Extreme Platform ONE™ for MSP v2.11 User Guide

Setup, Management, and Onboarding Instructions

9041272-00 Rev AA
September 2026

Copyright © 2026 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Table of Contents

Abstract v

Preface 6

Text Conventions 6
Documentation and Training 7
Open Source Declarations 8
Training 8
Help and Support 8
Subscribe to Product Announcements 8
Send Feedback 9

Introduction to Extreme Platform ONE for MSP 10

Extreme Platform ONE Networking 10
ExtremeCloud IQ 10
Extreme Platform ONE for MSP 11
Navigation Pane 12
Content Pane 14
Common Functionality 16

Log In To Your Account 17

MSP License Account Setup 17
Login Behavior for MSPs Using Classic MSP Workspace 18
Forgot Password 18
Change Password 19
Choose a Theme 19

Dashboard 20

Global 20
Wired/Wireless 22
SDWAN Devices 22
Security 24

Tenant Management 25

Tenants 25
View Tenant Details 26
Enable Agent ONE 26
Add a Tenant 27
Edit a Tenant 28
Export Tenants 28
Access a Tenant Account 28
Tenant Tags 28
Tag Categories 28
Add a Tenant Tag 29
Create a Tag Group 29

Usage & Allocation 29
Usage 29
Allocation 30
View Historical Data Usage 30
View License Usage 30
Allocate License 31
Third-Party Management Support 31

Subscriptions & Services 32
Subscriptions & Licensing 32
Subscription Status 34
Synchronize Subscriptions 34
View License Usage 35
Contracts 35
Inventory 36
Inventory Table 37
Change Device State 38
Upgrade Firmware from Inventory 38

Administration & Settings 40
License Accounts 40
Access Management 41
Role-Based Access 43
Create a New Admin User 43
Create a New Team 43
Edit a Team 44
Identity Providers 44
Create IdP Application - Microsoft Entra ID 47
Create IdP Application - Okta 51
Add an IdP Profile 55
Manage IdP Profile 57
Manage IdP Profile Certificates 58
Configure Idle Session Timeout 59
Integrations 59
Create a New API Key 59
Logs 60

MSP Definitions 62

Troubleshooting 64
MSP CUID Linking Error 64
Add MSP Admin Error 65
Default Admin Migration 65
Local Admin Migration 65
License Consumption 66

Abstract

This user guide for Extreme Platform ONE for MSP version 2.11 provides technical instructions for Managed Service Providers (MSPs) for provisioning accounts, configuring license pools, assigning admin roles, and onboarding customer networks. The guide explains how to manage tenants, allocate licenses across applications such as ExtremeCloud IQ, SD-WAN, Extreme Platform ONE Security, and Intuitive Insights, and monitor network health via real-time dashboards. It includes procedures for creating admin teams, accessing tenant accounts, and troubleshooting common issues like CUID linking errors and admin role conflicts. Designed for technically proficient users, it emphasizes operational efficiency, secure access control, and scalable license management in MSP environments.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

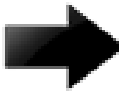
Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Non-printing characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a "soft" line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and Software Compatibility for Extreme Networks products

Extreme Optics Compatibility

Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.

3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at https://www.extremenetworks.com/documentation-feedback/.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

Introduction to Extreme Platform ONE for MSP

This guide provides instructions for Managed Service Providers (MSP) on onboarding customers (tenants) into Extreme Platform ONE for MSP, including Day-0 provisioning, licensing, and administrative setup. This user guide is designed to introduce key features and tools that enhance productivity, streamline operations, and improve overall efficiency.

Extreme Platform ONE Networking

Extreme Platform ONE Networking is a central management platform that simplifies the user experience and provides automation at scale. Extreme Platform ONE Networking eliminates the need to log in separately to the Extreme Networks multi-domain network management solutions by unifying them within a single user interface.

Extreme Platform ONE Networking supports the following applications:

- **ExtremeCloud IQ:** Provides centralized configuration and network monitoring, reporting, alarms, and statistics for cloud-enabled Extreme Networks devices.
- **ExtremeCloud SD-WAN:** Provides unified wired and wireless management through fabric services. You can enable a secure network, automate application performance management, and create a centralized management of applications with intuitive user experiences.
- **Extreme Platform ONE Security:** Provides network, application, and device access security within a single solution.
- **Extreme Intuitive Insights:** Provides cloud-based deployment and monitoring of Zebra hand-held devices.

Extreme Platform ONE Networking features advanced automation driven by conversational, interactive, and autonomous AI agents. These agents assist, advise, and enhance the productivity of networking, security, and business teams, cutting down the time needed to complete complex tasks from hours to minutes.

For more information, see the Extreme Platform ONE Networking documentation.

ExtremeCloud IQ

ExtremeCloud IQ is an industry-leading approach to cloud-driven networking, designed to take full advantage of the Extreme Networks end-to-end networking solutions.

ExtremeCloud IQ offers the following:

- Unified, full-stack management of access points, switches, and SD-WAN

- Innovative ML technologies to analyze and interpret millions of network and user data points from the edge to the data center
- Network automation and intelligence to streamline operations.

For more information, see the **ExtremeCloud IQ** documentation.

Extreme Platform ONE for MSP

Extreme Platform ONE for MSP helps Managed Service Providers (MSPs) to efficiently manage all tenants through a unified platform. This multi-tenant architecture simplifies and reduces the cost of managing multiple tenants. This streamlined approach significantly reduces the time and IT resources required for operations, accelerating time to revenue.

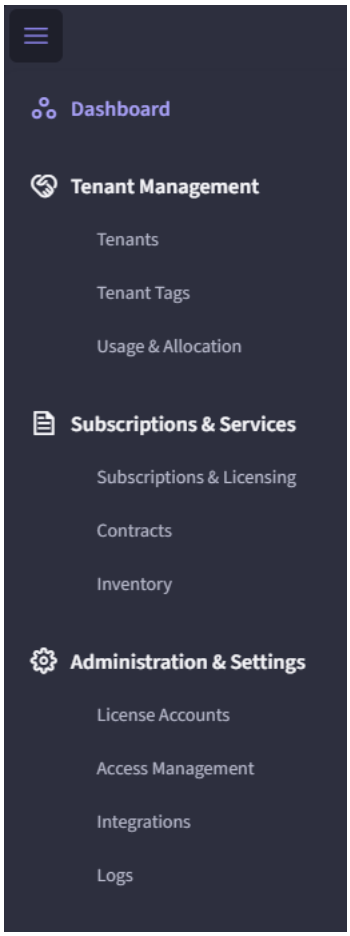
Use Extreme Platform ONE for MSP to:

- Link your license accounts.
- Onboard and manage customers.
- Manage licenses.
- Manage administrators.
- Migrate administrators, customers, and subscriptions.

Extreme Platform ONE for MSP consists of the following major sections:

- The navigation pane
- The content pane

Navigation Pane



Note

Select to toggle the left navigation menu on and off.

The following options are available in the navigation pane:

Navigation Pane	Description
Dashboard	The following main tabs show aggregated customer data: • Global • Wired/Wireless • SDWAN • Security Customer data includes customers with issues, alerts, connected wireless clients, device status, and licenses.
Tenant Management	

Navigation Pane	Description
Tenants	The **Tenants** screen consists of the following icons and buttons: • **Add Tenant:** Adds a new Tenant. • **Search:** Search for tenants. • **Download:** Downloads tenant details in a CSV file. • **Refresh:** Displays the most recent tenants.
Usage & Allocation	The **Usage & Allocation** screen consists of the following icons and buttons: • **Synchronize:** Synchronizes changes for faster updates across applications. • **Select License Account:** Searches for or select your license account from the drop down menu. • **Show all**: Shows all time data usage • **Go to Historical Data Usage**: Shows historical data usage for the selected period. • **Usage** tab: Shows the total number of licenses, the number of licenses used, and the remaining number of licenses for each customer. Shows available licenses for the following: ◦ Wired & Wireless ◦ Security ◦ SD-WAN • **Allocation** tab: Shows license allocation and usage for each customer.
Subscriptions & Services	
Subscriptions & Licensing	The **Subscriptions & Licensing** screen consists of the following icons and buttons: • **Search:** Search for subscriptions or licenses. • **Download:** Downloads subscription and license details in a CSV file. • **Synchronize Subscriptions:** Synchronizes changes for faster updates.
Contracts	The **Contracts** screen consists of the following: • **Search**: Search for contracts. • **Filters Applied**: Shows the filter applied to the list of contracts. Filters available are: ◦ None ◦ Expires in 30 Days ◦ Expires in 60 Days ◦ Expires in 90 Days • **Download:** Downloads the displayed contracts details in a CSV file. Select a contract to view contract details.

Navigation Pane	Description
Inventory	The **Inventory** page consists of the following: • An aggregated list of devices that you manage, such as wireless devices, switches, routers, appliances, SD-WAN, and other devices. Select each asset to view firmware status and hardware life cycle. • Search: Use the search feature to show devices on the screen. • Sorting: All fields are sortable.
Administration & Settings	
License Accounts	The **License Accounts** screen consists of the following icons and buttons: • **Synchronize:** Synchronizes changes for faster updates. • **Add License Account:** Adds a new license account.
Access Management	The **Access Management** screen consists of the following tabs and buttons: • **Users:** ◦ Creates a new administrative user. ◦ Shows a list of users, contact information, roles, login information, and status. • **Teams:** ◦ Creates a new team. ◦ Shows a list of teams, users, and tenants.
Integrations	Integration provides the ability to use APIs to customize **Extreme Platform ONE for MSP**.
Logs	The **Logs** screen consists of the following icons and buttons: • **Date and Time Picker:** ◦ Displays activities for up to 30 days. ◦ Shows audit logs for last week, last month, or last quarter. ◦ Shows date range.

Content Pane

The following table describes the standard fields, columns, and tiles in the user interface.

Table 4: Standard Buttons & Icons

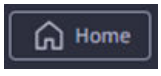
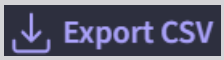
Icon	Description
	Takes you back to the MSP homepage from Extreme Platform ONE Networking.
	• Opens the tenant account in Extreme Platform ONE Networking Visualize view. From this view, you can perform all functions available in Extreme Platform ONE Networking for that tenant. • Adds a tab for the selected tenant account to the MSP toolbar for quick access. • The active tenant tab on the MSP toolbar is highlighted.

Table 4: Standard Buttons & Icons (continued)

Icon	Description
	You can scroll through a list of tenants.
	Use the Filter by panel to limit the tenants displayed in the MSP workspace. The panel provides the following filter options: • Groups: Displays saved tenant groups. Select Apply to display only tenants that belong to the selected group. • Tags: Filters tenants based on assigned tags. Tags are organized by categories, such as Size and Industry. Select one or more tags and then select Apply Filter. • Tenants: Displays all available tenants along with their Tenant ID and VHM ID. Select one or more tenants and then select Apply Filter to display only the selected tenants. Use the Search field to locate specific groups, tags, or tenants. Select Create Group to create a new tenant group from the selected tenants. Select Apply Filter to apply the selected filters.
	Select your initials at the top right corner of the screen to view the following: • Name and email address • Profile icon • Choose a light or dark theme for your administrative environment. • About Extreme Platform ONE: displays MSP application version, Data Center Name, and software component versions. • Sign Out • Various Terms & Conditions, and the dates of acceptance. The Profile icon displays your name and login details. To edit your first and last name, place your cursor in the respective fields, make the changes and when you are done, select **Save Changes**. To change your password, select **Change Password** and complete fields in the pop up window as follows: 1. In the **Current Password** field, type your current password. 2. In the **New Password** field, type the new password. 3. In the **Confirm Password** field, retype the new password. 4. Select **Save**. Note: To display passwords on the screen, select the Eye Icon  .

Table 4: Standard Buttons & Icons (continued)

Icon	Description
	Shows the following Resource Center menu options: • User Guide • Program Guide • Product Updates • API Documentation Links • Share Your Feedback Each selection opens an external site from which you can add feedback or get product-related information.
Search	Displays results based on your search criteria.
	Based on the selected filter, downloads data in a CSV file. Exports are based on filter views.
	Refreshes the screen and displays the latest information.

Common Functionality

The Extreme Platform ONE for MSP user interface offers the following common functions across the platform:

- Select the information icon for more information.
- Use the Search field to find and display information based on the criteria that you enter.
- Tables:
  - Select and drag the left or right border of the column header to adjust the column width.
  - Select and drag the column headers to change the order of the columns.
  - Select a column header to sort column data in ascending or descending order.
  - Select **Columns** to add, remove, and reorder the columns.
  - Select **Filters** to narrow your search. You can filter by column or by selecting the **Filter** button and using check boxes.
  - Filters Applied: indicates that the data is filtered. To remove filtered data, select X.
  - **Page Size**: Specify the number of rows to display per page.
  - Right click a data field for options to copy field values: Copy, Copy With Headers, Copy With Group Headers.



Note
You cannot move the primary column.

Log In To Your Account

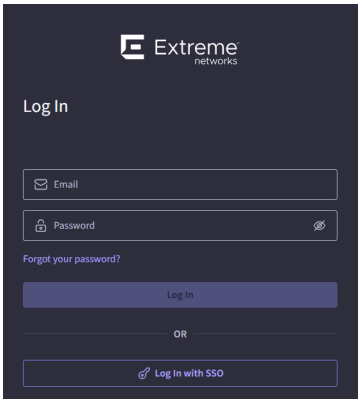
MSP License Account Setup on page 17
Login Behavior for MSPs Using Classic MSP Workspace on page 18
Forgot Password on page 18
Change Password on page 19
Choose a Theme on page 19

- Check your Welcome email to create password for your MSP Super Admin account.
- Extreme Platform ONE for MSP displays all accounts the user has shared access to through the Teams feature.

Use this procedure to log in to Extreme Platform ONE for MSP.

Extreme Platform ONE for MSP is integrated with Extreme Platform ONE Networking. Upon login, MSP Super Admin or MSP Admin is directed to the Extreme Platform ONE for MSP.

1. Go to Extreme Platform ONE for MSP.



2. Enter your business email and password.
3. Select **Log In**.

Note
SSO is currently unavailable for MSP users and is planned for a future release.

MSP License Account Setup

Upon registration, you are assigned two license pools:

- **Non-chargeable CUID**: Includes 25 Home-VIQ licenses for demo or testing purposes.

- **Chargeable CUID**: Starts with 25,000 licenses in a consumption-based billing pool. There is no upper limit.

Follow instructions in the welcome email to set the default MSP Super Admin password for your MSP home VIQ.

Login Behavior for MSPs Using Classic MSP Workspace

When MSPs using the **Classic MSP Workspace** attempt to access **Extreme Platform ONE Networking**, they are presented with access options related to their enterprise view prior to migration. During the login process, these MSPs will see the following options:

- Link a license account
- Continue as a Connect customer

Selecting the Connect customer option impacts the existing access to the Classic MSP Workspace. To prevent this issue, do the following:

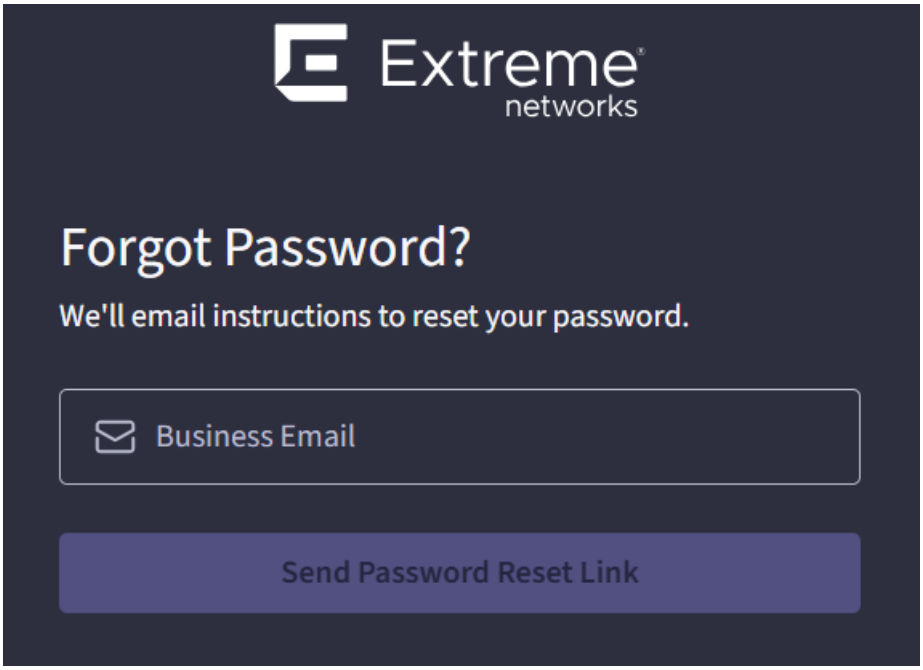
1. Ensure that the license account or CUID is linked to the MSP workspace.
2. (Optional) Assign the license account to the home VIQ.

Forgot Password

When logging in to Extreme Platform ONE Networking, if you forget your password, select the **Forgot Password** text link to get a new password.

Use this procedure to get a new password.

1. In the Log In dialog, select **Forgot Password?**



2. In the **Forgot Password** dialog, type your **Business Email**, type the email address for your account.

3. Select **Send Password Reset Link.**
4. Open your email and select the reset password link.
5. Follow the instructions to reset your password.

Change Password

Use this procedure to change your password.

1. In the upper-right of the page, select **<your initials>** > **Profile**, and the select **Change Password** from the **Profile** area.
2. Populate the dialog as follows:
   a. In the **Current Password** field, type your current password.
   b. In the **New Password** field, type the new password.
   c. In the **Confirm Password** field, retype the new password.
   d. Select **Save**.

Choose a Theme

Use this procedure to choose a light or dark theme for your administrative environment. This task requires you to be logged in to your account.

1. Select your **Profile** (initials), and then select **Theme**.
2. Depending on your preference, select either **Light** or **Dark**.

   You can repeat these steps to switch between light and dark themes.

Dashboard

Global on page 20
Wired/Wireless on page 22
SDWAN Devices on page 22
Security on page 24

The **Dashboard** shows real-time network statistics with widgets such as Alerts, Customers with Issues, Connected Wireless Clients, Device Status, and Subscriptions. Select **View** on each widget to open the corresponding tenant-level dashboard.

The **Global, Wired/Wireless, SDWAN Devices** and **Security** tabs give you a comprehensive at-a-glance overview of how your network is performing to help you manage your network.

Use the **Search Customers** field filter network statistics by customer.

The **Columns** icon customizes how columns appear on the screen. To realign columns, drag and drop left or right.

Global

The Global tab shows a summary of how your network is performing to help you manage your network.

Table 5: Global Elements

Element / Field	Description
Customers with Issues	The total number of Wired/Wireless and SDWAN critical issues. Select **View** to see customers with critical alerts. Alerts legend:  red = critical alerts, amber = major alerts, teal = minor alerts, blue = information alerts
Alerts	The total number of Wired/Wireless and SDWAN alerts. Hover over each alert to see the alert type. Select the Wired/Wireless and SDWAN icons to see how alerts are distributed. Selecting a tenant within the Alerts breakdown opens Tenant instance onto the Alerts page.

Table 5: Global Elements (continued)

Element / Field	Description
Connected Wireless Clients	The total number of connected wired/wireless devices on the network.
Device Status	The total number of connected and disconnected devices on the network. Select Wired/Wireless and SDWAN icons to see the total number of connected and disconnected devices for these networks. Select **View** to go to the **Device Status Details** screen. On the **Device Status Details** screen, select **View**: • To see the total number of connected and disconnected devices by device type • Next to each device type to see a breakdown by customer of online and offline devices Select **Back** to exit the screen.
Subscriptions	The total number of used and available Wired/Wireless, SDWAN and Security subscriptions.
Search	Search by column headings.
Wired/Wireless and SDWAN	Shows respective tenants in the table
Tenants	Select a tenant to go to the **Tenant Detail** screen which shows detailed information about a particular tenant. Select the overflow menu ⋮ to edit a tenant. For more details see, the Tenants topic.
Connected Clients	The total number of online clients.
Devices Down	The total number of offline devices.
Alerts	Alert status of each tenant

Wired/Wireless

The Wired/Wireless tab shows a summary of how your network is performing.

Table 6: Wired/Wireless Elements

Element / Field	Description
Alerts	The total number of wired/wireless alerts. Hover over each alert to see the alert type. Alerts legend:  red = critical alerts, amber = major alerts, teal = minor alerts, blue = information alerts
Connected Wireless Clients	The total number of connected wired/wireless devices on the network. Select **View** to see a breakdown of online devices by customer.
Device Status	The total number of connected and disconnected devices on the network. Select **View** to see more details. Hover over each alert to see the alert type. Select **Back** to exit the screen.
Licenses	The total number of used and available wired/wireless licenses.
Search	Search by column headings.
Tenants	Select a tenant to go to the **Tenant Detail** screen which shows detailed information about a particular tenant. Select the overflow menu ⋮ to edit a tenant. For more details see, the Tenants topic.
Connected Clients	The total number of wired/wireless online devices.
Devices Down	The total number of wired/wireless offline devices.
Alerts	Alert status of each wired/wireless tenant

SDWAN Devices

Experience Quality Score (EQS): Compares application/application group performance and connectivity. An administrator may increase the network capacity based on the EQS.

The EQS value is between 0 and 10 and the colors range from green (EQS = 10) to red (EQS = 0). A zero 0 score is extremely bad quality and 10 is excellent quality.

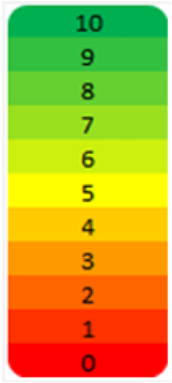


Table 7: SDWAN Devices

Element / Field	Description
Alerts	The total number of SDWAN alerts. Hover over each alert to see the alert type. Alerts legend:  red = critical alerts, amber = major alerts, teal = minor alerts, blue = information alerts
Device Status	The total number of connected and disconnected appliances on the network. Select **View** to see more details. Hover over each alert to see the alert type. Select **Back** to exit the screen.
Licenses	The total number of used and available SDWAN licenses.
Search	Search by column headings.
Tenants	Select a tenant to go to the **Tenant Detail** screen which shows detailed information about a particular tenant. Select the overflow menu ⋮ to edit a tenant. For more details see, the Tenants topic.
Throughput	How much traffic passes through per second.
Connected Appliances	The total number of SDWAN online appliances.
Disconnected Appliances	The total number of SDWAN offline appliances.
EQS Top	Top application/application group performance and site connectivity metric.
EQS High	High application/application group performance and site connectivity metric.
EQS Medium	Medium application/application group performance and site connectivity metric.

Table 7: SDWAN Devices (continued)

Element / Field	Description
EQS Low	Low application/application group performance and site connectivity metric.
Alerts	Alert status of each SDWAN tenant

Security

The **Security** tab has Service Connectors, RadSec Proxies, and Network Application Access Events that show the current status of the appliances and network access events such as Accepted, Disconnected, and Rejected.

Service connectors and RadSec proxies are small virtual appliances that perform a specific task. If your service connector is down, users cannot access their applications.

If the RadSec proxy is down, the network cannot authenticate users and therefore users cannot access the network.

Tenant Management

Tenants on page 25
Tenant Tags on page 28
Usage & Allocation on page 29

Use the **Tenant Management** section to add, export, view, edit, or delete tenants.

The Tenant Management section consists of the following sections:

- Tenants
- Usage & Allocation

Tenants

The following table describes fields, buttons and icons in the **Tenants** screen.

Table 8: Manage Tenants

Field	Description
Search	If you have a large list of tenants, use the **Search** option to search by tenant name to find a particular tenant.
Add Tenant	Enables tenant creation
Tenants	Shows a list of tenants. Select a tenant to see the following detailed information: • Device Status • Connected Clients • Alerts • Historic Usage • SDWAN, Security and Wired/Wireless networks license allocation - view total license allocation, license in use and available licenses • Use the **Allocation** tab on the Tenant Details page to allocate licenses. **Note:** You can exceed the total available number of licenses. Select the overflow menu to **Edit** or **Delete** tenants. Select the refresh icon to view your changes.
Tenant ID	(Optional) Unique tenant identification.

Table 8: Manage Tenants (continued)

Field	Description
Status Chip	Displays the current state or condition of a tenant. Select the chip to initiate the corresponding task. • Ready for Allocating Licenses • Ready for Migration • Managed by Another MSP
VHM ID	System generated unique tenant identification.
Products	Identifies the type of network application.
License Account	(Optional) The name of the license account associated with the tenant.
Teams	(Optional) The name of the team(s) to which the tenant belongs.
Overflow Menu	Allows you to edit or delete a tenant.
Download	Downloads tenant data in a CSV file.
Refresh	Refreshes table data

View Tenant Details

1. Select **Tenant Management** > **Tenants**.
2. Select a tenant from the list of tenants to view details.
   - Select **Tenant View** to view the tenant specific dashboard.
   - Select **Device Status** to view **Inventory**.
   - Select **Go to Usage** to view **Usage & Allocation**.

Enable Agent ONE

MSP Super Admins can enable **Agent ONE** access for individual tenant VIQs within the MSP.

Note

- **Agent ONE** is available only with an Extreme Platform ONE license.
- To disable **Agent ONE** for your own MSP VIQ and all associated tenant VIQs, contact Extreme Networks.
- Toggling **Agent ONE** off not only removes the AI features from the tenant level UI, but also removes tenant information from AI access on the backend.

1. Select **Tenant Management** > **Tenants**.
2. Select a tenant from the list of tenants to view details.
3. Turn on **Enable Agent ONE**.

Add a Tenant

Use this procedure to add a tenant to Extreme Platform ONE for MSP.

When a tenant VIQ is linked to the MSP License Pool CUID, devices added to the account automatically consume MSP licenses. MSP Admins assigned to relevant groups are granted External Admin access within the tenant VIQ.

Note
When a tenant is assigned a different CUID outside the MSP Workspace, an email notification is sent to all administrators of the tenant.

1. Select **Tenant Management** > **Tenants** > **Add Tenant**.
2. In Step 1 - **Tenant Details**, provide **Tenant Details** and select **Next**.
3. In Step 2 - **Tenant Tags**, provide tags details.
   a. Select tag category and sub tag attributes from the available options.
   b. Select **Next**.
4. In Step 3 - **Admin & Teams**, provide Admin and Teams details.
   a. To create a tenant administrator, select the **Create Tenant Admin** toggle and provide the tenant details.
   b. To add teams to the tenant, select the **Select Teams** toggle and select teams from the list of teams.
5. Select **Next**.
6. In Step 4 - **Deployment**, select the following as required:
   a. Turn on **Enable Agent ONE**.
   b. If the tenant will utilize the SDWAN application to connect the tenant to the SDWAN network, select the **SD-WAN Supported** toggle.
   c. If the tenant will utilize the Extreme Platform ONE Security application to connect the tenant to the Extreme Platform ONE Security, select the **Extreme Platform ONE Security Supported** toggle.
   d. Select the **Data Center**.
   e. To select a **License Account**, select the **Select License Account** toggle and select an account.

      Data center availability is affected by SDWAN and Extreme Platform ONE Security selections.
   f. Select the **Allocate Subscriptions** toggle and allocate the required licenses.
   g. Select **Next**.
   h. Verify the Tenant **Summary** and select **Save**.

      Tenant details can be modified from the Manage Tenants section.

      Note
      - A compliance check is triggered for the new tenant. If the check fails, a failure message is displayed. If the check succeeds, the tenant is created.
      - After the tenant is added, the **Tenant Detail** area is displayed. It is highly recommended that licenses are allocated to the tenant at this stage.

Edit a Tenant

Use this procedure to make changes, such as updating the license pool or admin groups for a tenant.

1. Select **Tenants**.
2. From the overflow menu of the tenant, select **Edit**.
3. Make your changes and select **Save**.

Export Tenants

1. Select **Tenant Management** > **Tenants**.
2. Select to export the tenant data.

   You can export specific tenant data using the check boxes.
3. In the **Export Tenants** dialog, select **Export**.

Access a Tenant Account

Use the procedure to access a tenant account.

1. Select from the MSP toolbar.
2. From the **Choose a Tenant** dialog, select a tenant account.

   Use the **Search** field to narrow the list of tenant accounts.
   - The tenant account opens in the **Visualize** view of **Extreme Platform ONE Networking**. From this view, you can perform all functions available in **Extreme Platform ONE for Networking** for that tenant.
   - You can also use the **Tenant View** button in the **Tenant Detail** page.
   - The tenant account is added as a tab in the MSP toolbar for quick access. You can add up to 10 tenant accounts to the quick access toolbar.
   - For advanced configuration or to access tenant-specific applications, go to the **9-dots menu**.
3. Select **Home** to return to Extreme Platform ONE for MSP.

Tenant Tags

Use **Tenant Tags** to manage tenants. The Tenant Tags act as labels and help in organizing and categorizing tenants.

Tag Categories

Extreme Platform ONE for MSP supports the following tag categories:

- Business Tags (Organizational attributes)
  - Region: Geographic region of the customer
  - Country: Country of the customer
  - Contract/License Type: Contract or license type of the customer

- Technical Tags (Infrastructure attributes)
  - Size: Size classification of the customer deployment
  - Industry: Industry vertical of the customer

Add a Tenant Tag

1. Go to **Tenant Management** > **Tenant Tags**.
2. Select the **Tenant Tag** category:
   - **Business Tags**: Region, Country, Contract/License Type
   - **Technical Tags**: Size, Industry
   - Use the **Search** field to quickly locate specific tags or sub tags.
   - Multiple Tenant Tag selection is not supported.
3. In the **Tags** section, select sub tag attributes from the available options.
4. Select **Add/Remove Tenants**.
5. Select the check boxes for the corresponding tenants to apply the tag.
6. (Optional) Clear the check boxes to remove tenants from the tag.
7. Select **Save**.

Create a Tag Group

1. Go to **Tenant Management** > **Tenant Tags**.
2. Select **Create Tag Group**.
3. Provide tag group details and select a category.
4. Select **Create Tag Group**.
5. Once a tag group is created, select **Add Tag(s)** to add a tag to the group.
6. Provide a tag name and select the desired tenants.
7. Select **Save**.

Usage & Allocation

Synchronize changes for faster updates across applications. Search or select your license account from the drop down menu. Export tenants to a CSV file and refresh the page to show the most recent tenants.



Note

Extreme Platform ONE for MSP 2.5 and later releases support third-party device license type. Only one license type per tenant is supported.

Usage

A real time snap shot of available licenses and license usage for your **Wired/Wireless**, **SDWAN**, and **Security** applications.

Extreme Platform ONE for MSP 2.7 and later releases support SDWAN tenant configurations:

- Extreme Platform ONE SDWAN Standard
- Extreme Platform ONE SDWAN Advanced

Allocation

The following table describes fields, buttons and icons in the **Allocation** screen. Select a **Tenant** from the table to view summary.

Field	Description
Tenant	Select a tenant to see more detailed information.
Feature Name	Applications linked to the tenant.
License Usage	The number of licenses the tenant has used.
Current Allocation	Total number of licenses the tenant can use. Ranges from zero to no limit.
% of Allocation	A percentage of the total number of licenses that a tenant has.
VHM ID	System generated unique tenant identification.
License Account	Name of the license account.
Overflow menu 	Allows you to edit a tenant.

View Historical Data Usage

1. Select **Tenant Management** > **Usage & Allocation**.
2. Select the **License Account**.
3. Select **Go to Historical Data Usage**.
4. Select **Period** to filter the view by Daily, Month, Quarter, Half Year, and Year in Wired and Wireless, SDWAN, and Security tabs.

View License Usage

Use this procedure to view license type, total number of licenses and the count of active and available licenses for all subscription types including Tier A, Tier B, Tier C, Tier D, and Third-party.

1. Select **Tenant Management** > **Tenants**.
2. Select a tenant from the list of tenants.
3. In the **Manage Tenants** view, select **Licenses** > **Usage**.

Allocate License

Unlike traditional term-based contracts, the Managed Services Licensing Agreement provides access to a dynamic pool of licenses. To ensure fair usage, it's important to allocate license limits to each tenant.

Note
You can assign licenses from the MSP Workspace even when the license is already assigned to the tenant in ExtremeCloud IQ (XIQ).

Note
By default, tenants are allocated zero Extreme Platform ONE Networking licenses.

To avoid automatic consumption of Extreme Platform ONE Networking licenses during assignment, follow these steps when assigning a license account with Extreme Platform ONE Networking entitlements to a tenant:

1. Unmanage the devices.
2. Assign the license account.
3. Set the license limit for pilot.
4. Manage the devices again.

Use this procedure to set license limits for tenants.

1. Select **Tenant Management** > **Tenants**.
2. Select a tenant from the list of tenants.
3. In the **Tenant Detail** page, select **Licenses** > **Allocation**.
4. In the **License Allocation** dialog, enter the quantity of licenses for each Extreme application.
5. Select **Save**.

Third-Party Management Support

MSP supports Third-Party Management Engine (TPME) for MSP tenants operating on Extreme Platform ONE Networking licenses, enabling streamlined license management and assignment for tenant deployments.

Automatic License Allocation

When you allocate licenses to tenants, the system automatically selects the appropriate license model based on the tenant license type and configuration:

- For customers using Extreme Platform ONE Networking and third-party licenses, the system allocates TPME licenses.
- For customers using Pilot and third-party licenses, the system allocates Navigator licenses.

Subscriptions & Services

Subscriptions & Licensing on page 32
Synchronize Subscriptions on page 34
View License Usage on page 35
Contracts on page 35
Inventory on page 36

Licenses are required for the specialized applications. A subscription entitles you to an explicit allotment of Extreme Networks licenses for one or more applications to manage the devices in your network.

It is important to understand the following information about the relationship of contracts, subscriptions, and licenses:

- Contract: A contract is all-encompassing and can include multiple subscriptions and licenses.
- Subscription: A subscription applies to devices and comprises a specified number of software licenses for managing and viewing those devices. For example, an organization can buy an annual subscription with associated licenses based on the organization's needs.
- License: SaaS users have subscriptions, as do hardware devices but whereas hardware has a license associated with that subscription, SaaS has a right to use. These differences are reflected in the **Subscriptions & Licensing** interface.

You can manage subscriptions and licenses from the **Subscriptions** interface. The status of each license in your license pool is quickly identifiable, and you can search and use grouping and other filter criteria to view specific licenses and more detail about a license.

Note
The terms **License** and **Entitlements** appear throughout the Extreme Platform ONE for MSP interface. These terms are interchangeable. For clarity, this document uses license, licenses, and licensing in all cases, unless the term **Entitlement** is part of a product name or label in the user interface.

Subscriptions & Licensing

The **Subscriptions** screen is where you manage your subscriptions and contracts. A green status means you are connected. A red status indicates that you have lost connection.

- **Subscription:** Contains software licenses for managing devices
- **Contract:** Contains multiple licenses and subscriptions

This table describes fields, buttons, and icons in the **Subscriptions & Licensing** screen.

Table 9: Subscriptions & Licensing

Element	Description
Customer Unique Identifier (CUID)	Your CUID is used to bind the MSP license pools to your MSP account. You received your CUIDs in the MSP Welcome email.
Information Icon	Provides additional information about Extreme Portal.
Synchronize Subscriptions	Synchronizes subscriptions for faster updates across applications. Subscription synchronization is an automated process. When you select **Synchronize Subscriptions**. A 5-minute timer begins. After the timer expires, you can synchronize your subscriptions again. **Note:** You can select the **Synchronize Subscriptions** button once every 5 minutes. No new synchronization would occur under 5 minutes. Synchronize your subscriptions to correct incorrect data.
Overflow Menu	**Add Legacy Entitlement Key:** Adds an entitlement key to your product that links to your subscriptions and licenses. • In the **Add Legacy Entitlement Key** window, type the legacy entitlement key and provide a note for it. You can add or edit a description so it indicates something unique or searchable. • Select **Add Entitlement Key**. If accepted, Extreme Platform ONE adds the legacy entitlement key to the product.
Global	Shows entitlements (license name), and the total, active, and available licenses for each product.
Wired & Wireless	Shows entitlements (license name), and the total, active, and available licenses.
Security	Shows entitlements (license name), and the total, active, and available licenses.
SD-WAN	Shows SD-WAN entitlements (license name), and the total, active, and available licenses.
Intuitive Insights	Shows Intuitive Insights subscriptions: • Learn your network from the client device perspective. • View device analytics. • Access technology partnership to simplify device management and troubleshooting. • Isolate and proactively flag potential issues. • View 360 device-to-network visibility.
Search	If you have a large list, use the **Search** option to find a particular description, entitlement or product. You can search the description, entitlements and product columns.
Group By	Filters by Product, Description, Simple, or None.
Download Icon	Downloads table data in a .csv format.

Table 9: Subscriptions & Licensing (continued)

Element	Description
Refresh Icon	Refreshes the screen to show the most recent subscriptions and licenses.
Entitlement	Shows the name of each license. Hover to see the hamburger icon. Select the hamburger icon to filter and search.
Product	Shows the name of each product. Hover to see the hamburger icon. Select the hamburger icon to filter and search.
Total	The total number of licenses in the subscription. The total amount of licenses is the amount of licenses allocated to that subscription.
Active	The total number of consumed licenses. The amount of licenses that have been used up.
Available	The total number of licenses minus active licenses. The remaining amount is the total amount minus the active amount.

Subscription Status

Information about licenses and license pools is immediately visible in the Subscriptions & Licensing interface. Subscription details include license or entitlement, product name, number of days until the license expires, status, and license total, active, and available licenses. Select a row from the list of Subscriptions to view more details.

Status for each subscription license is indicated by color:

- Green: no problems
- Amber: attention needed, for example:
  - One or more licenses expire in fewer than 60 days and the renewal is not yet in progress
  - Trial is in progress
- Red: immediate attention required, indicating but not limited to the following conditions:
  - The grace period is active
  - One or more licenses expire in fewer than 30 days and the renewal is not yet in progress

Status color indicates license expiration date: early warning (amber), critical upcoming expiration or already expired licenses (red).

Synchronize Subscriptions

Subscription synchronization typically is automated and scheduled by the system, but you can initiate on-demand synchronization.

Synchronize Subscriptions to request out-of-the-schedule (on-demand) synchronization information. Subscriptions can be synchronized only once every 5 minutes.

Important
Do not use **Synchronize Subscription** just to refresh the information.

Use this task if you do not see your new licenses.

1. Got to **Subscriptions & Licensing**.
2. Select **Synchronize**.

   A 5-minute timer begins. After the timer expires, you can synchronize your subscriptions again.

View License Usage

Use this procedure to view license type, total number of licenses and the count of active and available licenses for all subscription types including Tier A, Tier B, Tier C, Tier D, and Third-party.

1. Select **Tenant Management** > **Tenants**.
2. Select a tenant from the list of tenants.
3. In the **Manage Tenants** view, select **Licenses** > **Usage**.

Contracts

You can view details for each contract in the Contracts interface. Detail for each contract includes the following details:

- Contract number
- Start and end dates
- Partner
- Contract status
- Number of line items for the contract
- Site location where the contract is in use.

Select each column heading to sort in ascending or descending order. To reorganize column headings, select **Columns** or drag and drop.

This table describes fields, buttons and icons in the **Contracts** screen.

Table 10: Contracts

Element	Description
Search	If you have a large list, use the **Search** field to find a particular contract. You can search by contract number or start and end dates.
Export CSV 	Based on the selected filter, downloads data in a CSV file. Exports are based on filter views.
Refresh Icon 	Refreshes the screen to show the most recent contracts.

Table 10: Contracts (continued)

Element	Description
Contract Number	A unique number for each contract.
Start Date	Contract start date
End Date	Contract end date
Partner	Partner/End customer name.
Contract Status	Status are: • Active (Green) • Canceled (Red)
Number of Items	Number of line items for the contract.
Site	Site location where the contract is in use.
Overflow Menu	View service contract.

Inventory

Use the **Inventory** view to manage your devices. This page provides an aggregated view of all devices under management. Select a Tenant from the Inventory table to view the tenant level dashboard.

Note
You can download inventory data directly using external APIs.

When you enable **Show Summary**, the following summary widgets are displayed.

Widget	Description
Device	The total count of all devices under management.
Device Status	Shows the number of devices by connection status: **Connected** and **Disconnected**. Select a status to filter the inventory table.
State	Shows the number of devices by administrative state: **Managed**, **Unmanaged**, and **New**. Select a state to filter the inventory table.
Model	Shows the distribution of device models, including AP, Switch, SD-WAN, NAC, and SE. Select a model to filter the inventory table.
Hardware Lifecycle	Shows hardware lifecycle status, including End of Sale, End of Software Maintenance, and End of Service milestones.

Widget	Description
Firmware Status	Provides firmware-related information across your inventory: **Total Updates**: The total number of available firmware updates across your inventory. **End of Version Maintenance**: The number of devices that have reached or passed the end-of-version maintenance date. **Security Vulnerabilities**: The number of detected security vulnerabilities. Select this value to filter the inventory table for bulk actions.
License Account	Shows the distribution of devices across license accounts. Select an account to filter the inventory table.

The following tabs are available to filter your devices in the inventory.

- All
- Wireless
- Switch
- Router
- Appliance
- SD-WAN
- Others

Inventory Table

The inventory table displays device information across all tenants. Use the **Search** field to locate specific devices. All columns are sortable. Select **Columns** to add, remove, or reorder columns. Right-click a data field for options to copy field values.

The following table describes each column in the inventory table.

Column	Description
Tenant	Name of the tenant that owns the device. Select a tenant to open the tenant-level dashboard.
Tenant ID	Unique identifier assigned to the tenant.
VHM ID	System-generated unique identifier for the tenant's Virtual IQ (VIQ) instance.
Status	Connection status of the device: **Connected** or **Disconnected**.
Hostname	Hostname assigned to the device.
Serial Number	Unique serial number of the device.
Site	Site location where the device is deployed.
MAC	MAC address of the device.

Column	Description
State	The administrative state of the device: **New**, **Managed**, or **Unmanaged**. A device transitions from **New** to **Managed** when it is fully configured, successfully communicates with ExtremeCloud IQ, and has a valid license.
Firmware	Firmware or OS version currently running on the device.
Subscription	License or subscription type assigned to the device.
Device Type	Device type, such as **Wireless**, **Switch**, **Third-Party Management Engine**.
Managed By	Application that manages the device: **Cloud**, **XIQ SE**, **Controller**, or **Locally**.
Service Contract	Service contract number associated with the device, if applicable.
Classification	Device classification: **Wireless**, **Switch**, **Router**, **Appliance**, **SD-WAN**, or **Others**.
Model	Product model of the device.
Country Code	Country code associated with the device deployment location.
Tenant Tags	Custom tags associated with the device.
Date Shipped	Date the manufacturer shipped the device.
License Account	Name of the associated license account.

Change Device State

Use this procedure to change the administrative state of one or more devices.

1. Select one or more devices using the check boxes, or use **Select All** to select all devices on the current page.
2. Select **Change State**.
3. Select **Manage** or **Unmanage**.
4. Review the selected devices in the confirmation dialog.
5. Select **Confirm.**

A success message confirms the number of devices scheduled for the state change.

Upgrade Firmware from Inventory

1. Select **Inventory**.
2. Select the device or devices that you want to upgrade from the device list.

   You can select devices indivdually by putting a checkmark in the check box at the left of each column or you can select all by putting a checkmark in the check box in the header column.
3. Select **Upgrade Firmware**.
4. Select **Eligible for Upgrade**.

   Only devices managed by Cloud are eligible to be upgraded.

5. Select the desired device to upgrade.
6. Select **Next**.
7. Select the firmware version from the menu blow **Firmware Version**.
8. Select **Upgrade Firmware**.

View Firmware Upgrade History

1. **Inventory** >  > **Firmware Upgrade History**
2. On the **Firmware History** screen, select filters to see only devices that have failed, completed, or are upgrading.

Administration & Settings

License Accounts on page 40
Access Management on page 41
Integrations on page 59
Logs on page 60

Administration & Settings help you manage your license accounts, access management (users & roles) and audit logs.

The **Administration & Settings** screen consists of the following sections:

- **License Accounts**: Synchronize your license accounts, add a new license account and delete accounts applications.
- **Access Management:** add new uses and teams.
- **Logs**: Shows activities and violations such as administrative activities, data access and modification information, user denials, login failures, and system changes.

License Accounts

To enable full MSP functionality, you must associate chargeable license pools with tenant accounts. Once a license pool is assigned and saved, devices in the tenant VIQ begin consuming licenses automatically.

Use the **License Accounts** screen to synchronize license accounts, add a new license account, export table data, and delete a license account.

This table describes fields, buttons, and icons in the **License Accounts** screen.

Table 11: License Account

Element	Description
Synchronize	Synchronizes changes for faster updates across accounts.
Add License Account	Adds a new license account.
Search	If you have a long list of accounts, use the **Search** option to search by account name to find a particular account.
	Downloads table data in a .csv format.
Refresh 	Refreshes the screen to show the most recent license details.

Table 11: License Account (continued)

Element	Description
License Accounts	Shows a list of license accounts.
CUID	**Customer Unique Identifier (CUID):** Use your CUID to get access to your license pool. You received your CUIDs in the MSP Welcome email.
Overflow Menu	Use the overflow menu to delete a license accounts.

Access Management

Access Management enables administrators to add users, configure single sign-on for users, or integrate role-based access (RBAC) groups that you configure in an identity provider (IdP). You can:

- Create new users. Add new internal or external user accounts and assign roles to manage their access.
- Implement and assign role-based groups and assign them to sites.
- Allow users to log in with Single Sign-On (SSO) using credentials from an existing SAML-enabled identity provider (IdP).

Use the **Access Management** screen to create, export, and view users and teams.

The following tables describe fields and buttons in Access Management tabs: Users, Teams, Identity Providers, and Access Settings.

Table 12: Users

Element	Description
Create User	Creates a new administration user.
Search	If you have a large list, use the **Search** option to find a particular user.
	Based on the selected filter, downloads data in a CSV file. Exports are based on filter views.
Refresh	Refreshes the screen to show the most recent users.
Username	The first and last name of the MSP employee. Select the check box to show the **Create a New Team** field.
Email	The email address associated with the user.
Role	The type of role the user has. Role is either super administrator or administrator.
Last Logged In	The last time the user logged in.
Status	Green means active and logged in. Red means offline.

Table 12: Users (continued)

Element	Description
Teams	The teams the user is a member of.
Overflow Menu	Edit or delete a user.

Table 13: Teams

Element	Description
Create team	Creates a new team.
Search	If you have a large list, use the **Search** option to find a particular team.
	Based on the selected filter, downloads data in a CSV file. Exports are based on filter views.
Refresh	Refreshes the screen to show the most recent teams.
Teams	The name of the team.
Users	MSP employees.
Tenants	MSP customer accounts.
Overflow Menu	Edit or delete a team.

Table 14: Identity Providers

Element	Description
Add IdP Profile	Creates an IdP Profile.
Provider	The name of the identity provider.
Domain	The domain associated with the identity provider.
Status	The current status of the identity provider configuration.
Certificate Status	The status of the SSL/TLS certificate used by the identity provider.
Description	Additional details or notes about the identity provider.

Table 15: Access Settings

Element	Description
Idle Session Timeout	Specify whether to enforce idle session timeout. If you do not specify a time, the user session will not timeout.

Role-Based Access

Role-Based Access Access to MSP features is governed by user roles. Your assigned role determines feature access and visibility of features on the Navigation menu. For example, default Dashboard widgets are dependent on a user's role-based access.

Create a New Admin User

Use this procedure to create a new admin user.

Extreme Platform ONE for MSP supports the following user roles:

- MSP SuperAdmin
- MSP Admin



Note
Only the MSP Super Admin can create MSP Admins and Admin Teams.

1. Go to **Administration & Settings** > **Access Management**.
2. Select **Create User**.
3. Enter user information:
   - **First Name**
   - **Last Name**
   - **Email**
   - **Phone Number**
4. To make the user a super administrator, select the **Make this User a MSP Super Admin** toggle.

   Extreme Platform ONE for MSP supports multiple Super Admins.
5. Select **Team(s)**.
6. Select **Select Role(s)**
7. Select **Save**.

Create a New Team

Use the procedure to create a new team.

You can add MSP Admins to Teams, creating a unified workspace for managing access to multiple tenant accounts. This feature helps MSPs:

- Assign multiple admin accounts to tenant accounts quickly
- Streamline access management across accounts

- Monitor and control admin privileges more efficiently, improving security and compliance

Note

- An MSP Admin can be part of multiple Teams.
- Use clear and concise group names that reflect the team's function. For example: Level 1 Support Team, Escalation Team, or Operations Team.
- By default, Super Admin accounts are added to all tenant accounts.

1. Go to **Administration & Settings > Access management**.
2. Select **Create Team**.
3. In Step 1 – **Team Attributes**:
   a. Type the name of the team.
   b. Select team attributes.
   c. Use the >>, >, <, and << buttons to add or remove team attributes.
4. Select **Next**.
5. In Step 2 – **Select Tenants**:
   a. Select tenant details.
   b. Use the >>, >, <, and << buttons to add or remove tenant details.
6. Select **Next**.
7. Select **Confirm** to create the team.

Edit a Team

1. Select **Administration & Settings** > **Access Management** > **Teams**.
2. From the overflow menu ⋮ of the team, select **View** to view **Team Details**.
3. In Step 1 – **Team Attributes**:
   a. Select team attributes.
   b. Use the >>, >, <, and << buttons to add or remove team attributes.
4. Select **Next**.
5. In Step 2 – **Select Tenants**:
   a. Select tenant details.
   b. Use the >>, >, <, and << buttons to add or remove tenant details.
6. Select **Next**.
7. Select **Save** to save the changes.

Identity Providers

You can configure one or more identity providers (IdPs) to implement role-based access and single sign-on (SSO) functionality.

An IdP profile defines how MSP interacts with an external IdP for user authentication. By creating an IdP profile, you allow your system to authenticate users for the defined domain, governed by the role and site-assignment rules in the IdP profile. MSP SSO supports both

IdP and Service Provider (SP) login methods. IdP Multi-factor Authentication (MFA) rules are supported on login.

The following IdPs are supported by MSP:

- Generic SAML Server
- Active Directory Federation Service (ADFS)
- Ping
- Okta
- Microsoft Entra ID
- OneLogin
- Auth0

Within the IdP table the following columns displayed:

- Priority
- IdP Type
- Domain
- Status
- Certificate Status
- Last Updated
- Description

Note
As a prerequisite to adding an IdP to MSP, you must configure your IdP before you begin.

From **Administration & Settings** > **Access Management** > **Identity Providers**, you can integrate an external IdP with MSP. The configuration overview in the following table outlines the actions required to integrate an external IdP with MSP .

Table 16: IdP Integration Configuration Overview

Action Navigation	Action Description
Prepare the IdP Configure the IdP with the required users, groups, and application settings needed to support integration with MSP. This section summarizes the key IdP configuration actions performed prior to establishing trust.	
Create users	Create user accounts in your IdP. User identities must exist in the IdP before they can authenticate into MSP. User attributes (such as username or email) must align with MSP for identification and authentication. For detailed instructions, refer to your IdP documentation.

Table 16: IdP Integration Configuration Overview (continued)

Action Navigation	Action Description
Create groups	Create groups in your IdP that represent role or access boundaries. For detailed instructions, refer to your IdP documentation. **Note:** uses group membership information provided by the IdP to assign roles through its RBAC implementation. The IdP must be configured to send group membership claims to MSP during authentication.
Create IdP application	Create an application in your IdP to represent MSP. This application defines the trust relationship between the IdP and MSP and controls authentication behavior, claims, and attribute mappings. • To create a new application in Entra ID, see Create IdP Application - Microsoft Entra ID on page 47. • To create a new application in Okta, see Create IdP Application - Okta on page 51.
Export metadata	Export the IdP metadata from the IdP application. The metadata contains the information MSP requires to establish trust with the IdP, such as entity identifiers, endpoints, and signing certificates. This metadata is later imported into MSP to complete the IdP configuration. To export the metadata from your IdP, refer to your IdP documentation.
Prepare MSP The following section summarizes the configuration actions performed when adding an IdP profile. To prepare for integration with an external IdP, complete the steps in Add an IdP Profile on page 55. To modify an existing external IdP, see Manage IdP Profiles.	
Select an IdP provider	Select the IdP type to be used for authentication. The selected provider determines the available configuration options, supported authentication protocols, and metadata format used during integration.
Define the domain	Define the fully qualified domain name (FQDN) based on the selected IdP. This domain is used by MSP to route authentication requests to the correct VIQ.
Import IdP Metadata	Import the metadata file exported from the IdP. The IdP metadata establishes the trust relationship between MSP and the IdP. It contains the IdP's entity information, endpoints, and signing certificates required to validate authentication assertions.
Define attributes for info sharing	Define and map the attributes that are exchanged between the IdP and MSP during authentication. These attributes identify users and can include values such as username, email address, or display name. Attribute mappings must align with the attributes configured in the IdP so that MSP can correctly identify and authenticate users.
Define IdP group membership to RBAC role assignment	Map IdP group membership to MSP RBAC roles. MSP relies on group membership claims provided by the IdP to assign roles during user authentication. Each IdP group must be explicitly mapped to one role to ensure users receive the appropriate permissions upon login.

Table 16: IdP Integration Configuration Overview (continued)

Action Navigation	Action Description
Export metadata	Export metadata from MSP. The exported metadata contains the service provider information required by the IdP, such as entity identifiers and endpoints. This metadata is imported into the IdP application to complete the trust configuration between the IdP and MSP.
Finalize the IdP Complete the final integration steps to establish trust between MSP and the IdP. This section outlines the key actions required to finalize configuration and align the IdP with the MSP profile.	
Import metadata	Import the metadata exported from MSP into the IdP application. This step completes the trust relationship by providing the IdP with Extreme Platform ONE service provider information, such as entity identifiers, endpoints, and certificates.
Adjust attributes	Review and update user and group attributes in the IdP. Ensure that attributes and claims used for user identification and group membership align with the mappings defined in .
Clean up temp values	Some IdPs require manual cleanup of temporary values created in an earlier step, while others remove those values automatically during the metadata exchange.
Test Logins Validate the IdP integration by performing authentication tests using both SP- and IdP-initiated login flows. These tests confirm that trust is established, attributes are mapped correctly, and users can successfully authenticate into MSP.	
Entra ID Test — IdP initiated	Initiate a login from the Microsoft Entra ID application and authenticate into MSP. This test validates the IdP-initiated SSO flow, confirming that Entra ID can launch authentication to MSP and that assertions are accepted and processed correctly.
Entra ID Test — SP initiated	Initiate a login to MSP directly and authenticate through Microsoft Entra ID. This test validates the SP–initiated SSO flow, ensuring that authentication requests are correctly redirected to Entra ID and that users can successfully access MSP.
Okta Test — IdP initiated	Initiate a login from the Okta application and authenticate into MSP. This test validates the IdP-initiated SSO flow for Okta, confirming that Okta can successfully authenticate users and pass assertions to MSP.
Okta Test — SP initiated	Initiate a login to MSP directly and authenticate through Okta. This test verifies the SP–initiated SSO flow for Okta, ensuring successful redirection, authentication, and access to MSP.

Create IdP Application - Microsoft Entra ID

1. Create a New Enterprise Application in Entra ID:
   a. From the Azure Portal, under **Azure services**, select **Enterprise applications**.

b. From **Enterprise Applications**, select **New application** > **Create your own application**.

   The **Create your own application** dialog displays.

c. Provide the application name, select **Integrate any other application you don't find in the gallery (Non-Gallery)**, and then select **Create**.

   The application **Overview** page opens.

2. Assign Users and Groups in Entra ID:

   Note
   MSP uses group membership information provided by the IdP to assign roles through its RBAC implementation. The IdP must be configured to send group membership claims to MSP during authentication.

   a. From the application **Overview** page, select **Assign Users and Groups**, and then select **Add user/group**.

      The **Add Assignment** page opens.

   b. From the left pane, select the link under **Users and groups**.

      Azure displays the MSP required user group.

   c. Select the check box for each MSP required user group, and then click **Select**.

   d. Select **Assign**.

      The selected groups are mapped to the selected role. Azure displays the selected groups on the **Users and Groups** page.

      Note
      Only users assigned to the defined groups have access to the defined roles in .

3. Select `SAML` as the Single Sign-On Method in Entra ID:

   a. From the application **Overview** page, navigate to **Manage** > **Single sign-on**, and then select **Get Started**.

   b. Select the **SAML** single sign-on method.

   c. On the **Set Up Single Sign-On with SAML** page, from the **Basic SAML Configuration** section, select **Edit**.

   d. For **Identifier (Entity ID)**, select **Add identifier** and provide a temporary URL.

      For example: `https://temp_ID`

   e. For **Reply URL (Assertion Consumer Service URL)**, select **Add reply URL** and add a temporary reply URL.

      For example: `https://temp_reply`

   f. Select **Save**.

4. Import Entra ID Metadata to MSP:

   To see Identity Provider (IdP) profile settings, log in to MSP using the Global Data Center (GDC) SSO URL. For example, `https://extremeplatformone.com`.

   Note
   Single Sign-on integration can only be configured by MSP users with Administrator permissions in their home account (VIQ). External Administrators cannot access the IdP profile configuration page when administering other customer accounts. An External Administrator is an administrative user whose identity and authentication are managed by an external identity provider rather than being created directly in MSP.

   a. From MSP, go to **Administration & Settings** > **Access Management** > **Identity Providers**.
   b. Select **Add IdP Profile**.
   c. Select the **Microsoft Entra ID** provider, and then select **Next**.
   d. Enter the Fully Qualified **Domain** name of the Azure Tenant and optional **Description**.

      Note
      You can only define a single domain name per IdP Profile. If your IdP supports multiple domains, you must create a separate IdP Profile for each domain. For example, user `gradya@testdomain.onmicrosoft.com` cannot log in when the IdP profile specifies `onmicrosoft.com`.

   e. Select **Next**.
   f. Select **Import From URL** to import the data from the App Federation Metadata URL.
   g. From the *Azure Enterprise Application*, scroll down to Section 3: SAML Certificates, and select the **App Federation Metadata Url** copy to clipboard icon.
   h. In , paste the URL string into the **Enter URL** field, and then select **Import**.

      After importing, the fields in the **IdP Connection** tab display automatically including the Verification Certificate.
   i. Select **Next**.
5. Map MSP User Profile Attributes to SAML Attributes for Entra ID:

   In MSP, you must map the appropriate **User Profile Attributes** to the **SAML Attributes** sent from the IdP.

   The following table includes the required strings for integration with Microsoft Entra ID.

Table 17: MSP - Required Strings for Microsoft Entra

Attribute	Claim Name
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email
Group	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

6. Map MSP Group to Roles for Entra ID:

   roles must be mapped based on the user group membership that is created in Entra ID to enforce authorization.

   In , enter the exact **IdP Group** name (case sensitive) from Entra ID (for example, Operator1), and then select the corresponding role.
7. Map Entra ID Security Groups to MSP Roles:

   Configure the SAML attribute strings required to map the Entra ID security groups to the MSP Role-Based Access Control (RBAC) roles for authorization.

   In the *Microsoft Azure* application, in Section 2: **Attributes & Claims**, select **Edit**.

   a. Perform the following steps to adjust the default claims:
      i. Under **Required claim**, select the **Unique User Identifier (Name ID)** row, change the **Source attribute** field to `user.mail`, and then select **Save**.
      ii. Under **Additional claims**, from the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** row, select the 3-dot menu, select **Delete**, and then select **OK**.
      iii. Select **Add a group claim**, and then select **Groups assigned to the application**. Under **Source attribute**, select one of the following options, and then select **Save**:
         - If your Entra ID instance is cloud-only, select **Cloud-only group display names**.
         - If your Entra ID instance is hybrid-cloud and on premises, select **sAMAccountName**.
      iv. Under **Additional claims**, select the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name** row, change the **Name** field to `email`, and then select **Save**.
   b. Perform the following steps to add a group claim:
      i. Select **Add a group claim**.
      ii. Select **Groups assigned to the application**.
      iii. From the **Source attribute** list, select **Cloud-only group display names**.
8. Export SP Metadata and Import into Entra ID:
   a. After saving the completed **Add IdP Workflow** in MSP, download the SP metadata.
   b. In the *Microsoft Azure* application, on the **SAML-based Sign-on** page, select **Upload metadata file**, navigate to the saved exported file from , and then select **Add**.
   c. Confirm that the imported data is correct, and then select **Save**.

      Note
      When prompted to test the application, select **No I'll test later**.

9. Entra ID Test - IdP Initiated:

   After the integration is complete, test the application.

   a. Go to the Azure main Single Sign On page for the XIQ-SSO application.
   b. Scroll down to the **Test single sign-on with XIQ-SSO** section, and then select **Test**.
   c. Select **Test sign in**, and then sign in to the Microsoft Login Portal.

      After a successful login, you are redirected to the MSP default view. The MSP Audit Logs include the login action.

10. Entra ID Test - SP Initiated:
    a. Browse to the **GDC Login** page `https://extremeplatformone.com`, and then select **Log In with SSO**.
    b. Enter the email address of the IdP account and complete the IdP login process.

       The browser is redirected to the Microsoft Login Portal. After a successful sign in, the browser redirects to the MSP default view. The MSP Audit Logs include the login action.

Create IdP Application - Okta

1. Navigate to the Okta Admin Portal:
    a. Browse to `https://login.okta.com`, and then log in to your Okta Organization with an account with the necessary Administrator permissions to create user, groups, SAML applications, and Authentication Policies.
    b. From the Okta Dashboard page, select **Admin**.
2. Create a New SAML Application and Define User Group Mappings in Okta:



Note
You must create the user groups in the IdP before you can map the user roles in MSP.

    a. From *Okta*, navigate to **Applications** > **Applications**, and then select **Create App Integration**.
    b. Select **SAML 2.0**, and then select **Next**.
    c. Enter an **App name**, and then select **Next**.
    d. In the **SAML Settings** section, enter temporary URLs as a placeholder that will be updated later for the following fields:
       - **Single sign-on URL**: `https://replaceme`
       - **Audience URI (SP Entity ID)**: `https://replaceme`
    e. Scroll down to the **Attribute Statements** section.
    f. Set **Name** to `user.email` and the corresponding **Value** to `user.email`, and then select **Add Another**.
    g. Set **Name** to `user.firstName` and the corresponding **Value** to `user.firstName`, and then select **Add Another**.
    h. Set **Name** to `user.lastname` and the corresponding **Value** to `user.lastname`.
    i. Scroll down to the **Group Attributes** section:
       i. Set **Name** to `user.group`.
       ii. Set the corresponding **Filter** to `Matches regex`, and then set the **Value** to `.*` (a period followed by an asterisk).
    j. Select **Next**.
    k. On the **Help Okta Support understand how you configured this application** page, set **App Type**, and then select **This is an internal app that we have created**.
    l. Select **Finish**.

3. Assign Users and Groups in Okta:

   Note
   MSP uses group membership information provided by the IdP to assign roles through its RBAC implementation. The IdP must be configured to send group membership claims to MSP during authentication.

   a. Select the **Assignments** tab.
   b. Select **Assign**, and then select **Assign to Groups**.
   c. For each group you want to permit authentication to MSP with SSO login, select **Assign** next to the Group Name.

      Note
      For each group that you permit, ensure the Group is set to **Assigned**.

   d. Select **Done**.
4. Create New Password Authentication Policy in Okta:

   When a user logs in to MSP using SSO with Okta, the user must follow the rules defined in the Okta Authentication Policy. You can assign your new SAML application to use one of Okta's out-of-the box Authentication policies. By default, your SAML application uses the **Any Two Factors** Authentication Policy, which has been successfully tested with MSP.

   a. From the **Navigation Pane**, go to **Security** > **Authentication Policies**, and then select **Add a policy**.
   b. Enter a **Name**, and then select **Save**.

      You will be directed to the Rules tab of your new Authentication Policy, where we will modify the rules associated with the existing Catch-all Rule policy.
   c. For the **Catch-all Rule**, select **Actions**, and then select **Edit**.
   d. Scroll down to the **Then** section, for **AND User must authenticate with**, select **Password** from the list.
   e. For **Prompt for authentication**, select **Every time user signs in to resource**.
   f. Select **Save**.
   g. Select the **Applications** tab, and then select **Add app**.
   h. Find the SAML Application you created in Step 2, and then select **Add** for the associated row.
   i. Select **Done** to close the app assignment dialog box.
5. Export Metadata for your Okta SAML Application:

   a. From the **Navigation Bar**, go to **Applications** > **Applications**.
   b. Select the SAML Application you created in Step 2, and then select the **Sign On** tab.
   c. In the **Metadata Details** section, you will see the **Metadata URL**. Select **Copy** and retain the URL for use in the next step.
6. Create IdP Profile, Import Metadata, and Edit Settings in MSP:

   Note
   Single Sign-on integration can only be configured by MSP users with Administrator permissions in their home account (VIQ). External administrators cannot access the SSO configuration page when administering other customer accounts.

a. In , go to **Administration & Settings** > **Access Management** > **Identity Providers**
b. Select **+ Add IdP Profile**.
c. From the **Provider** drop-down list, select **Okta**.
d. Configure the following **IdP Profile Information**, and then select **Next**:
   - **Domain**: Enter a fully qualified domain name (FQDN) for which you want to provide single-sign on.
   - **Description** (optional): Enter a description of up to 64 characters.

   Note
   You can only define a single domain name per integration. If your IdP supports multiple domains, you must create a separate IdP profile for each domain.

e. Select **Import from URL**.
f. In the **ISP Metadata URL** field, paste the URL captured in Step 5, and then select **Import**.

   After successful import, metadata from Okta displays.

   Note
   There might be some critical elements not included in the Okta metadata. If the SLO URL and SLO Response URL fields are blank, enter placeholder values in each field, which we can update in a subsequent step.

g. To supply the placeholder values, copy the **SSO URL** and paste the value into the **SLO URL** and **SLO Response URL** fields.
h. From the **Choose Certificates** list, ensure the certificate that was included in the Metadata import is selected, and then select **Continue**.
i. On the **Attribute Mapping** page, enter the following values:
   - **First Name**: `user.firstName`
   - **Last Name**: `user.lastName`
j. Select **Add a group name mapping** for each Okta group to map to an MSP role.
k. In the **IdP group** field, enter the name of your Okta group, and then select the MSP role to map any users in the group.

   Add additional mappings as needed.

   Note
   Each of the values for First Name, Last Name, and Group Name are case sensitive. Ensure that the values entered here are an exact match for the information entered in Okta. The list is applied from top to bottom, with the first match taking precedence. If a user belongs to multiple groups listed here, they will be assigned the MSP role based on the order that you specify.

l. When there is no available group map, select one of the following options to define MSP behavior:
   i. **Deny user login**: A user that successfully logs into MSP with their Okta credentials, but is not in an Okta group that is mapped to an MSP access role, is denied access to the application.
   ii. **Allow user login and assign a default role and sites**: A user that successfully logs into MSP with their Okta credentials, but is not in an Okta group mapped to an MSP access role, is mapped to the role defined here.

m. Select **Save**.

7. Modify Okta SAML Application Metadata with MSP Settings:

   For this step, we recommend having MSP and Okta open in separate tabs, as you will select data from your new IdP profile in MSP and copy it over to your SAML application in Okta.

   a. In **Okta**:
      i. Browse to your Admin Portal, navigate to **Applications** > **Applications**, and then select your SAML application.
      ii. From the **General** tab, scroll down to **SAML Settings**, and then select **Edit**.
      iii. Select **Next**, and then select the **Configure SAML** tab.
   b. In MSP:
      i. From **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**, in the row for your IdP profile completed in Step 6, select , and then select **Edit**.
      ii. Navigate to **Extreme Cloud (SP) Connection**, and then select **Download Certificate** to save the file to your computer.
      iii. Copy the **SP Entity ID** value from and copy it to the **Audience URI (SP Entity ID)** field in Okta.
      iv. Copy the **ACS URL** value from and copy it to the **Single Sign-On URL** field in Okta.
   c. In **Okta**:
      i. Under **SAML Settings** > **General**, select **Show Advanced Settings**.
      ii. For **Signature Certificate**, select **Browse files**.
      iii. Select **All Files**, navigate to find the certificate file you downloaded in the previous step, select the certificate, and then select **Open** to upload the certificate.
      iv. Select **Enable Single Logout**.
      v. Copy the **SLO URL** value from and copy it to the **Single Logout URL** field in Okta.
      vi. Copy the **SP Entity ID** value from and copy it to the **SP Issuer** field in Okta.
      vii. Select **Next**, and then select **Finish**. Click to view your SAML application again.
      viii. Select the **Sign On** tab, and in the **SAML 2.0** section, select **More Details**.
      ix. Next to the **Single Logout URL** field, select **Copy**.

      Use this URL to replace the placeholder text we submitted earlier.
   d. In MSP:
      i. Return to the **IdP Connection** section of your IdP profile and paste that value into the **SLO URL** and **SLO Response URL** fields, replacing your placeholder values.
      ii. Select **Save Changes**.

      The integration is now complete.

8. Okta Test - IdP Initiated:After the integration is complete, test the application.
   a. Log in to your Okta Organization at `https://login.okta.com` with a user account that has been granted access to the SAML application.
   b. From the Okta Dashboard page, select your SAML application, and then from the right pane select **Launch App**.

      The browser redirects to the Okta Login Portal.
   c. Enter your **Username** and **Password**, and then select **Verify**.After a successful login, you are redirected to the default view.
9. Okta Test - IdP Initiated:

   After the integration is complete, test the application.

   a. Log in to your Okta Organization at `https://login.okta.com` with a user account that has been granted access to the SAML application.
   b. From the Okta Dashboard page, select your SAML application, and then from the right pane select **Launch App**.

      The browser redirects to the Okta Login Portal.
   c. Enter your **Username** and **Password**, and then select **Verify**.

      After a successful login, you are redirected to the MSP default view.
10. Okta Test - SP Initiated:
    a. Browse to the GDC Login page, and then select **SSO**.

       `https://extremeplatformone.com`
    b. Enter the email address of the IdP account and complete the IdP login process.

       The browser is redirected to the Okta Login Portal. After a successful sign in, the browser redirects to the MSP default view.

Add an IdP Profile

This task is part of a larger workflow. It is important to complete all steps in order. Skipping steps can result in incomplete configurations and require you to repeat parts of the process.

Use the Identity Providers tab to configure external identity providers (IdPs) for single sign-on (SSO) authentication. Identity Providers allow MSP Super Administrators to authenticate by using enterprise identity services instead of local credentials.

The following IdPs are supported by MSP

- Generic SAML Server
- Active Directory Federation Service (ADFS)
- Ping
- Okta
- Microsoft Entra ID
- OneLogin
- Auth0

To add an identity provider profile to your network:

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers**.
2. Select **Add IdP Profile**.
3. In step 1 - Configure the **Profile** information:
   a. **Domain**: Provide the domain name.

      Currently, only **Management SSO** is supported.
   b. **Description** (optional): Enter a description of up to 64 characters.
4. Select **Next**.
5. In step 2 - Configure **IdP Connection**:
   - **Import from Metadata**: Select Browse Files or drag and drop the metadata file in .xml format.
   - **Import from URL**: Provide the URL, and then select **Import**.
   - **Manually Enter**: Configure the following fields manually:
     a. Provide the **IdP Entry ID**.
     b. Enable or disable the **SSO Request toggle** as required.
     c. Configure **SSO Binding URL** as required:
        - **HTTP Post**
        - **HTTP Redirect**
     d. Configure **SLO Binding URL** and **Response URL**.
        - **HTTP Post**
        - **HTTP Redirect**
     e. Verify and import certificates using **Verification Certificates**:
        i. **View Certificates**
        ii. **Import Certificates:** Select Browse Files or drag and drop certificate files in .cer, crt, or .pem format.
6. Select **Next**.
7. In step 3, configure **Attribute Mapping.**

   You must map the appropriate User Profile Attributes to the SAML Attributes sent from the IdP. These strings must be created and be in sync with both IdP and SP.

   Note
   To generate the SP Metadata required to complete the IdP SAML configuration, the SAML strings cannot be configured on the IdP until the MSP workflow is completed. You must complete the MSP workflow first. If you do not know the SAML Attribute Strings, add place holder data to save and complete the configuration.

   a. Configure the following **SAML attributes**:
      - First Name: The URL or endpoint where the IdP provides the user's given name. For example, https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/ givenname
      - Last Name: The URL or endpoint where the IdP provides the user's family name or surname. For example, https://schemas.xmlsoap.org/ws/2005/05/ identity/ claims/ surname

- Email: The URL or endpoint where the IdP provides the user's email address. For example, https://schemas.xmlsoap.org/ws/2005/05/identity/ claims/ surname
- IdP Group: The URL or endpoint where the IdP provides the user's group memberships. For example, https://schemas.microsoft.com/ws/2008/06/ identity/ claims/groups



Note
Default SAML attributes are automatically populated based on the selected IdP type.

b. Configure **Group Mapping** for the identity provider group:
   - Provide the **IdP Group** name.
   - Select the corresponding **MSP Role**.

     The following MSP roles are available:
     - **MSP Admin**: Provides full read and write access to manage the MSP environment and tenant resources.
     - **MSP Super Admin**: Provides unrestricted access to all MSP features and can create and manage administrators, teams, and tenant groups.

8. Select **Add a Group Mapping**, to create an additional group mapping.
9. Select **Save**.
10. In Step 4, configure **SP Connections**.

    After mapping user profile attributes, you must export the SP metadata and import it to the IdP to complete the configuration.

    a. Review the Service Provider connections information.
    b. Use the following options to manage the service provider connection information:
       - Select **Download SP Metadata** to download the service provider metadata.
       - Select **Download Signing Certificate** to download the signing certificate.
       - Select the copy option next to a value to copy it to the clipboard.
11. Select **Done**.

Manage IdP Profile

Use this task to manage Identity Provider (IdP) profiles. IdP profiles define the configuration required to integrate an external IdP for user authentication and role assignment.

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers**.

2. Locate the Identity Provider from the list, select ⋮ from the corresponding row row, and then select one of the following actions:
   - To update an IdP profile, select `Edit`. Configure IdP Profile Settings, and then select `Save Changes`.
   - To prevent an existing IdP profile from being used for authentication, select `Disable`. Select Disable a second time to confirm.

     Note
     Disabling an IdP profile will make it temporarily inactive.

   - To allow an IdP profile to be used for authentication, select Enable.
   - To remove an existing IdP profile, select Delete. Select Delete a second time to confirm.

     Note
     Deleting an IdP profile permanently removes it from the system.

   For more information, see Add an IdP Profile on page 55.

Manage IdP Profile Certificates

Identity Provider (IdP) profile certificates are essential for securing communication between the IdP and Service Providers (SPs). Properly managing these certificates is key to maintaining the integrity and trustworthiness of your Single Sign-On (SSO) environment.

From the Certificates window for an IdP profile, you can:

- View a list of certificates associated with the IdP profile to view details, including certificate provider, days remaining, valid from date, valid to date, and fingerprint.
- Make active certificates inactive.
- Import a new certificate to the IdP profile.

1. Go to **Administration & Settings** > **Access Management** > **Identity Providers**.
2. Locate the IdP profile from the list, select ⋮ from the corresponding row, and then select `Edit`.
3. Expand IdP Connection, and then select Manage Certificates.
   a. To add a new certificate, select Import New Certificate, and then select Browse Files to browse to your local folder and select the certificate.
   b. To deactivate a certificate, select ⋮, and then select Make Inactive.
   c. To delete a certificate, select ⋮, and then select Delete. Note If only one certificate is listed, you cannot delete the last valid certificate.
   d. Select Certificates for the IdP you selected to return to the IdP profile list.

Configure Idle Session Timeout

Use this task to specify the idle period, after which an inactive session automatically times out, for all user accounts.

1. Go to **Administration & Settings** > **Access Management**, and then select the **Access Settings** tab.
2. Select **Timeout Duration**, and select the hour and minutes for duration from the HH and MM menus, respectively.
3. Select **Save**.

Integrations

Integrations provides administrators with tools to create and manage API keys. **Integrations** table displays the following information for the API keys that have been added to Extreme Platform ONE Networking:

- **Name**: The name of the API key.
- **Description**: A short description of the API key.
- **Expiration Date**: The expiration date of the API key.

To create a new API key, select **Create New API Key**. To edit an existing API key, select ⋮ at the end of the corresponding row, and then select **Edit Key**. To delete an API key, select **Delete Key**.

Note

- After generating a key, it cannot be modified.
- External administrators are not permitted to create the API keys.

Create a New API Key

Use this task to create a new API key.

1. Go to **Administration & Settings** > **Integrations** > **Create New API Key**.
2. Configure the settings:
   - **Name**
   - **Description**
   - **Expiration Date**
3. Select **Generate Key**.
4. Select **Copy API Key**, and then select **Close**.

Important

Make sure to copy your API key now. For security reasons, you won't be able to see it again once you close the window.

Logs

Audit Logs provides MSP administrators with a centralized view of user activity across all managed tenants. Audit logs include Organization Name, Tenant ID, and VHM columns, making it easier to identify the source tenant for each event. Administrators can filter logs by tenant, application, category, date range, or keyword, and export results to .CSV for reporting and compliance purposes.

Use this procedure to search, filter, schedule, and reset log activities.

Extreme Platform ONE for MSP 2.7 and later releases support audit logging of all configurable features.

The following table describes fields, buttons, and icons in the **Logs** tab.

Table 18: Logs

Element	Description
Search	If you have a long list, use the **Search** option to find a particular log.
Logs	The type of log to display: Audit, GDPR, Authentication, Accounting, Credential, SMS, Email, KDDR, Event, and Security.
Select Date Range	Select a date and time range to display.
	Based on the selected filter, downloads data in a CSV file. Exports are based on filter views.
Refresh 	Refreshes the screen to show the most recent logs.
Timestamp	The date and time the log was created.
Category	The log category type.
Email	The email of the user triggering the log.
User name	The user name of the user triggering the log.
Status	The status of the log event.
Description	Description of the the log event.
Application	The application triggering the log event.
Tenant	The name of the tenant.
Tenant Tags	The name of the tenant tag.
Organization	The name of the organization.
VHM	Unique identifier for the tenant VIQ instance.

Logs capture the following activities:

- **Audit Logs**
  - Administrative activity: For example, creating or deleting a user account or deleting a user from IAM
  - Data access and modification: When a user views, creates, or modifies data

- User denials or login failures: Captures when a user is unable to login to a system due to invalid credentials or is denied access to resources such as a specific URL
- System changes: Captures system activity. Audit logs must be compliant with all Extreme Network standards, for example, HIPPA, PCI, NIST.

Use logs to detect anomalies in the system and track past activity.

1. Go to **Administration and Settings > Logs**.
2. Select the **Date and Time** picker to do the following:
   a. Display logs for up to 30 days.
   b. View audit logs for last week, last month or last quarter.
   c. Use arrows to select a specific month.
   d. To view logs for a specific date, select that date directly from the calendar.
   e. Select start and end times.
   f. Reset to default.
   g. Select **Done** to exit the screen.
3. Search and filter by column headings.
4. Sort the **Date/Time** column in ascending or descending order.
5. Select **Column** to add, hide and reposition how specific columns appear on the screen.

MSP Definitions

The following table contains common Extreme Platform ONE for MSP definitions.

Term	Definition
CUID	Customer Unique Identifier links the tenant account to the ExtremeCloud IQ Licensing Service (LEM). When a CUID is associated with a Virtual IQ instance (VIQ), it establishes the licensing relationship between the tenant account and the VIQ.
Tenant	An MSP customer account
Administrator Group	A functional group of MSP Administrators, not an account. You can create multiple groups and associate them with MSP tenant accounts.
Default Administrator	The local administrator created when a VIQ is established. You cannot delete the default administrator from the VIQ, but you can modify the email address.
External Administrator	An administrator external to the MSP. When an administrator or administrator group is added to the VIQ, the administrator or administrator group becomes an external administrator for MSP. The administrator or administrator group can then perform functions on behalf of the end customer.
MSP Super Administrator	• An elevated virtual IQ (Onboarded Managed Service Providers VIQ) local administrator with access to all MSP Workspace features. • Sets up the MSP home VIQ • Create MSP administrators • Create and edit administrator groups
MSP Administrator	Have access to all Extreme Platform ONE for MSP features. • Can access VIQs to which they have been added. • Add license accounts. • Allocate licenses. • Can access any end customer VIQs within ExtremeCloud IQ to which they have been added. Cannot create the following: • New MSP administrators. • Administrator Groups.

Term	Definition
MSP Home Virtual IQ	All MSP Administrators are attached to a Home VIQ. You need the home VIQ to set up the MSP Super Administrator and MSP Administrators. The system then pushes permissions down onto end customer VIQs using external administrator APIs. Customer VIQs created through Workspace for MSPs are automatically associated with this MSP Home VIQ by attaching the MSP Partner ID to the customer VIQ.
MSP Partner ID	The MSP Partner ID is the Home VIQ code.
NAC	Network Access Controller.
VIQ	Virtual IQ is a singular management instance of an ExtremeCloud IQ account. VIQ includes all the cloud-based functionality required to manage and operate a tenant network.
Virtual IQ Local Administrator	An administrator that is added to a VIQ.

Troubleshooting

This section outlines common issues and best practices when working with MSP licenses and tenant configurations.

Avoid linking to the MSP CUID from XIQ

This causes configuration issues and requires coordination with the tenant to unlink.

Avoid creating VIQs through self-registration

This prevents association with the MSP Partner ID and requires a GTAC ticket for correction.

Set license allocations for NAC licenses

Without a defined allocation, if Site Engine (SE) is set to 100%, it may consume the entire MSP license pool.

Ensure Site Engine version 23.02.10 or higher

Using an older version of Site Engine can lead to inaccurate license reporting and impact invoicing.

Assign End Tenants as Operators, not Admins, in their local VIQ

This prevents tenants from viewing or modifying license configurations.

MSP CUID Linking Error

Issue: The most common issue when linking MSP CUIDs is a stale session handler from the Extreme Partner Support Portal.

Resolution:

1. Log out of both:
   - Extreme Support Portal
   - Extreme Platform ONE for MSP
2. Log back into Extreme Platform ONE for MSP and begin the process to add a license pool.
   - You are automatically redirected to the Extreme Support Portal login page.
3. Log into the Extreme Support Portal when prompted.
   - This action automatically synchronizes the account.

   For more information, see *Allocate License* section.

Add MSP Admin Error

Issue: When adding an MSP Admin in Extreme Platform ONE for MSP, you may encounter an error if the account already exists as a **Default Admin** or **Local Admin** in another VIQ.

Cause: Extreme Platform ONE for MSP inherits account restrictions from ExtremeCloud IQ, which does not allow:

- Registering more than one VIQ with the same account.
- Assigning the same user as a Local Admin in multiple VIQs.

Accounts created in Extreme Platform ONE for MSP are automatically assigned as **Local Admins** in the MSP Home VIQ. If the same account is already a Default or Local Admin in another VIQ, the system blocks the addition.

Resolution:

- Ensure the account you are trying to add is **not already assigned** as a Default Admin or Local Admin in any other VIQ.
- If needed, **remove the account** from its current VIQ role before adding it to Extreme Platform ONE for MSP.

Default Admin Migration

Issue: You cannot remove default Admin accounts from a VIQ, and reusing them in Extreme Platform ONE for MSP may cause errors due to their existing admin roles in other VIQs.

Cause: ExtremeCloud IQ prevents you from assigning the same account as a Local Admin or Default Admin in multiple VIQs. Since Extreme Platform ONE for MSP automatically assigns new accounts as Local Admins in the MSP Home VIQ, you must update any account with existing admin roles elsewhere before reusing it.

Resolution:

1. Log in to each VIQ where the account is currently a Default Admin.
2. Add a Super Admin account as an External Admin in those VIQs:
   - Navigate to **Global Settings** > **Account Management**.
   - This action links the VIQ to Extreme Platform ONE for MSP for further administrative control.
3. Edit the Default Admin account to free it up:
   - Go to **Global Settings** > **Account Settings**.
   - Click the edit icon next to the Default Admin account.
   - Change the email address to an alternate email or an alias such as admin+alias@example.com, if supported.
   - Click the save icon to apply changes.

Local Admin Migration

Issue: You may encounter errors when adding administrator accounts to Extreme Platform ONE for MSP if those accounts are already assigned as Local Admins in other VIQs.

Cause: ExtremeCloud IQ prevents you from assigning the same account as a Local Admin in multiple VIQs. Because Extreme Platform ONE for MSP automatically assigns new accounts as Local Admins in the MSP Home VIQ, you must resolve any conflicting roles before reuse.

Resolution:

1. Add the MSP Super Admin account to the affected VIQ:
   - Go to **Global Settings** > **Account Management**.
   - Add the Super Admin as an External Admin.
   - This links the VIQ to Extreme Platform ONE for MSP for administrative control.
2. Remove or edit the conflicting Local Admin accounts:
   - In the same VIQ, go to **Global Settings** > **Account Management.**
   - Delete the Local Admin account or edit the email address to an alternate or alias (if your email domain supports it).
3. Log back into Extreme Platform ONE for MSP and try adding the administrator accounts.

License Consumption

Issue: License consumption in ExtremeCloud IQ is unclear, particularly when devices are in varying administrative or connection states.

Device Admin Status

State	Description	License Usage
New	Device is recently added but not yet fully configured or integrated.	Yes
Managed	Device is fully configured and actively managed.	Yes
Unmanaged	Device is not actively managed, retains last configuration and cannot be modified.	No

Device Connection Status

Status	Description	License Usage
Connected	Device is online and communicating with ExtremeCloud IQ.	Yes
Disconnected	Device is offline.	Yes

Note

A device transitions from **NEW** to **MANAGED** when:

- It is fully configured with required settings and profiles.
- It successfully communicates with ExtremeCloud IQ.
- A valid license is assigned