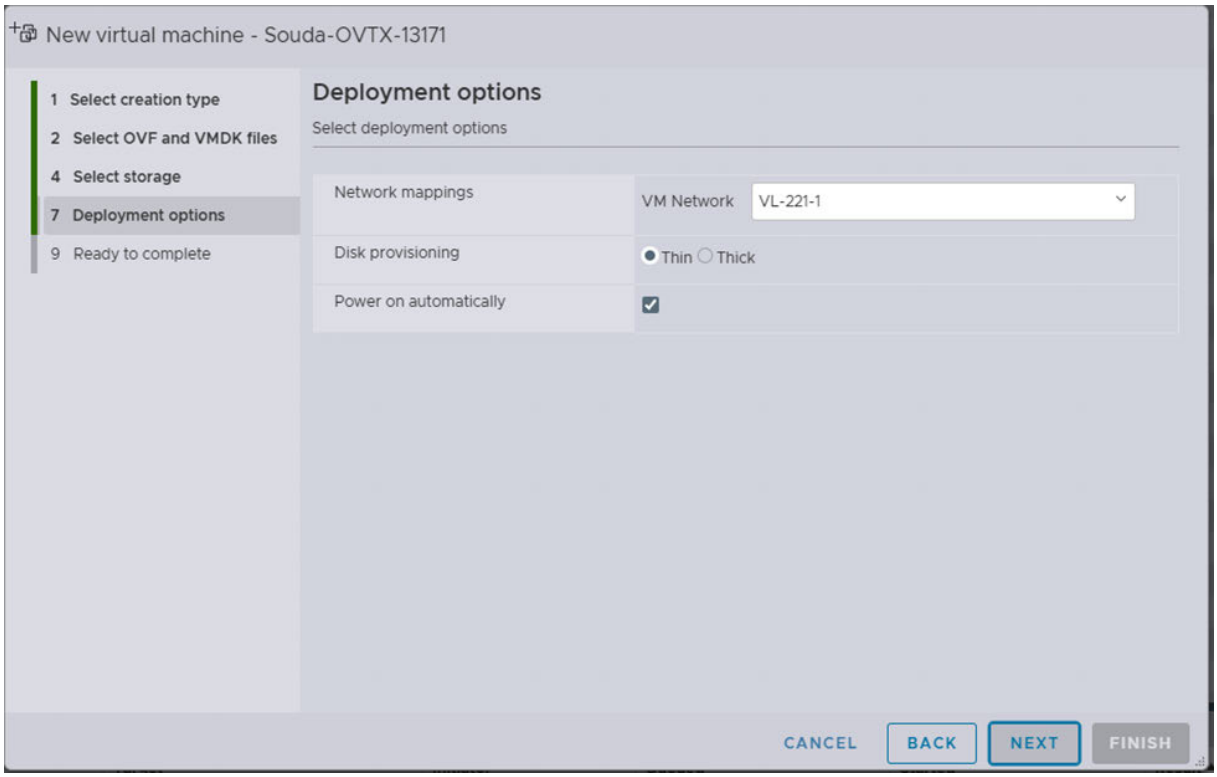


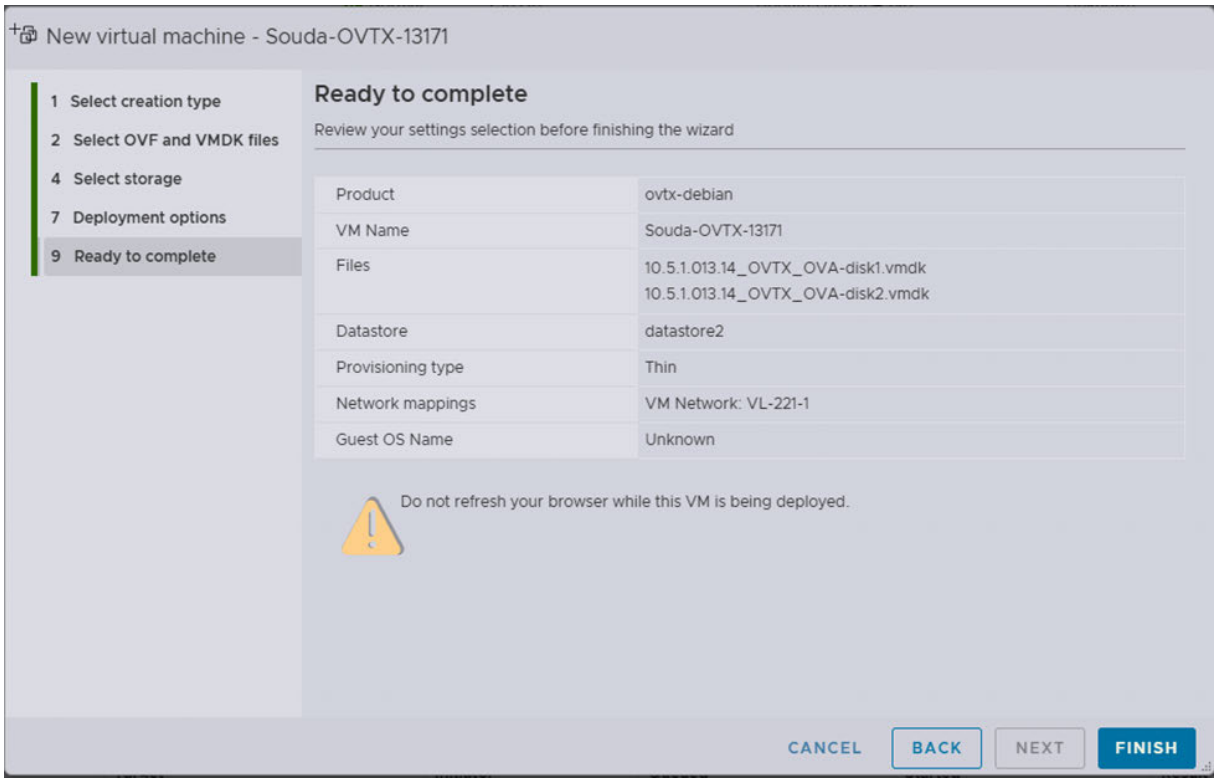
4. Click on **Next** button and then click on **Next** button again.
5. Select the storage option.

> Disk Provisioning may be set to Thick as the default option. Select the Thin option if the total disk available for 3 nodes together is less than 9TB.

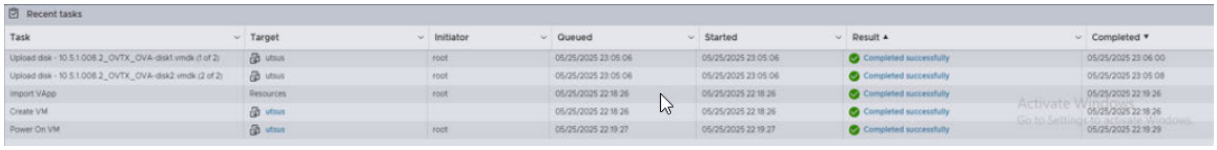


6. Select the NIC card from the dropdown based on your network and then click on **Next** button and then click on **Finish** button.

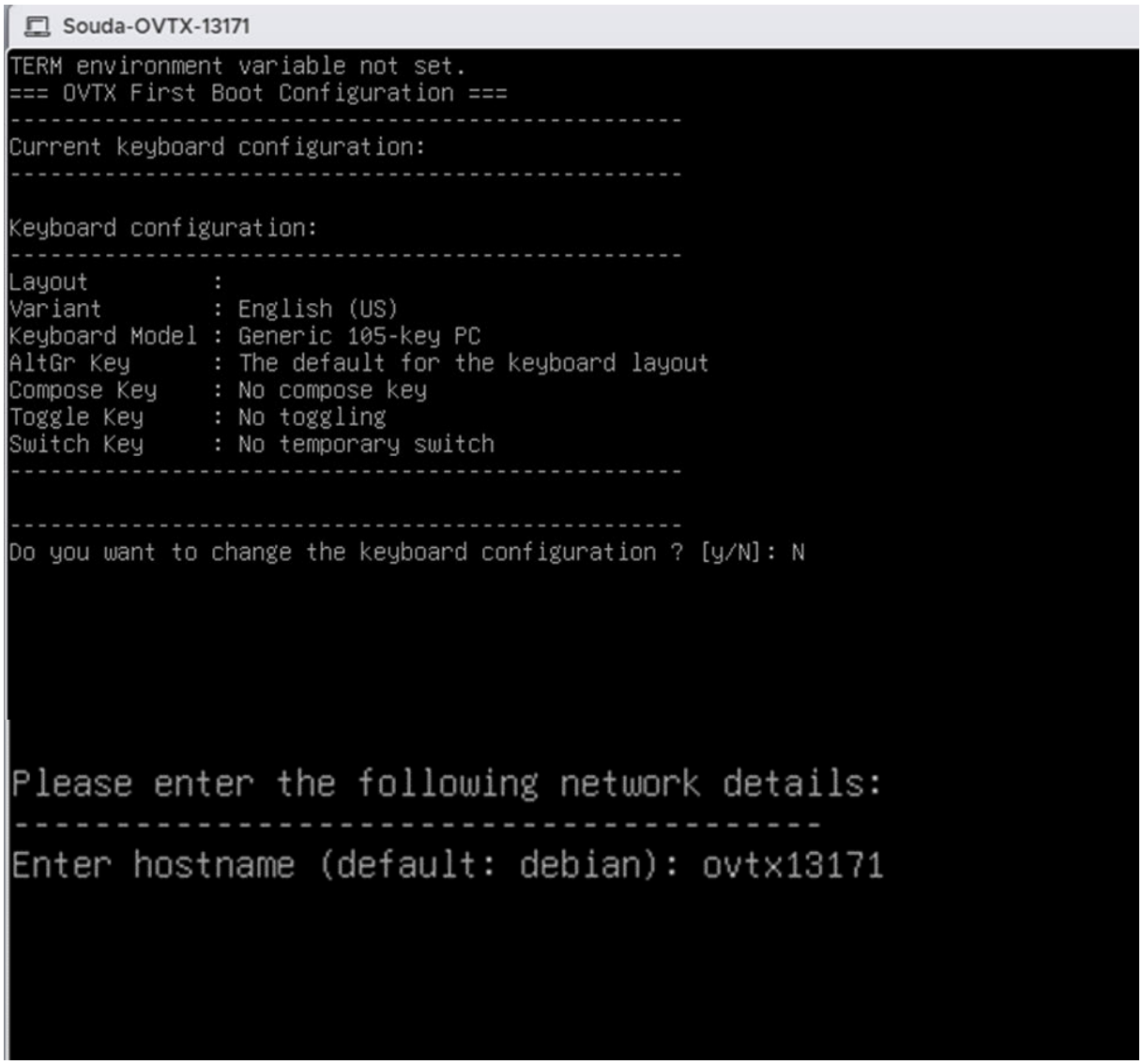




7. Wait until the process is completed.



8. Open the console of the created VM and click on **Enter**.
9. Follow the screen prompts to configure the keyboard options.
10. Enter the hostname: For example : **ovtx13171**. (Use any unique name for all the 3 VMs. The hostname should be unique for all the 3 VMs)



11. Enter IP address: For example **10.95.161.31**. (Use an available IP address from your network corresponding to the NIC selected in the step above)
12. Enter netmask: For example **255.255.255.0**.
13. Enter gateway IP: For example **10.95.161.1**.
14. Set the primary DNS and secondary DNS to the settings that will be able to resolve myovterra.myovcloud.com. If left blank, defaults will be used.
15. Configure the ovtx user password

- Enter ovtx user password:
- Confirm ovtx user password:
- Apply this configuration (y/n) : **y**
- The system will reboot. Wait for sometime and then the ovtx login prompt will be displayed.

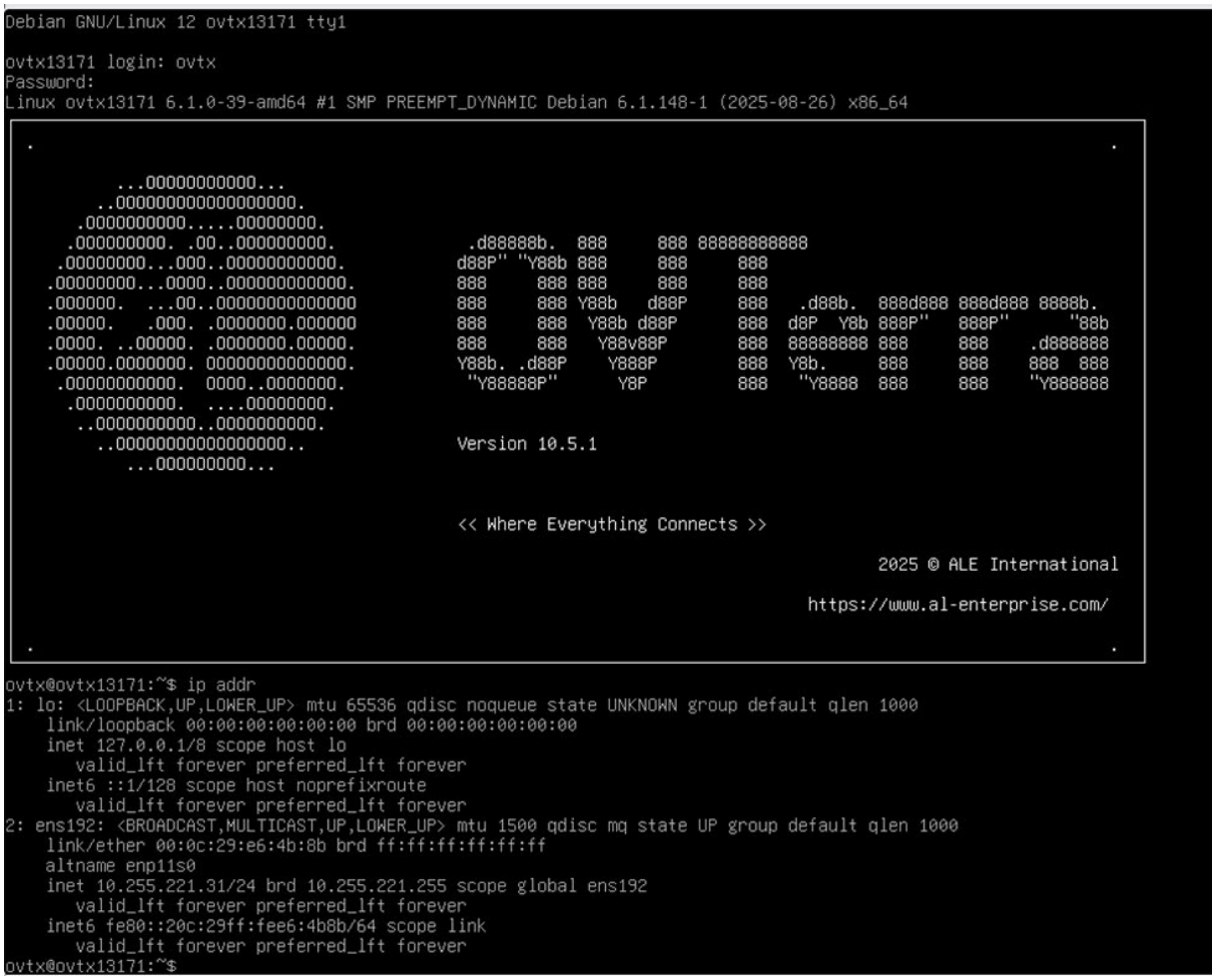
```
Please enter the following network details:
---------------------------------------
Enter hostname (default: debian): ovtx13171
One network interface found. Automatically selected: ens192
Enter IP address(default: 192.168.0.100): 10.255.221.31
Enter netmask (default: 255.255.255.0): 255.255.255.0
Enter gateway IP: 10.255.221.254
Enter primary DNS (default: 8.8.8.8):
Enter secondary DNS (default: 8.8.4.4):

=== OVTX User Configuration ===
---------------------------------------
Enter OVTX user password:
Password is strong and meets all criteria.
Confirm OVTX user password:

Summary of configuration:
------------------------------
Hostname: ovtx13171
IP Address: 10.255.221.31
Netmask: 255.255.255.0
Gateway: 10.255.221.254
Primary DNS: 8.8.8.8
Secondary DNS: 8.8.4.4
OVTX Password: [hidden]

Apply this configuration ?
Type Y - To apply the configuration and system will reboot
Type any key - To reconfigure
(Default Y): Y
Network settings applied successfully.
Replace IP address in /lib/systemd/system/rqlite.service with the newly set one
Restart rqlite service (May take a while)
```

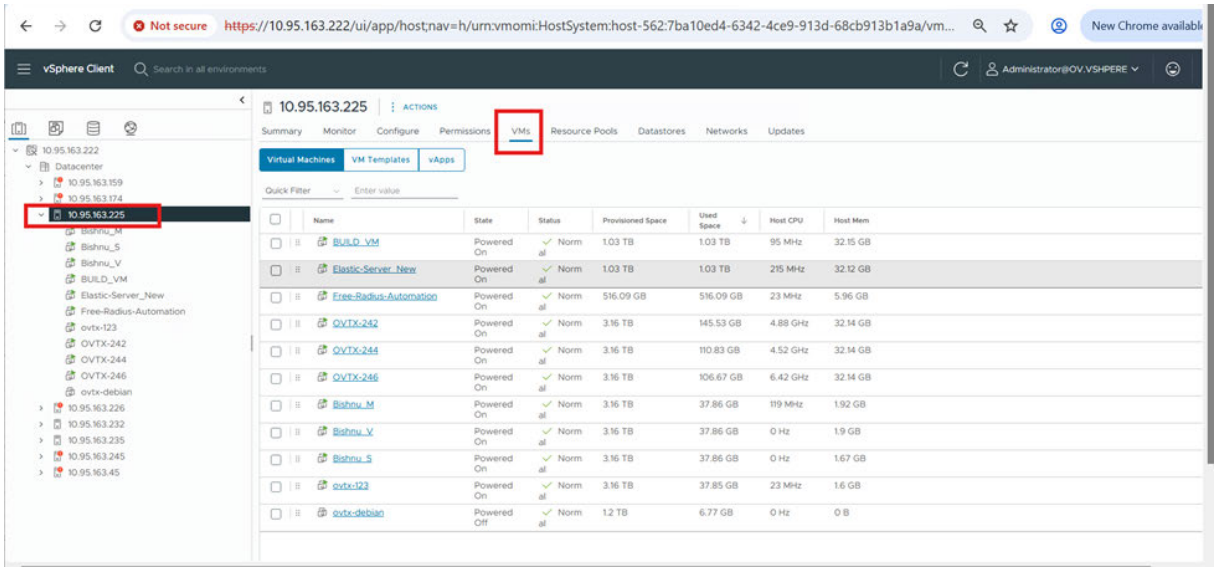
16. Login with username **ovtx** and with the configured password.
17. Run the command **ip addr** to confirm the IP address is correctly configured.



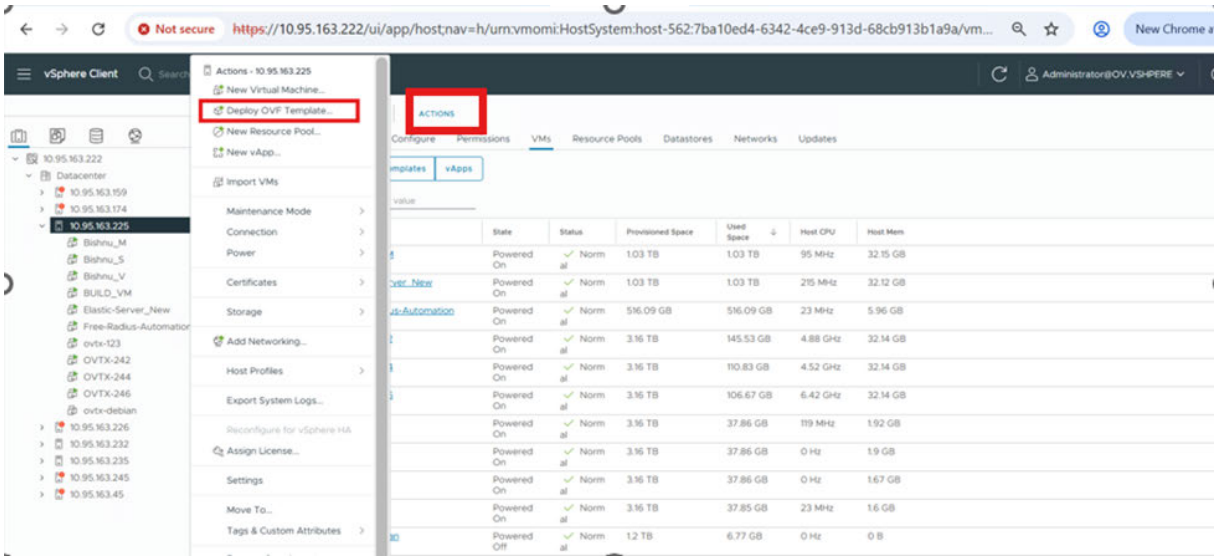
18. Create a 2nd and 3rd node following the above steps but with different IP addresses.

11.4 Deploying OmniVista Terra from vSphere Client

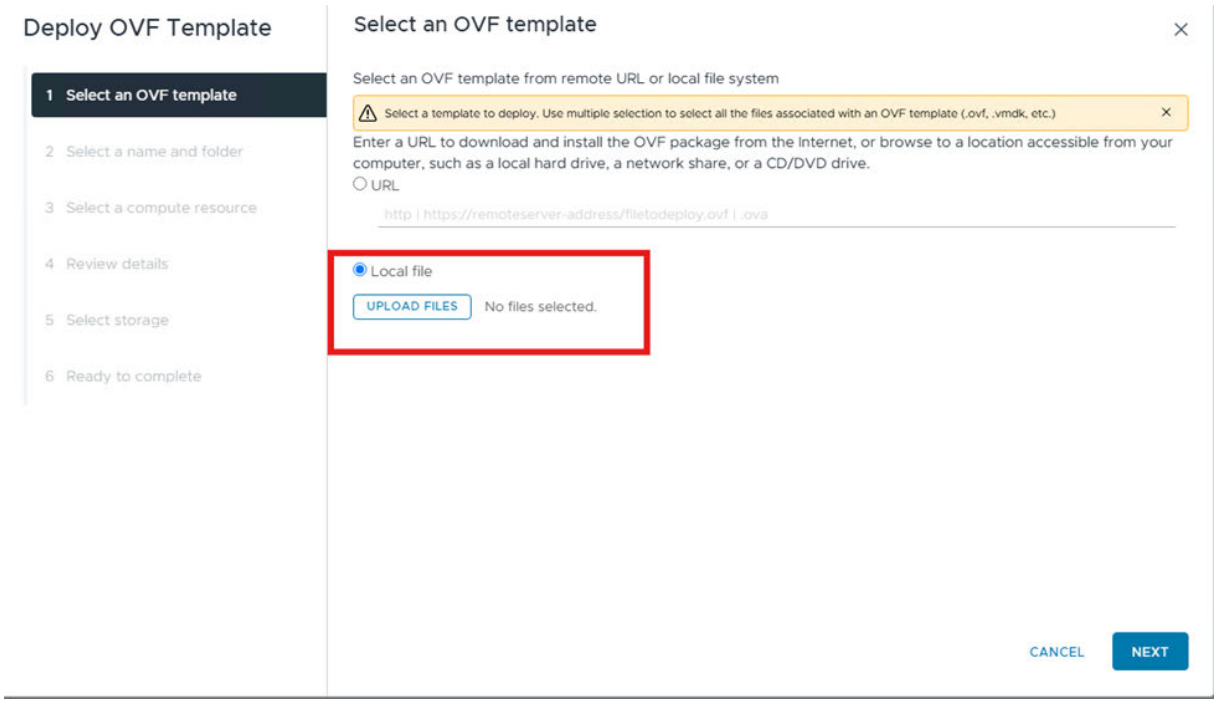
1. Login to vSphere Client and select the ESXI server on the left side of the screen from which you want to create the ovtx nodes.
2. Click on the **VMs** button.



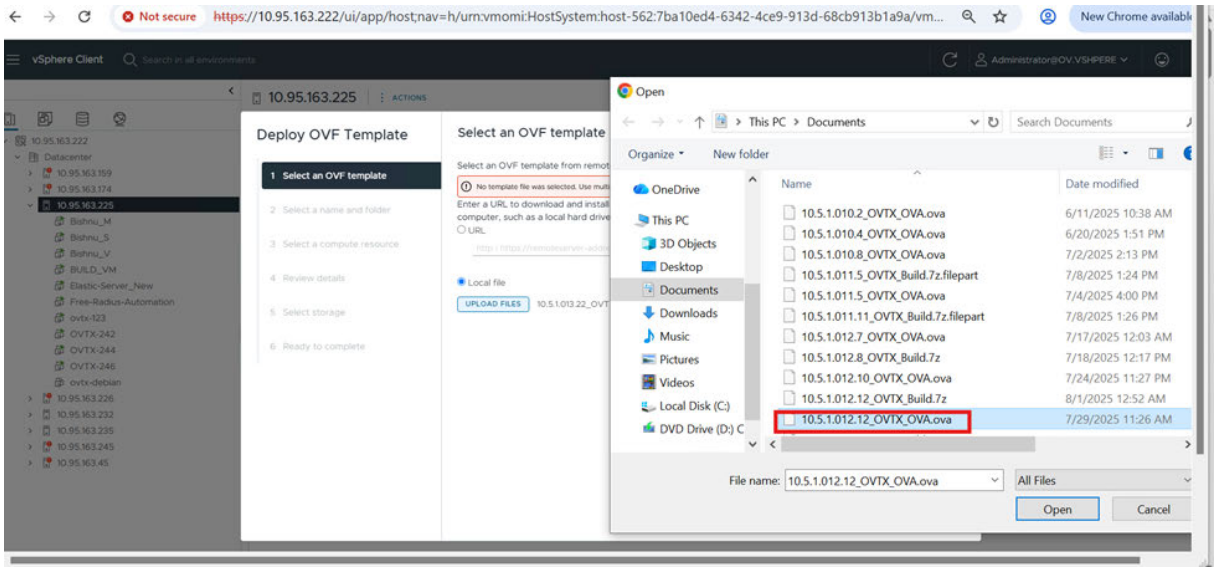
3. Click on the **Actions** button and then click on the **Deploy OVF Template** option or right-click on the required ESXI server and then click on the **Deploy OVF Template** option.



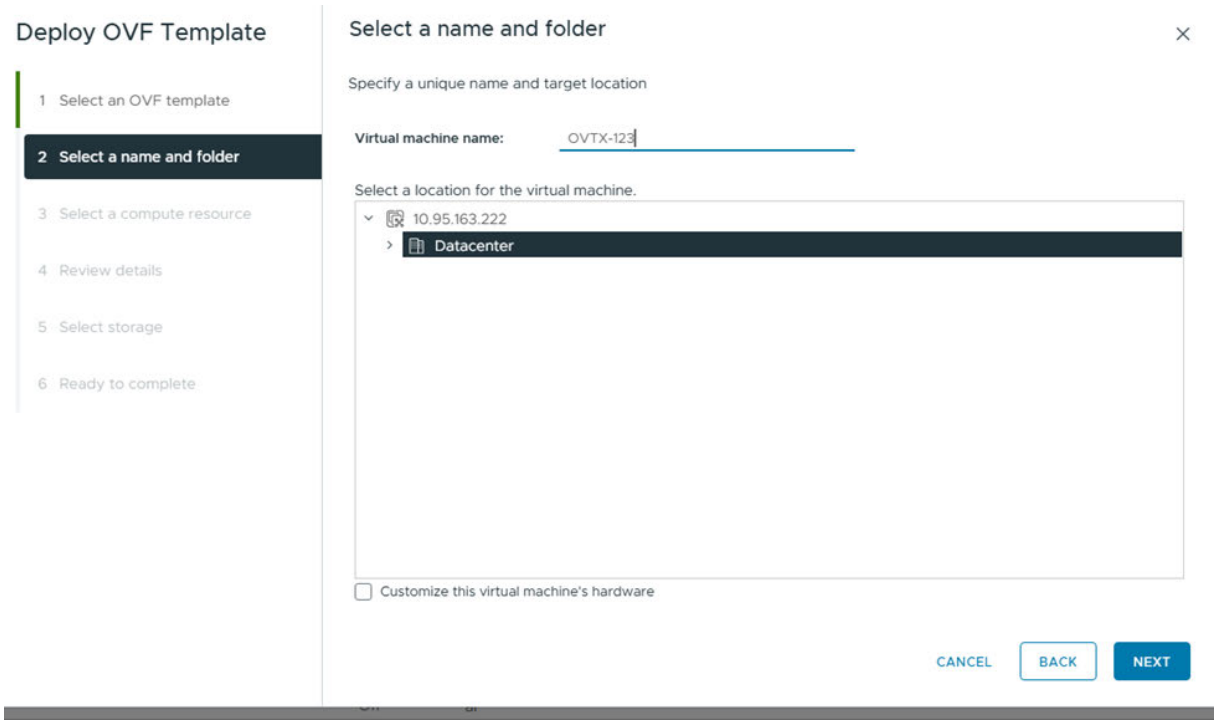
4. Select the **Local file** radio button and click on the **UPLOAD FILES** option.



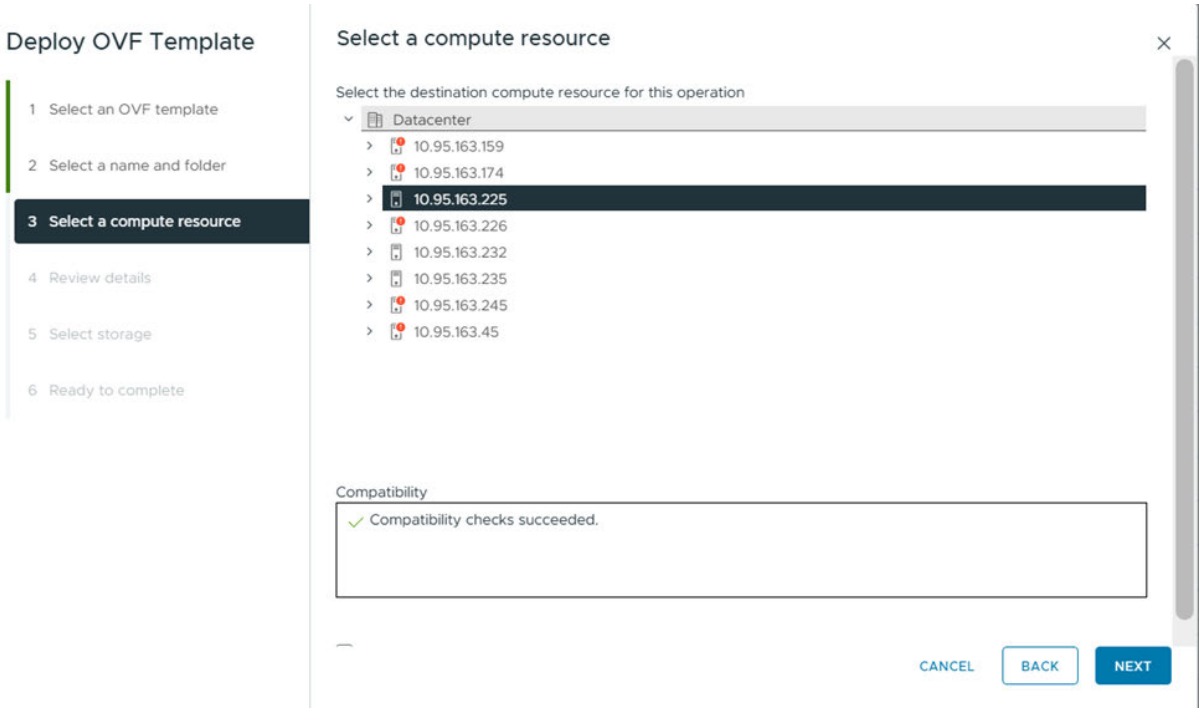
5. Select the downloaded OVA file and then click on **Open**.



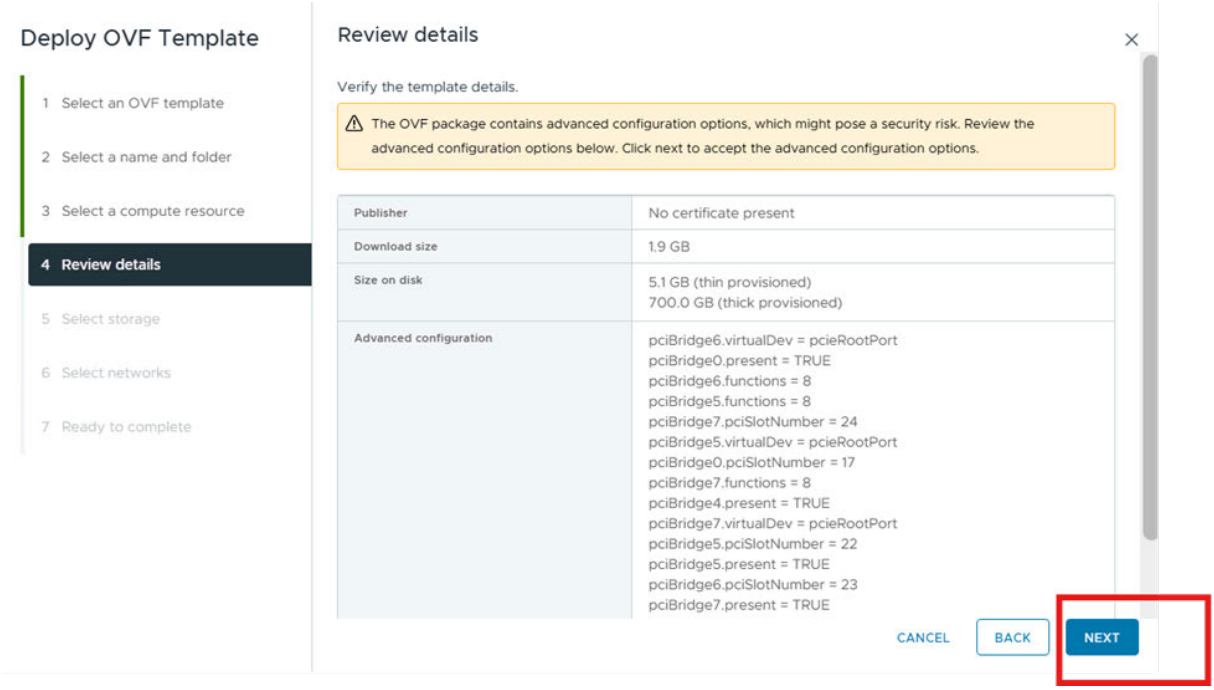
6. Click on the **Next** button.
7. Enter the virtual machine name and then click on the **Next** button.



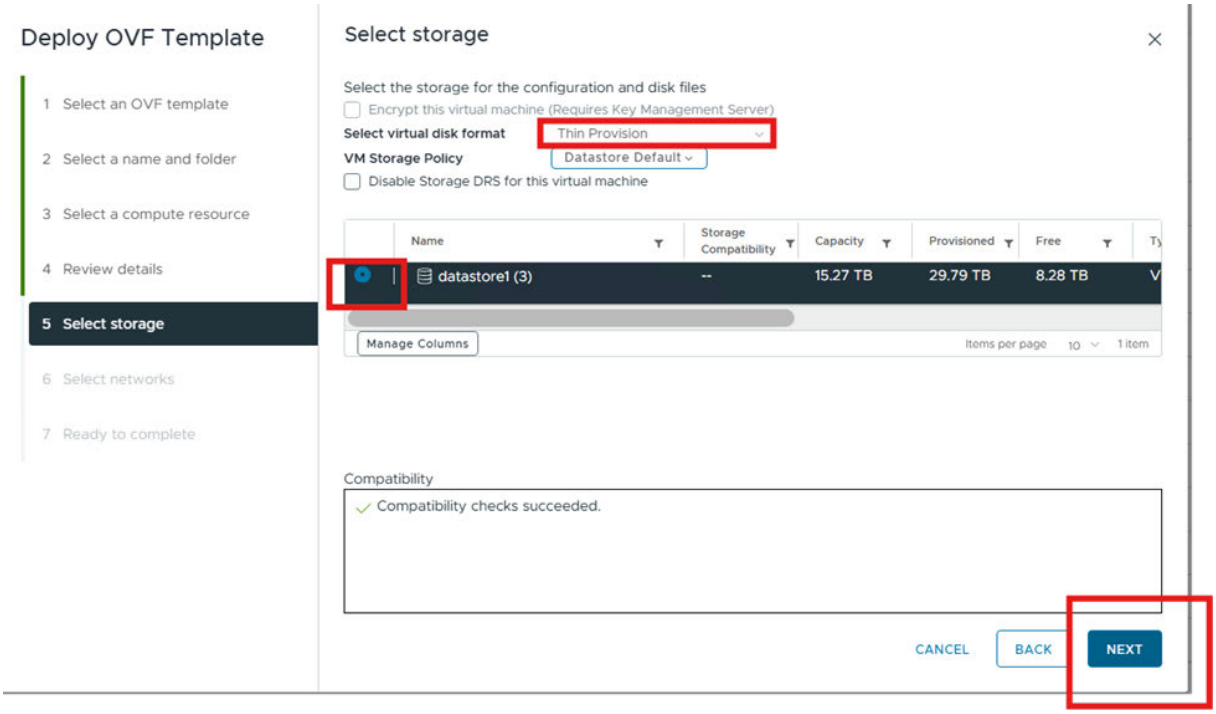
8. Choose the ESXI server or keep the default one and then click on the **Next** button.



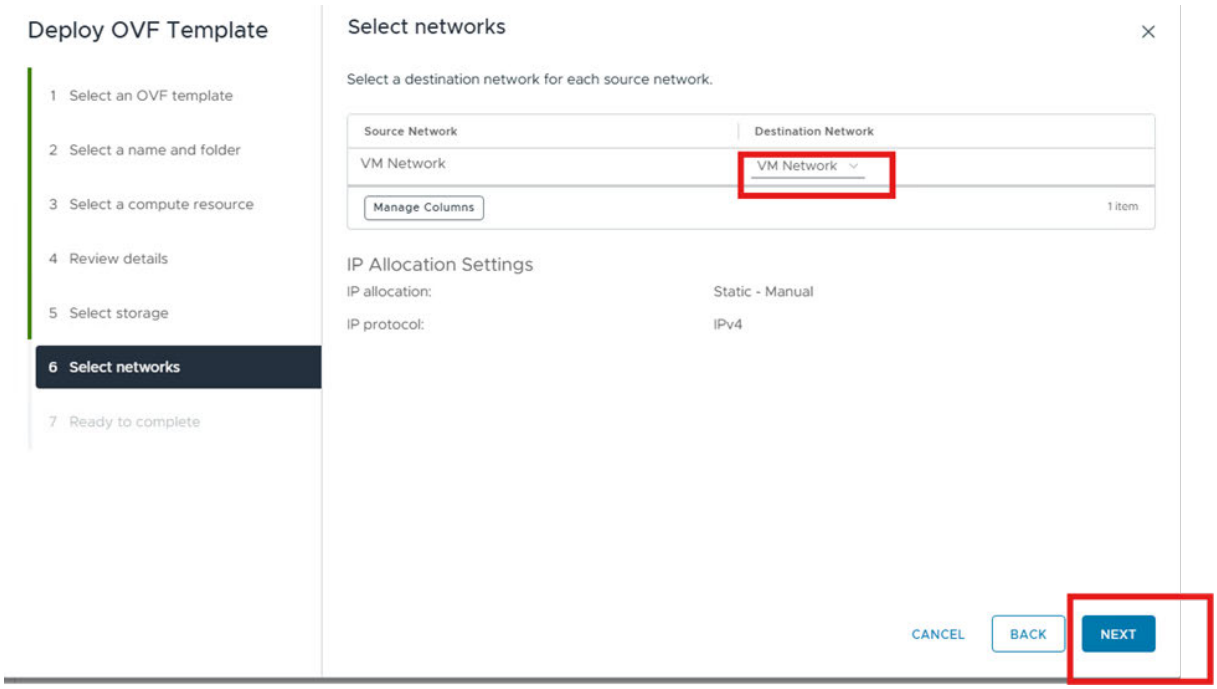
9. Click on the **Next** button.



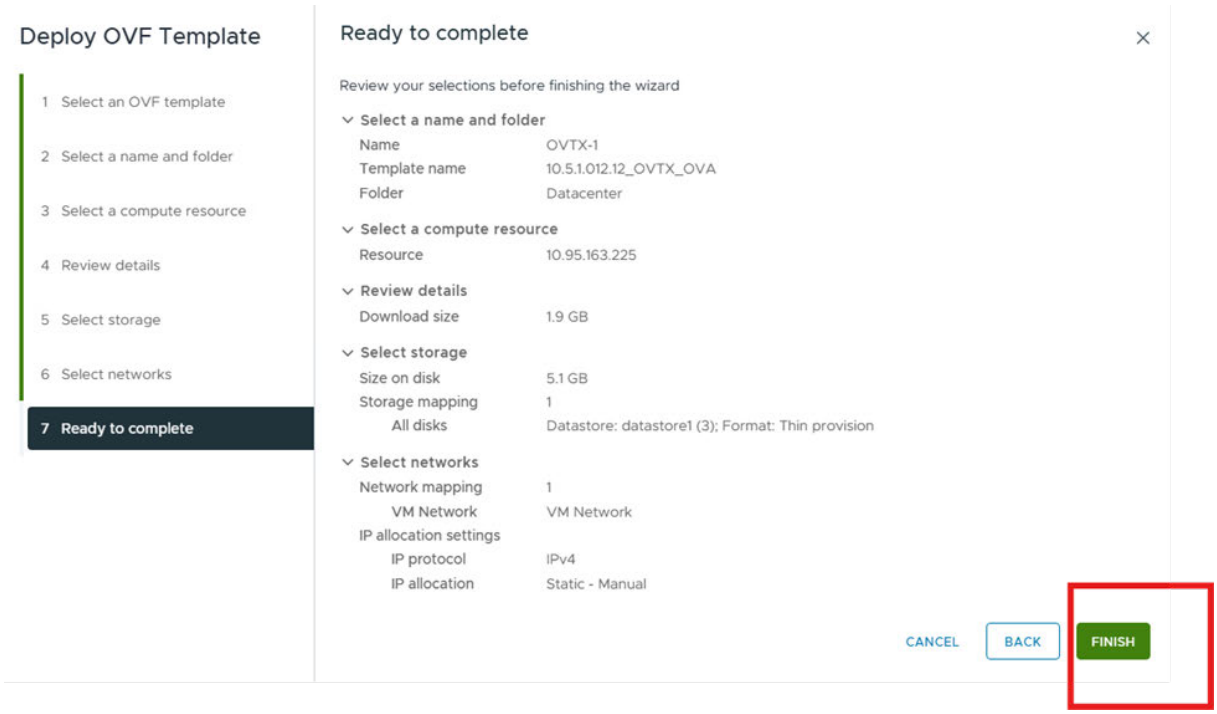
10. Select the datastore radio button and then select **select virtual disk format** as **Thin Provision** and then click on the **Next** button.



11. Select the network adapter based on your network and then click on the **Next** button.



12. Review the details and then click the **Finish** button.



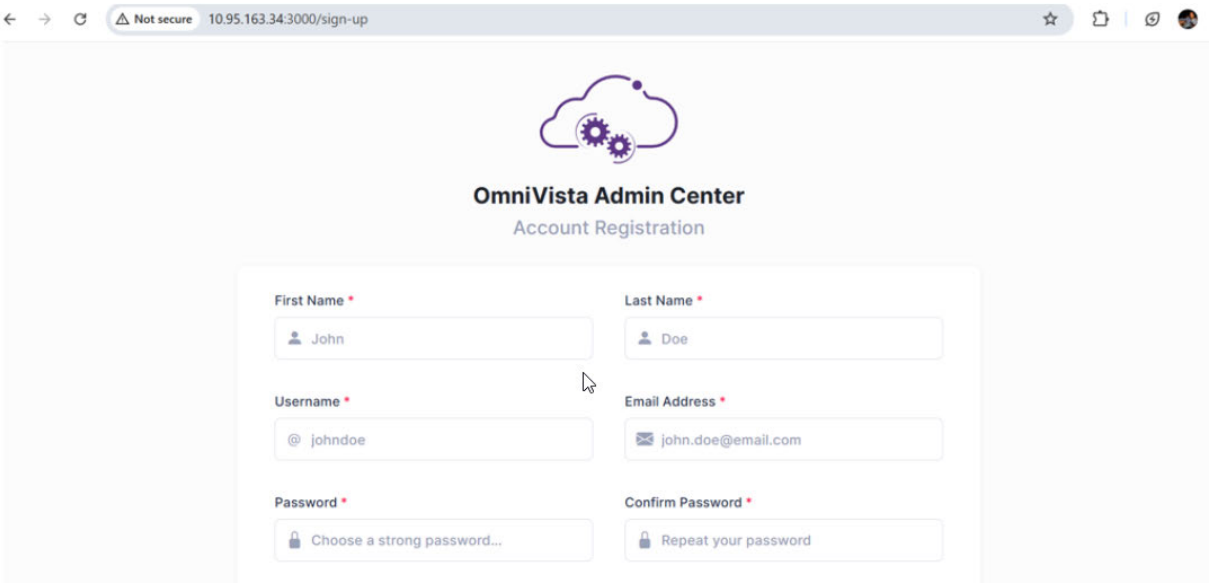
13. Wait until the process is completed.
14. Follow the remaining steps from **step 8** from the link below:

Deploying OmniVista Terra on VMware ESXi (see page 1052)

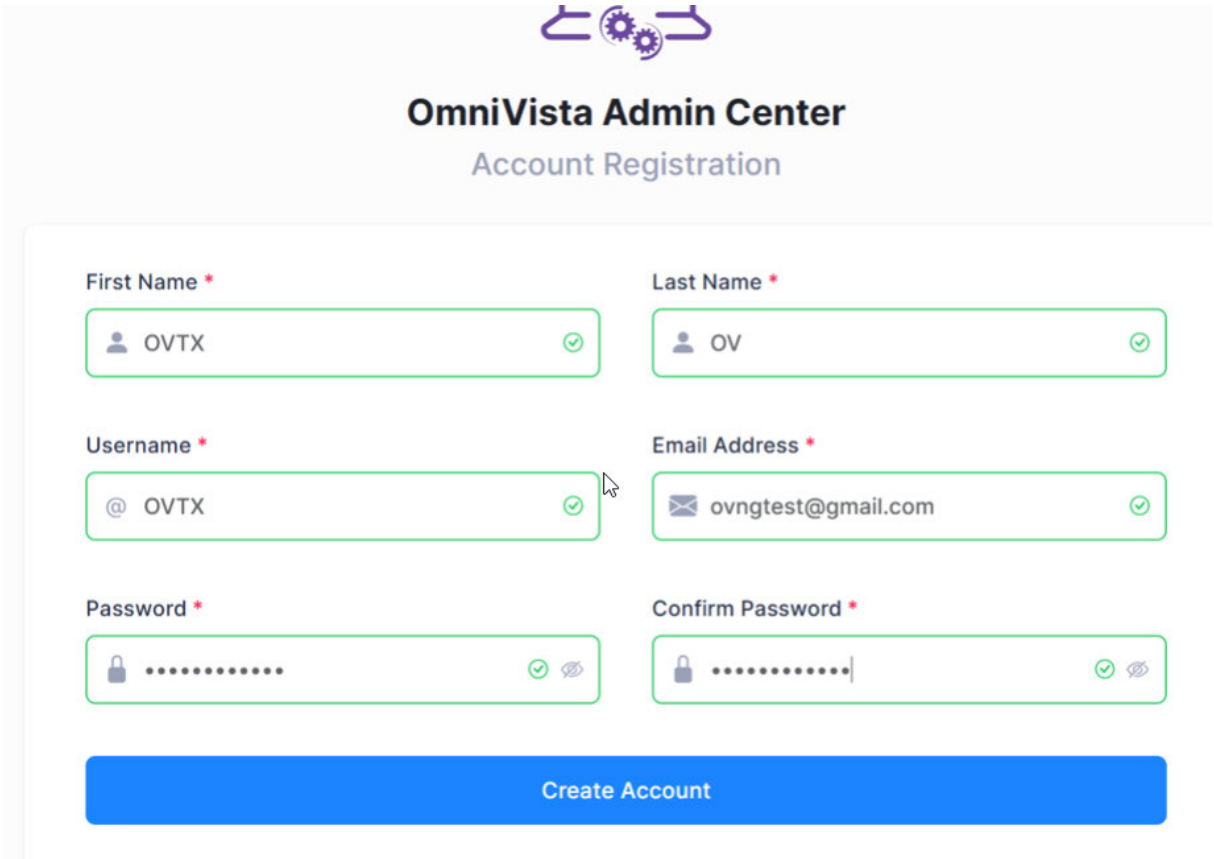
11.5 OmniVista Admin Center

11.5.1 Accessing the OmniVista Admin Center

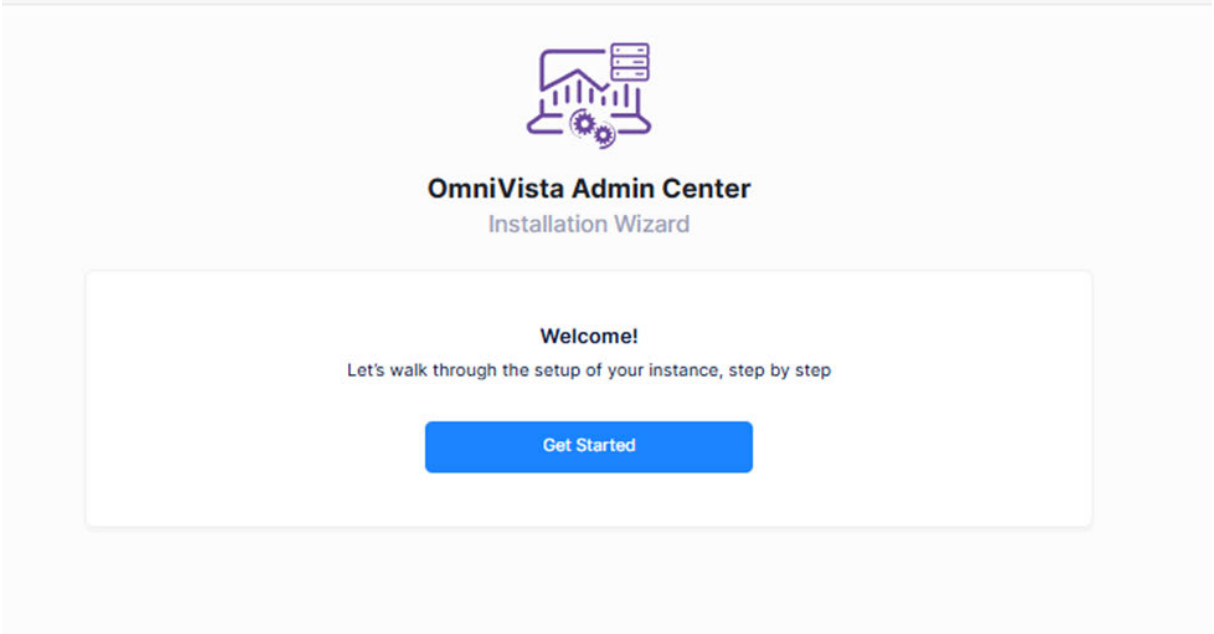
1. Using any one of the node IP addresses (ex:10.35.x.y) with port **3000**, the Admin Center can be opened.



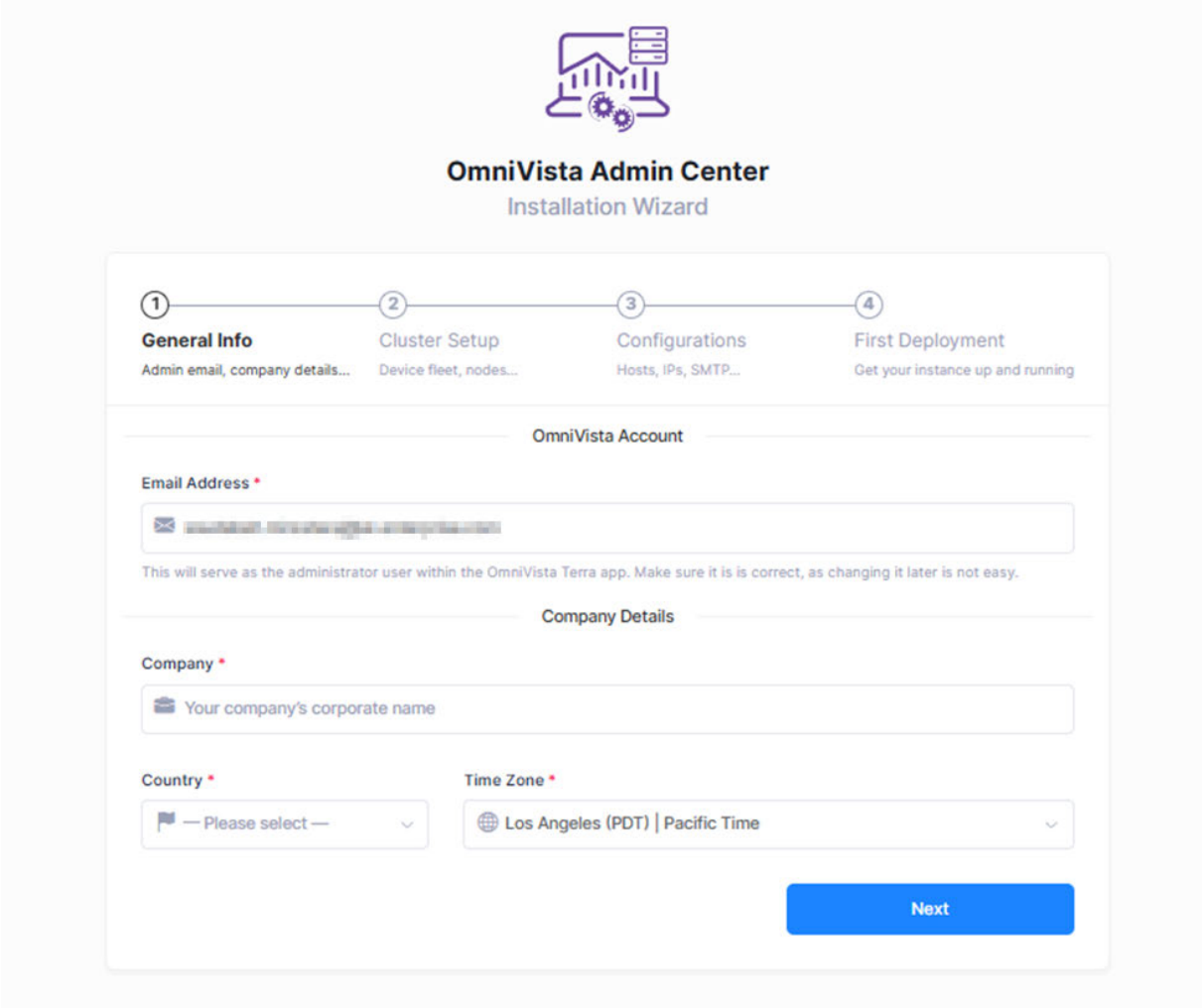
2. Enter all the required information and then click on **Create Account** button .



3. After receiving a successful message the Installation Wizard page will open. Click on the **Get Started** button.

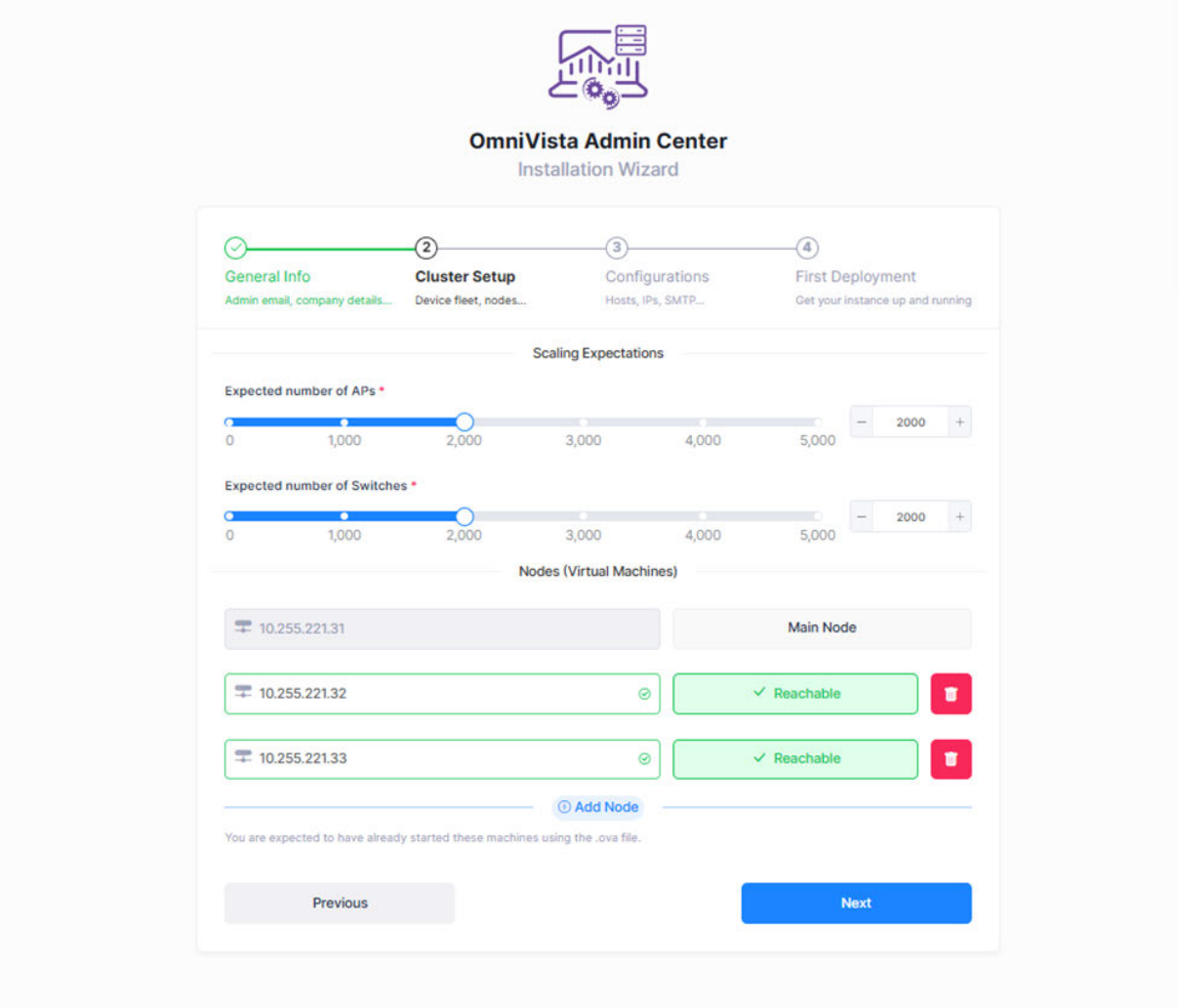


4. Enter the required details and click on **Next** button.



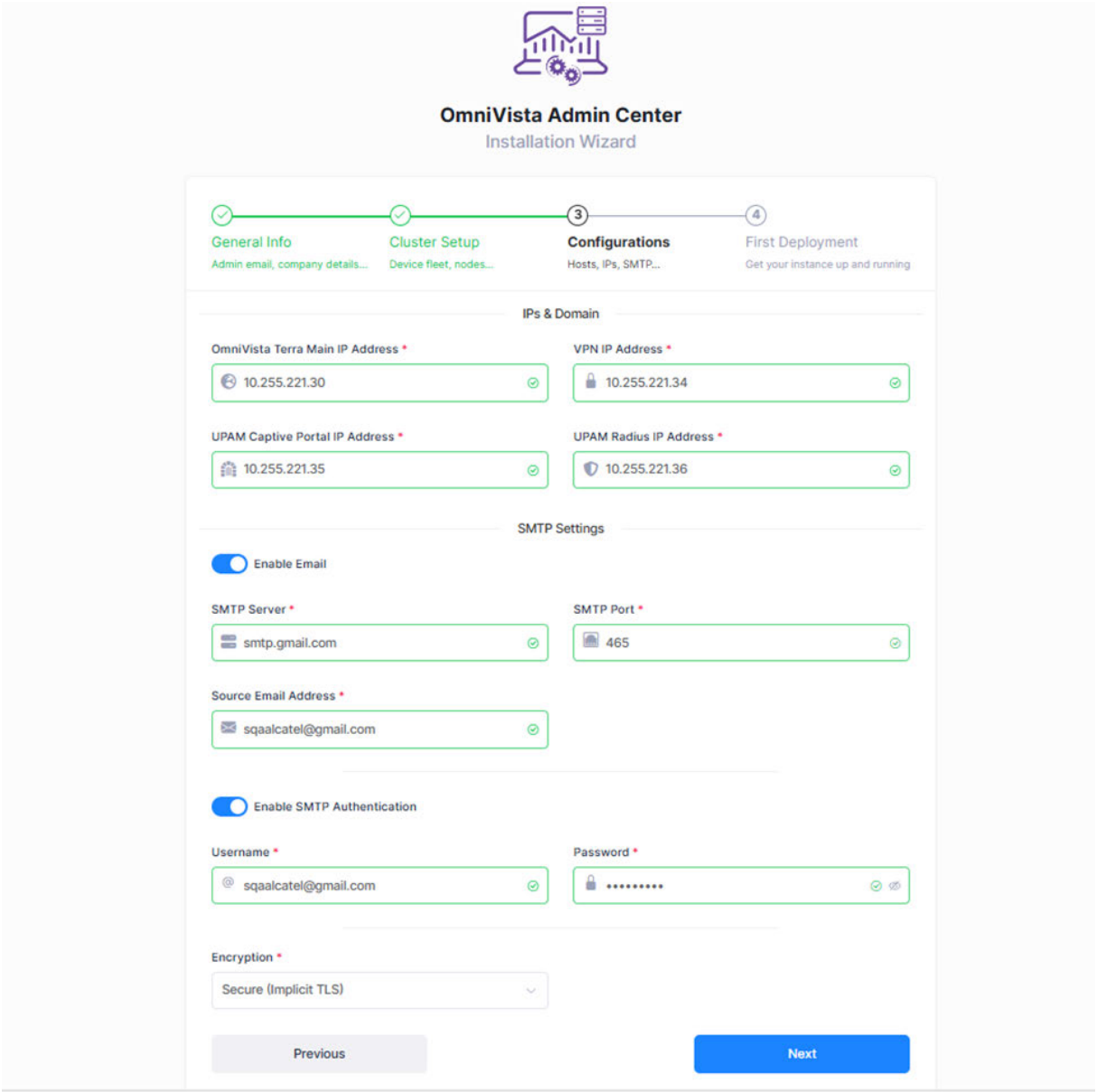
5. Select the expected number of APs , expected number of switches, enter the second node IP address and click on **Check** button. Enter the 3rd node IP address and click on **Check** button, nodes should be reachable. Click on **Next** button.

Configuring the expected number of APs and Switches is not currently implemented and has no effect during installation.



6. Enter the details below for IP & Domain and SMTP settings and click on **Next** button.

> The OmniVista Terra Main IP Address cannot be the same as the IP address for the main node. All IP addresses specified here should be unique and different from the node IPs.



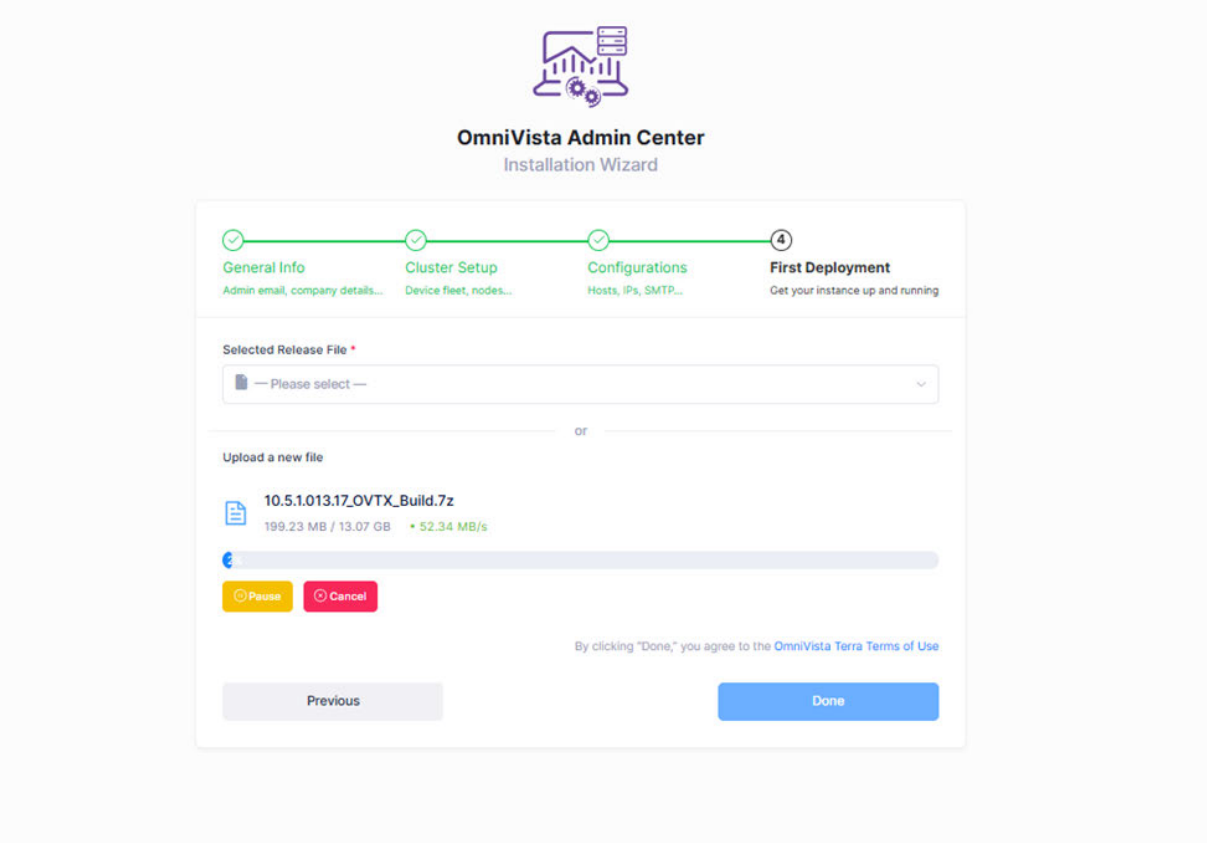
Enter your company's SMTP server settings, for example.
SMTP Settings:

- SMTP Server: smtp.gmail.com
- SMTP Port: 465
- Source Email address: mailto:example@gmail.com

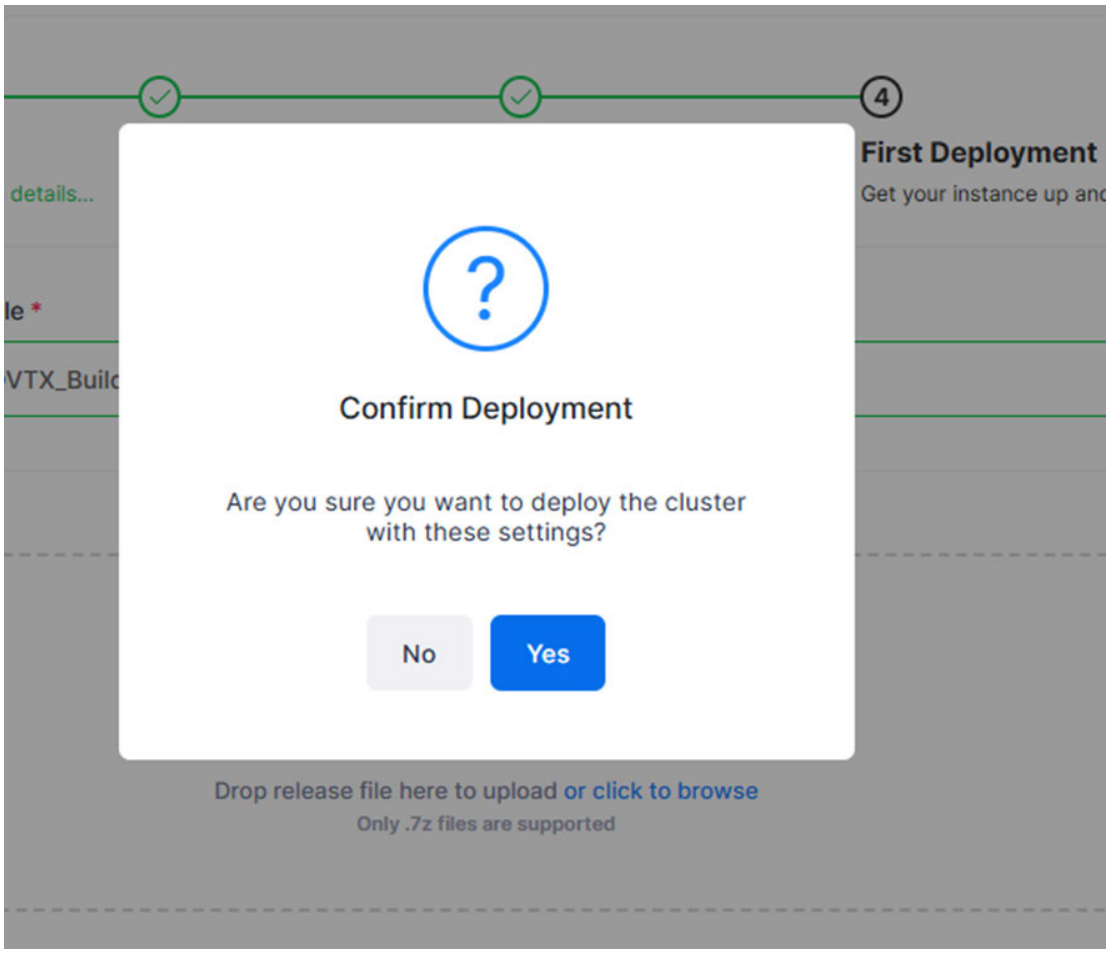
Enable SMTP authentication:

- User Name: mailto:example@gmail.com
- Password: **********
- Encryption: Secure (Implicit TLS)

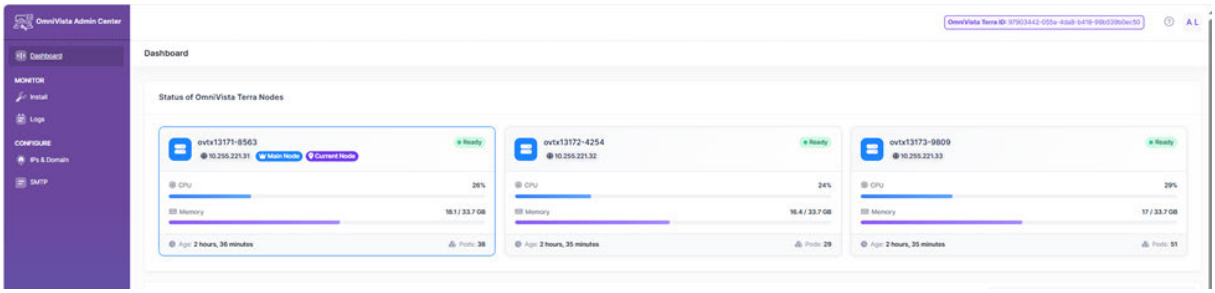
7. Select the build release file and wait until the release file is uploaded and then click on **Done** button.



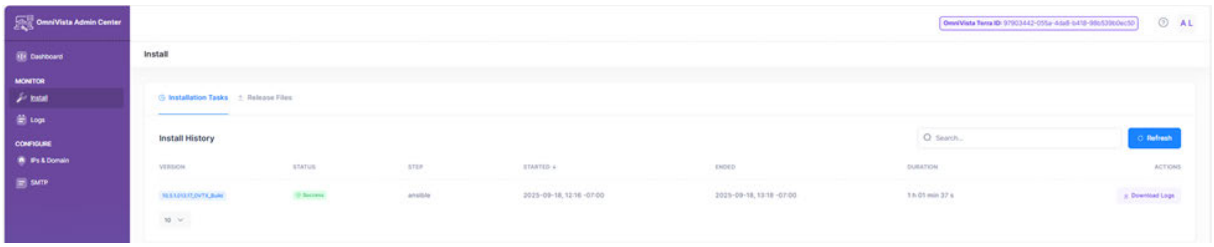
8. Click on **Yes** button on Confirm Deployment Page.


4
First Deployment
Get your instance up and
details...
le *
VTX_Build
Confirm Deployment
Are you sure you want to deploy the cluster with these settings?
No
Yes
Drop release file here to upload or click to browse
Only .7z files are supported

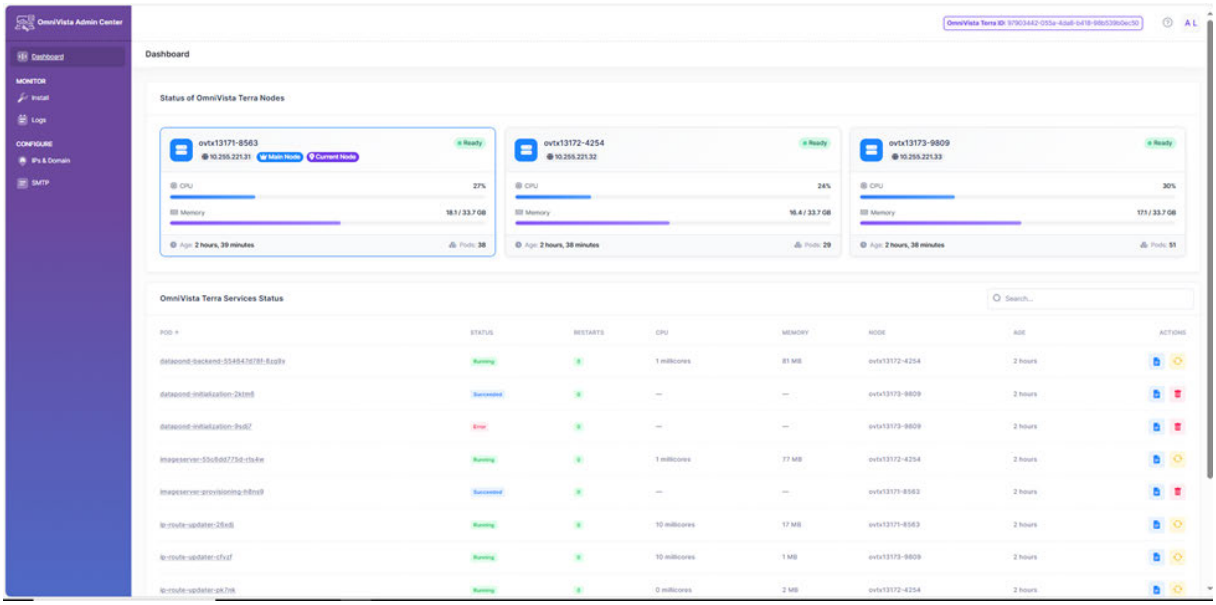
9. Wait until the deployment is finished. Refresh the same Admin Center URL, after sometime it will bring you to the dashboard page. (if it opens the login page, enter the username/password)



10. Click on **install** button on left side of the page.



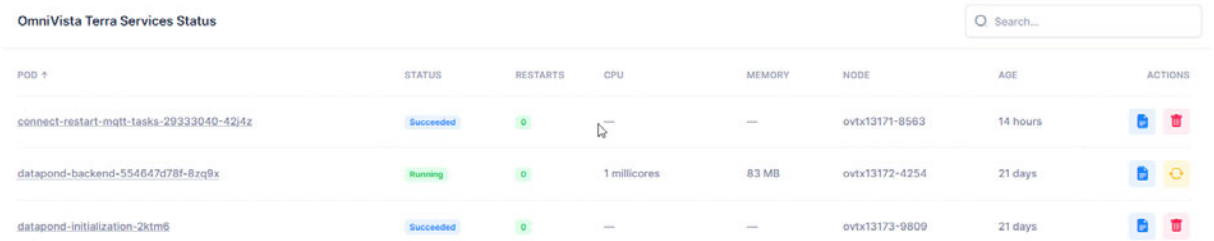
11. Check the Status of the deployment: ***success/failure/in progress***.
12. If the deployment fails click on **Download Logs** button. It will download the upgrade logs which can be viewed to see the if ovtx upgrade process logs contain any errors in the upgrade process.
13. Check the pods status from the dashboard page.



14. Login to ovtx https://myovterra.myovcloud.com/signin with the following ovngtest@gmail.com (configured at step 2) using the password ***changeme***.

11.5.2 Services Status (PODs)

The POD table displays the status and resource usage of Kubernetes pods running OmniVista Terra services. It provides real-time monitoring of service health, resource consumption, and operational metrics.



POD - Name of the Kubernetes pod. This is a unique identifier for each pod instance. This column can be sorted alphabetically using the arrow.

STATUS - Current operational state of the pod, provides a quick health check indicator.

- Running (green) - Pod is operational and healthy.
- Succeeded (blue) - Pod completed its task successfully (it is not running anymore).
- Error (red) - Pod encountered an error or failure and was not able to complete its task.
- CrashLoopBackOff (red) - Pod tried to restart too many times.

RESTARTS - The number of times the pod has restarted.

- 0 - No restarts (healthy).
- >0 - Pod has experienced issues requiring restarts.

CPU - The CPU resources allocated or being used, displayed in millicores. A dash "—" will be displayed when not applicable or not measured.

MEMORY - Memory consumption of the pod in Megabytes. A dash "—" will be displayed when not applicable or not measured.

NODE - Kubernetes node where the pod is running. Identifies the physical/virtual host machine, for example ovtx-1-5804, ovtx-2-5192, ovtx-3-9306.

AGE - The time elapsed since the pod creation, displayed in hours or days. This helps identify the pod lifecycle and stability.

ACTIONS - Available operations on the pod.

- **Download Pod Logs** - This allows for quickly retrieving the logs from the target pod. Useful to check for error tracing if a service is in error state.
  - This will only retrieve the last 500 lines of logs from each container running inside the pod. Use the dedicated “Logs” page for more advanced log retrieval options.
- **Delete Pod**
  - Deletion is only for “job” pods.
  - It is safe to delete as it is only possible to do on pods once they are in completed or error state.

- The main purpose is to remove the job from the history. The system will only keep the last few jobs for each job type, and the last few that were in error state.

> It's recommended not to delete pods manually unless instructed to do so as it is always useful to keep the last error.

- **Recreate Pod**
  - This deletes the target pods and restart a new instance immediately.
  - Some services are replicated on multiple nodes, in that case one instance can be safely deleted without any expected service disruption.
  - If you restart all instances (pods) of the same service at once, then you will encounter service disruption on the features managed by these services.

> - It's recommended only to restart pods if you are instructed to do so.

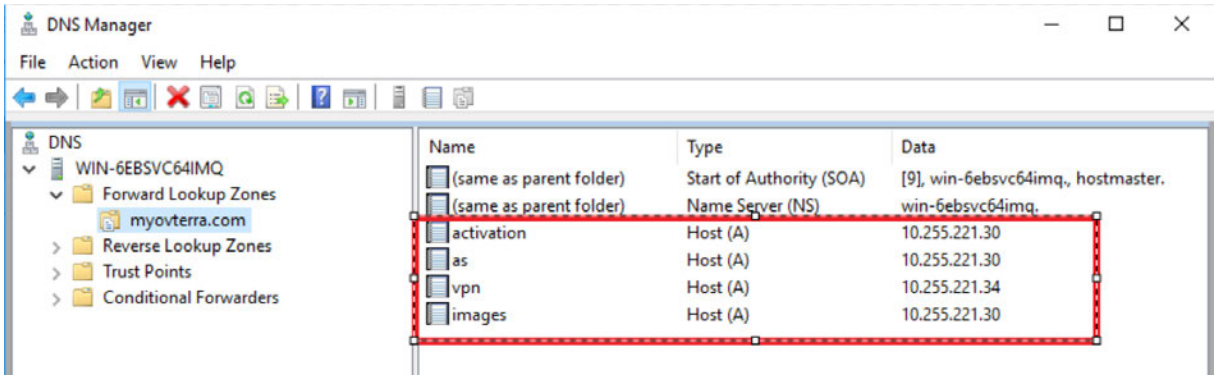
Usage Tips

- **Monitor Restarts**: Frequent restarts (>0) may indicate instability.
- **Check Resource Usage**: High CPU/memory may require scaling.
- **Node Distribution**: Verify pods are distributed across nodes for high availability. Restarting pods manually can help re-balance their distribution across all nodes, but future version of the product will have a way to do this automatically.

11.6 Configuring DNS for OmniVista Terra

Install the Windows DNS server and configure the below domains.

- **activation.myovterra.com / as.myovterra.com** – OmniVista activation server URL. Mapped to the OmniVista Terra Main IP Address.
- **vpn.myovterra.com** – VPN URL. Mapped to the VPN IP address.
- **images.myovterra.com** – Image Server URL. Mapped to the OmniVista Terra Main IP Address.
- **myovterra.myovcloud.com** – Omnivista Terra main URL. Mapped to the OmniVista Terra Main IP Address.
- **dfs.myovterra.com -** Debug File Server URL. Mapped to the OmniVista Terra Main IP Address.



11.7 How to Onboard an AP and Switch

The following steps provide an example of how to onboard an AP to OmniVista Terra.

11.7.1 AP Onboarding Steps

1. If the APs were previously managed in OVNG/OVC the certificates from those APs need to be removed before adding in OmniVista Terra. Run the below command to remove the certificates.

```
rm -rf /.ocloud/callhome_hash.json /.ocloud/certificateFile.cert
/.ocloud/cloudCaChain.pem /.ocloud/privateKey.key /.ocloud/csr.csr
/.ocloud/publicKey.key ./privateKey.key.dec
```

If the AP is factory default AP there is no need to remove any certificates.

Root access rights are required to remove certificates. Contact Service & Support for additional information.

2. Add the AP serial number in OVTX.
3. Configure ***option 43*** for the AP in the DHCP server. For example, to configure the ***dhcpd.conf*** file in the core switch to which the AP is connected:

Use this as an example only. Use IP addresses, domain name server and NTP server information specific to your deployment.

manual-dhcp dc:08:56:3c:2f:20 10.95.171.178 {
option subnet-mask 255.255.255.0;
option routers 10.95.171.1;
option domain-name "myovterra.com";
option domain-name-servers 10.95.163.213;
option ntp-servers 112.111.111.108;
option 43
[010C616C656E7465727072697365801F687474703A2F2F6163746976174696F6E2E6D796F7674657272612E636F6D]
;
option 43 activation.myovterra.com;
}

4. Enter **dhcp-server restart** command on the switch.
5. Enter **firstboot** and **reboot** commands on the AP.

6. The AP under the **Activation Status** column should be “OV Managed” and Management Connectivity is “ON”.

The option 43 hexadecimal string is equivalent to **alenterprisehttp://activation.myovterra.com**.

11.7.2 Switch Onboarding Steps

1. Edit the Activation server URL: ***activation.myovterra.com*** in the file ***flash/working/cloudagent.cfg*** in switch.
2. Add the switch serial number in OVTX.
3. If the switches were previously managed in OVNG/OVC remove the certificates from the switch before adding in OVTX. Remove the certificates listed below from the switch and then restart the callhome.

```
-> cd switch/cloud
-> rm -f client.crt cloudCAchain.pem csr.crt private.key public.key
```

Note: For factory default switches there is no need to remove any certificates from the switch.

4. Verify that the **Activation Status** column is “OV Managed” and **Management Connectivity** is “ON”.

11.8 License Management Overview

A license to an Organization is required to access and configure the Organization for network management. This release of OmniVista offers a Trial license that provides a period of 90 days and 20 devices to evaluate and utilize OmniVista features (additional time and number of devices can be requested). You can then upgrade from the free trial version to a paid licensed version of OmniVista Terra.

> OmniVista Terra licenses and OmniVista Cirrus 10 licenses are not interchangeable. For example, you cannot use OmniVista Terra licenses for OmniVista Cirrus 10 device management.

11.8.1 License Management Overview

The following components and individuals are involved in the process of obtaining a license for your OmniVista Terra Organization:

- **License Types**:
  - **Trial License** - Provides a free teaser period that is automatically activated when you create an Organization.
  - **CAPEX Subscription** - Paid license subscription.
- **Alcatel-Lucent Business Partner (BP)** - Your BP contact creates and activates the purchased CAPEX Subscription licenses. The BP forwards the paid licensing information to you, which you can then import into OmniVista and bind to Organization devices.

> The OmniVista ID is displayed in the top right corner of the OmniVista Admin Center.

11.8.1.1 How It Works

1. Create an Organization to manage devices in OmniVista. A free Trial License is automatically approved for the Organization, offering a 90-day teaser period to evaluate managing up to 20 devices.
2. Decide if you want to extend or renew the Trial License duration and number of devices.
3. Decide if you want to upgrade to a paid license subscription. If so, contact your Business Partner to discuss CAPEX Subscription licensing options.
4. Upgrading to a paid CAPEX Subscription involves the following process between you and your Business Partner:
   a. BP purchases and activates the required licenses using eBuy and Subscription Manager. Note that during the license activation process, the BP will require the OmniVista ID for your OmniVista Terra installation.
   b. BP sends an email to you containing a Subscription ID, an Activation Code, and an attached Subscription File.

c. When you receive the license confirmation email from the BP, use the information provided to import the licenses into OmniVista.
d. After you have imported the CAPEX licenses into OmniVista and assigned the licenses to your devices, export an Entitlement File from the License Management screen.
e. Send the Entitlement File to your BP to upload into Subscription Manager. This file identifies the devices assigned to the licenses for the CAPEX Subscription. Subscription Manager uses this information to track and manage licenses for your Organization.

See the **License Management in OmniVista Terra** section of the OmniVista Terra 10.5.1 Documentation for more information.

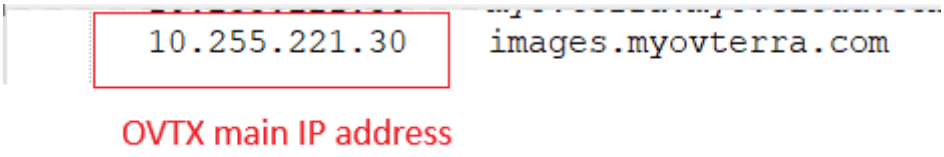
11.9 Uploading AOS/AWOS Images

Follow the procedure below to upload AOS/AWOS images to the image server.

1. Download the images from the Customer Support site to upload on OV Terra.

> Do not use ISSU images, they are currently not supported with OV Terra.

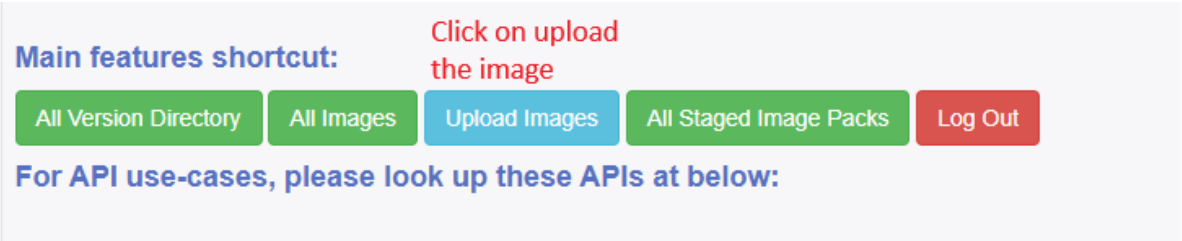
2. Add a DNS entry to resolve images.myovterra.com to OV Terra Main IP address.
3. (optional) If you are accessing from Windows PC, add this line to *C:\Windows\System32\drivers\etc\hosts*



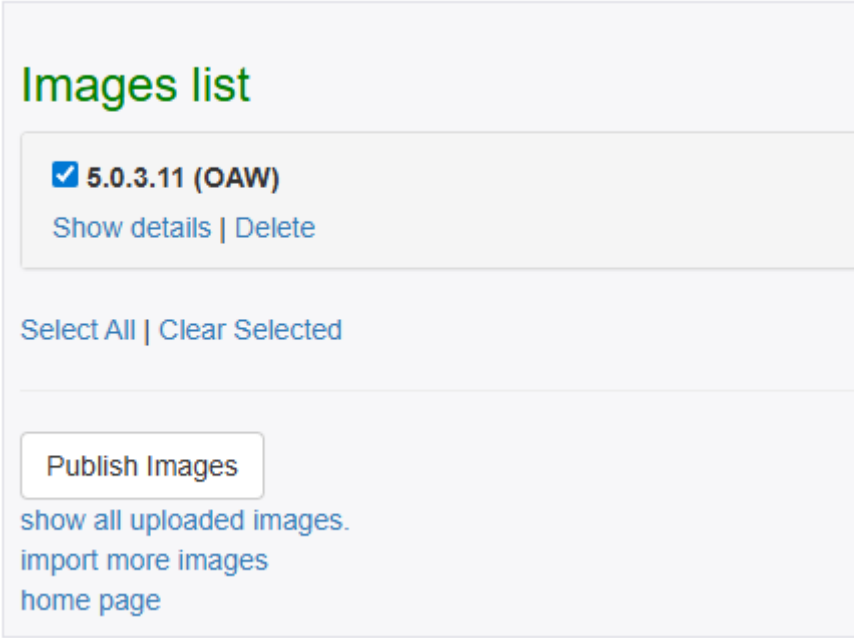
4: Log in with the following username and password:

- Username : admin
- Password: toor

5. Click on **Upload Images**.



6. Choose **File** and **Import**.
7. Click on **Publish Images**.


Images list
5.0.3.11 (OAW)
Show details | Delete
Select All | Clear Selected
Publish Images
show all uploaded images.
import more images
home page

11.10 Guidelines and FAQs

11.10.1 Accounts and Passwords

- The default password for logging into OVTX is **changeme**. A valid email address is required to change the default password. If a valid email is not available the default password cannot be changed.
- The OmniVista ID is displayed in the top right corner of the OmniVista Admin Center.

11.10.2 VM Backup and Maintenance Guidelines

The following are recommended procedures for VM Backup and Maintenance.

- VM snapshots without memory are the recommended method for backups.
- When snapshots with memory are taken, the OVTX UI and Admin Center will be temporarily inaccessible. If done on the main node this may also cause another node to be promoted to take its place.
- Old VM Snapshots should be deleted regularly to prevent performance degradation. Keep one VM snapshot at a time to avoid performance degradation.

11.10.3 Cluster and Node Guidelines

If a node disconnects from the cluster due to a power cycle or loss of network connectivity, note the following

- From 0–10 minutes: Downtime occurs and the system is not accessible.
- At the 10th minute: Users can access the UI (Web Admin and OVTX), but cannot perform any actions since some services are still not stable.
- At the 15th or 20th minute or later: Users can access the UI and perform actions as expected.

Replacing a node is not supported

If the cluster encounters a broken node there is currently no way to recover the cluster. The following options are not yet supported:

- Deleting the broken node.
- Adding a new node with the same configuration to the cluster.

If a node becomes broken (e.g., cannot start or cannot join the cluster) a fresh cluster must be installed.

The HA L2 cluster supports a 3-node setup ONLY in version 10.5.1.

In the event of two nodes being offline, OVTX becomes unavailable.

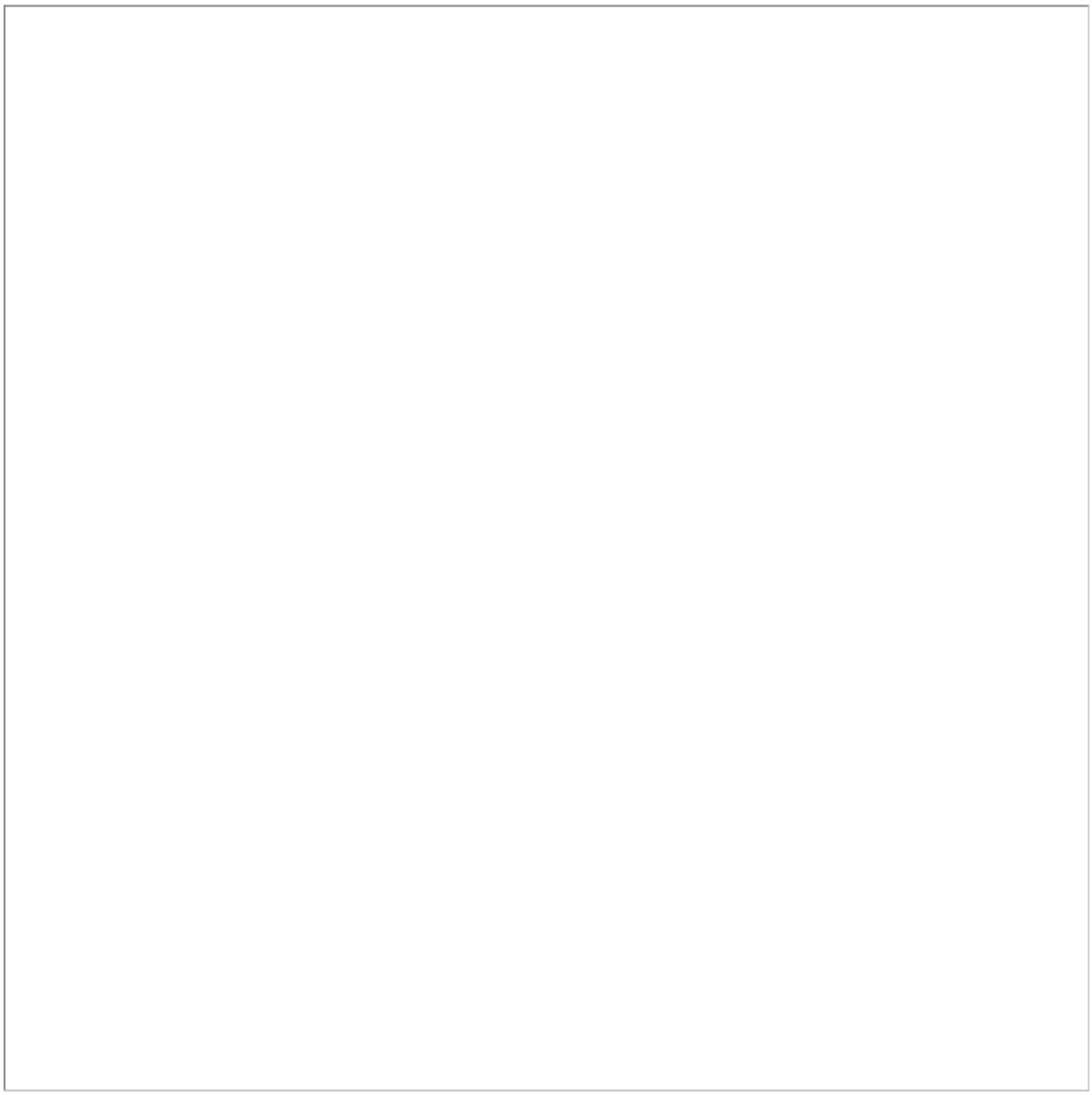
11.10.4 OmniVista Terra Installation

If a certificate error similar to one below is seen in the install log run the installation process again.

```
"Error: 1 error occurred:",
 "\t* admission webhook \"validate.nginx.ingress.kubernetes.io\" denied the request: ",
 "-------------------------------------------------------------------------------",
 "Error: exit status 1",
 "2025/07/15 10:15:07 [emerg] 1118#1118: SSL_CTX_load_verify_locations(\"/etc/ingress-controller/ssl/ovng-internal-ingress-t
 "nginx: [emerg] SSL_CTX_load_verify_locations(\"/etc/ingress-controller/ssl/ovng-internal-ingress-tls.pem\") failed (SSL: e
 "nginx: configuration file /tmp/nginx/nginx-cfg1518428072 test failed",
 "",
 "-------------------------------------------------------------------------------",
 "",
 "",
 "",
 "Error: calling helm upgrade: exit status 1",
 "Error: plugin \"spray\" exited with error"
```

Perform the following to re-install.

1. Access the Web Admin Center
2. Navigate to Install->Release Files
3. Click **Install** to restart the installation process



12 OmniVista Terra Release Notes

OmniVista Terra Release Notes 10.5.1 (October 2025) (see page 1086)

12.1 OmniVista Terra Release Notes (October 2025)

OmniVista Terra is an on-premise Network Management System that simplifies the monitoring and managing of Stellar Access Points and AOS Switches from an easy-to-read dashboard display. An on-premise version of OmniVista is particularly useful for customers with local installation requirements.

This release of OmniVista Terra is available as a free trial or paid version of the full OmniVista Terra Solution. The trial version extends for 90 days and can be used to monitor up to 20 Access Point and Switch devices combined (additional time and number of devices can be requested). You can then upgrade from the free trial version to a paid licensed version of OmniVista Terra.

You can access OmniVista Terra 10.5.1 using any approved browser and device (e.g., workstation, tablet). Access to OmniVista Terra is supported on the following browsers: Chrome 79+ (on Windows and Redhat/SuSE Linux client PCs), and Firefox 62+ (on Windows and Redhat/SuSE Linux client PCs).

These Release Notes detail features and functions, network/device configuration prerequisites, supported devices, and known issues/workarounds in OmniVista Terra 10.5.1. Please read the Release Notes in their entirety as they contain important operational information that may impact successful use of the application.

- Devices Supported (see page 1086)
- Software Supported (see page 1087)
- Features and Functions (see page 1087)
- Network and Device Prerequisites (see page 1087)
- Installing OmniVista Terra (see page 1087)
- Launching OmniVista Terra (see page 1088)
- REST API Management (see page 1088)
- Known Issues/Workarounds (see page 1088)
- Technical Support (see page 1089)

12.1.1 Devices Supported

Click here for a list of supported Stellar Access Points and AOS Switch models, which includes the supported software releases.

The following Access Point models are not supported:

- OAW-AP1101
- OAW-AP1201L
- OAW-AP1201H
- OAW-AP1201HL
- OAW-AP1201BG
- OAW-AP1261

12.1.2 Software Supported

- **AWOS 5.0.3** - OmniVista Terra 10.5.1 supports AWOS 5.0.3 on all supported Access Points.
- **AOS 8.9R4** - OmniVista Terra 10.5.1 supports 8.9R4 on all supported AOS Switches.
- **AOS 8.10R3** - OmniVista Terra 10.5.1 supports AOS 8.10R3 on all supported AOS Switches.

12.1.3 Features and Functions

Use the following links to familiarize yourself with OmniVista Terra 10.5.1 features and functionality:

- Introduction to OmniVista Terra 10.5.1 (see page 5)
- Getting Started (see page 6) – What you need to know to get up and running.
- Configuring Organizations for Network Management (see page 60) - How to create and manage Organizations, including creating/modifying sites, adding devices, and adding users.
- Onboarding Devices Workflow (see page 13) - The basic steps involved to onboard Switches and Access Points for management in OmniVista Terra.
- License Management (see page 139) - OmniVista Terra licensing is based on the license purchased. A user is allowed to manage up to the maximum number of devices allowed for that license. A free, teaser license is automatically authorized for each Organization.
- Documentation - The user documentation is contained in the on-line help installed with this product. Click on the Help link (?) in the upper-right corner of a page to access the online help for the page. You can also access the user documentation directly at http://docs.ovcirrus.com/ovtx.

12.1.4 Network and Device Prerequisites

To ensure the necessary communication between devices (Access Point/Switch) and OmniVista Terra 10.5.1, verify/configure the following prerequisites on your local network:

- Network Prerequisites (see page 9) - Network deployment, bandwidth, proxy, firewall, and NTP server requirements.
- Device Prerequisites - Supported Access Point software and models.
  - If your fully managed Access Points are running AWOS 4.0.8, it is recommended that you upgrade to AWOS 5.0.3 by setting the Desired Software Version first before accessing OmniVista Terra 10.5.1.
  - It is also recommended that you upgrade your OmniSwitch AOS release to 8.10R3.

12.1.5 Installing OmniVista Terra

OmniVista Terra is installed from a download file available on the Customer Support website. Refer to the OmniVista Terra Installation Guide (see page 1049) for information about how to install OmniVista Terra.

Notes: Consider the following guidelines when installing OmniVista Terra:

- The OmniVista Terra HA L2 cluster supports ONLY a 3-node setup.
- When managing more than 1000 devices in OmniVista Terra, setting the Data Persistency (see page 127) values to 7 days for all parameters is recommended to prevent a potential disk full scenario. This configuration helps maintain optimal system performance and storage efficiency in large-scale environments.

In addition to installing OmniVista Terra, you must also upload AOS and AWOS image files to the OmniVista Image Server. This process is required to support the upgrade of device images through OmniVista Terra. Refer to the “Uploading AOS/AWOS Images” section in the OmniVista Terra Installation Guide (see page 1080) for the step-by-step procedure.

When the installation is complete, you will have an initial Network Administrator login and an Organization that was created based on the information you provided during the installation process. The login consists of the email address entered during the installation process and “changeme” as the default password.

12.1.6 Launching OmniVista Terra

To launch OmniVista Terra, enter **myovterra.myovcloud.com** in your browser to access the login screen. When you login to OmniVista Terra for the first time, use the email address for your account (specified during the installation process) and “changeme” as the default password. You are then required to change the password at that time.

Email availability is required to change the login password. Make sure that Email is enabled and SMTP settings are configured for the OmniVista Terra installation (see the OmniVista Admin Center (see page 1064) online help).

12.1.7 REST API Management

You can use REST APIs for scripting or integration with any third-party systems in your management network. The complete API reference can be found at the following links based on your region:

- EU: https://eu.manage.ovcirrus.com/apidoc/apidoc.html
- US: https://us.manage.ovcirrus.com/apidoc/apidoc.html

For more information, see Automation with APIs (see page 1022).

12.1.8 Known Issues/Workarounds

Some Reports Fail When Scheduled to Run at the Same Time (OVNG-21932)
Summary: When multiple reports are scheduled at the same time, some reports may fail.

Workaround: Schedule a single report or reports to run at least 30 minutes apart to minimize failed reports.

12.1.9 Technical Support

Alcatel-Lucent Enterprise technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region Phone Number

North America 1-800-995-2696

Latin America 1-877-919-9526

Europe Union +800 00200100 (Toll Free) or +1(650)385-2193

Asia Pacific +65 6240 8484

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: https://myportal.al-enterprise.com/.

Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, and configuration file available for each switch.

Severity 1 - Production network is down resulting in critical impact on business—no workaround available.

Severity 2 - Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 - Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 - Information or assistance on product feature, functionality, configuration, or installation.