Extreme™ Platform ONE Security 25.5.0 User Guide

Identity-Based Secure Access Configuration and Integration

9041015-00 Rev AA
February 2026

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/

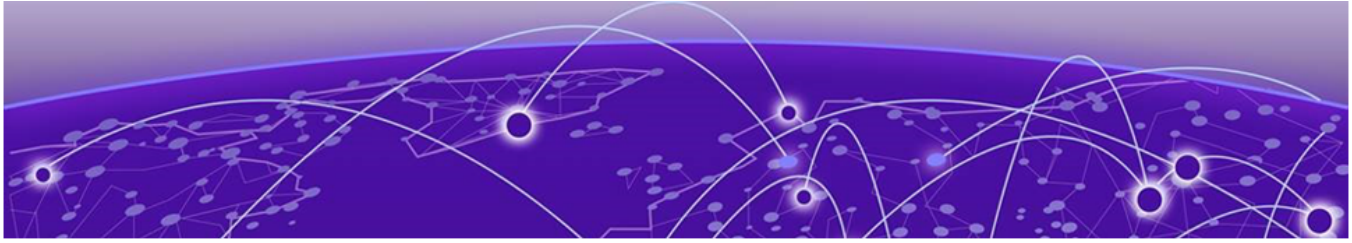
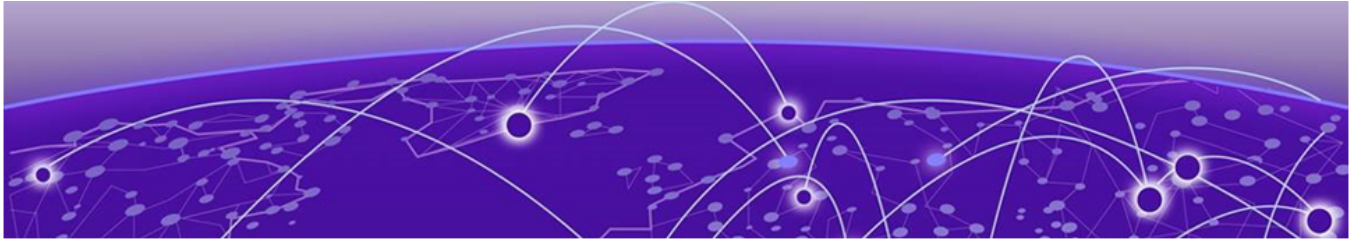


Table of Contents



Abstract

This user guide for Extreme Platform ONE Security version 25.5.0 provides comprehensive technical guidance for configuring, deploying, and managing identity based zero trust access across wired, wireless, cloud, and application environments. It details the platform's integrated security architecture, including ZTNA based application access, NAC driven campus access, RadSec secured RADIUS communications, device posture enforcement, policy driven network segmentation, and automated provisioning workflows with Switch Engine, Fabric Engine, and ExtremeCloud IQ. The guide explains onboarding methods for hybrid, application, and network access; configuration of Instant Secure Port Profiles, SSIDs, RADIUS templates, network devices, and service connectors; and integration with major identity providers such as Microsoft Entra ID, Google Workspace, and Okta using JIT, SCIM, OIDC, SAML, and secure LDAP. It also outlines wireless integration procedures, policy creation for network, application, and hybrid access, application onboarding and discovery workflows, and administration tasks such as RBAC configuration, certificate management, MDM integration with Intune, Jamf, and Google Workspace, subscription management, and log analysis. Monitoring capabilities cover dashboards, alerting, client visibility, troubleshooting workflows, packet capture, and policy evaluation, providing a complete operational framework suitable for experienced technical administrators seeking to secure distributed enterprise networks.

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.
< >	Nonprinting 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.

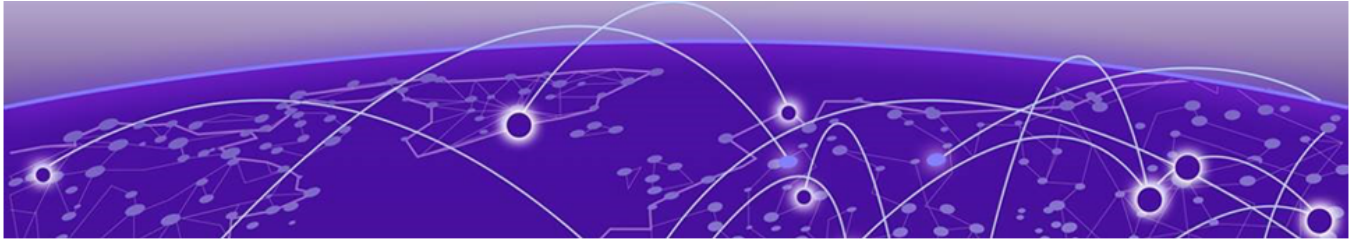
Send Feedback

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 Product-Documentation@extremenetworks.com.

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.



Welcome to Extreme Platform ONE Security

Extreme Platform ONE Security integrates network, application, and device access security within a single solution.

With Extreme Platform ONE Security:

- Establish a consistent, identity-level zero trust policy across your network for all users.
- Maintain a single policy that integrates the network, applications, and device access (including the Internet of Things (IoT) device access) independent of the client location.

Extreme Platform ONE Security combines and enhances remote and campus access security. Remote access leverages ZTNA continuous authentication and tunneled application sessions with direct to cloud routing. On campus access combines ZTNA and Network Access Control (NAC) capabilities to control access to the network and applications for headed and headless devices.

Extreme Platform ONE Security integration with mobile device solutions such as Microsoft Intune offers the following:

- Improved access by closely examining the condition of devices and their authentication features
- A single identity-based zero trust policy engine for networks and applications
- A single system for monitoring, visualizing, and reporting to gain better insights and simplify management
- Automatic set up for IoT and end user devices
- Automatic configuration for NAC, SSIDs, ports and VLANs on Universal APs and switches

Access Extreme Platform ONE Security

To go to other Extreme apps, select the top-right menu .

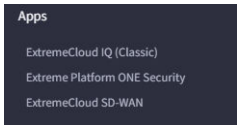


Figure 1: Extreme Platform ONE Networking Nine-dot Menu

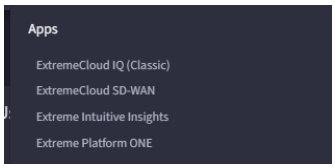


Figure 2: ExtremeCloud IQ Nine-dot Menu

Extreme Platform ONE Security consists of the following major sections:

- The navigation pane
- The content pane

Navigation Pane

Use the navigation pane to access the following workbenches and content:

- **Workspace**
- **Onboarding**
- **Monitoring**
  - Dashboard
  - Alerts
  - Clients
  - Troubleshooting
- **Configuration**
  - Sites
  - Network
- **Policy**
  - Security Policies
  - Users & Devices
  - Conditions

  - Network Services
  - Applications
- **Subscriptions & Services**
  - Subscriptions & Licensing
- **Administration and Settings**
  - Access Management
  - Security Services
  - Alerts Policies
  - External Notifications
  - Integrations
  - Logs

Content Pane

The content pane displays information related to your navigation pane selection.

Extreme Applications: Select  to access the following applications:

- ExtremeCloud IQ (Classic)
- ExtremeCloud SDWAN
- Extreme Intuitive Insights

Table 4 describes the icons available in the content pane.

Table 4: Standard Icons

Icon	Description
	AI-driven help, advice, and more. Use to get answers. AI Expert offers faster learning, troubleshooting, and purchasing with greater confidence and less risk.
Profile Icon 	Select your initials at the top right corner of the screen to view the following: • Name and email address • Profile icon • About Extreme Platform ONE Security displays the release version for each software component • Other Environments displays other available Extreme Platform ONE Security Environments. • Sign Out The **Profile** icon displays your name, login details, language preferences, and preferred application (Networking or Security). You can modify your name and password from this menu. You can choose a light or dark theme for your administrative environment.

Table 4: Standard Icons (continued)

Icon	Description
Resource Center icon 	The **Resource Center** icon expands to show the following menu options: • Product Tours • Share Your Feedback • User Guide • Release Notes • Legal Summary • Contact Sales Team Each selection opens an external site, from which you can add feedback or obtain product-related information.
 Download	You can download data and export in .csv format. Use the Filter option to tailor your content to specific views.
 Refresh icon	Refreshes the screen and displays the latest information

Workspace

The Extreme Platform ONE Security **Workspace** tab provides a unified view of network, security, and licensing insights. The tab is divided into two primary sections: Static Insights and AI Canvas Insights on page 17.

Static Insights

This section provides high-level, static widgets that summarize the current state of the network and subscriptions. These widgets include:

- Authentication Types - MAC Auth, EAP-TLS, EAP-TTLS
- Unique Clients - Number of clients, Timeframe
- Top Policy Usage

AI Canvas Insights

This section includes Licensing and Entitlements widgets powered by AI to provide security-related insights.

To add a customized widget, from the right-side panel select AI Expert, enter your query, and select **Add Widget**.

The **AI widget** is added to the **AI Insights** area of **Workspace**.

AI Expert

Extreme AI Expert is an AI-based Virtual Advisor developed by Extreme Networks. It assists users with network operations, troubleshooting, and analytics by combining documentation, knowledge base content, and real-time network data, all accessible through natural language conversation within Extreme Platform ONE.

It provides a unified way to ask questions, visualize data, and take action, from understanding device behavior to creating support cases, without switching tools or writing queries.

Extreme AI Expert Icons

The following icons are available within AI Expert, see Table 5:

Table 5: AI Expert Icons

Icon	Description
Extreme AI Expert	Provides context-aware responses using a conversational interface.
Dock	Docks the Extreme AI Expert panel to the Extreme AI Expert icon. This is the default setting.
Overlay	Separates the Extreme AI Expert panel from the Extreme AI Expert icon.
New Chat	Initiates a new chat.

Table 5: AI Expert Icons (continued)

Icon	Description
 Conversations	Provides access to previous conversations with the Extreme AI Expert.
 Canvases	Displays the selected network dashboard and provides the following options: • Update the existing dashboard using **Replace Widget** option. • Add a new widget to the Canvas using **Add to Canvas** option.

AI Conversations

AI Conversations is the core interface of Extreme AI Expert. Conversations facilitate natural interaction using text-based questions to query both knowledge and real-time network data.

Enablement Prompts

When you begin an AI conversation, AI Expert displays structured queries called enablement prompts that help you generate your first widgets and understand the types of data available for visualization. AI Expert also provides enablement prompts as suggestions for followup.

Talk to Knowledge

Access authoritative information across the Extreme ecosystem, including:

- Product documentation such as datasheets, configuration guides, and user manuals.
- GTAC Knowledge Base: more than 29,000 articles.
- Extreme Networks website content and AI Expert self-aware information.

Talk to Data

Query and analyze real-time network data using natural language. Start new conversations using the provided structured queries (enablement prompts). AI Expert retrieves, correlates, and visualizes information from Extreme Platform ONE APIs, ensuring consistency with the data displayed in dashboards.

Talk to Data offers the following capabilities:

- Query devices, clients, applications, and alerts
- Display structured results (tables, charts, graphs)
- Combine telemetry and configuration data
- Show reasoning visibility (data sources, API calls)

- Apply RBAC for permissions
- Suggest Follow-up Questions

AI Canvas

AI Canvas is an interactive workspace within Extreme Platform ONE offerings for users to build and visualize real-time network insights using AI-generated widgets. It extends the capabilities of Extreme AI Expert by enabling you to organize and monitor key metrics in a customizable dashboard format.

Create widgets from your AI queries that can display structured data in the form of tables, charts, and graphs. Then add the widgets to your canvas for ongoing visibility.

The following canvas states are available:

- **Draft**: A work-in-progress canvas for users to experiment with different widgets.

  Note
  Limit of 10 draft canvases, with up to 10 widgets per canvas.

- **Published**: A live canvas that auto-refreshes every 10 minutes.

  Note
  Limit of 3 published canvases, with up to 10 widgets per canvas.

- **Collaboration**: Published canvases can be shared with other users in the same organization, enabling team-wide visibility and collaboration without consuming their canvas limits.
- **Always-On Workspace Canvas**: A default canvas offered from the Extreme Platform ONE landing page. This canvas is always published with live data and never counts against your user limits.

To help users get started, AI Canvas includes enablement prompts - suggested questions that demonstrate how to interact with Extreme AI Expert and build useful widgets. These prompts are currently available in English and are designed to accelerate onboarding and discovery.

Select any widget on your canvas to open a contextual conversation with AI Expert. The widget data automatically loads as context, enabling you to ask follow-up questions without recreating the original query.

AI Canvas has the following known limitations:

- **Canvas Sharing Scope**: Sharing is currently limited to users within the same organization.
- **Think It Through** Integration: The **Think It Through** feature is not yet supported within AI Canvas. While **Think It Through** enables multi-step reasoning and deeper analysis, it cannot currently generate widgets or visualizations for canvas use.

AI Canvas Actions

The following actions are available in AI Canvas:

- **Select an existing canvas** - Select the canvas from the list of canvases shown.
- **Delete an existing canvas** - Select the delete icon associated with the canvas.
- **Add a new canvas** - Select **Add New**.

  Note
  Maximum of 10 draft and three published canvases.

- **Edit the title of a canvas** - Select the edit icon associated with the canvas. Change the title as required, then select the confirm icon.
- **Delete all canvases** - Select **Delete All**. Confirm the deletion to delete.
- **Publish a canvas** - Select the existing canvas, and select **Publish**.
- **Unpublish a canvas** - Select the existing canvas, then select **Unpublish**.

Security and Permissions

Extreme AI Expert enforces role-based access control (RBAC) consistent with Extreme Platform ONE.

All API calls run depending on user credentials. This control improves security by meeting the following requirements:

- Access only to data permitted by the assigned user role, for example Admin, NetSecOps, or Observer.
- Prevention of unauthorized access attempts.
- Alignment with the Extreme Networks data security and privacy standards.

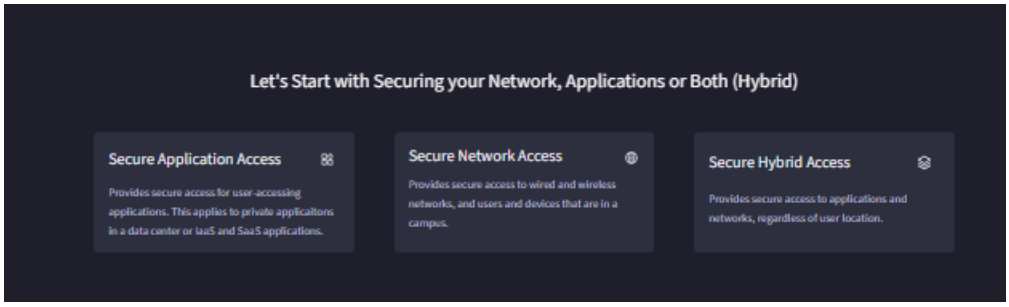
All data handling adheres to the Extreme Networks privacy, compliance, and security policies, ensuring confidentiality and system integrity across all AI interactions.

Onboarding | Access & Workflows

Extreme Platform ONE Security provides secure access to applications and networks from anywhere, making it easy for users to connect seamlessly to their resources.

The following types of secure access are offered by Extreme Platform ONE Security:

- **Secure Application Access** provides secure access for user-accessing applications. This applies to private applications in a data center or IaaS and SaaS applications.
- **Secure Network Access** provides secure access to wired and wireless networks, and users and devices that are in a campus.
- **Secure Hybrid Access** provides secure access to applications and networks, regardless of user location.

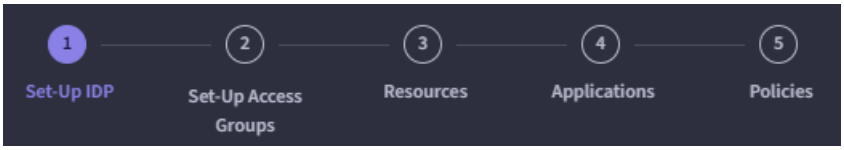


The primary goal of a secure access method is to ensure safe access to applications and networks from anywhere, making it easy for users to connect seamlessly to their resources.

Note
Secure Hybrid Access onboarding method is the most comprehensive method. Secure Application Access and Secure Network Access are subsets of Secure Hybrid Access.

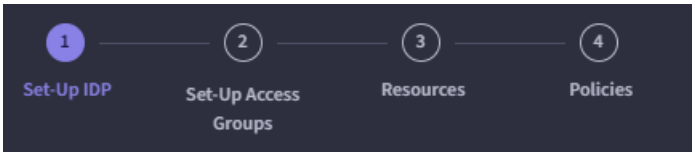
The following workflows are provided for each onboarding method:

- **Secure Application Access**



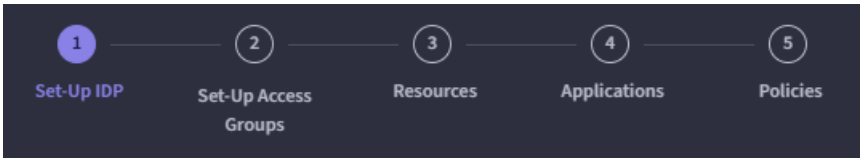
1. Set-Up IdP
2. Set-Up Access Groups
3. Resources
4. Applications
5. Policies

- **Secure Network Access**



1. Set-Up IdP
2. Set-Up Access Groups
3. Resources
4. Policies

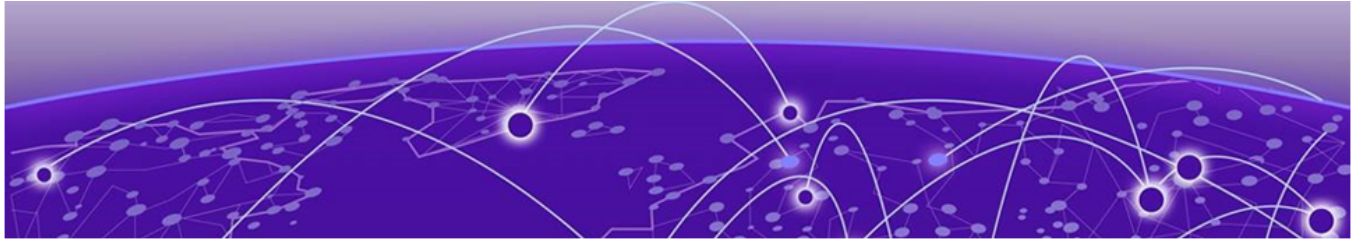
- **Secure Hybrid Access**



1. Set-Up IdP
2. Set-Up Access Groups
3. Resources
4. Applications
5. Policies

Each access method offers the following types of Identity Providers (IdPs).

For more information, see Identity Providers | Network & Applications on page 91.



Onboarding | Resources

Use these required resources for onboarding using Secure Hybrid Access:

- Sites enable you to define your virtual or physical network boundaries. Sites are synchronized using Extreme Platform ONE Networking and in general should be created and managed using that interface. To manage a site, see Configuration | Sites on page 46.
- Deploy Service Connector enables you to add secure application access over encrypted protocols. For more information on Service Connectors, see Deploy Service Connectors on page 165.
- Deploy RadSec Proxy ensures RADIUS communications over untrusted networks. For more information on RadSec Proxies, see Deploy RadSec Proxies on page 169.

These are two required tasks to set up resources for Secure Application Access:

- Service Connector Location enables you to add and manage network sites by defining your virtual and physical network boundaries. A site can contain one or more service connectors. The same site is global and can be used for other places in Extreme Platform ONE Security to define boundaries
- Deploy Service Connector allows you to select an encryption protocol such as IPsec or WireGuard and deploy a service connector on the customer premises such as private data center or public cloud (AWS, Azure, GCP) managed by tenant admin.

Use these optional resources for onboarding using Secure Network Access:

- RadSec Proxy Location: A site can contain none, one, or more RadSec proxies. The same site is global and can be used for other places in Extreme Platform ONE Security to define boundaries
- Deploy RadSec Proxy:
  - For network devices (switches/AP) that cannot do RadSec, the RadSec Proxy secures RADIUS traffic into a secure Transport Layer Security (TLS) tunnel
  - The RadSec Proxy server forwards an auth-request to the RADIUS server and another auth-request back to the switch or access point
  - The RadSec Proxy sends a Change of Authorization (CoA) packet when a user selects reauth on the **Clients** page for users attached to the proxy network devices.

Note
Network devices must be enabled to accept CoA packets.

Once the onboarding is complete, you can access additional resources:

- RADIUS Server enables authentication for remote access. For more information, see View RADIUS Servers on page 153.
- enables you to manage Network Devices, SSIDs, and RADIUS Template.
- enables you to manage Trusted Root, RADIUS server, and intermediate certificates. For more information, see Certificate Management on page 153.
- enables you to manage DNS servers and policies. For more information, see Manage DNS Servers on page 171 or Add a DNS Policy on page 172.

Onboarding | Supported Platforms and Hardware Requirements

Minimum Supported versions for mobile agents

Android: 11

Chrome OS: 11

iOS and iPadOS: 15

Browser Support List

Chrome: Latest two versions

Firefox: Latest two versions

Safari: Latest two versions

Minimum Supported OS versions for Desktop Agents across all supported platforms

Mac Agent = > macOS 11 and later

Windows Agent => Windows 10 and later

Linux Agent = > Ubuntu 22.04 and 24.04

Note

The tenant admin cannot download Extreme Platform ONE Security agents. To download Extreme Platform One Security Desktop agents Log into the End User Portal and go to the **Downloads** page.

Once the Extreme Platform ONE Security agent is installed, open the agent and select **Login**. Upon redirect to the browser for authentication, and successful login, the session automatically returns to the agent.

RadSec Proxy hardware requirements and prerequisites

Minimum hardware requirements: vCPU: 2 Ram: 1.5 GB

Supported Deployment:

VMware OVA

Ubuntu 20.04, 22.04, and 24.04 Packaged Install.

Service Connector hardware requirements and prerequisites (local and cloud)

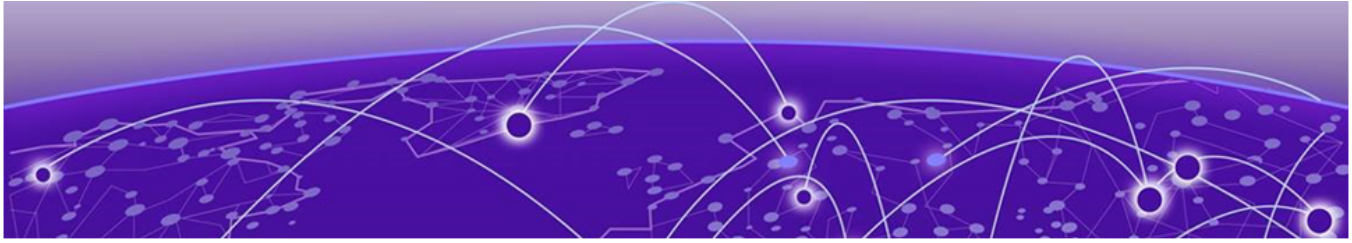
Note
For Extreme Platform ONE Security releases, we recommend the latest version of Service Connectors and End User Agents.

- Supported Deployments:
  - System Requirements for Packaged Deployment - Recommended OS - Ubuntu 22.04 and 24.04.
  - VMware OVA
  - Dockerized Deployment - C-Supported Platform: amd64 Compatible with multiple operating systems; requires only Docker to be installed.
  - Cloud-based Deployment:
    - AWS
    - Azure
- Inbound ports are not required for the service connector as it will communicate directly with the cloud. However, if there is a need to have local clients communicate directly to the service connector rather than through the cloud, the following ports and protocols should be allowed inbound to the Service Connector.
  - WireGuard Encryption Protocol: 51820, 51821 (UDP)
  - IPsec Encryption Protocol: 500, 4500 (UDP)

Minimum hardware requirements:

vCPU: 4

RAM: 16 GB



Onboarding | Wired Guidelines

Extreme Platform ONE Security supports SwitchEngine and FabricEngine. It can also be configured to work with third-party devices via manual configuration. Extreme Platform ONE Security supports the minimum versions of the following products:

- Switch Engine 33.4
- Fabric Engine 9.3

There are three management options:

- Managed Mode
- Locally Managed Mode on page 29
- Third-party Mode on page 29

Managed Mode

Supported NOS: Switch Engine and Fabric Engine switches are onboarded directly using **Manage your Devices**.

Extreme Platform ONE Networking and ExtremeCloud IQ (Classic) manage switch configuration. Use Configure a Switch for Instant Secure Port in ExtremeCloud IQ (Classic) on page 32 to provision the following components on the switch:

- Certificate for RadSec communication
- RADIUS/RadSec configuration to the cloud RadSec server or locally deployed RadSec proxy
- 802.1X or MAC authentication

For Switching Engine, Extreme Platform ONE Security updates the policy configuration on the switch, including static policy roles and rules, based on the provisioned network policy.

For Fabric Engine, Extreme Platform ONE Security sends Dynamical ACLs to the switch upon authentication to provision the client access policies.

Locally Managed Mode

Supported NOS: Switch Engine and Fabric Engine. Switches are onboarded using **Manage your Devices Locally**.

ExtremeCloud IQ does not configure switches in local managed mode. In local managed mode, based on the provisioned network policy, Extreme Platform ONE Security provisions policy on the switch using dynamic ACLs (dACL) conveyed using RADIUS vendor-specific attributes (VSAs) during the authentication process.

Users configure the following components manually:

- Certificate for RadSec communication
- RADIUS/RadSec configuration to the cloud RadSec server
- 802.1X or MAC authentication, along with supporting feature sets, depending on the deployment model

Third-party Mode

Extreme Platform ONE Security provisions policy on the switch using dynamic ACLs (dACL) conveyed using RADIUS vendor-specific attributes (VSAs) during the authentication process. Third-party or non-ExtremeCloud IQ devices are onboarded through **Network**.

Users configure the following components manually:

- Certificate for RadSec communication
- RADIUS/RadSec configuration to the cloud RadSec server
- 802.1X or MAC authentication, along with supporting feature sets, depending on the deployment model
- Cloned and modified Extreme, Cisco, HP, and Aruba templates or newly created vendor-specific RADIUS templates. For more information, Manage RADIUS Templates on page 52.
- SSIDs for wireless devices. For more information see Manage SSIDs on page 51.
- Network devices. For more information, see Add a Network Device on page 49.

Configuration Details for Fabric Engine and Switch Engine

- To configure Fabric Engine, select Fabric Engine Locally Managed Sample Configuration on page 183.
- To configure Switch Engine, select Switch Engine Locally Managed Sample Configuration on page 187.

Fabric Engine and Switch Engine Reference Guides

- Switch Engine OnePolicy
- Switch Engine Netlogin
- Fabric Engine Auto-sense/Zero-Touch Capabilities
- Fabric Engine - EAP (Extensible Authentication Protocol over LAN)

Instant Secure Port Profiles

Instant Secure Port Profiles (ISPP) in Extreme Platform ONE Security enables you to configure user authentication and MAC authentication per port and to specify a RADIUS server to use in conjunction with Extreme Platform ONE Security.

Only one Instant Secure Port Profile can be configured per switch, with the ability to enable and disable user authentication and MAC authentication per port.

Specify a RADIUS server configured in the Extreme Platform ONE Security/Raas application. Only those Regional Data Centers (RDCs) that support this configuration and users that have a license are able to use ISPP.

An instant secure port profile is created separately from any existing instant port profiles.

Creating a New Instant Secure Port Profile

Note
The Instant Secure Port Profile (ISPP) option will only become available when Extreme Platform ONE Security is activated.

You must create a network policy.

Use the **Configuration** > **Network** page to see all the devices that have been onboarded to Extreme Platform ONE Security. Add the network policy to the desired .

The type must have the **Switching** box checked. Other options like **Wireless** can be checked as needed. The **Policy Name** is a required attribute.

Instant Secure Port Profiles (ISPPs) are created within the Switch Settings subsection of the Network Policy creation and editing page.

To create a new Instant Secure Port Profile:

1. Select +.
2. Enter the name for your ISPP. The name is unique within Extreme Platform ONE Security but is not pushed to the device.
3. Choose whether to use Unauthenticated VLAN. Unauthenticated VLAN is either a common object or can be created when the profile is created. If the Enable Unauthenticated VLAN is selected, then this VLAN will override the untagged VLAN in the port type and will be used as the Unauthenticated VLAN on the device when the configuration is pushed.
4. Specify the order in which to execute authentication. The order is per profile; therefore the same order is used for the entire device once the configuration is pushed. Use the arrows to change the default order.

5. Pick the RADIUS server for the Instant Secure Profile. Selecting **Use Extreme Platform ONE Security RADIUS Cloud configuration** uses either the free cloud RADIUS server set up per RDC, or configured proxy RADIUS servers in the Extreme Platform ONE Security application. Select one of the radio buttons to decide which type to use. Further, in the case of proxy RADIUS, you can select up to two proxy RADIUS servers; it is assumed that the ones selected have reached a deployed state after being configured in Extreme Platform ONE Security.
6. Select **Save**.

ISPP Configuration from Switch Template

To configure and select an existing Instant Secure Port Profile from within a switch template:

1. Go to **Configuration** > **Network** select **Create or Edit a Policy** > **Switching** > **Switch Templates** page.
2. Either edit an existing template, or create a new switch template for a specific device model such as a 5420M-48T-4YE.
3. Select **Port/VLAN Configuration**.
4. If you are creating a new template, supply a template name.
5. Select the Instant Secure Profile from the **Instant Port Profile** list.

Enable Instant Secure Port Profile on a Port

Create the Instant Secure Port Profile (ISPP) switch template, see ISPP Configuration from Switch Template on page 31.

Use this task to enable ISPP on a port.

1. Go to **Configure** > **Network Policies** page.
2. Edit an existing template, or create a new switch template.
3. From the left pane, select **Port/VLAN Configuration**.
4. Enable or disable the Instant Secure Port Profile for any specific ports:
   a. Select the profile to use in the **Port Profile** drop-down list.
   b. Enable or disable the profile on a port by using the **Instant Profile** toggle switches in the **Configure Ports Individually** section.

   Note
   The switch can only have Instant Port or Instant Secure Port enabled, but not both.

5. Enable User Auth or MAC Auth or both.
6. Specify the Port Type, such as Access, Trunk, or Phone:
   a. Create or edit your selected **Port Type**.
   b. Select the Port Usage within the **Port Name & Usage** tab.
7. After all the ports are configured, select **SAVE**.

Configure a Switch for Instant Secure Port in ExtremeCloud IQ (Classic)

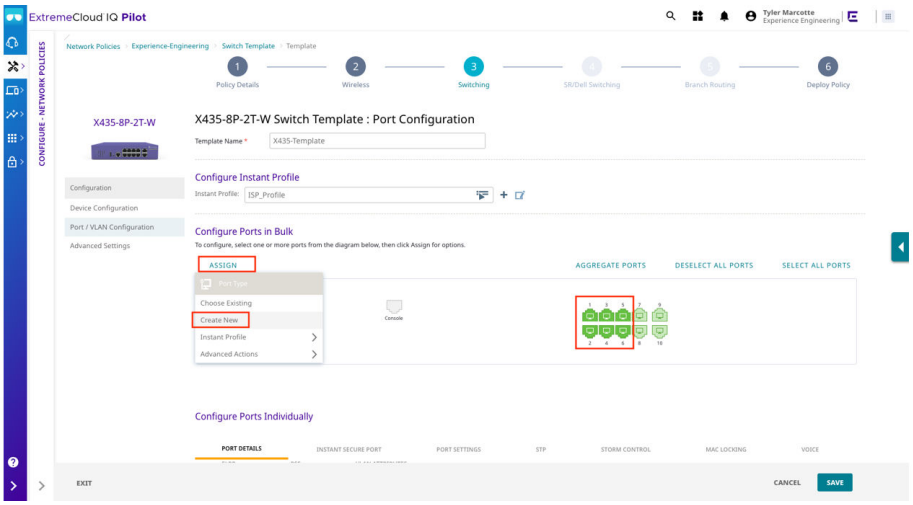
Use this task to configure a switch for Instant Secure Port in .

1. Go to **Configure** > **Network Policies**.
2. On an existing network policy, select to edit.
3. Select the Switching section of the configuration. Go to **Switch Settings** > **Instant Secure Port Profiles**.
4. Select to create a new profile and configure the settings.
   a. In the **Create Instant Secure Port Profile** dialog, enter a name.
   b. To assign a VLAN on an authentication failure, an unreachable server, or other non-authenticated conditions, select the **Enable Unauthenticated VLAN** check box and select or create an **Unauthenticated VLAN**. Otherwise, any unauthenticated session will be rejected.
   c. Leave the option for **Use Extreme Platform ONE Security RADIUS Cloud configuration** enabled. This ensures the switch automatically installs the RadSec certificates and authentication configuration.
   d. Select **SAVE**.
5. Select **Switch Templates** and add or edit a switch template for the relevant device types.

   Note
   Instant Secure Port only works on Universal switches running Switch Engine and the X435 switch models.

6. Select **Port / VLAN Configuration**. Under **Configure Instant Profile**, select the previously created profile.
7. Click and drag a box around multiple ports or select an individual port to enable. Select **Create New** from the **Assign** > **Port Type** drop-down menu.

   Note
   Default port types cannot be edited.

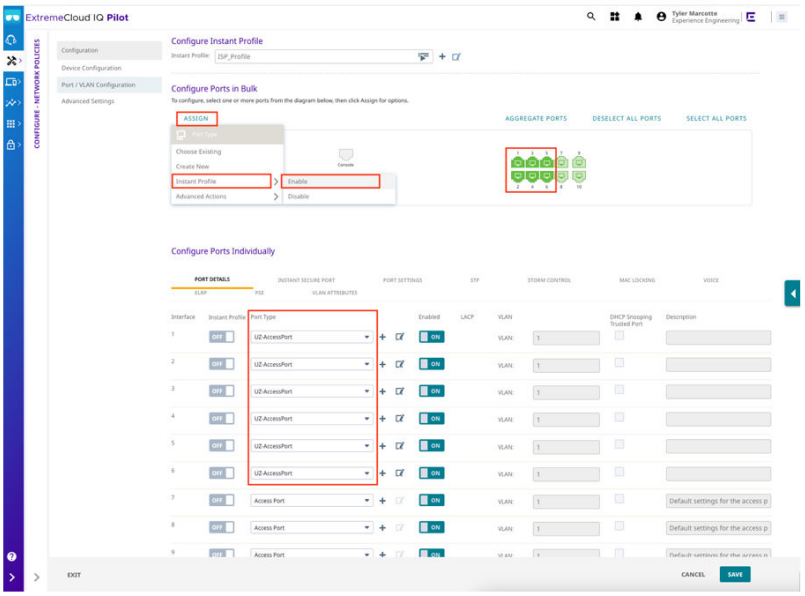


The system displays the **Create Port Type** dialog.

8. Configure the port type settings.
   a. Enter a name for the new port type.
   b. Select **NEXT** until the Instant Secure Port Settings section is selected.

      Note
      The VLAN doesn't require configuration in . It is assigned in Extreme Platform ONE Security.

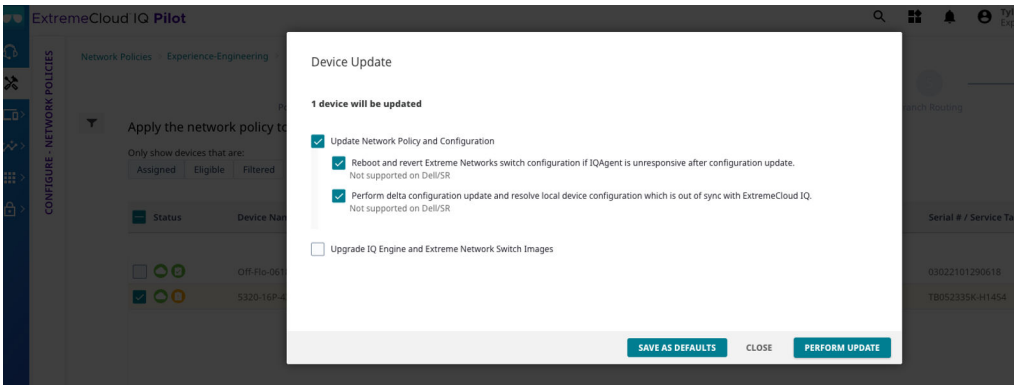
   c. On the **Instant Secure Port Settings** tab, enable the desired authentication types on the switch port.
   d. Continue selecting **NEXT** until the system displays the Summary screen.
   e. Select **SAVE**.
9. Select the ports again from the switch picture, and select **Assign** > **Instant Profile** > **Enable**. Alternatively, enable the slider for each port that Instant Profiles should be enabled.



Note
The port types are now assigned to the ports; however Instant Profiles are not enabled for those ports.

10. With the Instant Secure Port enabled, select **SAVE**.
11. Select the **Deploy Policy** workflow menu.

12. Update the relevant devices.



Onboarding | Wireless Guidelines

This chapter describes how Extreme Platform ONE Security can be used for mapping policies based on Extreme Platform ONE Security conditions and returning a filter ID that matches an automatically provisioned policy using Wireless.

Integrate Wireless with Extreme Platform ONE Security

Use this task to integrate ExtremeCloud IQ Wireless with Extreme Platform ONE Security.

1. From the ExtremeCloud IQ portal main navigation, select **Configure** > **Common Objects** > **Policy** > **SSIDs**.
2. Select your SSID and select the edit (pencil) icon.
3. Under **SSID Usage**, ensure the **SSID Authentication** and **Enterprise** tabs are selected.
4. Select the type first from SSID Authentication.
5. In the **MAC Authentication** tab, enable **MAC Authentication**.
6. Enable **Authentication with Extreme Platform ONE Security**.

Note
Authentication with Extreme Platform ONE Security cannot be used on the same SSID as PPSK or ExtremeGuest Essentials.

Configure the Network Policy in ExtremeCloud IQ

Use this task to configure the network policy in ExtremeCloud IQ.

1. From ExtremeCloud IQ, go to **Configure** > **Network Policies** and select **Add Network Policy**.
2. Select **Wireless**.
3. Enter a name for the policy and optional description.
4. Select **Save**.
5. Select **Next**.

Go to Configure SSID and Wireless in ExtremeCloud IQ on page 36.

Configure SSID and Wireless in ExtremeCloud IQ

Service Set Identifier (SSID) configuration in ExtremeCloud IQ depends on the type of authentication (802.1X or MAC) and the type of RadSec deployed.

Extreme Platform ONE Security RadSec is supported in all SSID types except for Private Pre-Shared Key SSIDs.

Use this task to configure SSID and wireless in ExtremeCloud IQ.

1. Go to **Configure** > **Common Objects** > **Policies** > **SSIDs**.
2. Select + to create a new SSID.
3. Enter a username and broadcast name.
4. Under **SSID Usage**, ensure the **SSID Authentication** and **Enterprise** tabs are selected.
5. (Optional) To enable MAC authentication toggle to **ON**.
6. Under **Authentication Settings**, enable **Authentication with Extreme Platform ONE Security**.

Manage SSID in Extreme Platform ONE Security

Extreme Platform ONE Security automatically creates and deletes common objects in ExtremeCloud IQ and associates them with managed SSIDs to integrate with the ExtremeCloud IQ wireless solution.

Use this task to enable SSID management for Extreme Platform ONE Security.

1. Log in to Extreme Platform ONE Security.
2. Select **Configuration** > **Network** > **SSID**.
3. Select  .
4. Select **Managed SSID** > **Managed** > **Confirm**.

Extreme Platform ONE Security Common Object Management

Common objects created by Extreme Platform ONE Security are named with a UZTNA_ prefix. The administrator must not use these objects to modify or associate them

with other common objects. Extreme Platform ONE Security automatically deletes or modifies their configuration when changes are made through the Extreme Platform ONE Security portal.

ExtremeCloud IQ User Profiles

Extreme Platform ONE Security creates a user profile for each hybrid or network policy created in Extreme Platform ONE Security. User profiles are visible to the administrator in ExtremeCloud IQ. Go to **Configure** > **Common Objects** > **Policy** > **User Profiles**.

ExtremeCloud IQ VLAN Profiles

Extreme Platform ONE Security creates a VLAN Profile for each VLAN ID selected for use in a hybrid or network policy created in Extreme Platform ONE Security.

Extreme Platform ONE Security automatically associates the VLAN Profile to the corresponding user profile.

ExtremeCloud IQ IP Firewall Policies

When you configure a network service group for a Extreme Platform ONE Security policy, Extreme Platform ONE Security creates an IP firewall policy.

The IP Firewall Rules uses other common objects such as IP address and network services which are also created by Extreme Platform ONE Security when network service groups are configured for a policy.

The IP Firewall Policy is automatically associated to the outbound traffic policy for the corresponding user profile in ExtremeCloud IQ.

ExtremeCloud IQ User Profile Assignment Rules

Extreme Platform ONE Security creates user profile assignment rules for each hybrid or network policy created in Extreme Platform ONE Security and automatically attaches them to managed SSIDs in Extreme Platform ONE Security.

The user profile assignment rules map user profiles to the corresponding Filter-ID RADIUS Attribute to ensure that users are assigned the appropriate policy when authenticating to an SSID.

The administrator can control which user profile assignment rules are attached to an SSID by configuring an SSID location condition in the hybrid or network policy in Extreme Platform ONE Security.

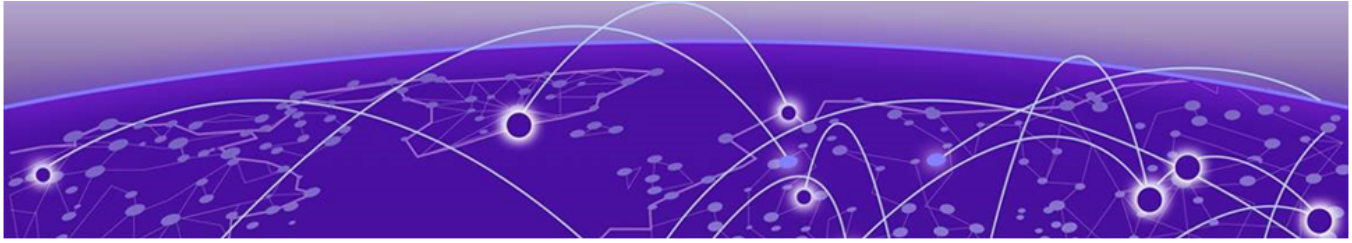
ExtremeCloud IQ Deployment

Extreme Platform ONE Security automatically deploys configuration updates to ExtremeCloud IQ Access Points which are assigned a network policy in ExtremeCloud IQ that contains SSIDs managed by Extreme Platform ONE Security.

Changes to hybrid, network policies or managed SSIDs in Extreme Platform ONE Security triggers an automatic configuration deployment.

Note
Extreme Platform ONE Security will deploy automatically to ExtremeCloud IQ if there is no staged configuration from ExtremeCloud IQ.

If there is staged configuration, you can manually trigger this deployment by (Re)-Syncing the configuration. Go to **Resources** > **Network Resources** > **Network Devices**.



Monitoring | Dashboard

Go to **Monitoring** > **Dashboard** for a summary of network security with a focus on health status, license status, applications, networks, and policies.

Monitoring | Alerts

The **Alerts** view provides a comprehensive overview of network alerts, allowing operators to detect, record, and report specific events. It evaluates performance metrics and reports occurrences where specific criteria are met. Alerts can be filtered by time range, severity, status, site, and source.

Users can receive alert notifications through email or Webhooks.

Select **Alert Policies** to view and manage global and site policies, see Administration & Settings | Alert Policies on page 174.

Note
Site policies take precedence over global policies.

In the **Alerts** section, enable **Show Summary** to display the following widgets:

- Severity
- Category
- Top 3 Alerts
- Application

Alert Details

By default, the **Alerts** page displays information about alerts raised at all sites for the last 24 hours.

The Alerts table displays the following information:

- Alert Name
- Summary
- Severity
- Status
- Application
- Location
- Categories
- Source
- Detected
- Comment

You can filter the **Alert Details** list using the following methods:

- Use the **Time Range** controls to specify a time range, within the last 30 days, for which you want to view alerts.
- Use the **Severity** filter to view alerts based on specific severity:
  - Critical - Red
  - Major, Minor, and Warning - No color combination

  - Info - Blue
- Use the **Status** drop-down list to view **All** (default), **Acknowledged**, or **New** alerts.
- Use the **Sites** filter to view alerts associated with a specific site.
- Use the interactive device host name in the **Source** column for more information about the alert.
- Use the **Refresh Alerts** button to view the most recent alerts.
- Use the **Export to CSV** button to download the alert data in `.csv` format.

Note
The column filter settings do not persist.

Monitoring | Clients

The filter options are Identity, Auth State, ZTNA Agent, Policy, Device Type, Last Seen, MAC Address, OS Name, Host Name, NAS Port ID, Network Device Name, Compliance Status, NAS IP, NAS Port, SSID, IS Name, and Auth Type.

From the **Monitoring** > **Clients** > **3-dot Menu** (⋮), you can perform a number of actions on a client. The available actions depend on the device type selected.

- **View History**: The screen displays the client identity and MAC Address. Select a timeframe from the drop-down list.
- **Add to Device Group**: Select a device group from the drop-down list and select **Add**.
- **Add to User Group**: Select a user group from the drop-down list and select **Add**.
- **Re-authenticate**: To confirm client re-authentication, select **Re-authenticate**.
- **Restore Access**: To confirm restoration, select **Restore Access**.
- **Revoke Access**: To confirm revocation, select **Revoke Access**.
- **Delete**: To confirm, select **Delete.**
- **Network Policy Evaluation**: To evaluate a combination of input fields for an authentication request, see Evaluate Network Policy on page 43.

Monitoring | Troubleshooting

Within the **Policy Evaluation & Troubleshooting** section to troubleshoot the Extreme Platform ONE Security configuration or operational state.

- Network Policy Evaluation - This process will evaluate a combination of input fields for an authentication request. Based on the Hybrid and Network policy configuration a test of authentication success or failure and expected policy assignment will be displayed.
- Application Policy Evaluation - This process will evaluate whether a specific user should have access to an application. If they should have access but are experiencing issues, a troubleshooting workflow can be started to gather logs and troubleshooting data to share with Extreme Networks Support.

Evaluate Network Policy

Use this task to evaluate the network policy.

1. Go to **Monitoring** > **Troubleshooting**.

   The **Network Policy Evaluation** tab displays.
2. Configure the settings in Table 6.

Table 6: Settings for Network Policy Evaluation

Field	Description
MAC Address	Enter the MAC address.
Authentication Type	Select an authentication type from the drop-down list.
Optional options	You can update optional fields: • Username • Password • Service Set Identifier (SSID) • AP/Switch IP • Switch Port • Date & Time

3. Select **Evaluate**.

   If Authentication Type was set to EAP-TTLS an email and password can entered to test validity. If EAP-TLS was selected, an option to upload a client certificate is available to validate the certificate chain of trust.

Evaluate Application Policy

Use this task to evaluate application policy.

1. Go to **Monitoring** > **Troubleshooting** and select the **Application Policy Evaluation** tab.
2. Configure the settings in Table 7.

Table 7: Settings for Application Policy Evaluation

Field	Description
User	Select a user from the drop-down list.
Application	Select an application from the drop-down list.
Access Mode	Select the **Agentless** or **Agent-Based** option.
Location-Based Condition	Select a geographic location from the drop-down list.
Device (Optional)	If testing agent-based, a device must be selected. If agentless is being tested, no device is required. **Note:** Extreme Platform ONE Agent must be connected and online before the evaluation.
Time-Based Condition	Select a time zone from the drop-down list. You can also select a start time and end time.

3. Select **Evaluate**.

The **Evaluation Results** and **Application Troubleshooting** sections display. To enable troubleshooting, select **Troubleshoot**.

To end the process before all items have been analyzed, select **End Troubleshooting**.

To export evaluation results, select **Export Results**.

Manage Packet Capture

Enabling a packet capture is used when troubleshooting issues on the network. It collects captures from points in the network authentication flow defined in the options. These captures are made available for download upon stopping the capture.

Use this task to enable or delete packet capture.

1. Go to **Monitoring** > **Troubleshooting** and select **Packet Capture**.
2. Configure the settings in Table 8.

Note
If incorrect data is populated in the form, to clear the form, select **Clear**.

Table 8: Packet Capture Configuration Settings

Field	Description
MAC Address	Select **Any MAC Address** or enter a client MAC Address in the **Client MAC Address** field. **Note:** To capture all server-side traffic, select **Any Mac Address** and leave the Network Locations field empty.
Network Locations (Optional)	Select a network location from the drop-down list.
Time Duration	enter the capture duration time between 5 and 30 minutes.

3. Select **Start**.
4. After packet capture is started, select **Stop** to stop capturing.

Warning

If packet capture is stopped before 5 minutes, no data is captured but when stopped after ample time, a new **Packet Capture Results** section appears.

5. To download completed Packet Capture, select **Download**.
6. To delete an existing packet capture download for switches, access points, or sites, select the delete button and in the **Delete Downloaded Data** window, select **Delete**.

Configuration | Sites

From the **Sites** window provides options to import a site tree, add a site, or add a site group.

Import a Site Tree

Use this task to import a site tree to your network plan.

Note
This feature is available only if the site tree is empty.

1. Go to **Configuration** > **Sites** and select **Import Site Tree**.
2. Select **Browse Files** or drag and drop the the site tree file.

   The files must be in .xml format.
3. Select **Import**.

Add a Site group

Use this task to add a new site group folder to your network plan.

1. Go to **Configuration** > **Sites** and select **Add Site Group**.

   Alternatively, select for the corresponding parent group, and then choose **Add Site Group**.
2. Type a **Name** for the new site group.
3. (Optional) Add the **Description** text.
4. To add the new site group to an existing group, select an existing parent site group from the **Association** list.
5. Select **Save**.

Add a Site

Use this task to add a new site to your network plan.

1. Go to **Configuration** > **Sites** and select **Add Site**.

   Alternatively, to add a site to an existing site group, select and choose **Add Site**.

2. Type a **Name** for the new site.
3. Select the **Country**.
4. To add the new site group to an existing group, select an existing parent site group from the **Association** list.
5. (Optional) Enter the address manually, use GPS coordinates, or select the location on the map.
6. Select **Save**.

Configuration | Network

From the **Network** window provides options to add or import a network device, enable global timeout, manage and configure SSIDs, or manage RADIUS Templates.

The Network Devices table displays the following information:

- IP Address
- Device Type
- Alias
- RadSec Status
- Connection Status
- Policy Status
- Site
- RADIUS Template

Select the 3-dot menu to import devices, resync all devices, or enable global timeout.

Within the Network Device table, you can select  to perform actions depending on how the device was added to Extreme Platform ONE Security.

- Download Certificate Bundle
- Sync Device
- Update
- Remove

The actions include:

- The SSIDs section contains a list of all SSIDs known to Extreme Platform ONE Security. SSID are automatically added from or can be manually added.
- When enabling an SSID to be managed, policies will be pushed to all Access Points that are broadcasting that SSID based on the location conditions defined.

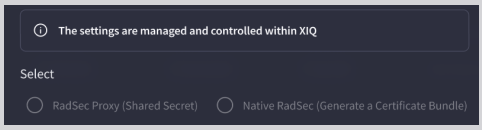
- When enabling BYOD on an SSID, an option appears in the Extreme Platform ONE Security Agent to automatically provision the wireless network profile for a client device.
- The RADIUS Template section contains a list of RADIUS templates. You can add, clone, export, or import Radius templates.

Add a Network Device

Use this task to add a network device to your resources.

1. Go to **Configuration** > **Network** and click **Add Network Device**.
2. Configure the settings in Table 9.

Table 9: Network Device Configuration Settings

Field	Description
IP Address	Enter an IP address for your network device in the text field.
Alias (Optional)	Enter a network device alias.
RADIUS Template	Search for and select an existing RADIUS template from the drop-down menu.
Select	• RadSec Proxy (Shared Secret) - If you select **RadSec Proxy (Shared Secret)**, enter the Shared Secret into the associated text field. • Native RadSec (Generate a Certificate bundle) - If you select **Native RadSec (Generate a Certificate bundle)**, the **Create a certificate bundle** check box appears pre-selected. 
Type	Select **Wired** or **Wireless** from the network device Type drop-down list.
Sites	Search and select an existing site from the Sites drop-down menu.
Session Timeout for Device (Optional)	If 'Use Global Timeout' is selected, this option is disabled. If an individual session timeout for the device is required, disable 'Use Global Timeout'.
Use Global Timeout	To set an individual session time out for this device, de-select this option and set the desired session timeout in the above field.

3. Click **Save**.
4. To edit an existing network device, select ⋮ for the device, and select **Edit**. Make changes and select **Save**.
5. To delete a network device, select ⋮ for the device, and select **Delete**.

Import a Network Device

Use this task to import a list of network devices.

1. Go to **Configuration** > **Network**.
2. Select , and select **Import Devices** and configure the settings in Table 10.

Table 10: Configuration Settings for Importing Network Devices

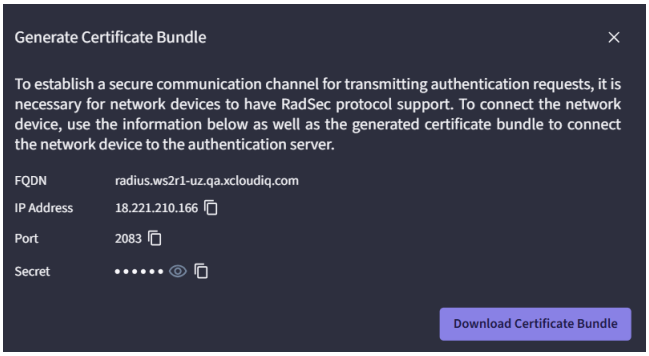
Field	Description
RADIUS Template	Select a RADIUS template from the drop-down list.
Shared Secret (Optional)	For RadSec Proxy, provide a Shared Secret in the field. For Native RadSec, download the certificate from the device menu by navigating to network devices.
Sites	Select a site from the drop-down list that is associated with the imported devices.
Template Upload	Download the csv template and fill in your network device information. Drag and drop or browse to your csv file.

3. Select **Import**.

Generate Certificate Bundle

Use this task to generate a certificate bundle for a network device.

1. Go to **Configuration** > **Network**.
2. Select , and select **Generate Certificate Bundle**.
3. Select **Generate Certificate Bundle**.



Enable Global Timeout

Use this task to enable global timeout for network devices. Modifying the Global Timeout will apply to all network resources using Global Timeout.

1. Go to **Configuration** > **Network**.

2. Select , and select **Global Timeout** and configure the settings in Table 11.

Table 11: Global Timeout Configuration Settings

Field	Description
Seconds	Enter the number of seconds for global timeout. **Note:** Recommended session timeout is 3600 seconds.
Override all custom/individually set timeout to default session timeout of 3600 seconds	Select this check box to apply to all.

3. Select **Save**.

Manage SSIDs

Use this task to add, manage, or remove an SSID.

1. Go to **Configuration** > **Network**.
2. Select the **SSID** tab.
3. Select **Add SSID** and configure the settings in Table 12.

Table 12: SSID Configuration Settings

Field	Description
Name	Enter at least three alphanumeric characters.
Broadcast Name	Enter a broadcast name.

4. Select **Save**.

   The system displays existing SSIDs.

5. To manage preferences for an existing SSID, select within the table and select **Manage SSID**.
   a. To allow Extreme Platform ONE Security to configure the SSID for authentication and authorization, select **Managed**. This will apply to all devices utilizing this SSID.

      Note
      An SSID does not appear as an available location condition unless it is Managed.

   b. To enable an option in the Extreme Platform ONE Security Agent to configure the client device to connect to the selected SSID, also select **BYOD**.

      Extreme Platform ONE Security Agent's BYOD can automatically configure the Wi-Fi profile and install certificates, to assist end-user onboarding. Once BYOD is enabled, the SSIDs appear for end users on Extreme Platform ONE user agents. This allows users to configure the agents following the screen instructions.

6. To delete an existing SSID, select within the table and select **Delete**.

Configure SSID and Wireless in ExtremeCloud IQ

Service Set Identifier (SSID) configuration in ExtremeCloud IQ depends on the type of authentication (802.1X or MAC) and the type of RadSec deployed.

Extreme Platform ONE Security RadSec is supported in all SSID types except for Private Pre-Shared Key SSIDs.

Use this task to configure SSID and wireless in ExtremeCloud IQ.

1. Go to **Configure** > **Common Objects** > **Policies** > **SSIDs**.
2. Select + to create a new SSID.
3. Enter a username and broadcast name.
4. Under **SSID Usage**, ensure the **SSID Authentication** and **Enterprise** tabs are selected.
5. (Optional) To enable MAC authentication toggle to **ON**.
6. Under **Authentication Settings**, enable **Authentication with Extreme Platform ONE Security**.

Manage RADIUS Templates

Note
It is recommended that a RADIUS Template be created by cloning (step 3) an existing template and adjusting the necessary values. However, if a new template is desired it can be added using steps 4-5.

Use this task to add or clone a RADIUS template. To import an existing template, see Import a RADIUS Template on page 53.

1. Go to **Configuration** > **Network**.
2. Select the **RADIUS Template** tab.
3. To clone an existing RADIUS template, within the column associated with the template to clone, select ⋮ and select **Clone**.
   a. Enter a **Name** and **Description** for the cloned template.
   b. Select RADIUS VSA's from the drop-down list.
   c. Variables in the drop-down list correspond to the elements of a network policy. Select the matching variables to assign to the RADIUS VSA.
   d. Select **Clone**.
4. To export an existing RADIUS template, within the column associated with the template to clone, select ⋮ and select **Export**.

5. To add a new template, select **Add RADIUS Template** and configure the settings in Table 13.

Table 13: RADIUS Template Configuration Settings

Field	Description
Name	Enter at least three alphanumeric characters.
Description	Enter a description.
RADIUS VSA'S	Select RADIUS VSA's from the drop-down list.
Variables	Variables in the drop-down list correspond to the elements of a network policy. Select the matching variables to assign to the RADIUS VSA.
Additional VSA Mappings (Optional)	The selected combination of VSA's and Variables will be displayed here.
Use Message_Authenticator (BlastRADIUS mitigation)	Enable toggle to use message_authenticator.

6. Select **Save**.

Import a RADIUS Template

Use this task to import a RADIUS template.

Note
Export an existing RADIUS Template to retrieve the proper format. To export an existing RADIUS template, within the column associated with the template to clone, select  and select **Export**.

1. Go to **Configuration** > **Network** and select the **RADIUS Template** tab.
2. Select **Import**.
3. Drag and drop your template or select **Browse Files**.
4. Once you have chosen or added a file, select **Import**.

Policy | Security Policies

Policies contain distinct conditions that provide different levels of authorization to your infrastructure.

You can search for or create the following three types of policies:

- Hybrid policies allow you to manage your applications and network access.
- Application policies allow you to manage only your applications.
- Network policies allow you to manage only your network.

Note
To update the order of existing network policies, select and drag the policy into the desired order.

Create Hybrid Policy

Use this task to create a hybrid policy.

1. Go to **Policy** > **Security Policies**.
2. Select **Add Policy** and select **Add Hybrid Policy** from the drop-down list and configure the settings in Table 14.

Table 14: Hybrid Policy Settings

Field	Description
Enable This Policy	Toggle to enable this policy. **Note:** This does not restrict the ability to reorder and prioritize policies.
Policy Name	Enter at least 3 alphanumeric characters.
Description (Optional)	Enter a description.

Table 14: Hybrid Policy Settings (continued)

Field	Description
Conditions **Note:** All conditions are mutually exclusive.	Select desired conditions: • Any User (Default) - If the default is not selected, search and select from the User Group(s) drop-down menu or create a new user group. • Any Device (Default) - If the default is not selected, search and select from the Device Group(s) drop-down menu or create a new device group. • Any Location (Default) - If the default is not selected, you can search, select, and edit from the optional Location-based Condition drop-down menu or create a new condition. • Any Time (Default) - If the default is not selected, search, select,and edit from the optional Time-based Condition drop-down menu or create a new condition. • Any Authentication Type (Default) - If the default is not select and edit from the optional Authentication-based Condition drop-down menu or create a new condition.
Applications Access	Select one from the **Application Group** drop-down menu or create one, for details, see Create Application Groups on page 79.
Access Mode	Select Agent-based or Agentless to determine whether the applications defined in the application group should be available via the agent, the agentless web portal, or both.
Network Access	Select the default access for the network. By default, all network access is dropped except for agent-based traffic.
Select Existing VLAN	You can use your own VLAN or a VLAN defined in ExtremeCloud IQ . • To use your own VLAN, ensure **Select VLAN from ExtremeCloud IQ** is deactivated (default) and enter a **VLAN ID**. • To use a VLAN from ExtremeCloud IQ, activate **Select VLAN from ExtremeCloud IQ** and select a VLAN from the list.

Table 14: Hybrid Policy Settings (continued)

Field	Description
VLAN ID (Optional)	Select a VLAN from the drop-down menu. **Note:** To add additional tagged VLANs, the first ID is always the untagged VLAN and should match the VLAN being assigned by the policy. In the **Advanced Settings** (below), you can use the FA-VLAN-ISID attribute to tag any extra VLANs. Even though the switch is not doing fabric attach, the attribute will allow for additional tagged VLANs. The format is: FA-VLAN-ISID=1:1,1101:1101,1102:1102,1201:1201,1202:1202 In the above example, 1 is the first VLAN and is untagged and VLANs 1101,1102,1201,1202 are all tagged.
ISID (Optional)	Fabric Service Identifier (ISID).
Network Service Group (Optional)	Select **Network Service Group** and continue as follows: a. Select **Add Network Service Group**. b. Select **Allowed** or **Denied**. c. The following actions are available from the 3-dot menu: • **Reorder Network Service Group** - The Network Service groups, and their associated actions are ordered. To re-arrange the order, drag the network service group up or down. • **Delete** - To delete an existing network service group.
Advanced Settings (Optional)	• RADIUS VSA's - Select from the drop-down menu. • Variables - Select from the drop-down menu. • AP Aware - Ability to determine AP attachment to port to prevent auth for wireless clients when Auth for wireless clients is handled via AP.

3. Select **Save**.
4. To edit or delete and existing Hybrid policy, select  and select **Edit** or **Delete** from the drop-down list.

Create Application Policy

Use this task to create an application policy.

1. Go to **Policies** > **Security Policies**.
2. On the **Application Policies** tab, select **Add Application Policy**.

3. Configure the settings in Table 15.

Table 15: Application Policy Settings

Field		Description
Enable This Policy	Toggle to enable this policy. **Note:** This does not restrict the ability to reorder and prioritize policies.	
Policy Name		Enter at least 3 alphanumeric characters.
Description (Optional)		Enter a description.

Table 15: Application Policy Settings (continued)

Field		Description
Conditions	User Groups	Select **Any User Group** checkbox or select a user group from the drop-down list.
	Location Based Condition (Optional)	Select **Any Location** checkbox or select a location condition from the drop-down menu.
	Time Based Condition (Optional)	Select **Any Time** checkbox or select a time condition from the drop-down menu.
Application Access		Select one or more Application Groups from the drop-down list. **Note:** A maximum of 50 Application Groups can be selected per policy. If the selected number exceeds 7 Application Groups expand to view the menu. Select the Agent-based or Agentless checkbox to determine whether the applications defined in the application group should be available via the agent, the agentless web portal, or both. **Note:** When application policies with Agent based only or Agent-based and Agentless enabled are created, deleted, or modified the user associated with that policy will have a notification sent on the agent.

4. Select **Save**.

5. To edit, delete, enable,or disable an existing Application policy, select ⋮ and select **Edit**, **Disable**, **Enable**, and **Delete** from the drop-down list.

Note
Disabling a future policy has no affect on the agent. When an active policy is disabled, the Agent displays a message to enable the policy to access services.

Create Network Policies

Use this task to create a network policy.

1. Go to **Policy** > **Policies** and in the Network Policies tab, select **Add Policy** > **Network**.
2. Configure the following network policy settings in Table 16.

Table 16: Network Policy Settings

Field	Description
Enable This Policy	Toggle To enable this policy. **Note:** This does not restrict the ability to reorder and prioritize policies.
Policy Name	Enter at least three alphanumeric characters for the name of the new network policy.
Description (Optional)	Enter a policy description.
Conditions **Note:** All conditions are mutually exclusive.	Select desired conditions: • Any User (Default) - If the default is not selected, search and select from the User Group(s) drop-down menu or create a new user group. • Any Device (Default) - If the default is not selected, search and select from the Device Group(s) drop-down menu or create a new device group. • Any Location (Default) - If the default is not selected, you can search, select, and edit from the optional Location-based Condition drop-down menu or create a new condition. • Any Time (Default) - If the default is not selected, search, select,and edit from the optional Time-based Condition drop-down menu or create a new condition. • Any Authentication Type (Default) - If the default is not select and edit from the optional Authentication-based Condition drop-down menu or create a new condition.

Table 16: Network Policy Settings (continued)

Field	Description
Network Access	• Default Access - Select the default access for the network. By default, all network access is dropped. **Note: Deny** blocks IPv6 traffic. • AP Aware - Enable this option to only authenticate the first MAC address connecting to the port of an Extreme Networks switch. The primary use case for this is an access point. All other MAC addresses will be authenticated by the access point. • Enter a VLAN ID or enable the toggle to select an existing VLAN ID from ExtremeCloud IQ. Enter a Fabric Service Identifier if one is needed. **Note:** To add additional tagged VLANs, the first ID is always the untagged VLAN and should match the VLAN being assigned by the policy. In the **Advanced Settings** (below), you can use the FA-VLAN-ISID attribute to tag any extra VLANs. Even though the switch is not doing fabric attach, the attribute will allow for additional tagged VLANs. The format is: FA-VLAN-ISID=1:1,1101:1101,1102:1102,1201:1201,1202:1202 In the above example, 1 is the first VLAN and is untagged and VLANs 1101,1102,1201,1202 are all tagged. • Network Service Group (Optional): ◦ Select **Add Network Service Group**. **Note:** Drag Network Service Groups in the order to respond within the RADIUS response. ◦ Select **Allow** or **Deny**. ◦ The following actions are available from the 3-dot menu: ▪ **Reorder Network Service Group** - To change the order of the network service groups within the list. ▪ **Delete** - To delete an existing network service group. **Note:** In the Network Group table, select **Revert Policy Order** to reorder the columns.
Advanced Settings (Optional)	• RADIUS VSA's - Select from the drop-down menu. • Variables - Select from the drop-down menu. • Additional VSA Mappings - Add additional mappings within the text box.

3. Select **Save**.

Your network policy displays in the list showing the **Network Access** status as **Active**.

To edit or delete an existing Network policy, select  and select **Edit** or **Delete** from the drop-down list.

Configure Device Posture

Device Posture checks the security data of connected devices and reduces the devices' cybersecurity risks by enforcing access controls and policies on those devices.

1. Go to **Policy** > **Security Policies** and select **Device Posture**.
2. Configure the settings in Table 17.

Table 17: Device Posture Application Access Configuration Settings

Field	Description
Matching Criteria	Select a **Matching Criteria** from the drop-down list: • Allow when all match • Allow when some match
Posture Check Frequency	Select a **Posture Check Frequency**: • At the time of login and restart • At the time of login/restart and every <select the amount of time> from the **Select Time** drop-down list.
Attributes	Select the **Attributes** you want to use: • Anti-virus and Anti-malware — For desktop agents installed on Windows OS only. **Note:** Enable the **Check the Real Time Protection** toggle to actively monitor device activity, scan files, programs, and network traffic to quickly detect and block malware threats. • Screen Lock — For mobile agents only. • Operating System Check — For all user agents (mobile and desktop). ◦ Select **Add OS Check.**. ◦ Select an **OS Name** from the drop-down list. ◦ Under **OS Version** select **Any** or **Custom**. ◦ Select **Save**. • Browser Check — For the end user portal only. ◦ Select **Add Browser Check.**. ◦ Select a **Browser Name** from the drop-down list. ◦ Under **OS Version** select **Any** or **Custom**. ◦ Select **Save**.

3. Select **Save**.
4. To edit, select the edit icon and in the resulting **Update Posture Checking** screen enable the **Posture Checking** and select the **MDM Posture** or **Extreme Platform ONE Posture** as the **Posture Type**.
5. Select **Save**.

6. To disable, select the edit icon and in the resulting **Update Posture Checking** screen disable the **Posture Checking** and select **Save**.

Policy | Users and Devices

Manage individual users and devices or groups of users and devices by controlling their access to enterprise applications and the network.

Local User Authentication

Local user authentication allows customer to create up to 100 local users accounts that when enabled on a proxy, will be able to log in even if their connection to the cloud is down from the proxy. The proxy will actually perform the local authentication for these 100 local users. This is an optional proxy enhancement. Generally, local accounts are used for local IT to troubleshoot issues. Enabling Local Authentication limits the event of an internet outage.

Note
Users are cloud-enabled by default. If local-only is selected the users can only authenticate in a failover situation when an authentication is performed on the proxy.

When you enable local authentication on a proxy, it takes up to 3 minutes for that to download and install and then sync the local users down to the proxy database. The way the local authentication works on the proxy is that it is a failover only. Initially when the client requests come in for authentication to the proxy, it will try and proxy everything to the cloud until it gets a timeout. That timeout can take up to 3 minutes for us to detect that the connection to the cloud is broken and that instead of proxying requests we send them to our local authentication service to perform the authentication. Once the connection to the cloud is down and authentication will only work for the local Admin users that we added. It won't work for the other users that are synced to the cloud from IDP.

Considerations

- Locally created users will authenticate using EAP-TTLS.
- Local users can be used for both application and network access.
- Local-Only Authentication is only for network access and only supports local users and mac authentication.
- Policy changes will not be deployed and Posture and Compliance checks will be paused until cloud connectivity is restored.

Minimum System Requirements

- CPU Cores: 2
- Total Memory: 1.5 GB
- Disk Available: 2 GB

Add Users

Use this task to add a local user.

Use the 3-dot menu to access the following actions:

- Edit User Groups
- Local-Only Authentication
- Reset Password
- Delete

1. Go to **Policy** > **Users and Devices** and select **Add Local User**.
2. Configure the settings in Table 18.

Table 18: Local User Configuration Settings

Field	Description
Email Address	Enter an email address.
Password	Enter a password.

3. Select **Save**.

Manage User Groups

Use this task to create, manage, and review user groups synchronized from the IdP.

1. Go to **Policy** > **Users & Devices** and select **User Groups**.

2. To create a user group, select **Create User Group** and configure the settings in Table 19.

Table 19: User Group Creation Settings

Field	Description
User Group Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description.
Select Users (Optional)	Select or search for one or multiple users.

3. Select **Save**.

   The **User Groups** page contains a list of user groups.

4. To add users or make an update to an existing group, select ⋮ within the table and select **Edit**.
   a. You can update the **User Group Name** or **Description**.
   b. To add users to the user group, select users you would like to add.
   c. Select **Save**.

5. To delete an existing group, select ⋮ within the table and select **Delete** .

Add Devices

Use this task to manually add devices.

1. Go to **Policy** > **Users & Devices** and select **Devices**.
2. Select **Add Devices** and configure the settings in Table 20.

Table 20: Device Configuration Settings

Field	Description
MAC Address	Enter a MAC address.
Alias (Optional)	Enter an alias for your device.
Description (Optional)	Enter a description.

3. Select **Save**.

   Your device displays in the device list.

4. To delete a device, select ⋮ within the table and select **Delete** devices.

Import Devices

Use this task to import devices in bulk.

1. Go to **Policy** > **Users & Devices** and select **Devices**.
2. Select **Import Devices**.

Note
Maximum import of 10,000 devices.

3. (Optional) Select and existing device group or **Create a Device Group** from the Device Group drop-down list.
   a. Enter a device name and description (optional) and select **Save**.
4. Select one of the following:
   - **Browse** to locate your .csv file.
   - **Download the CSV** template to create your device list to import.

   When you finish creating your template, then repeat the **Browse** step.
5. Select **Next**.

   A confirmation pop-up window displays: **File uploaded and validated successfully. You can now continue.**
6. Select **Next**.

   The list of devices from the .csv file displays.
7. Select specific MAC addresses to import or all addresses to import.
8. Select **Import**.

Your devices display in the device list.

Managed Device Groups

Use this task to create device groups.

1. Go to **Policy** > **Users & Devices** > **Devices** and select **Device Groups**.
2. Select **Create Device Group** and configure the settings in Table 21.

Table 21: Device Group Configuration Settings

Field	Description
Device Group Name	Enter at least three alphanumeric characters for the device group name.
Description (Optional)	Enter a description.
Select Type	Select one of the following: • Devices • MAC OUI - To add a new MAC OUI, select **Add MAC OUI** and configure the settings: ◦ Search - Select MAC OUIs can be tagged and searched by any given name mentioned as the alias. ◦ Select **Add**. • Custom MAC OUI - Any MAC address starting with the entered hex value will be matched.

Table 21: Device Group Configuration Settings (continued)

Field	Description
Available	Select **Existing Devices**. Select the check box associated with the devices you want to add to the group and select **Add**.
Add device	a. Enter a **MAC Address**. b. Enter an **Alias** (optional). c. Enter a **Description** (optional). d. Select **Save**.

3. Select **Save**.

   Device Group displays in the device group list.

4. To make an edit to an existing group, select ⋮ within the table and select **Edit**.
   a. You can edit the **Device Group Name** or **Description**.
   b. To add devices to the device group, select **Existing Devices** or **New Device** from the **Add device**.
   c. Select **Save**.
5. To delete an existing group, select ⋮ within the table and select **Delete** .

Policy | Conditions

Conditions provide a distinct level of authorization to your infrastructure. Policy requirements regulate secure access to your enterprise applications and networks. There are three types of conditions:

- Location
- Time
- Authentication

Location-Based Conditions

Use this task to create location based conditions.

1. Select **Policy** > **Conditions**.
2. Select **Add Condition** and configure the settings in Table 22.

Table 22: Location-Based Conditions Settings

Field	Description
Condition Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description of the condition.

Table 22: Location-Based Conditions Settings (continued)

Field	Description
User Geographic Location(s)	Select one or more geographic locations from the drop-down list. **Note:** Geographic Location conditions are only applicable to Application Based Policies.
Network Location (Optional)	Select one of the following: If you select **Site**, select the existing sites from the drop-down list. • **SSID** - select the existing SSID from the drop-down list. Only SSIDs that are currently managed in the **Network Resources** > **SSID** view are listed. • **Sites** - select a site from the drop-down list. • **Access Point** - select the existing APs from the drop-down list. • **Access Point & SSID** - select the existing SSIDs and AP from the associated drop-down lists. • **Switch** - select the existing switches from the drop-down list. **Note:** Network Locations are only applicable to Network Based Policies.

3. Select **Save**.
4. To edit or delete an existing location-based condition, select  and select **Edit** or **Delete** from the drop-down list.

Your location condition displays in the list.

Time-Based Conditions

Use this task to create time-based conditions.

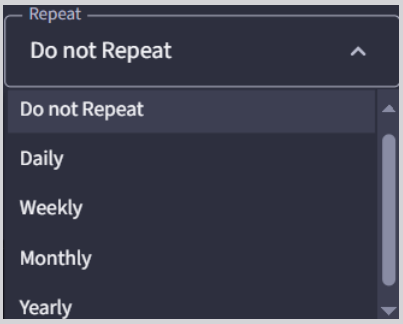
1. Select **Policy** > **Conditions**.
2. Select the **Time** tab at the top of the window.

   The **Time Based Conditions** window displays.
3. Select **Add Condition** and configure the settings in Table 23.

Table 23: Time-Based Conditions Settings

Field	Description
Condition Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description of the condition.
Select Time Zone	Select a time zone from the drop-down list.
Start Date	Select a start date with the **Start Date** calendar.

Table 23: Time-Based Conditions Settings (continued)

Field	Description
End Date (Optional)	Select an end date with the **End Date** calendar. **Note:** When not selected a non-ending time-based condition is created.
Start Time	Select a start time with the **Start Time** clock.
End Time	Select an end time with the **End Time** clock.
Repeat	Under the **Repeat** drop-down list, select how often you want the condition to repeat. 

4. Select **Save**.
5. To edit or delete an existing time-based condition, select ⋮ and select **Edit** or **Delete** from the drop-down list.

Your time condition displays in the list.

Authentication-Based Conditions

Use this task to create authentication-based conditions.

1. Select **Policy** > **Conditions**.
2. Select the **Authentication-Based Conditions** tab at the top of the window.
   The **Authentication-Based Conditions** window displays.
3. Select **Add Condition** and configure the settings in Table 24.

Table 24: Authentication-based Condition Configuration Settings

Field	Description
Condition Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a description of the condition.
Authentication Method	Select a method from the drop-down list or search for a method.

4. Select **Save**.
5. To edit or delete and existing authentication-based condition, select ⋮ and select **Edit** or **Delete** from the drop-down list.

Your authentication condition displays in the list.

Policy | Network Services

Network Services are leveraged in Network and Hybrid policies to define network resources that should be allowed or denied via the policy. These are installed via ACL or firewall rules in the network device depending upon its capabilities.

Configure Network Services

Use this task to add network services.

1. Go to **Policy** > **Network Services**.
2. Select **Add Network Service** and configure the settings in Table 25.

Table 25: Network Service Configuration Settings

Field	Description
Network Service Name	Enter at least three alphanumeric characters.
Protocol	Select a protocol.
IP Address	Enter an IP address.
Ports (Optional)	Enter one or multiple ports separated by commas.

3. Select **Save**.
4. To delete an existing network service, select  and select **Delete** from the drop-down list.

Your network displays in the network services list.

Create Network Services Groups

Use this task to create network service groups to share policies or rules with a set group of network services. A policy using this group applies to all network services defined in the group.

1. Go to **Network Services** > **Network Service Groups**.

2. Select **Create Network Service Group** and configure the settings in Table 26.

Table 26: Network Service Groups Configuration Settings

Field	Description
Network Group Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a group description.
Select Network Services	Search for or select an existing network service and select **Add Network Service**.

3. Select **Save**.
4. To edit or delete and existing Network Service Group, select  and select **Edit** or **Delete** from the drop-down list.

Your network displays in the group list.

Policy | Applications

Integrating your site infrastructure with Extreme Platform ONE Security ensures secure access to your enterprise applications. There are several application categories. Each one is optional, and you can add them in any order.

Application groups are created that combine similar applications policies to be leveraged within a single application or hybrid policy. Therefore, any policy added to the application group automatically applies to all the applications within the group.

To access the end user portal from Extreme Platform ONE Security, select the **End User Portal Link** to copy and share the URL with end users. Upon opening the link, enter your credentials to be redirected to the synced IdP user. Log in to finish setting up access to the End User Portal.

To edit or delete and existing application, select  and select **Edit** or **Delete** from the drop-down list.

Add Private Web Applications

Use this task to add web applications.

1. Go to **Policy** > **Applications**.
2. Select **Add** > **Add Application** and configure the settings in Table 27.

Table 27: Private Web Application Configuration Settings

Field	Description
Application Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter an application description.

Table 27: Private Web Application Configuration Settings (continued)

Field	Description
Application Type	Select **Private Web App** from the drop-down list.
Site	Select the site associated with the deployed Service Connector. When a site is selected the **Connector** field is enabled and the associated connectors are displayed.
Connector	Select a connector.
Application Information	Enter the complete URL (e.g., https://<website>.com). **Note:** If a specific port is required for the address, add it to the URL, (i.e., https://<website>.com:8443).
Enable Single Sign-On (SSO) for agentless access	If enabled, changes to the public DNS records are required. **Note:** Application URL's public DNS entry must point to relevant relay node's CNAME. CNAME is found while adding an application. **Note:** Connector requires a private DNS setup which points the application domain to the correct IP where application is hosted. This is used while adding the application and Agentbased access.

3. Select **Save**.
4. To edit an existing private web access application, select ⋮ and select **Edit**.
5. To remove an application in activating, deactivating or DOWN status, select ⋮ and select **Force Delete**.
6. To remove an application in UP status, select ⋮ and select **Delete**.

Add Custom Applications

Custom applications provide support for adding applications using customized TCP or UDP ports.

Use this task to add custom applications.

1. Select **Policy** > **Applications**.
2. Select **Add** > **Add Application** and configure the settings in Table 28.

Table 28: Custom Applications Configuration Settings

Field	Description
Application Name	Enter a name for the application.
Description (Optional)	Enter an application description.
Application Type	Select **Custom Application**.

Table 28: Custom Applications Configuration Settings (continued)

Field	Description
Site	Select an associated site.
Connector	Enter an associated Connector.
Application Information	Enter a hostname or IP address.
Any Ports	Enable toggle or enter specific ports.
TCP Ports	Enter up to 5 TCP ports separated by commas.
UDP Ports	Enter up to 5 UDP ports separated by commas.

3. Select **Save**.
4. To edit an existing custom application, select ⋮ and select **Edit**.
5. To remove an application in activating, deactivating or DOWN status, select ⋮ and select **Force Delete**.
6. To remove an application in UP status, select ⋮ and select **Delete**.

Add Multi-Cloud Web Applications

Use this task to add multi-cloud web applications.

1. Go to **Policy** > **Applications**
2. Select **Add** > **Add Application** and configure the settings in Table 29.

Table 29: Multi-cloud Web Application Configuration Settings

Field	Description
Application Name	This is already supplied when load balancer is selected.
Description	Enter an application description.
Application Type	Select **Multi-Cloud Web App**.
Site	Select an associated site.
Connector	Select an associated connector.
Cloud Hosting Provider	Select one of the following options: • AWS • AZURE **Note:** These options are enabled when an integration is added. If no Public Cloud integration is added these options appear as disabled.
Application Information	Select a load balancer.

3. Select **Save**.
4. To edit an existing application, select ⋮ and select **Edit**. Make changes and select **Save**.

5. To remove an application in activating, deactivating or DOWN status, select and select **Force Delete**.
6. To remove an application in UP status, select and select **Delete**.

Add Terminal Access Applications

Use this task to add terminal access applications:

1. Go to **Policy** > **Applications**.
2. Select **Add** > **Add Application** and configure the settings in Table 30.

Table 30: Terminal Access Configuration Settings

Field	Description
Application Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter an application description.
Application Type	Select **Terminal Access** from the drop-down list.
Site	Select an existing site from the drop-down list or create a new site.
Connector	Enter an associate Connector.
Application Information	• Under **Protocol**, select **Secure Shell (SSH)** or **Telnet** protocols. **Note:** Default Port Number is provided when any protocol SSH/Telnet is selected. The field is also editable to enter a specific port number. • Enter a **Hostname (or IP Address)**.

3. Select **Save**.
4. To edit an existing terminal access application, select and select **Edit**.
5. To remove an application in activating, deactivating or DOWN status, select and select **Force Delete**.
6. To remove an application in UP status, select and select **Delete**.

Add Remote Desktop Applications

Use this task to add remote desktop applications.

1. Go to **Policy** > **Applications**.

2. Select **Add** > **Add Application** and configure the settings in Table 31.

Table 31: Remote Desktop Configuration Settings

Field	Description
Application Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter an application description.
Application Type	Select **Remote Desktop** from the drop-down list.
Site	Select an existing site from the drop-down list.
Connector	Enter an associate connector.
Application Info	• Under **Protocol**, select **RDP** or **VNC**. • For **Hostname (or IP Address)**, enter the hostname or IP address. • A default number is provided for RDP protocol. The field is also editable to enter a specific port number.

3. Select **Save**.
4. To edit an existing remote desktop application, select ⋮ and select **Edit**.
5. To remove a remote desktop application, select ⋮ and select **Delete**.

Add Application Segment

Application Segments are not displayed on the Desktop Agent UI or accessible using Mobile Agents. The user is able to access the service directly in the segment if the agent is connected. Use this task to add an application segment.

1. Go to **Policy** > **Applications**.
2. Select **Add** > **Add Application Segment** and configure the settings in Table 32.

Table 32: Application Segment Configuration Settings

Field	Description
Application Segment name	Enter an application segment name.
Description (Optional)	Enter an application segment description.
Application Type	Defaults to Application Segment.
Connector	Select an associated connector.
Site	Select a site from the drop-down list.
Application Segment Info	Enter the subnets separated by commas.
Any Ports	Enable toggle or manually enter ports.
TCP Ports	Enter up to 5 TCP ports separated by commas.
UDP Ports	Enter up to 5 UDP ports separated by commas.

3. Select **Save**.
4. To edit an existing application segment, select ⋮ and select **Edit**.

5. To remove an application segment, select and select **Delete**.

Create Application Groups

Use this task to create application groups.

1. Go to **Policy** > **Applications** > **Application Groups**.
2. Select **Create Application Group** and configure the settings in Table 33.

Table 33: Application Groups Configuration Settings

Field	Description
Application Group Name	Enter at least three alphanumeric characters.
Description (Optional)	Enter a group description.
Select Application	Select all the applications you want to add to your group.

3. Select **Save**.
4. To update or remove an existing Application group, select and select **Edit** or **Delete** from the drop-down list.

Note
An Application Group associated with a policy can't be deleted until the user removes the association in policy.

Your application group displays in the list. You can also see the number of applications in your group.

Application Discovery

Application Discovery is used to access all applications and determine what application policies are needed for specific user groups. Applications are discovered by signing into the Agent and connecting with the domain of the applications enter within the domain listing.

Note
Only applications with domains listed in the **Domain Name** field appear in the **Enable Application Discovery** modal.

Go to **Policy** > **Applications** > **Application Discovery**, you can view the following application analytic information:

- Most Used Applications by Users
- Least Used Applications by Users
- Total Applications Discovered

- Total Users
- Total Apps

Note
Application Discovery will allow all users, all subnets, on all ports effectively acting as a wide-open VPN.

To enable, extend, and end application discovery, see Manage Application Discovery on page 80.

Total Apps

The Total Apps table represents discovered and published applications. The table displays the following information pertaining to discovered applications:

- Name
- Status
- Type
- Access URL
- Associated Connector
- Number of Users
- Last Accessed

Once an application is discovered and appears in the **Total Apps** list, you can select the 3-dot menu and select **Add Application**. Enter a name and select **Add** to publish the application.

For published applications, the three-dot menu displays an option to **Add to Application Group**. Select an application group from the drop-down list and add the application to the respective group.

Manage Application Discovery

Application Discovery allows access to all applications and can be used temporarily to help determine what application policies are needed for specific user groups. Use this task to enable application discovery.

For a successful result, the Service Connector must be deployed, a DNS server should be associated with the Service Connector and Application Discovery must be enabled on the tenant associated with the created DNS server. Once the user signs into the Agent, the tunnel connects. If the user directly accesses a service that is part of the

subnet used in Application Discovery, the application is discovered and appears in the listing on the tenant.

Note

For applications to be discovered via domain name, and not just the IP address, add domains as per your forecast. For example, the applications select domain like "jira.extremenetworks.com" and "wiki.iq.extremenetworks.com".

For apps to be discovered by any users, add only the ending domain "extremenetworks.com". If the domain is not specified the application will be discovered only by the IP address.

1. Go to **Policy** > **Applications** > **Application Discovery**.
2. Select **Enable Application Discovery**, select a **DNS** and enter a **Domain Name**.
3. To confirm, select **Enable Application Discovery** and configure settings in Table 34.

Note

This will allow all users, all subnets, on all ports effectively acting as a wide-open VPN.

Table 34: Application Discovery Configuration Settings

Field	Description
DNS Server	Set up DNS server to capture DNS packets from the client to discover applications. Select a DNS server from the drop-down list or select **Create a new DNS Server** and do the following: a. Add a name and IP Address for the DNS Server. b. Select a **Service Connector** from the drop-down list. c. Select **Save**.
Subnet	To add a subnet of the required applications that are to be discovered: a. Select **Add Subnet** enter the subnets or subnet IPs. b. Select a **Service Connector** from the drop-down list. c. Select **Save**.
Domains (Optional)	Add domains of the required applications that are to be discovered. Select **Add domain** enter the domain name and select **Add**.

4. Select **Enable Application Discovery**.

   A default Application Policy is created.
5. To copy and send the end portal user link, select **End User Portal Link**.
6. Discovery will run for 30 days, to extend an additional 30 days up to a maximum of 90 days, at the top-right corner of the page, select **Extend Application Discovery**, read the message, and select **Extend**.
7. To end Application Discovery, select **End Application Discovery**, read the message, and select **End Now**.

   The default Application Policy is now removed.

Manage Agent Settings

Use this task to manage agent setting.

1. Go to **Policy** > **Applications**.
2. Select **Agent Settings** and configure the settings in Table 35.

Table 35: Agent Settings Configuration

Field	Description
Agent Session Timeout	To set the session timeout duration for agents, select a duration from the **Session Timeout Options** drop-down list. The default setting is 24 hours. The value will take effect on all new connections and user is logged out of the Agent when the selected time interval is completed. Upon Agent sign in the selected value in the drop-down takes effect.
SSO Auto Reconnect	Enable automatic agent reconnection for seamless and uninterrupted connectivity. When enabled extends the session timeout for Active User Agents as per the timeout option selected in the drop-down menu.
Pass-through Authentication	Enable Agent to login using the logged in user. **Note:** Entra ID joined device is required. This is enabled on the Windows Agent Sign in screen, under "SSO Login". This feature is available on Windows and MAC Agent. Enable toggle to have Agent Automatic Sign-in, if disabled, you will receive an error that SSO Login is disabled by your Administrator. Select **Prerequisites** to view initial tasks to complete by Operating System.
Select **Save**.	
Trusted Networks	When your device is on a trusted network, the Agent disconnects all tunnels and remains in a disconnected state for users to attempt direct/local access. Select **Add Trusted Networks**, enter a public IP address or CIDR range to mark as trusted, and select **Save**. **Note:** Manually added Trusted Networks can be removed from the table by selecting **Delete**. Service Connector Public IP entries can not be removed unless the associated Service Connector instance is removed.

Subscriptions and Services

Manage subscriptions, licenses, and trials on the **Subscriptions & Licensing** page. You can search for licenses, verify the license status, and you can group and filter to view specific license details.

It is helpful to understand the interrelationship between contracts, subscriptions, and licenses in Extreme Platform ONE Security. See .

Contracts, Subscriptions, and Entitlements Terminology

Link your Extreme Portal Account

Use this task to link your account and Extreme Platform ONE Networking or ExtremeCloud IQ (New).

1. Go to **Subscriptions & Services** > **Subscriptions & Licensing**.
2. Select the **Global** tab.
3. Select **Link Extreme Portal Account** and type your credentials.

Synchronize Subscriptions

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

Use this task if you do not see your new subscriptions and licenses on the **Subscriptions & Licensing** page. You can synchronize subscriptions only once every 5 minutes.

Important
Do not use **Synchronize Subscriptions** just to refresh the information in the management application.

1. Go to **Subscriptions and Services** > **Subscriptions & Licensing**.
2. Select **Synchronize Subscriptions**.

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

Subscriptions & Licensing User Interface

Figure 3 identifies elements and features available on the **Subscriptions & Licensing** page. See Table 36 for descriptions of the numbered elements.

Figure 3: Subscriptions & Licensing interface

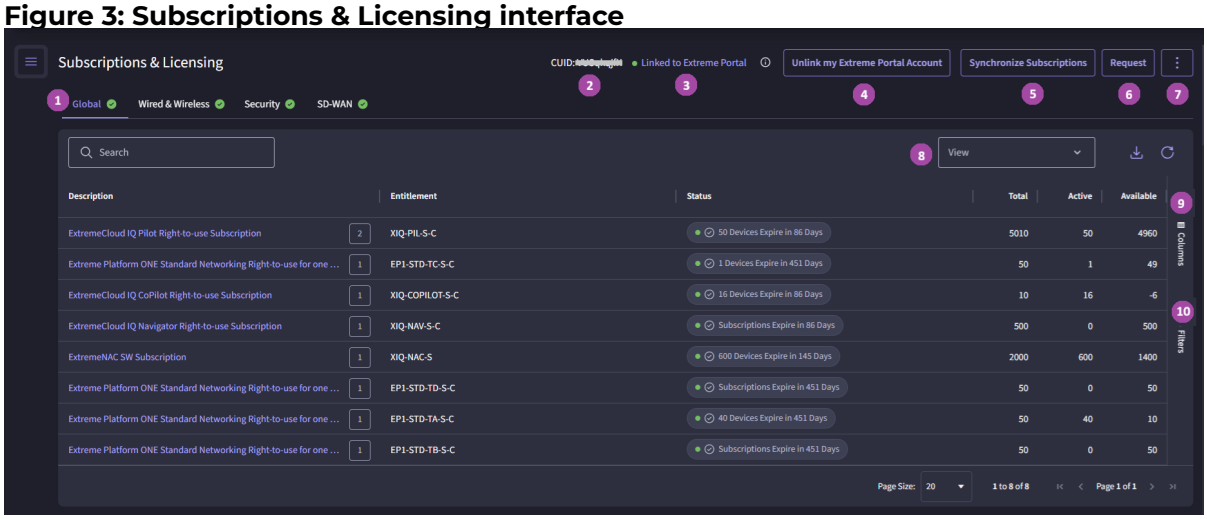


Table 36: Subscriptions & Licensing interface descriptions

Callout	Interface Area	Description
1	Global tab	Displays all subscriptions for all applications and services when unfiltered. The following columns display the total number of subscriptions, the number of active subscriptions, and the number still available. • **Total** = sum of all subscriptions available to use = sum all of the same subscription type with start date in the past and end date in the future = exclude expired and not yet valid • **Active** = sum of all subscriptions currently in use • **Available** = **Total** minus **Active** These numbers fluctuate as subscriptions are applied or removed from a device or devices. To display details for a specific application or service, select the corresponding tab.
2	CUID	The unique ID associated with the license pool. The CUID is very important when communicating with support personnel.
3	Extreme Portal link status	Indicates whether Extreme Platform ONE Security is linked to your Portal account. The account must be linked to see content of the license pool.

Table 36: Subscriptions & Licensing interface descriptions (continued)

Callout	Interface Area	Description
4	Link / Unlink	Toggle the link status between Extreme Platform ONE Security and your account. **Caution:** Use **Unlink** only for troubleshooting when directed by Support personnel.
5	Synchronize Subscriptions	Synchronize the display of your Extreme Platform ONE Networking subscriptions with the license pool.
6	Request	Create a purchase request that you can submit to your partner for review and to get a quote.
7	3-dot menu	Displays action options: • Request History • Manage NAC Allocations • Contact Support • Contact Sales
8	View	Select **Simple**, or group subscriptions according to the **Description** or by **Product**.
9	Columns	Customize the columns that you see on the page.
10	Filter	Filter the table by **Entitlement**, **Product**, or **Status**.

Search, Group, and Filter

You can search for an item and organize lists in the **Subscriptions & Licensing** user interface.

You can group records based on the predefined criteria that vary for different windows.

Use the **Previous** (**<**) and **Next** (**>**) icons to scroll through the results lists.

1. To search for records, start typing a search attribute such as product, subscription or subscription type, status, or a complete or phrase or words from a description in the **Search** field.

   Note
   Search terms are not case-sensitive.

   To clear the search, select **X** in the **Search** field.
2. To group the records according to product, select **View** and choose **Product**.

   The default view displays all records in alphabetical order according to the **Description**.
3. To filter records in a page, select **Filter** ( ) and choose the filter attribute.

   To clear an individual filter, click **X** for the appropriate filter. To clear all the filters, select **Clear All Filters**.

Subscriptions & Licensing Details

Information about subscriptions is immediately visible in the **Subscriptions & Licensing** interface. Details include subscription or entitlement, product name, number of days until the subscription expires, status, entitlement total, total active, and available entitlements. Colored icons indicate the status for each subscription or entitlement:

- Green: no problems
- Amber: attention needed, for example:
  - One or more subscriptions 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:
  - One or more subscriptions expire in fewer than 30 days and the renewal is not yet in progress
  - Expired subscriptions

Trial Subscription Eligibility

Request a trial subscription only if you meet the following criteria:

- You are a new or ExtremeCloud IQ (New) customer.
- You are an existing , ExtremeCloud IQ (New), or ExtremeCloud IQ customer who has never purchased or requested a trial subscription for the application you are considering.

Note
If you requested and were granted a trial in the past but never used it, you are disqualified from a new trial.

Purchase a Subscription

Contact your partner to purchase an subscription or add additional licenses to an existing subscription. You can add additional licenses to a subscription incrementally, as required.

Request a Trial Subscription

Use this task to request a 90-day trial subscription.

1. Go to **Subscriptions & Services** > **Subscriptions & Licensing**
2. On the **Subscriptions & Licensing** page, select **Start Trial**.

Note
On first request, a **Request Process** diagram opens.
- (Optional) Select **Do not show this message again**.
- Select **OK**.

a. Select the checkbox to **Accept Terms and Conditions** and acknowledge the policy.
b. Select the check box to agree to share contact information.
c. Select **Accept and Continue**.

3. In **Select Request**, select **Subscriptions**, and then select **Next**.
4. Select the application that you want to trial, and select **Add** adding each one to the cart.
5. When you finish adding applications to the cart, select **Next**.
6. Type your phone number and fill out any optional information, then select **Next**.
7. Review your request, and then select **Next** to download the request document.
8. Submit the request document to your Extreme Networks partner or contact your account team to submit the request.

Note
Depending on the application and regulatory requirements, the trial subscription is available after a few minutes or up to five working days after verification. In addition to the in-product subscription-request notification, you receive email notification regarding the status of your request.

If you have not received the licenses after two business days, contact your account team.

If the trial subscription request is rejected, contact your account team.

Renew a Subscription

Before a subscription expires, your Preferred Partner will send you a renewal quote. If you prefer, you can contact your partner proactively. To find a new partner, use the Partner Locator.

To renew a subscription, send a subscription request to your Preferred Partner. You can change license quantities when you renew a subscription, and you can purchase new subscriptions as required. After a subscription request is processed, subscriptions are added to the license pool for your CUID.

View Subscription History

Use this task to view the history of subscription purchases, or trials and trial requests.

1. Go to **Subscriptions & Services**, select ⋮, and then select **Request History**.

   The **Subscriptions & Licensing / Request History** page lists all subscriptions and requests.
2. (Optional) Use the **Search** feature to refine the result set and view for a specific subset of subscriptions.

   You can view details in the columns.
3. (Optional) To download summary information for a subscription or a subscription request, select ⋮ for the corresponding entry, and then select **Download**.

   To complete the download, save the file when prompted.

Administration & Settings | Access Management

Users and Roles

You can add multiple users and roles of the following types to Extreme Platform ONE Security.

- Internal users
- External users

You can also implement single-sign-on via SAML-based identity providers.

Note
Roles for all applications can be assigned only in Extreme Platform ONE Networking. You cannot create or assign roles or custom roles that were previously assigned in individual applications.

Create a New User

User access is controlled by the roles you assign. Use this task to add a new internal or external user account and assign roles to manage their site access.

1. Go to **Administration & Settings** > **Access Management**.
2. In the **Users & Roles** area, select one of the following account-types:
   - **Internal Users**: Select this tab to grant access to users within your organization.
   - **External Users**: Select this tab to grant access to users outside of your organization; for example, resellers, distributors, technical support, and sales.
3. Select **Create New User**.

4. For an Internal user account, perform the following steps:

   For an External user account, go to step 5.

   a. Type the email address for the user and select **Next**.
   b. Configure the following settings:.

Table 37: User configuration settings

Field	Description
Email	Email address, not more than 128 characters.
First Name	First name, not more than 63 characters.
Last Name	Last name, not more than 63 characters.
Primary Role	Specify access to Extreme Platform ONE Networking, ExtremeCloud IQ (New), and if applicable Security, SD-WAN, and other Platform ONE applications. The primary role is the platform role that is common across all accessible applications.
Classic Role	Specify access to ExtremeCloud IQ (Classic). **Note:** Options are limited by Primary Role selection for application access.
Sites	Specify access to sites. Administrators have access to all sites and locations if a site hierarchy is created. **Note:** It is imperative that you assign users to a site or sites.
Idle Session Timeout	Specify whether to enforce idle session timeout. If you do not specify a time, the user session will not timeout. **Note:** A non-expired timeout configuration overrides any admin-configured timeout. Otherwise, all admin-configured user timeout settings follow those that the admin configured.

   c. Select **Save**.
   d. You can review the access and roles assigned to the new user by selecting **Internal Users** in the **Users & Roles** area.

5. For an External user account, perform the following steps:

   a. Type the external email address and select **Next**.

      Note
      Extreme Platform ONE Security validates the email address for availability. An error message provides notification if the address was already added or is ineligible to be added for an external user.

   b. Configure **Application Access** for the user. Select the user role value for the **Primary Role** and the **Classic Role**.

c. **Configure site access** from the role-specific menu choices.
d. (Optional) Select the access duration:
   - **Time Dependent:** Select start and end dates (optional). Select the respective drop-down menus to assign workspace and application access, and roles to the external user.
   - **Indefinite:** Do not define start and end dates, meaning that site access is not time-limited until the value changes.
e. Select **Save**.

   You can review the access and roles assigned to the new user in the **Users & Roles** area by selecting **External Users** in the **Users & Roles** area.

Role-Based Access

Access to Extreme Platform ONE Security features is governed by user roles. Your assigned role determines feature access and visibility of features on the Navigation menu. Examples include dashboard widgets and Extreme AI Expert.

Note
Extreme Platform ONE Security user roles cannot be configured in ExtremeCloud IQ.

Identity Providers | Network & Applications

An Identity Provider (IdP) is the source of your users' identities for your organization. Begin by configuring your IdP. You can do this by establishing connections with one of the following IdPs:

- Microsoft Entra ID
- Google Workspace
- Okta

The ability to support multiple identity providers (IdPs) within a single tenant is supported for complex identity management needs, such as during cloud service migrations, acquisitions, or ensuring redundancy. It also addresses the growing requirement to manage contractors with separate IdPs securely. This enhancement increases flexibility especially for customers.

There are three primary purposes for integrating with an Identity Provider for Extreme Platform ONE Security. The applications created in the Identity Provider are to be different even if the type is the same, however they can be reused if desired

The purposes are:

- User and User Group Synchronization – Used to make users and user groups available within Extreme Platform ONE Security for policy assignment.

  Note
  Synced User and User Groups cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

- Application Access authentication – Used for logging into the Extreme Platform ONE Security Agent or the End User web portal.
- Network Access authentication – Used for 802.1X EAP-TTLS authentication of clients on access points and switches.

For more information, see IdP Network & Applications | Support Multiple IdPs on page 127.

Microsoft Entra ID | JIT User and User Groups Synchronization

This method has Extreme Platform ONE Security reach into Microsoft Entra ID and pull users and user groups on a polled basis. The synchronization leverages an OIDC application to integrate with the Entra ID APIs.

JIT integration is configured in these steps:

1. Configure Microsoft Entra ID.
2. Configure Extreme Platform ONE Security.

Microsoft Entra ID

1. Go to **Applications** > **App registration** and select **New registration**.

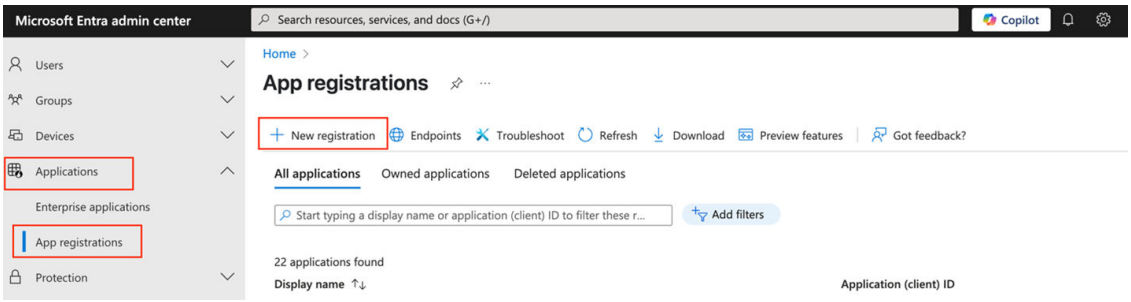


Figure 4: App registrations page

2. Under **Register an application**.

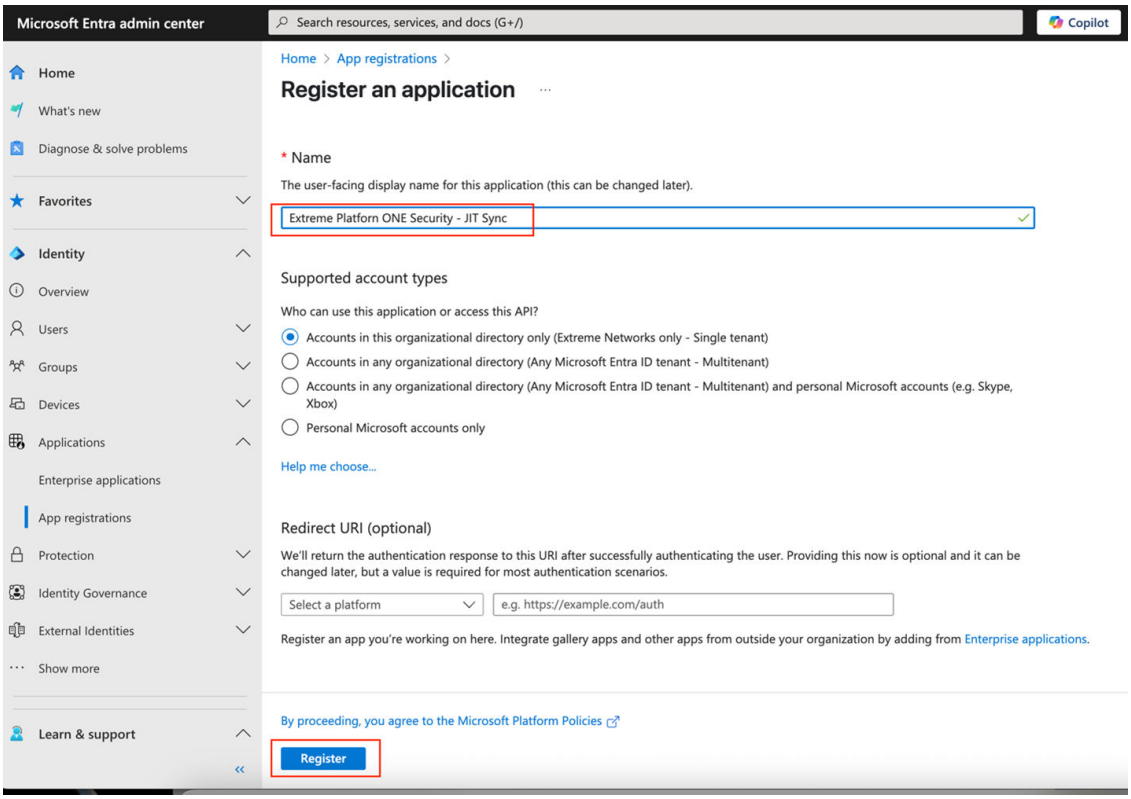


Figure 5: Register an application page

a. Name the application appropriately for JIT Integration.
b. Leave the default fields selected and select **Register**.

3. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.

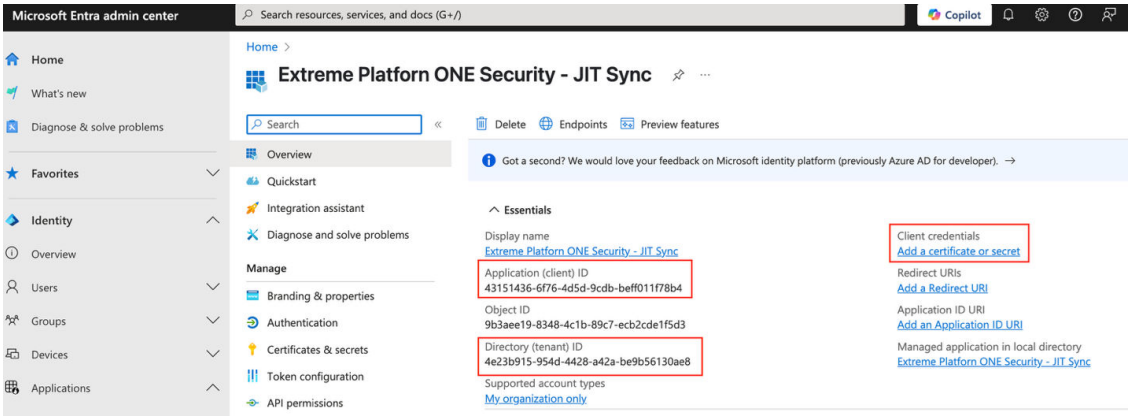


Figure 6: Client credentials

4. Select **New client secret**.

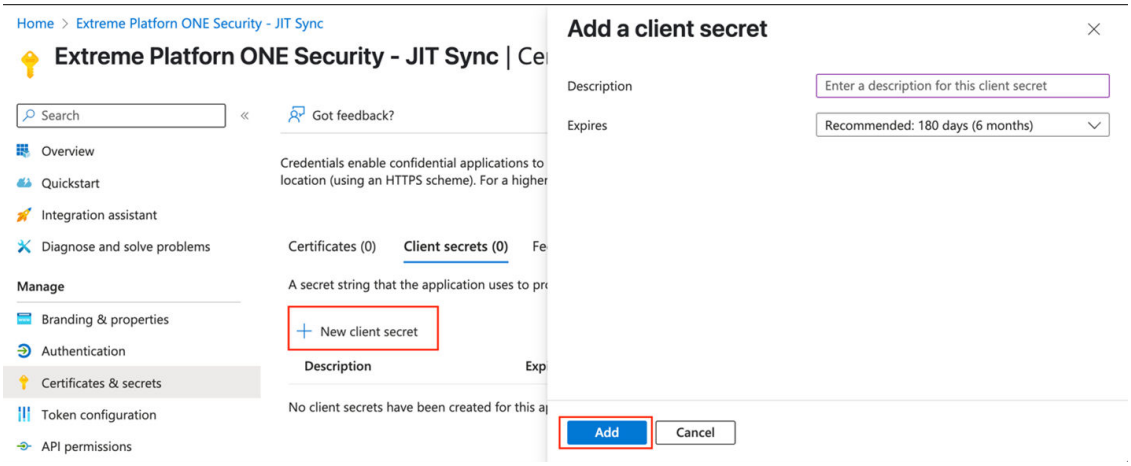


Figure 7: Add a client secret window

a. Enter a description if desired and a preferred expiration date of the secret.
b. Once complete, select **Add**.

5. Copy the value of the new secret for use later.

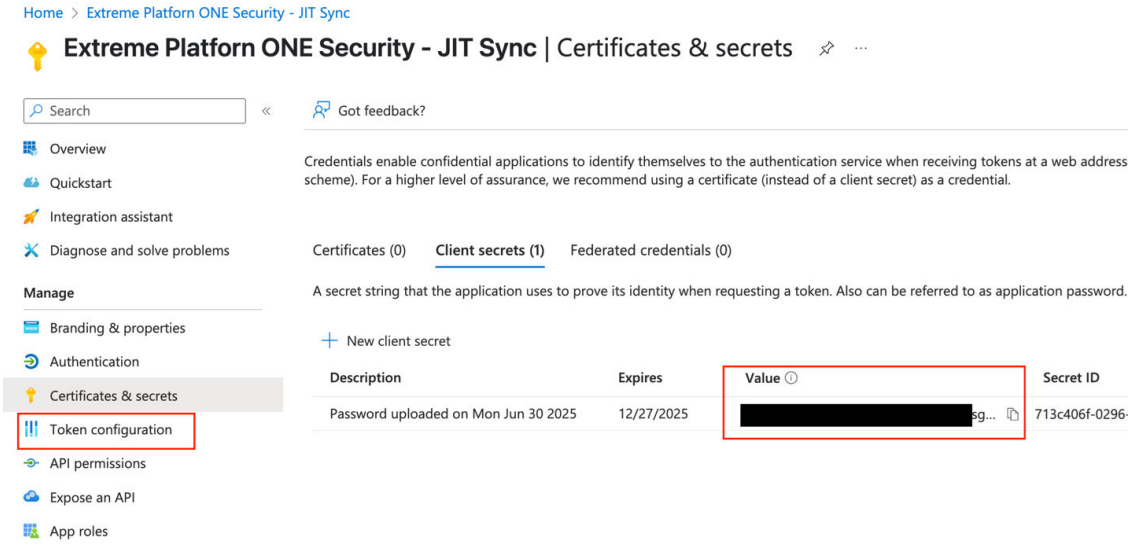


Figure 8: Client secrets

6. Go to **Manage** > **Token Configuration**, select **Add optional claim** and configure the settings in Table 38.

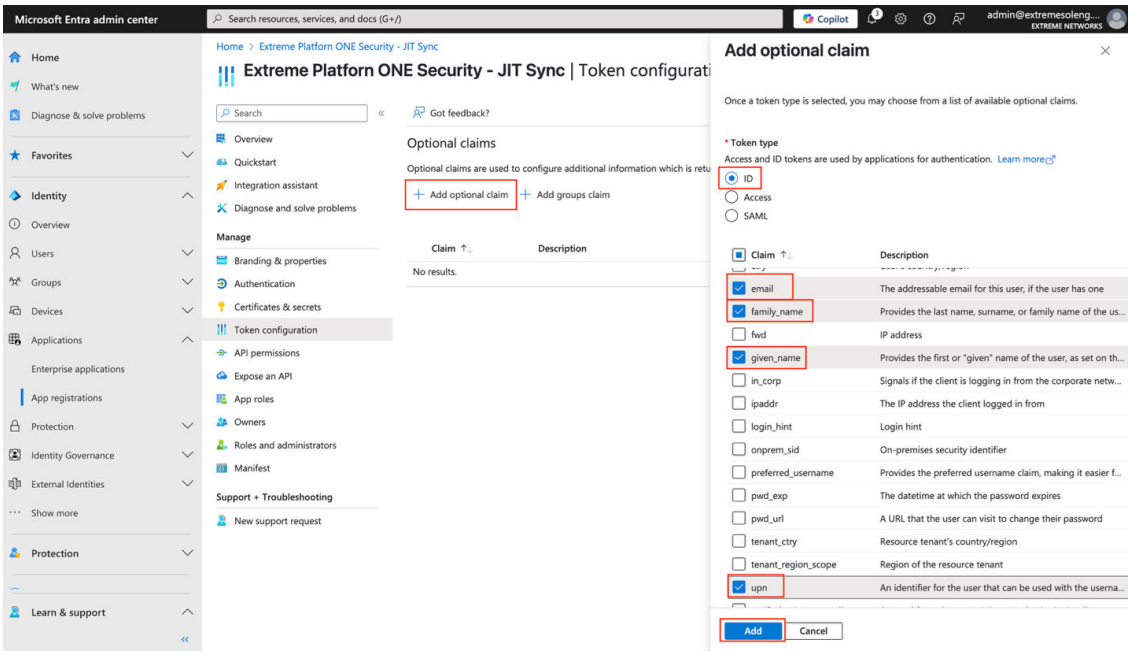


Figure 9: Add optional claim window

Table 38: Optional Claim Configuration Settings

Field	Description
Token Type	Select the **ID** radio button.
Claim	Select the following from the available list: • email • family_name • given_name • upn
Turn on the Microsoft Graph email, profile permission (required for claims to appear in token).	Enable the toggle if prompted to turn on Microsoft Graph.
Select **Add**.	

7. Select **Add groups claim** and configure settings in Table 39.

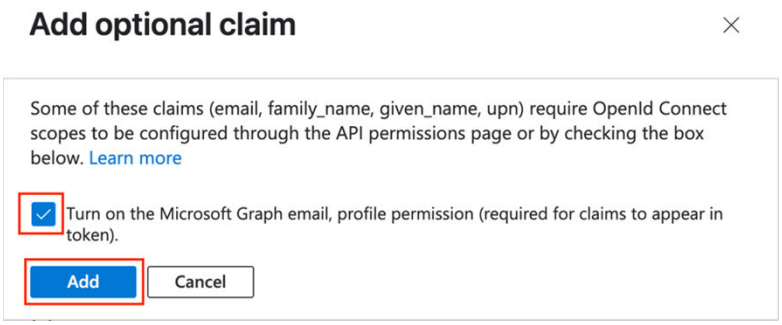


Figure 10: Add optional claim

Table 39: Group Claim Configuration Settings

Field	Description
Select group types to include in Access, ID, and SAML tokens.	Select **Groups assigned to the application**.
Customize token properties by type	Select **Group ID**.
Select **Add**.	

8. Go to **Manage** > **API permissions** and select **Add a permission**.

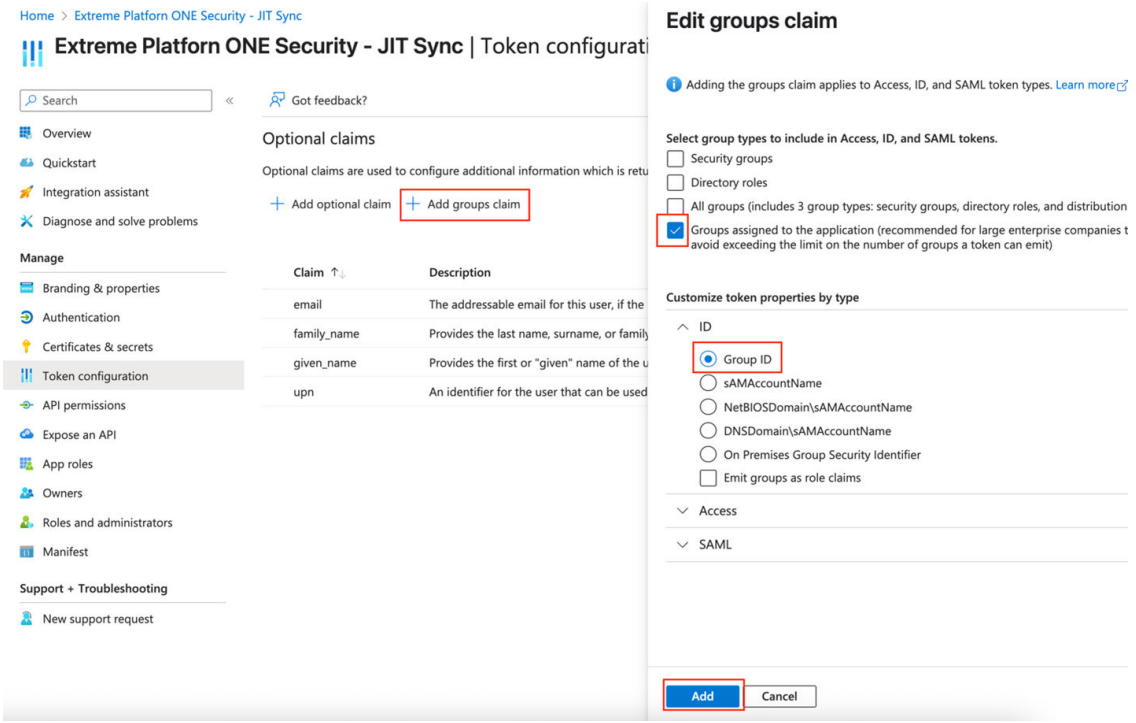


Figure 11: Edit groups claim

9. Select **Microsoft Graph** and configure the settings in Table 40.

Table 40: Microsoft Graph Configuration Settings

Field	Description
What type of permissions does your application require?	Select the **Application permissions**.
Select permissions	Filter on text of the permission needed and select it from the drop-down list. The following permissions are required: • User.Read.All • Group.Read.All • GroupMember.Read.All
Select **Add permissions** and the **Configured permissions** window is displayed.	
Configured permissions	Select **Grant admin consent for <Company Name>**.

10. Go to **Overview**, scroll to the bottom, and select **Go to Enterprise applications**.

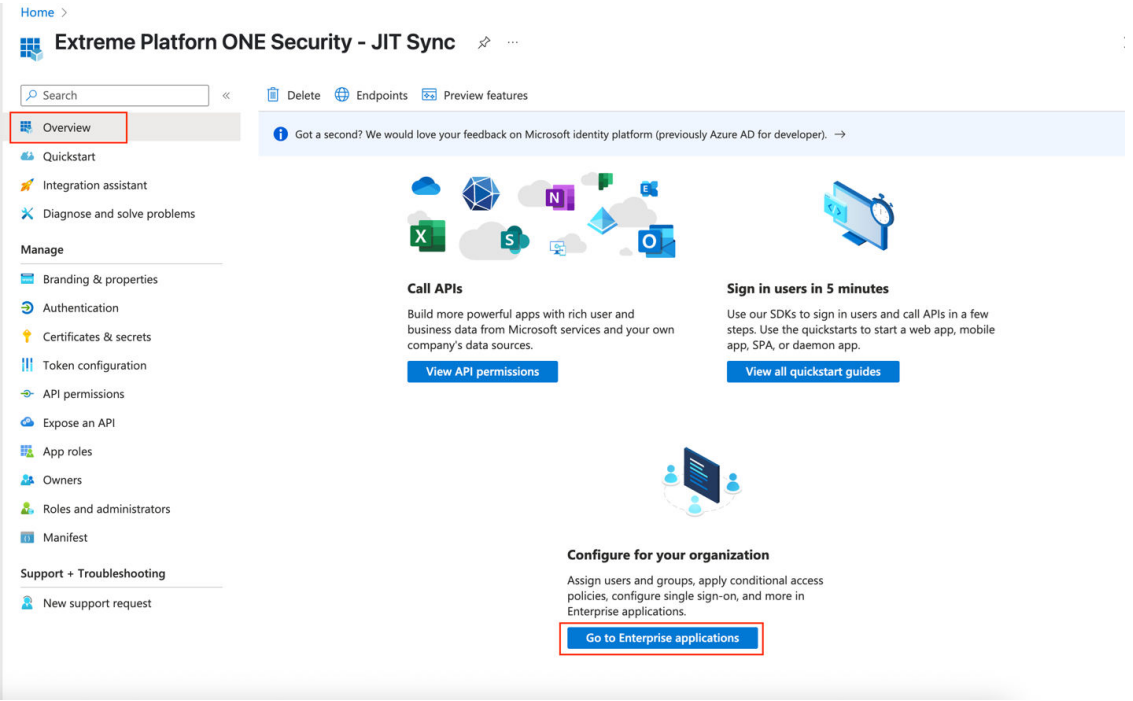


Figure 12: Enterprise applications

11. Go to **Manage** > **Properties**.
    a. Set **Assignment required?** to **Yes**
    b. Select **Save**.

12. Go to **Manage** > **Users and groups**.

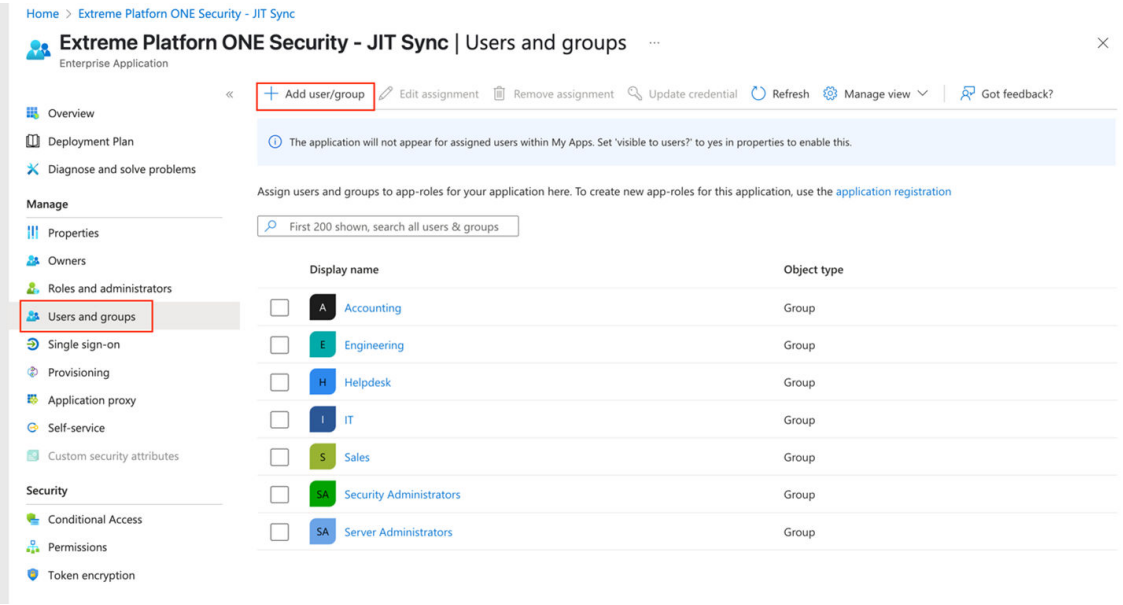


Figure 13: Users and groups

a. Select **Add user/group**.
b. Assign all groups that should be leveraged in Extreme Platform ONE Security.

Extreme Platform ONE Security

13. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

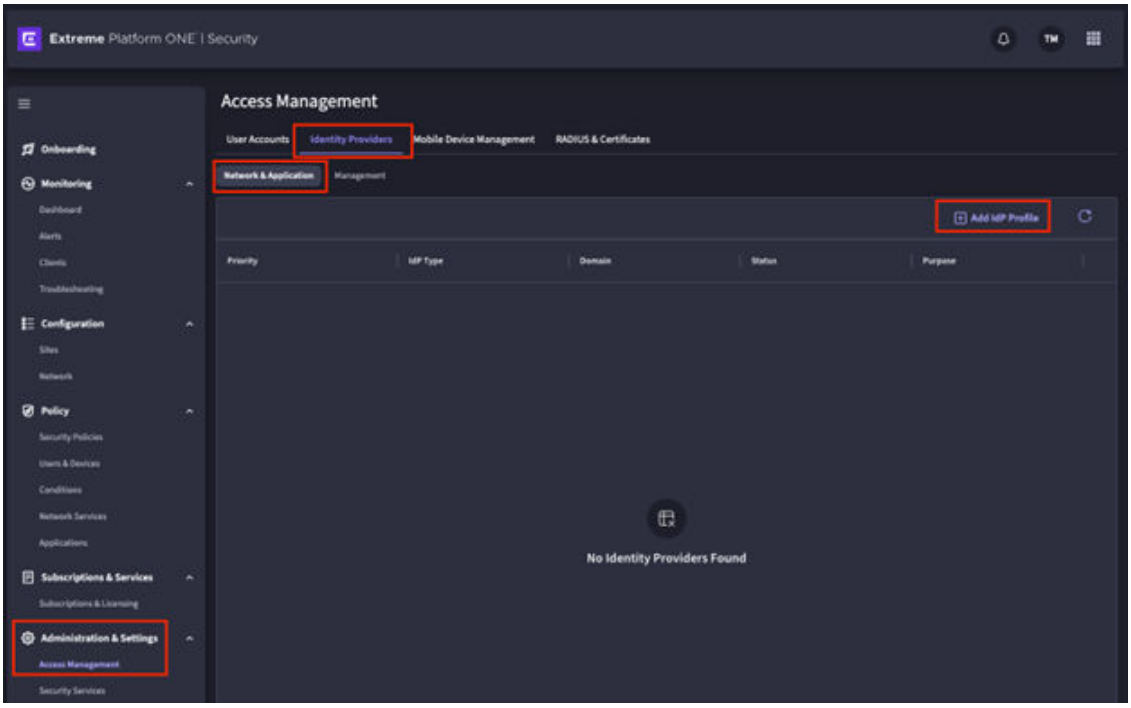


Figure 14: Access Management

14. Select **Add IDP Profile** and configure the settings in Table 41.

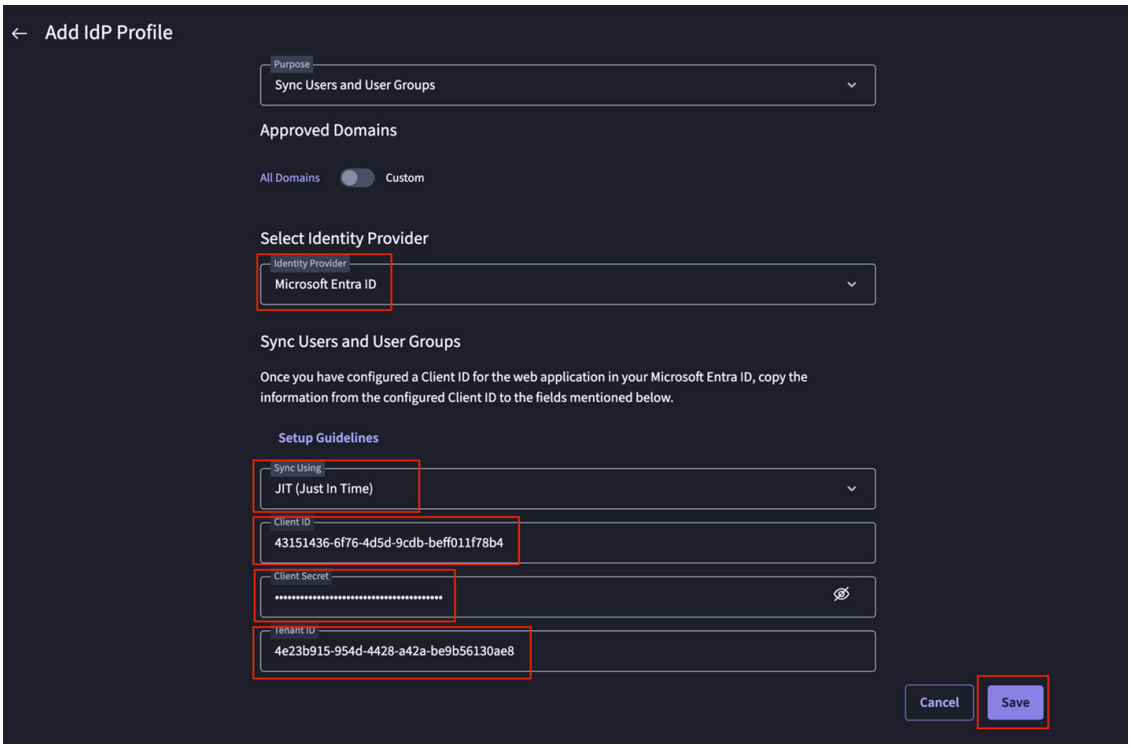


Figure 15: IdP Profile Settings

Table 41: JIT for Microsoft Entra ID Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **JIT (Just in Time)** for the **Sync Using** drop-down list.
	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret • Tenant ID

15. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To force a sync, go to **Access Management** > **Identity Providers**, select ⋮ and select **Sync Now**

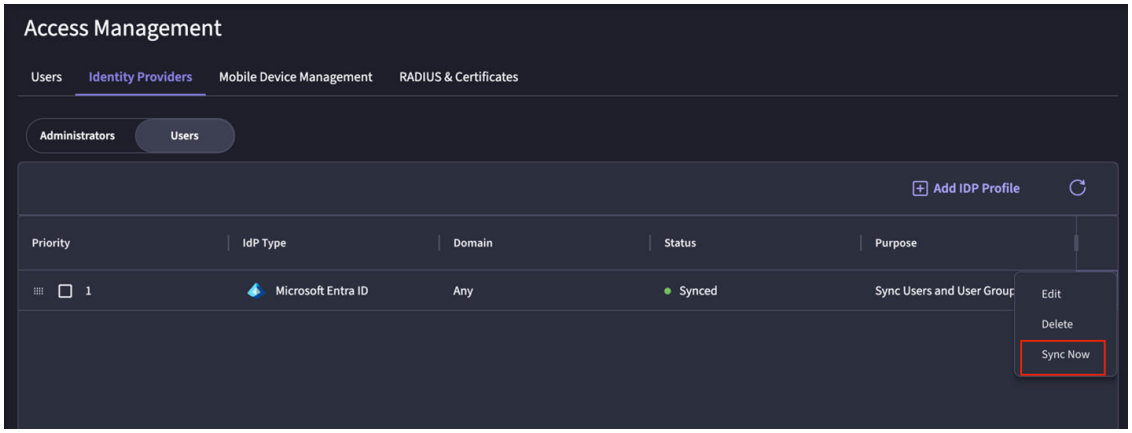


Figure 16: Sync Now

.

Microsoft Entra ID | SCIM User and Groups Synchronization

This method has Microsoft Entra ID push users and user groups from Entra into Extreme Platform ONE Security. This method requires an enterprise application to be set up in Microsoft Entra ID to enable automatic provisioning.

SCIM integration is configured in these steps:

1. Configure Extreme Platform ONE Security.
2. Configure Microsoft Entra ID.

Extreme Platform ONE Security

1. Go to **Access Management** > **Administration & Settings** > **Identity Providers** and select **Network & Applications**.
2. To create a new profile, select the **Add IdP Profile** and configure the settings in Table 42.

Table 42: SCIM for Microsoft Entra ID Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** as the **Purpose** from the drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **SCIM (System for Cross-domain Identity Management)** for the **Sync Using** drop-down list.

3. Select **Save**.

4. Once saved, from the 3-dot menu, select **Edit**.
   a. In the **Edit** window, select **Entra Syncing Credentials**.
   b. In the **Entra ID Syncing Credentials** window, save the **Tenant URL** and **Secret Token** for use within Entra ID.

Microsoft Entra ID

5. Go to **Enterprise application** > **New application**.
6. Select **Create your own application**.
   a. Name the application with Provisioning in the title so that it can be easily located.
   b. Select the **Non-gallery** option.
7. Select **Properties** for the application.
   a. Toggle **Assignment Required** to **Yes**.
   b. Toggle **Visible to Users** to **No**.
   c. Select **Save**.
8. Select **Users and groups** and assign the User groups to included in Extreme Platform ONE Security.
9. Go to **Manage** > **Provisioning** and select **New configuration**.
   a. Under **Admin Credentials**, paste the **Tenant URL** and **Secret Token** that were previously copied from Extreme Platform ONE Security.
   b. Select **Test Connection** and on resulting success.
   c. Select **Create**.
10. On the **Attributes Mapping** page and complete the following:
    a. Select **Provision Microsoft Entra ID Users**.
    b. Under **Source Object Scope**, select **All records**.
    c. Select **Add new filter group**.
    d. In **Add Scoping Filter**, select **mail** as the source attribute.

Note
The mail attribute needs to exist for the user to be imported into Extreme Platform ONE Security. If the desire is to only have corporate email accounts imported into Extreme Platform ONE Security, matching on the email extension for the organization will work. For this example, select **INCLUDES** as the operator and the email domain as the clause value.

    e. Name the scoping filter and select **Apply**.
    f. In the resulting screens, select **Apply** and **Save** to save the filter to the provisioning profile.

11. Go to **Overview**, select **Start Provisioning** to begin the provisioning process.

Note
Provisioning can take up to an hour to start. If desired **Provision on Demand** can be selected from the **Provisioning Overview** to immediately start a provisioning cycle. Select the group or users to provision at that moment.

In Extreme Platform ONE Security the users and user groups should now be available in the **Policy** > **Users & Devices** > **Users** section. If the users or user groups do not show up, review errors or messages in Entra ID for why the provisioning failed.

Microsoft Entra ID | Network Access

If user-based 802.1X EAP-TTLS network authentication is going to be used with Microsoft Entra ID, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

Network Authentication requires that multi-factor authentication be disabled for an Entra ID application when using EAP-TTLS. If Entra ID premium is used, a rule can be created to exclude this only for the Network Access OIDC application. If Entra ID premium is not in use, this must be disabled for all users.

For more information on Conditional Access Policies, refer to Microsoft documentation here: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview Disable MFA using a conditional access policy for Entra ID.

For Network Access is configured in these steps:

1. Configure Microsoft Entra ID.
2. Configure Extreme Platform ONE Security.
3. Disable MFA using a conditional access policy for Entra ID.

Microsoft Entra ID

1. Go to **Applications** > **App registration** and select **New registration**.
2. Under **Register an application**, name the application appropriately for the Network Access Integration. Leave the default fields selected and select **Register**.
3. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.
4. Select **New client secret**.
   a. Enter a description if desired and a preferred expiration date of the secret.
   b. Once complete, select **Add**.
5. Copy the value of the new secret for use later.
6. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

Extreme Platform ONE Security

7. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
8. Select **Add IdP Profile** and configure the settings in Table 43.

Table 43: Entra ID IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Network Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Setup Guidelines	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret • Tenant ID

9. To complete the setup, select **Save**.

Disable MFA in Microsoft Entra ID

10. Go to **Manage** > **Properties** and configure the settings.
    a. Select **Manage Security defaults**.
    b. Disable the toggle **Disabled** and select **Save**.
11. Go to **Identity** > **Protection** > **Conditional Access** and configure the settings in Table 44.

Table 44: Conditional Access Configuration Settings

Field	Description
User ad groups	Select **All users**.
Cloud apps or actions	Under **Exclude** select the OIDC app created earlier in the **Select excluded cloud apps**.
Grant	Select **Grant access** and check **Require multi-factor authentication** and any other settings your organization requires.
Enable policy	Set to **On**.
Select **Create**.	

Microsoft Entra ID | Application Access

Application access for users can be authenticated via Microsoft Entra ID in two ways:

- OpenID Connect (OIDC)

1. Retrieve Redirect URI in Extreme Platform ONE Security.

2. Set up Microsoft Entra ID.
3. Configure Extreme Platform ONE Security.

- SAML

1. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
2. Configure Microsoft Entra ID.
3. Finalize in Extreme Platform ONE Security.

The setup process is different in Microsoft Entra ID depending on the type of integration being leveraged.

Application Access using Open ID Connect (OIDC)

1. Retrieve Redirect URI In Extreme Platform ONE Security.
   a. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
   b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 45.

Table 45: Entra ID Application Access OIDC IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Microsoft Entra ID** from the Identity Provider drop-down list.
Application Access	Select **OpenID Connect** from the Single Sign-On drop-down list.
Setup Redirect URIs	Copy the Redirect URI.

   c. Select **Cancel**.
2. Set up Microsoft Entra ID.
   a. Go to **Applications** > **App registration** and select **New registration**.
   b. Under **Register an application**.
      i. Name the application appropriately for the Application Access Integration.
      ii. Leave the default fields selected and select **Register**.
   c. Select **Add a Redirect URI**.
   d. Select **Add a platform** followed by **Web**.
   e. Enter one of the Redirect URIs that was previously copied from Extreme Platform ONE Security and select **Configure**.
   f. Select **Add URI**.
      i. Paste in the second Redirect URI that was copied from Extreme Platform ONE Security.
      ii. Select **Save**.

g. Copy the **Application (client) ID** and **Directory (tenant) ID** for use later. Under **Client Credentials**, select **Add a certificate or secret**.
h. Select **New client secret**.
   i. Enter a description if desired and a preferred expiration date of the secret.
   ii. Once complete, select **Add**.
   iii. Copy the value of the new secret for use later.
i. Go to **Manage** > **API permissions** and select **Grant admin consent for <Company Name>**.

3. Configure Extreme Platform ONE Security.
   a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.
   b. Select **Add IdP Profile** and configure the settings in Microsoft Entra ID | Application Access on page 104.

Table 46: Entra ID Application Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Microsoft Entra ID** from the **Identity Provider** drop-down list.
Secure Application Access	Under **Single Sign-On Method**, select **OpenID Connect**.
Setup Extreme Platform One Security	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret • Tenant ID

   c. To complete the setup, select **Save**.

Application Access using SAML

4. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
   a. In Extreme Platform ONE Security, go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
   b. To create a new profile, select **Add IdP Profile** and configure settings in Table 46 on page 106.

Table 47: Microsoft Entra ID SAML Preparation Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Microsoft Entra ID** from the Identity Provider drop-down list.

Table 47: Microsoft Entra ID SAML Preparation Configuration Settings (continued)

Field	Description
Single Sign-On Method	Select **SAML**.
Setup Up SSO in Microsoft Entra ID	Copy the Identifier and the Reply URL.

> **Note**
> Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Microsoft Entra ID application.

c. Select **Save**.

5. Configure Microsoft Entra ID.
   a. Go to **Enterprise application** > **New application**.
   b. Select **Create your own application**.
      i. Name the application so that it can be easily located.
      ii. Select the **Non-gallery** option.
   c. Go to **Manage** > **Single Sign-On** and select SAML.
   d. Under **Basic SAML Configuration** select **Edit**.
      i. Select **Add identifier** and paste in the Identifier from Extreme Platform ONE Security then select **Add reply URL** and paste in the **Reply URL** that was previously copied.
      ii. Select **Save**.
      iii. When prompted to test the integration, select **No, I'll test later**.
   e. Further down the SAML application, download the SAML Certificate in Base64 format. Copy the Login URL and the Microsoft Entra Identifier.
6. Finalize in Extreme Platform ONE Security.
   a. In the **Application Access IdP** screen that was left open, paste in the Login URL, the Microsoft Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

> **Note**
> If this page was canceled, the Identifier will need to be updated in the Microsoft Entra ID application.

Google Workspace | Synchronize Users and User Groups

User and User Group synchronization is performed using the Directory APIs in Google Workspace. They are retrieved on a polled basis from Extreme Platform ONE Security.

To synchronize user and user groups using Google Workspace:

1. Configure Google Cloud.
2. Configure in Google Admin Console.

3. Configure Extreme Platform ONE Security.
4. Adjust Security Defaults for Google Workspace.

Note
In cases where a newer Google Workspace or Google Cloud Platform instance was created, security defaults may be enabled so that the administrator cannot download keys for service accounts. If this is the case, use this task to adjust security defaults for Google Workspace.

Configure Google Workspace.

1. Log into Google Cloud via https://console.cloud.google.com.
2. To create a new project, from the drop-down menu at the top of the screen and select **New Project**.
   a. Name the project appropriately and select **Create**.
   b. Under **Quick Access**, select **APIs & Services**.
   c. Select **ENABLE APIS AND SERVICES**.
   d. In the search field, enter and select **Admin SDK API**.
   e. Select **ENABLE**.
3. Go to **APIS and SERVICES** > **Credentials**.
4. Select **CREATE CREDENTIALS** and from the drop-down select **Service account**.
   a. Enter a service account name to use for the syncing. Select **CREATE AND CONTINUE**, then leave the optional fields blank.
   b. Select **DONE**.
   c. Select the newly created service account. Copy the Email and Unique ID to be used in later steps and select **KEYS**.
5. From the **ADD KEY** drop-down menu, select **Create new key**.
   a. In the **Create Private Key** screen, select JSON as the key type and **CREATE**. This will download the private key to be used.

Note
If an error is received here due to a permissions issue, see <enter a link to the new security topic>. This restriction appears for newly created Google Cloud Accounts.

Google Admin Console Configuration

6. Log into Google Admin Console via https://admin.google.com.
7. Go to **Security** > **Access and data control** > **API controls** and select **MANAGE DOMAIN WIDE DELEGATION**.

8. Under **API clients**, select **Add new** and configure the settings in Table 48.

Table 48: API Client Configuration Settings

Field	Description
Client ID	Enter the Unique ID that was previously copied from the Service Account entry.
OAuth Scopes	https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group.member https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.user.alias

9. Select **AUTHORIZE**.
10. Go to **Account** > **Admin roles**.
    a. If no User and User Group with read privileges appears, select **Create role** and configure the settings in Table 49.

Table 49: Role Configuration Settings

Field		Description
Role Info	Name	Enter a group name.
	Description (Optional)	Enter a role description.
Select **CONTINUE**.		
Select Privileges	Users	Within this group select **Read**.
	Groups	
Select **CONTINUE**.		
Review Admin API Privileges	The review screen confirms that Read privileges are allowed for API calls for Users and Groups.	
Select **CREATE ROLE**.		

    b. If the role was just created, select Assign service accounts. If not, select **Assign role** > **Assign service accounts**.
    c. Enter the email of the service account, select **ADD** then **ASSIGN ROLE**.
11. Go to **Account** > **Account Settings** and copy the customer ID of Google Workspace.

Extreme Platform ONE Security Configuration

12. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

13. Select **Add IDP Profile** and configure the settings in Table 50.

Table 50: Google Workspace IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** from the Purpose drop-down list.
Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Google Workspace** from the **Identity Provider** drop-down list.
Sync Users and User Groups	Use this option to sync your Google Workspace users and user groups with Extreme Platform ONE Security. • Setup Guidelines - Upload the private key JSON file that was downloaded from Google Cloud Console and paste in the Customer ID that was saved from the Google Admin Console. • Customer ID - To get the Customer ID, go to the Google Admin Console, under **Account Settings**. • Select User Groups (Google Workspace Only) - Select group-specific APs and sync only those groups.The table retrieves all available groups. a. Select available groups and select the side arrow to them to the **Added** box. **Note:** There is no maximum for added groups. b. Select **Save**. c. To view synced users, go to **Policy** > **Users & Devices**, under **Users** and Google Workspace appears in the **Type** column. d. Under **User Groups**, from the 3-dot menu, select **Sync Now** to view new groups. e. To view the sync event details, go to **Administration & Settings** > **Logs**, select **Security Logs** from the drop-down menu.

Adjust Security Defaults for Google Workspace

14. Log into Google Cloud via https://console.cloud.google.com.
15. From the top left, if you are already in a project, select the parent project from the drop-down list.
16. Go to **IAM & Admin** > **IAM**.
17. Under **IAM**, ensure that your account has an Organization Policy Administrator. If it does not, select Edit (pencil icon) next to your account to edit the roles. If your account isn't listed here, to add it select **GRANT ACCESS** and configure settings:
    a. Within the **Edit** window, select **Add Another Role**.
    b. Select the **Organization Policy Administrator** condition from the drop-down list.
    c. Select **SAVE**.
18. Once the roles are set, go to **Organization Policies** > **IAM & Admin**.
19. In the Organization Policies, search for iam.disableServiceAccountKeyCreation. Select edit to make updates.

20.Select **MANAGE POLICY**.

21. Select **Override the parent's policy**. Then edit or create a rule to set the enforcement to **Off**. Finish by selecting the **SET POLICY**.

A successful configuration should look similar to the below screenshot. The creation and download of a private key for a service account should now be successful.

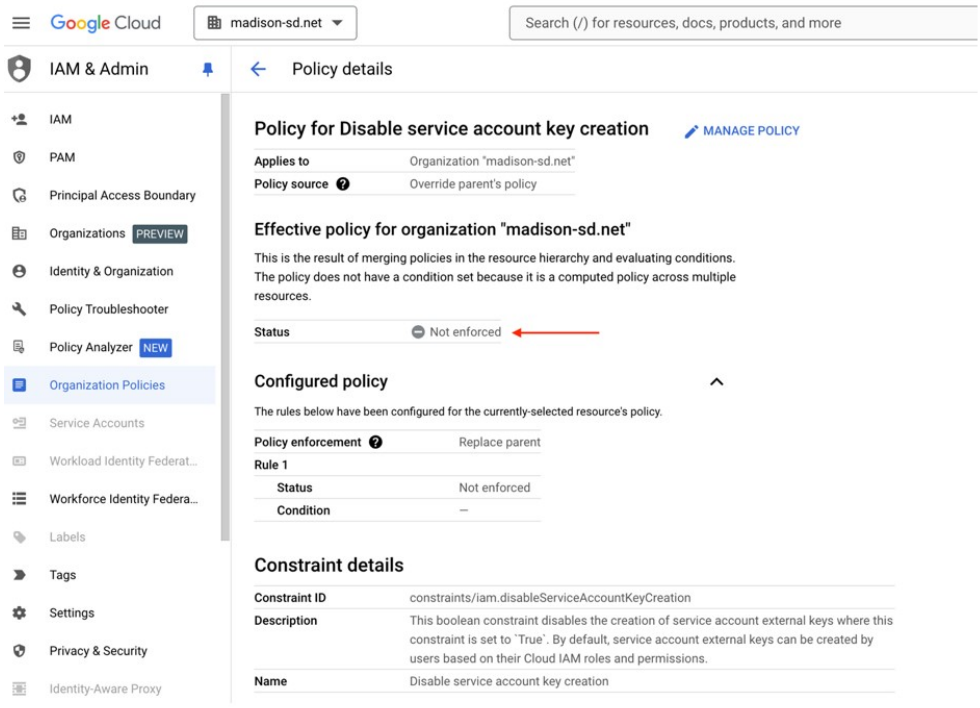


Figure 17: Successful Configuration

Google Workspace | Network Access

If user-based 802.1X EAP-TTLS network authentication is going to be used with Google Workspace, a secure LDAP integration must be created.

If EAP-TLS (Certificate-based authentication) is going to be the only source of 802.1X user and device authentication, this setup is not required.

To configure Google Workspace for Network Access:

1. Configure the Google Admin Console.
2. Configure Extreme Platform ONE Security.

Google Admin Console

1. Go to **Apps** select **LDAP**.

2. Select **Add Client** and configure the settings in Table 51.

Table 51: Client Configuration Settings

Section	Field	Description
Client Details	LDAP client name	Enter a client name.
Select **Continue**.		
Access permissions	Verify user credentials	Select **Entire domain**.
	Read user information	Select **Entire domain**.
Select **ADD LDAP CLIENT**.		

Once the certificate is done generating, download and save it for use in Extreme Platform ONE Security.

3. Select **Continue to Client Details**.
   a. By default, the LDAP client is not enabled. To enable it, select the drop-down list under **Service Status**.
   b. Select **ON for everyone**.

Extreme Platform ONE Security

4. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
5. Select **Add IDP Profile** and configure the settings in Table 52.

Table 52: Google Workspace Network Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Network Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Google Workspace** from the **Identity Provider** drop-down list.
Setup Extreme Platform ONE Security	Upload the saved Secure LDAP configuration from Google Admin Console.

6. To complete the setup, select **Save**.

Google Workspace | Application Access

For OIDC integration, the setup in Google Workspace will be completed first, followed by the configuration of Extreme Platform ONE Security. A Redirect URI will be needed from Extreme Platform ONE Security.

Application access for users can be authenticated via Google Workspace in two ways:

- Open ID Connect (OIDC)
  1. Retrieve Redirect URI in Extreme Platform ONE Security.
  2. Set up Google Workspace with Open ID Connect (OIDC) in Google Cloud (GCP).
  3. Configure Extreme Platform ONE Security.
- SAML
  1. Retrieve identifier and Reply URL in Extreme Platform ONE Security.
  2. Configure Google Admin Console.
  3. Finalize in Extreme Platform ONE Security.

Application Access using Open ID Connect (OIDC)

1. Retrieve Redirect URI In Extreme Platform ONE Security.
   a. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Users**.
   b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 45 on page 105.

Table 53: OIDC Application Access IdP Profile Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Google Workspace** from the Identity Provider drop-down list.
Application Access	Select **OpenID Connect** from the Single Sign-On drop-down list.
Setup Redirect URIs	Copy the Redirect URI.

   c. Select **Cancel**.
2. Set up Google Workspace.
   a. Log in to Google Cloud using https://console.cloud.google.com.
   b. To create a new project:
      i. From the drop-down menu at the top of the screen, select **NEW PROJECT**.
      ii. Enter a name in the **Project Name** field and select **CREATE**.
      iii. Select the newly created Project, then from the left navigation screen select **VIEW ALL PRODUCTS**.
      iv. Under the **All products**, select **Google Auth Platform**.
      v. Select **GET STARTED**.
      vi. In the **App Information** section, enter the App Name, select a User support email from the drop-down list then select **Next**.
      vii. In the **Audience** section, select **Internal** and then select **Next**.

viii. Under **Contact Information**, enter an email address and select **NEXT**.

ix. Finally, agree to the User Data Policy and select **CREATE**.

c. Go to **Overview**, select **CREATE OAUTH CLIENT** and configure the settings in Table 54.

Table 54: OAuth Client Configuration Settings

Section	Field	Description
CREATE OAuth client ID	Application Type	Select **Web application** from the drop-down list.
	Name	Name the OAuth client.
Authorized redirect URIs	URIs 1	Create two entries and paste the two Redirect URIs that were previously copied from Extreme Platform ONE Security.
	URIs 2	
Select **Create**.		

d. Under **OAuth 2.0 Client IDs**, select the newly created client.

e. Under **Additional information**, copy the **Client ID** and **Client secret**.

3. Configure Extreme Platform ONE Security.

a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.

b. Select **Add IdP Profile** and configure the settings in Table 55.

Table 55: Google Workspace Application Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Google Workspace** from the **Identity Provider** drop-down list.
Secure Application Access	Under **Single Sign-On Method**, select **OpenID Connect**.
Setup Extreme Platform One Security	Paste the copied credentials from Microsoft Entra ID: • Client ID • Client Secret

c. To complete the setup, select **Save**.

Application Access using SAML

4. Retrieve identifier and Reply URL in Extreme Platform ONE Security.

a. In Extreme Platform ONE Security, go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 56.

Table 56: SAML IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Google Workspace** from the Identity Provider drop-down list.
Single Sign-On Method	Select **SAML**.
Setup Up SSO in Microsoft Entra ID	Copy the Identifier and the Reply URL.

Note
Leave this page open. If it is canceled, the Identifier will change, and this will need to be updated in the Google Workspace application.

c. Select **Save**.

5. Configure Google Admin Console.
   a. Log into the Google Admin Console and go to **Apps** > **Web and mobile apps**.
   b. From the **Add app** drop-down list, select **Add custom SAML app** and configure the settings in Table 57.

Table 57: SAML Application Access Configuration Settings

Section	Field	Description
App details	App name	Name the App.
Select **Continue**.		
Google Identity Provider Details	SSO URL	Under **Option 2** copy the SSO URL and Entity ID.
	Entity ID	
	Certificate	Download certificate.
Select **Continue**.		
Service provider details	ACS URL	Paste in the **ACS URL** and **Entity ID** that was previously copied from Extreme Platform ONE Security.
	Entity ID	
Name ID	Name ID format	Set the **Name ID format** to **EMAIL**.
	Name ID	Set the **Name ID** to **Basic Information** > **Primary email**.
Select **Continue**.		

Table 57: SAML Application Access Configuration Settings (continued)

Section	Field	Description
Attribute Mapping	Select **ADD MAPPING**.	
	First name	Enter **first_name**.
	Last name	Enter **last_name**.
	Primary email	Enter **email**.
Select **FINISH**.		

6. Finalize in Extreme Platform ONE Security.
   a. In the **Application Access IdP** screen that was left open, paste in the SSO URL, the Entity ID Identifier, and upload the certificate that was downloaded. Select **Save**.

   Note
   If this page was canceled, the Identifier will need to be updated in the Google Workspace application.

Okta | JIT Synchronize Users and User Groups

This method has Extreme Platform ONE Security reach into Okta and pull users and user groups on a polled basis. This method leverages an OIDC application to integrate with the Okta APIs.

JIT integration is configured in these steps:

1. Configure Okta Administrator Portal.
2. Configure Extreme Platform ONE Security.

Note
Synced User cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

Okta Administrator Portal

1. Go to the **Applications** > **API Service Integrations**.
2. Select **Add Integration**.
3. From the list, select **Extreme Platform ONE Security API Service**, then select **Install and Authorize**.

   The following API scopes are automatically applied:

   - `okta.users.manage`
   - `okta.apps.manage`
   - `okta.groups.manage`

4. To copy the Client Secret, when prompted, select **Copy to clipboard**.

> **Note**
> The Client Secret is only shown once. Ensure it is copied and stored securely.

5. Select **Done**.
6. Copy and securely store the following:
   - Okta Org Domain (without the https prefix. e.g. trial-4343365.okta.com)
   - API Service Client ID
7. Under **Assignments**, locate and copy the Client ID of the OIDC application you wish to sync users and groups.

> **Note**
> Reference the image below oktauser@tempmail.com is assigned to OIDC App which will be synced after successful setup.

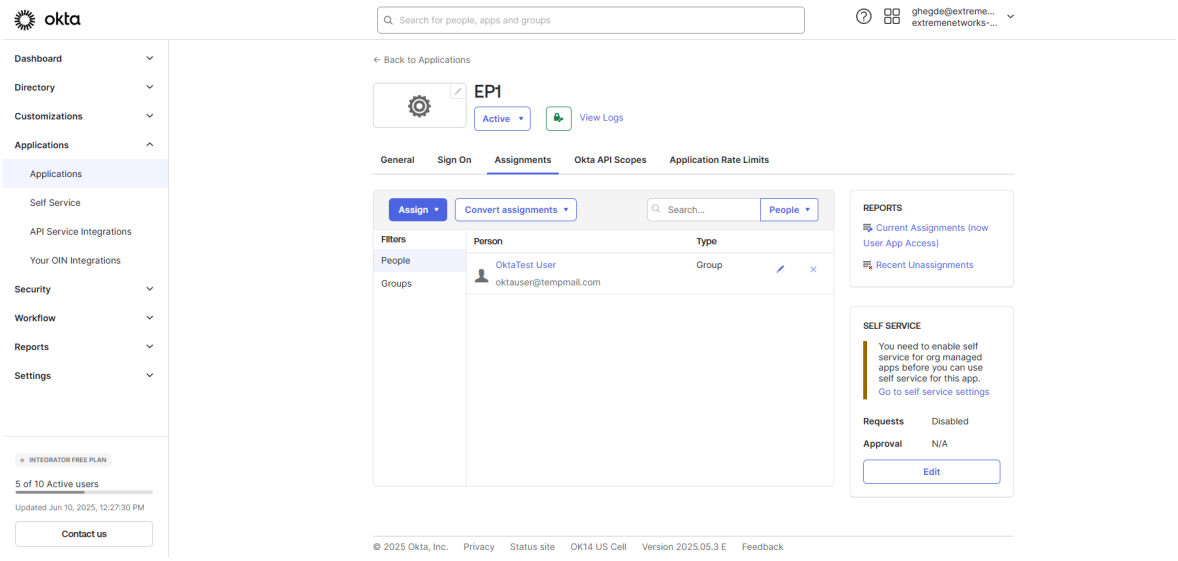


Figure 18: Assign Users and Groups

Extreme Platform ONE Security

8. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
9. Select **Add IdP Profile** and configure the settings in Table 58.

Table 58: JIT IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**

Table 58: JIT IdP Profile Configuration Settings (continued)

Field	Description
Select Identity Provider	Select **Okta** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **JIT (Just in Time)** for the **Sync Using** drop-down list.
	Paste the copied credentials from Okta: • API Service Client ID • API Service Client Secret Key • Application Access Client ID • Org Domain

10. To complete the setup, select **Save**.

A dynamic sync workflow will be schedule automatically. To view synced users and groups, go to **Policy** > **Users & Devices**.

Okta | SCIM Synchronize Users and User Groups

This method has Okta push users and user groups from Okta into Extreme Platform ONE Security. This method requires an enterprise application to be set up in Okta so that automatic provisioning can be enabled.

SCIM integration is configured in these steps:

1. Configure Extreme Platform ONE Security.
2. Configure System for Cross-Domain Identity Management (SCIM) in Okta.

Note
Synced User cannot be removed from Extreme Platform ONE Security. It must be removed from the Identity Provider and then a syncing cycle should be initiated again.

Extreme Platform ONE Security

1. Go to **Access Management** > **Administration & Settings** > **Identity Providers** and select **Network & Applications**.
2. To create a new profile, select the **Add IdP Profile** and configure the settings in Table 59.

Table 59: Okta SCIM IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Sync Users and User Groups** as the **Purpose** from the drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**.

Table 59: Okta SCIM IdP Profile Configuration Settings (continued)

Field	Description
Select Identity Provider	Select **Okta** from the **Identity Provider** drop-down list.
Setup Guidelines	Select **SCIM (System for Cross-domain Identity Management)** for the **Sync Using** drop-down list.

3. Select **Save**.
4. Once saved, from the 3-dot menu, select **Edit**.
5. In the **Edit** window, select **Okta Syncing Credentials**.
6. In the **Okta Syncing Credentials** window, save the **Tenant URL** and **Secret Token** for use within Okta.

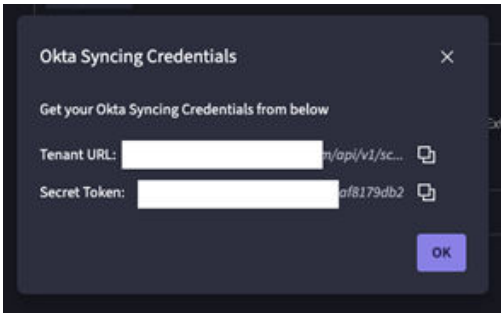


Figure 19: Okta Syncing Credentials

Okta Administrator Portal

7. Go to the **Applications** > **Browse App Catalog**.

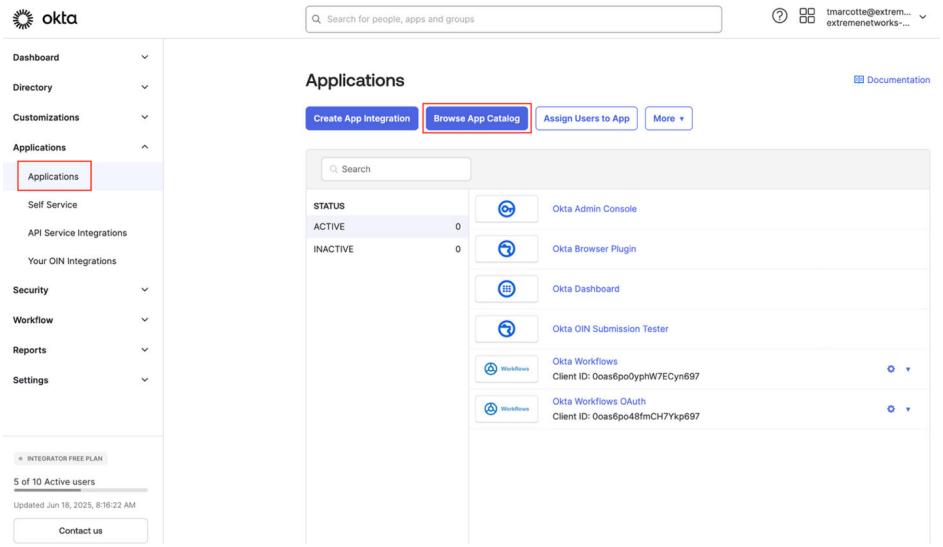


Figure 20: Applications Menu

8. In the search field, enter and select **(OAuth Bearer Token) Governance with SCIM 2.0**.
9. Select **Add Integration**.

10. On the **General Settings** tab, in the **Application label** field, enter **Extreme Platform ONE Security - SCIM** and select **Next**.
11. On the **Sign-On Options** tab, scroll to the bottom and select **Done**. No additional information needs to be added for the SCIM integration.
12. In the new application, select the **Provisioning** > **Configure API Integration** and configure the settings in Table 60.

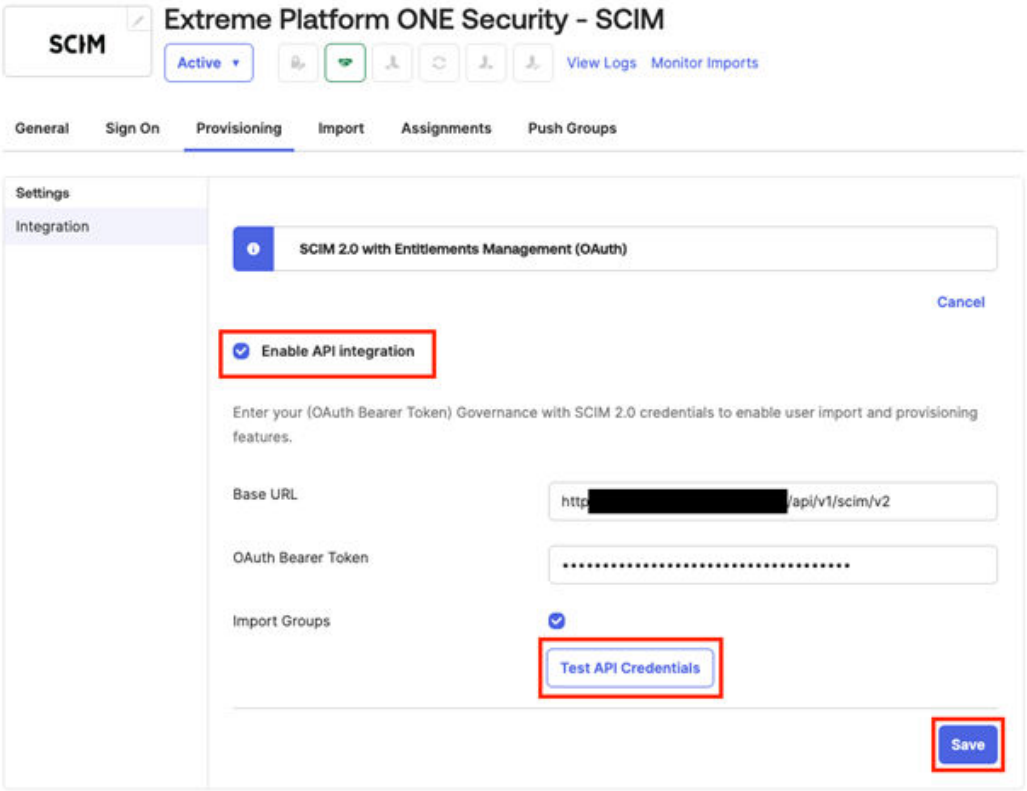


Table 60: API Integration Configuration Settings

Field	Description
Enable API Integration	Select this option.
Base URL	Paste in the Tenant URL that was saved from Extreme Platform ONE Security.
OAuth Bearer Token	Paste the Secret Token that was saved from Extreme Platform ONE Security.

13. Select **Test API Credentials**.

Note
If the credentials do not verify successfully, ensure there are not typos in the Tenant URL or Secret Token from the **IdP Profile** entry in Extreme Platform ONE Security.

14. Upon successful verification, select **Save** and configure the settings in Table 61.

Table 61: API Configuration Settings

Field	Description
Create Users	Enable this option.
Update User Attributes	Enable this option.
Deactivate Users	Enable this option.

15. Select **Save**.
16. Go to **Assignments** > **Assign** and select **Assign to Groups** from the drop-down list.
17. Select **Assign** next to the groups that should be included with the synchronization into Extreme Platform ONE Security.

Note
When assigning groups, do not change any defaults. Once you have selected the assign option, when prompted select **Save and Go Back**.

18. On the **Push Groups** tab, from the **Push Groups** drop-down list, select **Find groups by name**.
19. In the **Search** field enter the name of the group and select **Save** or **Save & Add Another** to add multiple. Repeat this action for each group that should be synchronized with Extreme Platform ONE Security.
20. To view or change the status of the groups, go to the **Push Groups** tab. To force a push, select **Active** and select **Push now** from the drop-down list.

The users and user groups are now available in Extreme Platform ONE Security under **Policy** > **Users & Devices** > **Users**. If the user or group is not displayed, review errors or messages in Okta for the push failed description.

Okta | Network Access

Use this task to configure Extreme Platform ONE Security.

If user-based 802.1X EAP-TTLS network authentication is going to be used with Okta, a separate application is required to be created that bypasses MFA as 802.1X does not have a native method to provide real-time multi-factor authentication prompt. This can only be done with an OpenID Connect (OIDC) Application.

To configure Okta for Network Access:

1. Configure Okta Open ID Connect (OIDC).
2. Configure Extreme Platform ONE Security.

Okta OIDC

1. In the **Create a new app integration** window select **OIDC – OpenID Connect** as the sign-in method. For Application type select **Native Application** and then **Next**.
   a. In **New Native App Integration** window, name the application appropriately.
   b. Under **Grant Type** select **Advanced**.

c. Under **Other Grants** select **Resource Owner Password**.
d. Within the redirect URI sections maintain default settings.
e. Under **Assignments**, if there is a preference it can be used, however access is granted based on the policies in Extreme Platform ONE Security.
f. If there is no preference, under **Controlled access** select **Allow everyone in your organization to access**.
g. Leave the checkbox for **Enable immediate access with Federation Broker Mode** enabled.
h. Select **Save**.

2. Under **General**, under **Client Authentication** select **Client secret**.
   a. Select **Require PKCE as additional verification**.
   b. Select **Save**.
3. To create a password-only authentication policy in Okta that is attached to this new application, go to **Security** > **Authentication Policies** and select **Add a policy**.
   a. In the **Add Authentication Policy** window, enter a policy name and description.
   b. Select **Save**.
4. Within the Password-Only authentication policy, under **Catch-all Rule** select **Edit** from the **Actions** drop-down list.
5. Within the **IF** section maintain default settings. Under **THEN** update the **User must authenticate with** to **1 factor type - Password** from the drop-down list and select **Save**.

   Once saved, the Authentication Policy should look similar to below:

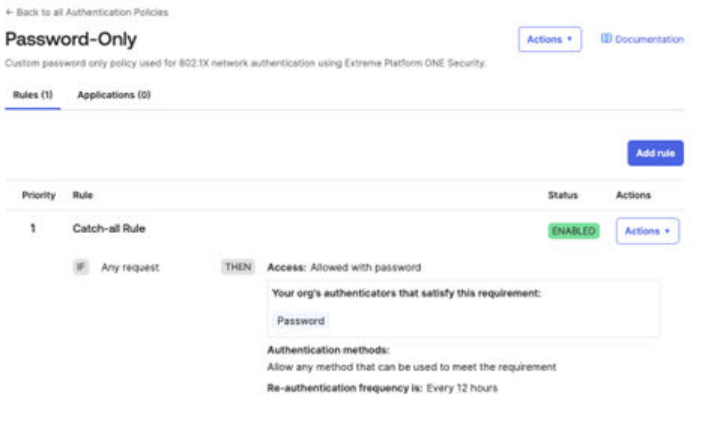


Figure 21: Authentication Policy

6. Go to **Applications**, select the Network Access Application previously created and do the following:
   a. Under **Sign One** > **User authentication** select **Password-Only** from the **Authentication policy** drop-down list.
   b. Select **Save**.
   c. Under **General** copy the generated Client ID and Client Secret.

7. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.

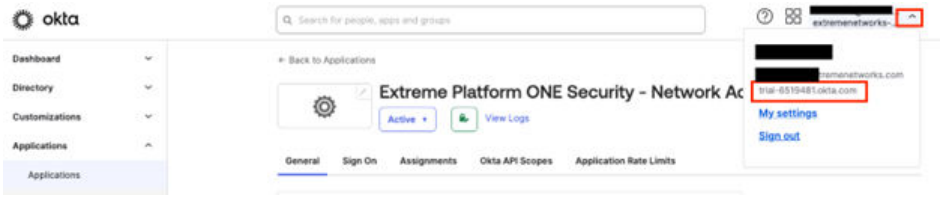


Figure 22: Tenant Name

Extreme Platform ONE Security

8. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
9. To create a new profile, select **Add IdP Profile** and configure the settings in Table 59 on page 118.

Table 62: Okta OIDC IdP Profile Configuration Settings

Field	Description	
Set Up IdP	Select **Network Access** from the Purpose drop-down list.	
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.	
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.	
Set Up Extreme Platform ONE Security	Client ID	Paste in the Client ID, Client Secret, and Tenant ID previously copied in Okta.
	Client Secret	
	Org Domain	

10. Select **Save**.

Okta | Application Access

Application access for users can be authenticated via Microsoft Entra ID in two ways:

- Open ID Connect (OIDC)
  1. Retrieve Redirect URI in Extreme Platform ONE Security.
  2. Set up Okta Administrator Portal.
  3. Configure Extreme Platform ONE Security.
- SAML
  1. Configure Okta.
  2. Configure in Extreme Platform ONE Security.

The setup process is different in Okta depending on the type of integration being leveraged.

Application Access using Open ID Connect (OIDC)

1. Retrieve Redirect URI In Extreme Platform ONE Security.
   a. Go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
   b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 63.

Table 63: Okta OIDC Application Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.
Application Access	Select **OpenID Connect** from the Single Sign-On drop-down list.
Setup Redirect URIs	Copy the Redirect URI.

   c. Select **Cancel**.
2. Set up Okta Administrator Portal.
   a. Go to **Applications** then select **Create App Integration** and configure the settings. In the resulting window, select OIDC – OpenID Connect as the sign-in method. For **Application type** select **Web Application** and then **Next** and configure the settings in Table 64.

Table 64: Web Application Configuration Settings

Field	Description
Sign-in method	Select **OIDC – OpenID Connect**.
Application Type	Select **Web Application**.

   b. Select **Next**.
   c. In the **New Web App Integration** window, enter a new integration name in the the **App Integration name** field and select **Client Credentials** under **Grant Type**.
   d. Under **Sign-in redirect URIs**, paste the redirect URI saved when starting to create the application in Extreme Platform ONE Security.
   e. Leave the **Sign-out redirect URIs** and **Trusted Origins** to their defaults or clear them as they are not needed.
   f. Under **Assignments** if there is a preference it can be used, however access is granted based on the policies in Extreme Platform ONE Security. If there is no preference, select the **Allow everyone in your organization to access** option under **Controlled access**. Disable the checkbox for Enable immediate access. Select Save.
   g. Disable the checkbox for **Enable immediate access with Federation Broker Mode** and select **Save**.

h. Under the **General** tab, copy the generated Client ID and Client Secret.
i. If the Org Domain of the Okta tenant is required, select **Profile** and copy the tenant name.

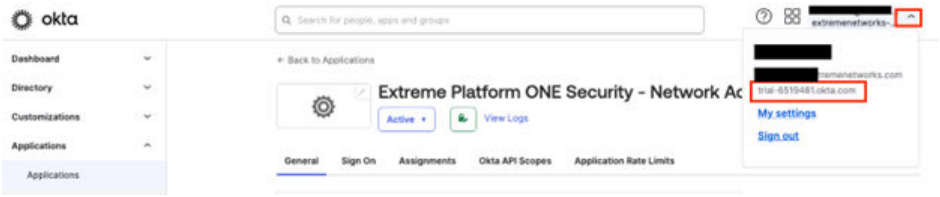


Figure 23: Tenant Name

3. Configure Extreme Platform ONE Security for OIDC.
   a. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Application**.
   b. Select **Add IdP Profile** and configure the settings in Table 65.

Table 65: Entra ID Application Access IdP Profile Configuration Settings

Field	Description
Set Up IdP	Select **Application Access** from the Purpose drop-down list.
Approved Domains	If the domain needs to be limited, it can be selected here with the **Custom** toggle, otherwise leave it to **All Domains**
Select Identity Provider	Select **Okta** from the **Identity Provider** drop-down list.
Secure Application Access	Under **Single Sign-On Method**, select **OpenID Connect**.
Setup Extreme Platform One Security	Paste the copied credentials from Okta: • Client ID • Client Secret • Tenant ID

   c. To complete the setup, select **Save**.

SAML

4. Configure the Okta Administrator Portal for SAML.
   a. Go to the **Applications** then select **Browse App Catalog**.
   b. Search for **(OAuth Bearer Token) Governance with SCIM 2.0**. Select the app, then **Add Integration**.
   c. Under **Application label** enter **Extreme Platform ONE Security – SAML** and select **Next**.

d. Under **Sign On Options**, expand the Attributes under SAML 2.0 and configure the settings in Table 66.

Table 66: SAML 2.0 Configuration Settings

Field	Description
First Name	user.firstName
Last Name	user.lastName
Email	user.email
UserName	user.username

e. Under **SAML 2.0**:

i. Expand **Metadata details**.

ii. Copy the Sign on URL and the Issuer for use in Extreme Platform ONE Security.

iii. Download the Signing Certificate.

iv. Under **Advanced Sign-on**, paste the copied Reply URL Advanced Sign-on Settings section, paste the Reply URL previously copied from Extreme Platform ONE Security into the ACS URL field and the Identifier previous copied into Audience URI field.

v. Select **Done**.

f. Under **Assignments**, select **Assign to Groups** from the Assign drop-down list.

g. Select specific users or groups and select **Done**.

All users are now displayed as assigned to the application.

5. Configure in Extreme Platform ONE Security for SAML.

a. In Extreme Platform ONE Security, go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.

b. To create a new profile, select **Add IdP Profile** and configure the settings in Table 67.

Table 67: SAML for Okta Configuration Settings

Field	Description	
Set Up IdP	Select **Application Access** from the Purpose drop-down list.	
Approved Domain	If the domain needs to be limited, it can be selected here, otherwise leave it to **All Domains**.	
Select Identity Provider	Select **Okta** from the Identity Provider drop-down list.	
Single Sign-On Method	Select **SAML**.	
Setup Extreme Platform ONE Security	Login URL	Paste in the Sign On URL in Okta.
	Okta Identifier	Paste in the Issuer from Okta.

c. Select **Save**.

IdP Network & Applications | Support Multiple IdPs

Use this task to support and prioritize multiple IdP with a single tenant.

1. Log into your Extreme Platform ONE Security tenant.
2. Go to **Administration and Settings** > **Access Management** > **Identity Providers** > **Network & Applications**.
3. To prioritize IdPs, select and drag the IdPs in the correct order or the checkbox next to an Idp and from the select and select **Move to the top** or **Move to the bottom** from the drop-down list.
4. In the IdP Priority popup message, select **Save**.

Identity Providers | Management

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 Extreme Platform ONE Security 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.

The following IdPs are supported by Extreme Platform ONE Security:

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

From **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**, you can perfom the following actions:

- Add an IdP profile to your network. See Add an Identity Provider Profile on page 128.
- Locate the IdP profile from the list, select from the corresponding row, and then select one of the following actions:
  - **Edit**: Manage an existing IdP profile. Configure IdP Profile Settings, and then select **Save Changes**.
  - **Disable**: Disable an existing IdP profile. Select **Disable** a second time to confirm.

  Note
  Disabling an IdP profile will make it temporarily inactive.

- **Enable**: Enable an existing IdP profile.
- **Delete**: Delete an existing IdP profile. Select **Delete** a second time to confirm.

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

Note
As a prerequisite to adding an IdP to Extreme Platform ONE Networking, you must configure your IdP before you begin.

Add an Identity Provider Profile

You add an identity provider profile to begin the workflow that integrates an IdP with your application to enable single sign-on (SSO) authentication for your Extreme Platform ONE Security users. SSO authentication can be used with both IdP- and SP-initiated SSO.

Important
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 this task to add an IdP profile to your network.

1. Go to **Administration & Settings** > **Access Management**, and then select **Identity Providers**.
2. Select **+ Add IdP Profile**.
3. Select an IdP **Provider**, and then select **Next**.
4. Configure the following **IdP Profile Information**, and then select **Next**:
   - **Domain**: Enter a fully qualified domain name (FQDN) based on the identity provider you selected in the preceding step.
   - **Description** (optional): Enter a description of up to 64 characters.
5. Configure IdP Connection Metadata, and then select **Next**.
6. Map User Profile Attributes, and then select **Save**.
7. Export/Import SP Connections on page 133, and then select **Done** to save the IdP profile.

Related Links

Integrating with Microsoft Entra ID on page 136

Integrating with Okta on page 141

Configure IdP Connection Metadata

Identity Provider (IdP) Metadata provides structured information that is used to configure and establish a connection between an IdP and a Service Provider (SP) in

a SAML (Security Assertion Markup Language) environment. This metadata includes details such as the following:

- **IdP Entity ID**: A unique identifier for an IdP used to identify the IdP to an SP.
- **SSO URLs**: Endpoints where the SP sends authentication requests.
- **Binding Methods**: Methods for communication between the IdP and SP.
- **Certificates**: Used for signing and encrypting SAML assertions.

Important
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.

Metadata can be provided as a file (Import Metadata), as URL (Import from URL), or you can Enter Metadata Manually.

Import Metadata

1. Select **Import From Metadata**.
2. Select **Browse Files**, then select the metadata file from your local folder.
3. Configure any missing settings that are specific to the selected IdP. For more information, see IDP Metadata Settings Descriptions.
4. Click **Next** to map user profile attributes.

Note
If there is a problem uploading your file, check the file format and then try again. For further assistance, reach out to the Support Center.

Import from URL

1. Select **Import From URL**.
2. Type or paste an **IdP Metadata URL**, and then select **Import**.

Note
If the import was not successful, clear the URL and try again.

3. Configure any missing settings that are specific to the selected IdP. For more information, see IDP Metadata Settings Descriptions.
4. Click **Next** to map user profile attributes.

Enter Metadata Manually

1. Select **Manually Enter**.
2. Configure the IdP metadata settings that are described in IDP Metadata Settings Descriptions.

3. Click **Next** to map user profile attributes.

Table 68: IDP Metadata Settings Descriptions

Setting	Description
IdP Entity ID	The IdP unique identifier URL. URLs must begin with `https`.
SSO Binding	Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request.
SSO URL	The endpoint where SSO authentication requests are sent. URLs must begin with `https`.
SSO Request	Select **SSO Request** to enhance SSO security. By signing the SSO request, you ensure its authenticity and integrity, confirming that it has not been tampered with.
SLO Binding	Single Logout (SLO) allows users to sign out from multiple applications or services with a single action. Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request.
SLO URL	The endpoint where logout requests are sent to start the SLO process. This URL ensures that when a user logs out from one service, they are also logged out from all connected services. URLs must begin with `https`.
SLO Response URL	The endpoint where the Service Provider (SP) sends logout response messages after receiving a logout request from the IdP. This URL is used to confirm the completion of the SLO process. URLs must begin with `https`.
Verification Certificate	The digital certificate used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. Select an existing certificate from the drop-down list, or Import a new certificate.

Import Verification Certificates

1. Select **Import Certificates**.
2. Drag and drop the certificate or browse to upload it to the **Verification Certificates** area.
3. Click **Next**.

Related Links

Add an Identity Provider Profile on page 128

Map User Profile Attributes

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 Extreme Platform ONE Security workflow is completed. You must complete the Extreme Platform ONE Security workflow first. If you do not know the SAML Attribute Strings, add place holder data to save and complete the configuration.

Use this task to map user profile attributes to SAML profile attributes when you add a new IdP profile.

Important
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.

1. 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.

2. (Optional) To add a new group mapping, select **+ Add a Group Mapping** and configure the settings in Table 69. Repeat this step to add as many group mappings as needed.

Table 69: Group Mapping Settings

Field	Description
IdP Group	The IdP group name.
Primary Role Classic Role	Select the **Primary Role** for this group from the list. The corresponding **Classic Role** populates based on the selected primary role. **Note:** Hover over ⓘ for information about access and access limitations for each role type. The **Primary Role** determines the scope of access for the group.
Sites	Assign site access for the group: • To give the group access to all sites, toggle the setting to **All**. **Note:** When the primary role is set to Administrator, **Sites** is set to **All** by default and cannot be modified. • To give the group access to specific sites, from the sites drop-down list, select one or more sites from the tree menu, and then select **Done**. **Note:** This feature is only available if the VIQ has created sites. If no sites have been created within the VIQ, the default VIQ site is assigned to the IdP group.
• Select 🗑 to delete a group map. • Select ⋮⋮ and drag the row to reorder the group mappings. The first group that the user matches the rule, in the order, the process stops. Rules are enforced top down. Once a user is in the first group in a rule, the remaining groups in that rule are ignored for that user.	

3. When there is no available group map, select one of the following options to define Extreme Platform ONE Security behavior:
   a. **Deny user login**: Restrict user login access.
   b. **Allow user login and assign a default role and sites**: Assign user roles and site access permissions. See Group Map Settings.
4. Select **Save** to Export/Import SP Connections on page 133.

Related Links

Add an Identity Provider Profile on page 128

Export/Import SP Connections

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

Important
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 this task to export or import SP connections.

1. Obtain SP connection information:
   - Select **Download SP Metadata** for IdPs that support Metadata files.
   - To manually add SP metadata into the IdP, copy the URL to your clipboard, and then paste it into your IdP. Repeat this process for each URL.
   - Select **Download Signing Certificate** to acquire the signing certificate.
2. Select **Done**.

Related Links

Add an Identity Provider Profile on page 128

Manage IdP Profile Settings

Field	Description
Purpose	Defines the purpose of the IdP within your network.
Last Updated	Indicates the last time the IdP profile was updated.
Configuration Status	The configuration status of the IdP profile.
Disable	Select to disable the IdP profile. Select **Disable** a second time to confirm. **Note:** Disabling an IdP profile will make it temporarily inactive.
Enable	Select to enable the IdP profile.
Delete	Select to delete the IdP profile. Select **Delete** a second time to confirm. **Note:** Deleting an IdP profile permanently removes it from the system.

IdP Profile Information

Field	Description
Domain	The domain used by the IdP to manage and authenticate user identities.
Description	A brief summary of the IdP profile.

IdP Connection

Field	Description
IdP Entity ID	The IdP unique identifier URL. URLs must begin with `https`.
SSO Request	Select **SSO Request** to enhance SSO security. By signing the SSO request, you ensure its authenticity and integrity, confirming that it has not been tampered with.
SSO Binding	Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request. Data is visible in the URL and is limited by the maximum URL length supported by browsers and servers.
SSO URL	The endpoint where SSO authentication requests are sent. URLs must begin with `https`.
SLO Binding	Single Logout (SLO) allows users to sign out from multiple applications or services with a single action. Select **HTTP POST** to send messages within the body of an HTTP POST request. Select **HTTP Redirect** to send encoded messages as query parameters in the URL of an HTTP GET request.
SLO URL	The endpoint where logout requests are sent to start the SLO process. This URL ensures that when a user logs out from one service, they are also logged out from all connected services. URLs must begin with `https`.
SLO Response URL	The endpoint where the Service Provider (SP) sends logout response messages after receiving a logout request from the IdP. This URL is used to confirm the completion of the SLO process. URLs must begin with `https`.
Verification Certificates	The digital certificates used to verify the authenticity and integrity of messages exchanged between the IdP and SPs. Select **Show Certificates** to view valid certificates. To update the verification certificates for this IdP profile, select **Manage Certificates**. For more information, see Manage IdP Profile Certificates.

Attribute Mapping

Field	Description
First Name	The URL or endpoint where the IdP provides the user's given name.
Last Name	The URL or endpoint where the IdP provides the user's family name or surname.
Email	The URL or endpoint where the IdP provides the user's email address.
Group	The URL or endpoint where the IdP provides the user's group memberships.
Group Mapping	Specifies how group names from the IdP are translated, or mapped, to the corresponding group names in Extreme Platform ONE Security: • Select **Add a Group Mapping** to add a new group map row. • Select the **IdP Group**, **Primary Role**, **Classic Role**, and **Site(s)** for each group name map. For more information, see Group Map Settings. • Select to delete a group map. • Select and drag the row to reorder the group mappings. The first group that the user matches the rule, in the order, the process stops. Rules are enforced top down. Once a user is in the first group in a rule, the remaining groups in that rule are ignored for that user. Determine what action Extreme Platform ONE Security should take when there is no available group map: • **Deny User Login**: Restrict user login access. • **Allow user login and assign a default user group**: Assign user roles and site access permissions. For more information, see Group Map Settings.

Extreme Cloud(SP) Connection

To obtain SP connection information:

- Select **Download SP Metadata** for IdPs that support Metadata files.
- To manually add SP metadata into the IdP, copy the URL to your clipboard, and then paste it into your IdP. Repeat this process for each URL.
- Select **Download Signing Certificate** to acquire the signing certificate.

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.

Use this task to ensure your IdP profile certificates are correctly configured and up-to-date.

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

4. Select **Certificates for** the IdP you selected to return to the **Management** IdP profile list.

Integrating with 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 the 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:

   Important
   User groups must be created in the IdP before you can map the user roles in Extreme Platform ONE Security.

   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 Extreme Platform ONE Security required user group.

c. Select the check box for each Extreme Platform ONE Security required user group, and then click **Select**.

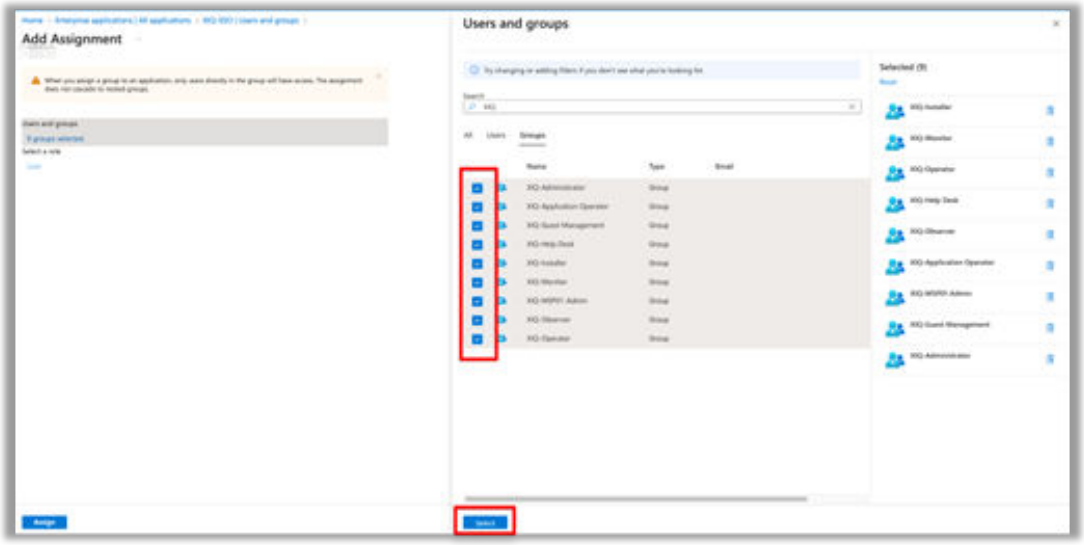


Figure 24: Azure - Assigning Extreme Platform ONE Security User Groups to an Azure User Role

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 Extreme Platform ONE Security.

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 Extreme Platform ONE Networking:

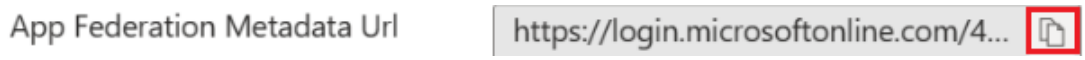
   To see Identity Provider (IdP) profile settings, log in to Extreme Platform ONE Security using the Global Data Center (GDC) SSO URL. For example, `https://extremeplatformone.com`.

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

   a. From *Extreme Platform ONE Security*, go to **Administration & Settings** > **Access Management** > **Identity Providers** > **Management**.
   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.

   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 *Extreme Platform ONE Security*, 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 Extreme Platform ONE Networking User Profile Attributes to SAML Attributes for Entra ID:

   In *Extreme Platform ONE Security*, you must map the appropriate **User Profile Attributes** to the **SAML Attributes** sent from the IdP. For more information, see Map User Profile Attributes on page 131.

Table 70 includes the required strings for integration with Entra ID.

Table 70: Extreme Platform ONE Security- Required Strings for Microsoft Entra

User Profile Attribute	SAML Attribute
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 Extreme Platform ONE Networking Group to Roles for Entra ID:

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

   In Extreme Platform ONE Security, enter the exact **IdP Group** name from Entra ID (for example, EP1-Operator), and then select the corresponding role. For more information, see Add a Group Mapping.

   Important
   The Operator, Monitor, Help Desk, Installer, or Observer RBAC roles require the definition of one or more sites to gain visibility over managed devices. In the rule definition for those roles, specify one or more sites in the rules. Failure to do so will lead to the administrator being unable to view any devices after login. Administrator and Guest Management roles do not leverage sites, and will ignore any site definition in the rule.

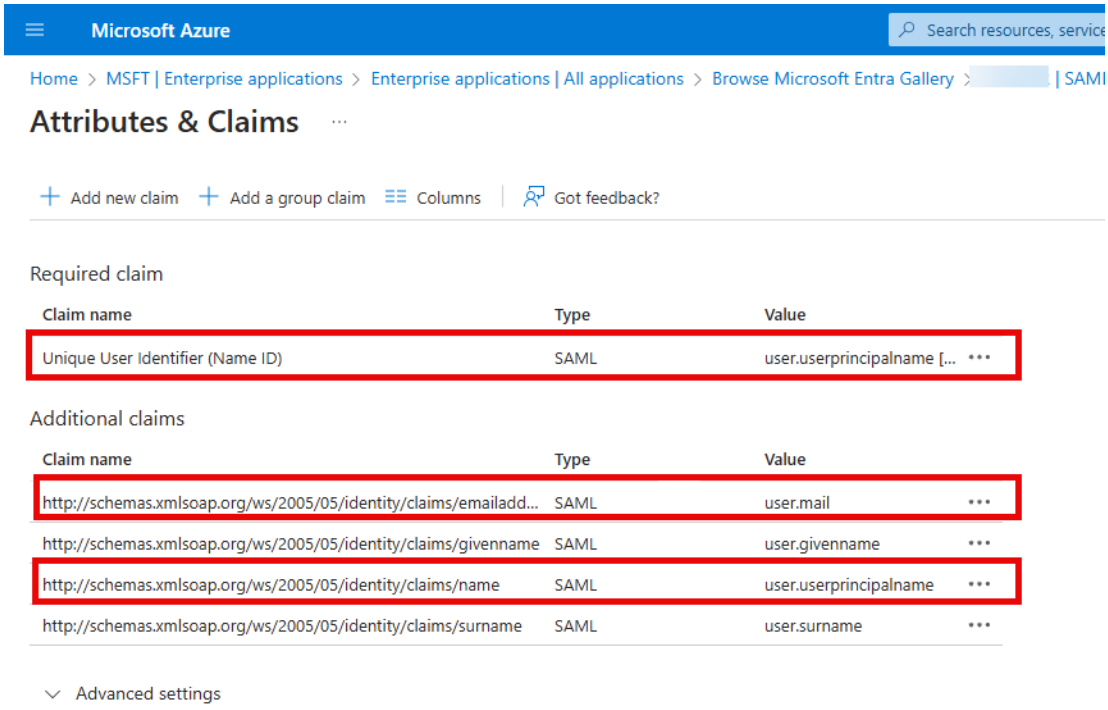
7. Export SP Metadata and Import into Entra ID:
   a. After saving the completed **Add IdP Workflow** in *Extreme Platform ONE Security*, download the SP metadata. For more information, see Export/Import SP Connections on page 133.
   b. In the *Microsoft Azure* application, on the **SAML-based Sign-on** page, select **Upload metadata file**, navigate to the saved exported file from Extreme Platform ONE Security, 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**.

8. Map Entra ID Security Groups to Extreme Platform ONE Networking Roles:

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

   a. In the *Microsoft Azure* application, in Section 2: **Attributes & Claims**, select **Edit**.
   b. Under **Additional Claims**, perform the following steps to adjust the default claims:
      i. Select the **Unique User Identifier (Name ID)** row, change the **Value** field to `user.mail`, and then select **Save**.
      ii. In the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** row, select ••• , and then select **Delete**.
      iii. Select the **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name** row, change the **Name** field to `email`, and then select **Save**.



   c. To add a group claim, from the Attributes and Claims page, select **Add a group claim**.
   d. Select **Groups assigned to the application**.
   e. From the **Source attribute** list, select **Cloud-only group display names**.

9. 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 Extreme Platform ONE Security default view. The Extreme Platform ONE Security Audit Logs include the login action.

10. 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 Extreme Platform ONE Security default view. The Extreme Platform ONE Security Audit Logs include the login action.

Integrating with 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 Extreme Platform ONE Security.

   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:
   a. Select the **Assignments** tab.
   b. Select **Assign**, and then select **Assign to Groups**.
   c. For each group you want to permit authentication to Extreme Platform ONE Security 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 Extreme Platform ONE Security 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 Extreme Platform ONE Security.

   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 Extreme Platform ONE :

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

   a. In Extreme Platform ONE Security, go to **Administration & Settings** > **Access Management**, and then select **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**.

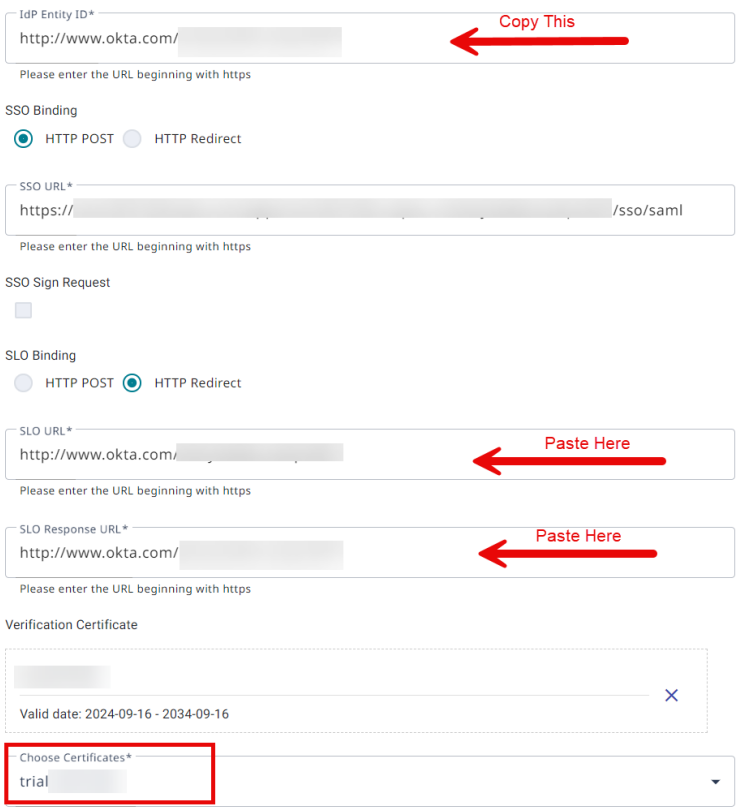


Figure 25: Extreme Platform ONE - Placeholder Values for Single Logout

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 Extreme Platform ONE Security role.

k. In the **IdP group** field, enter the name of your Okta group, and then select the Extreme Platform ONE Security 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 what you enter here exactly matches the information 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 EP1 role based on the order you specify.

l. When there is no available group map, select one of the following options to define Extreme Platform ONE Security behavior:
   i. **Deny user login**: A user that successfully logs into Extreme Platform ONE Security with their Okta credentials, but is not in an Okta group mapped to EP1 RBAC role, is denied access to the application.
   ii. **Allow user login and assign a default role and sites**: A user that successfully logs into with their Okta credentials, but is not in an Okta group mapped to XIQ RBAC role, is mapped to the role defined here. See Group Map Settings.

m. Select **Save**.

Important
The Operator, Monitor, Help Desk, Installer, or Observer RBAC roles require the definition of one or more sites to gain visibility over managed devices. In the rule definition for those roles, specify one or more sites in the rules. Failure to do so will lead to the administrator being unable to view any devices after login. Administrator and Guest Management roles do not leverage sites, and will ignore any site definition in the rule.

7. Modify Okta SAML Application Metadata with Extreme Platform ONE Security Settings:

   For this step, we recommend having Extreme Platform ONE Security and Okta open in separate tabs, as you will select data from your new IdP profile in Extreme Platform ONE Security 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 **Extreme Platform ONE Networking**:
      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 Extreme Platform ONE Security and copy it to the **Audience URI (SP Entity ID)** field in Okta.
      iv. Copy the **ACS URL** value from Extreme Platform ONE Security and copy it to the **Single Sign-On URL** field in Okta.

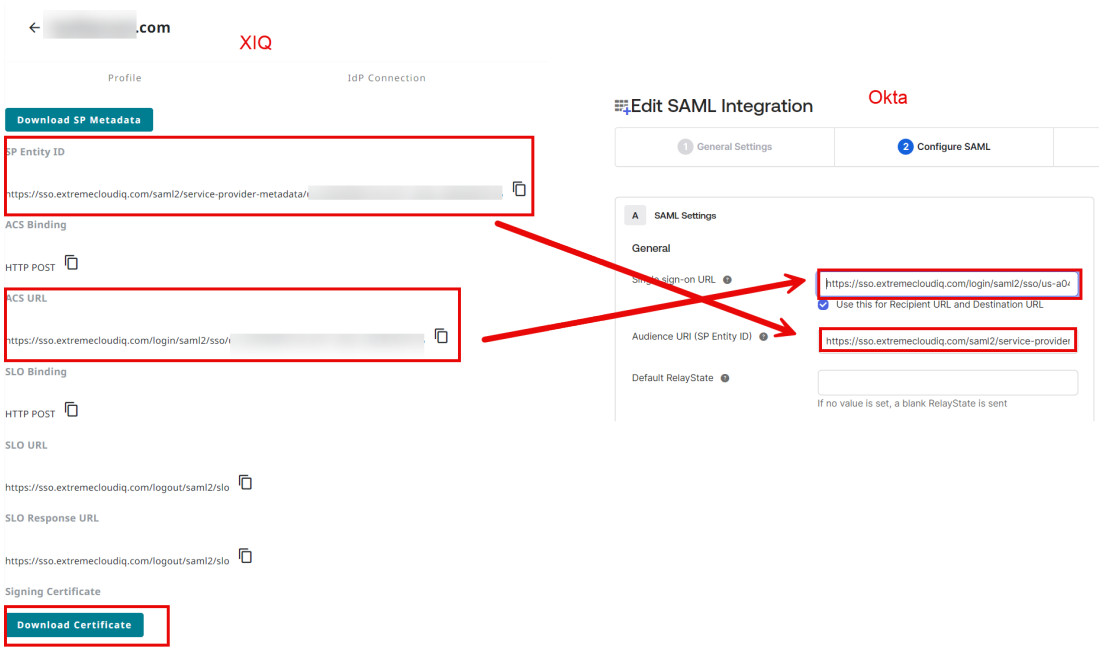


Figure 26: Okta - Replace Temporary Data for Single Sign-On URL and Audience URI

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 Extreme Platform ONE Security certificate.

   iv. Select **Enable Single Logout**.

   v. Copy the **SLO URL** value from Extreme Platform ONE Security and copy it to the **Single Logout URL** field in Okta.

   vi. Copy the **SP Entity ID** value from Extreme Platform ONE Security and copy it to the **SP Issuer** field in Okta.

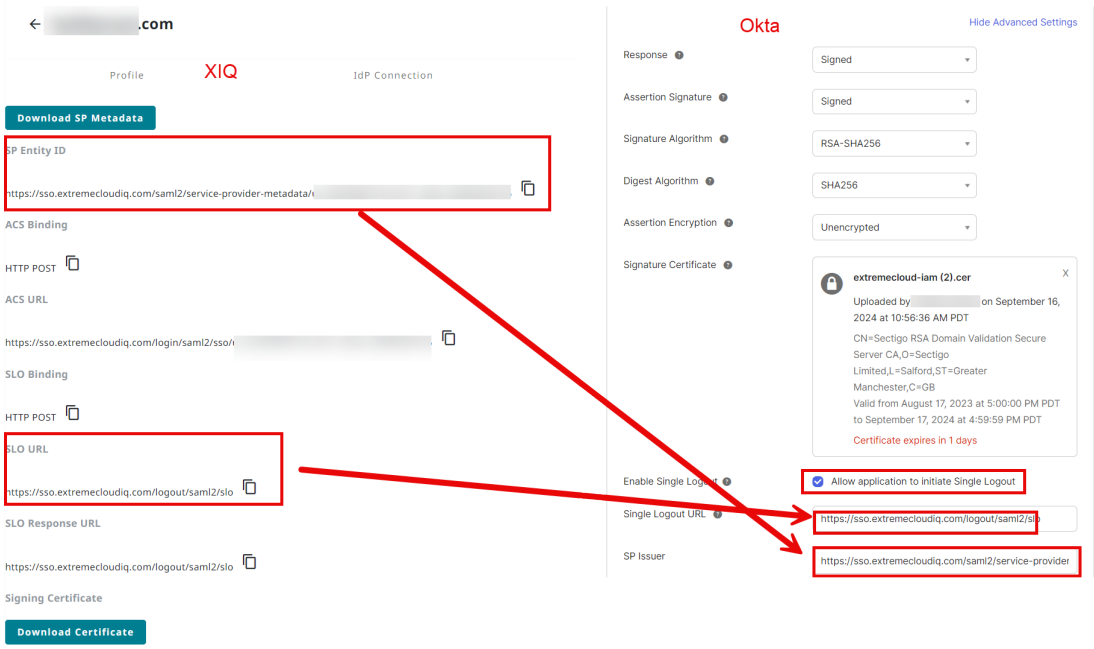


Figure 27: Okta - Single Logout Setting Definition

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 Extreme Platform ONE Security:

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 - 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 Extreme Platform ONE Security 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 Extreme Platform ONE Security default view.

Mobile Device Management

Mobile Device Management (MDM) in Extreme Platform ONE Security integrates with third-party MDM systems like Google Workspace, Microsoft Intune, and Jamf to discover/synchronize device inventory and groups and maintain activity logs to support audit and troubleshooting.

Extreme Platform ONE Security uses MDM as a source of device identity and posture for decision-making and visibility.

Microsoft Intune | MDM Integration

For Microsoft Intune integration:

1. Configure Microsoft Entra ID.
2. Configure Extreme Platform ONE Security.

Note
To identify orphaned devices, manually collect the Azure AD device ID from Microsoft Intune and then search for that ID in Azure Active Directory to verify whether the device exists.

Microsoft Entra ID

1. Go to **Manage** > **App Registrations**.
2. Select **New registration**.

   The system displays the **Register an application** page.
3. Enter an app name and ensure the **Single Tenant** option is selected under **Supported account types**.
4. Go to **Manage** > **API Permissions**.
5. Select **Microsoft Graph (1)**.

   The system displays the **Request API permissions** page.
6. **Note**
   Application permissions must be granted.

   Select the **Applications permissions** block.

7. Search for and select the following items:

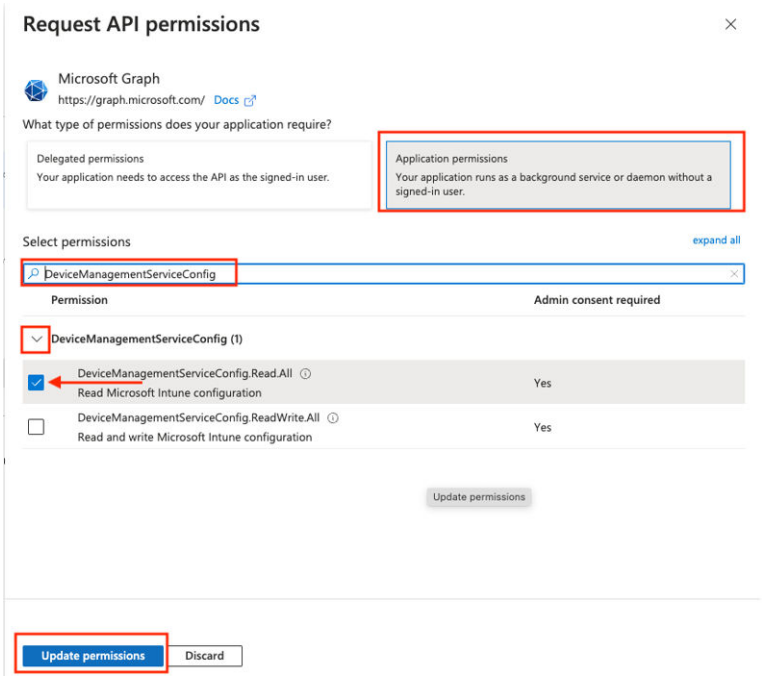
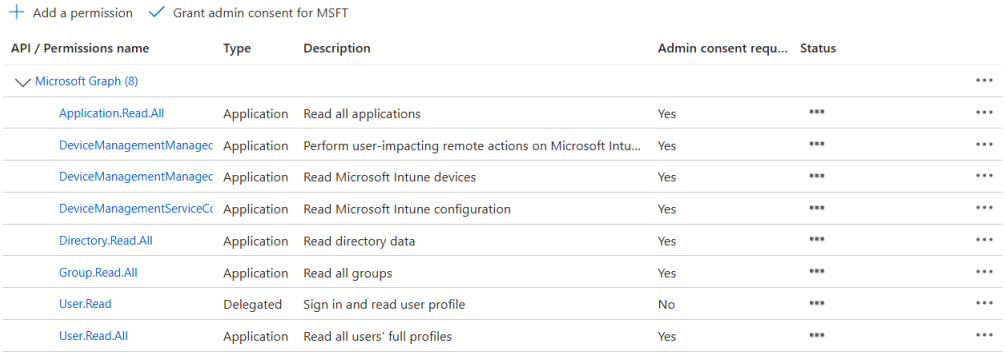


Table 71: Application Permissions

Main search	Specific permission
Application	• Application.Read.All
DeviceManagementManagedDevices	• DeviceManagementManagedDevices.PrivilegedOperations.All • DeviceManagementManagedDevices.Read.All
DeviceManagementServiceConfig	• DeviceManagementServiceConfig.Read.All
Directory	• Directory.Read.All
Group	• Group.Read.All
User	• User.Read.All

8. Once they are all enabled, select **Update permissions.**

9. To enable permissions, select **Grant admin consent for <domain>**.



Once complete the system displays the API permissions.

10. Go to **Manage** > **Certificates & secrets**.
11. Select **New client secret**. The system displays the **Add a client secret** page.
    a. Enter a description and select an expiry time from the drop-down list.
    b. Select **Add**.

    In the Value column the secret value is revealed.
12. Copy the secret value and store it in a secure place.

> **Note**
> The secret value can only be viewed from this screen. If you navigate from this screen, the value will no longer be accessible.

13. Select **Overview** and copy the **Application (client) ID** and the **Directory (tenant) ID**.

Extreme Platform ONE Security

14. Go to **Administration & Settings** > **Access Management** and select **Mobile Device Management**.
15. Select **Microsoft Intune**.
16. Select **Connect Mobile Device Management** and configure the settings in Table 72.

Table 72: Microsoft Intune Mobile Device Management Configuration Settings

Field	Description
Client ID	Enter the saved Client ID, Secret, and Tenant ID. Synchronization with Microsoft Intune occurs in the background. If the integration is successful, the system displays all synced compliant and non-compliant devices.
Client Secret	
Tenant ID	

17. Select **Connect**.
18. If there are any errors with the integration, check the permissions for the application that was created in Microsoft Entra ID.

Jamf | MDM Integration

For Jamf MDM integration:

1. Create new API roles and API client for Jamf integration. Copy the Client ID and Client Secret.
2. Configure Mobile Device Management (MDM) for Jamf in Extreme Platform ONE Security.

Note
Edit and Sync options are not available while update is in progress.

Jamf

1. Go to **Settings** > **API roles and clients**.
2. Create an **API role** with the following privileges:
   - Read Smart Computer Groups
   - Read Computer Inventory Collection
   - Read Mobile Devices
   - Read Smart Mobile Device Groups
   - Read Static Mobile Device Groups
   - Read Computers
   - Read Mobile Device Inventory Collection
   - Read Static Computer Groups
3. Create an **API Client**.
   a. Assign the role created in Step 1.
   b. Set the **Access token lifetime** to 600 seconds or more.
   c. Select **Enable API Client**.
   d. Select **Save**.
4. Select **Generate client secret**, copy for use in Extreme Platform ONE Security.
5. Onboard the device with local user or SSO login by user-initiated enrollment or profile-driven enrollment.

   After onboarding, the device is listed on UI of Jamf Pro.

Extreme Platform ONE Security

6. Log in to Extreme Platform ONE Security.
7. Go to **Administration & Settings** > **Access Management** and select **Mobile Device Management**.
8. Select **Jamf**.

9. Select **Edit Mobile Device Management** and configure the settings in Table 73.

Table 73: Jamf Mobile Device Management Configuration Settings

Field	Description
Tenant URL	Enter the associated tenant URL/
Client ID	Enter the Client ID copied from Jamf.
Client Secret	Enter the Client Secret copied from Jamf.

10. Select **Save**.

    To view Jamf, select **Policy** > **Users & Devices** and select **Device Groups**.
11. To sync the MDM, select **Sync Now** and **Confirm**.
12. To delete the MDM from the 3-dot menu, select **Delete Jamf**.
13. To verify authentication, go to **Monitoring** > **Clients** and select a client MAC Address within the Client table or on the 3-dot menu, select **View History**.

Google Workspace | MDM Integration

Use this task to edit existing Mobile Device Management (MDM) for Google Workspace.

1. Log in to Extreme Platform ONE Security.
2. Go to **Administration & Settings** > **Access Management** and select **Mobile Device Management**.
3. Select **Google Workspace**.
4. Select **Edit Mobile Device Management** and configure the settings in Table 74.

Table 74: Google Workspace Mobile Device Management Configuration Settings

Field	Description
Customer ID	Edit the customer ID.
Upload Service Account Private Key	Drag and drop your .json file or select **Browse File** to retrieve a saved copy. **Note:** The upload will override the existing key.

5. Select **Save**.
6. To sync the MDM, select **Sync Now**.
7. To delete the MDM from the 3-dot menu, select **Delete Google Workspace**.

Radius & Certificates

View RADIUS Servers

Use this task to view RADIUS servers in your environment.

1. Select **Access Management** > **RADIUS & Certificates** > **RADIUS Server**.

   The following displays:

   - Fully Qualified domain Name (FQDN)
   - IP Address
   - Authentication Port
   - Accounting Port
   - Shared Secret
   - Region

2. To refresh the screen, select  .

Certificate Management

Within **Administrations & Settings**, go to **Access Management** > **RADIUS & Certificates** > **Certificate Management**. The **Certificate Management** page is divided into the following sections:

- **CA Trusted Root Certificates** - Within this section update and download CA Trusted Root Certificates. For more information, see Manage CA Trusted Root Certificates in Extreme Platform ONE Security on page 155.
- **RADIUS Server & Intermediate Certificates** - Within this section edit and invalidate certificates. For more information, see Configure the Server Certificate on page 156.
- **Matching Criteria for Clients** - Select the client certificate attribute that Extreme Platform ONE Security should examine to detect the username (an email address). For more information, see Match Criteria for Clients on page 158.
- **Connecting with OCSP Responder** - Provide the OCSP responder server's URL or endpoint for checking the validity or revocation status of a specific digital certificate. For more information, see Edit OCSP Responder URL on page 159.

From this screen you can select the following:

- **Upload Certificates**

  1. Select **Upload Certificates** .
  2. Select **Browse Files** and navigate to your PEM file. This certificate is used solely to authenticate the EAP connection.
  3. Enter an **OSCP Responder URL**.

     Note
     If no URL is specified, certificate validation and revocation checked are skipped.

  4. To confirm, select **Save**.

- **Reset Certificates**

  1. To reset all the certificates, select **Reset Certificates**.

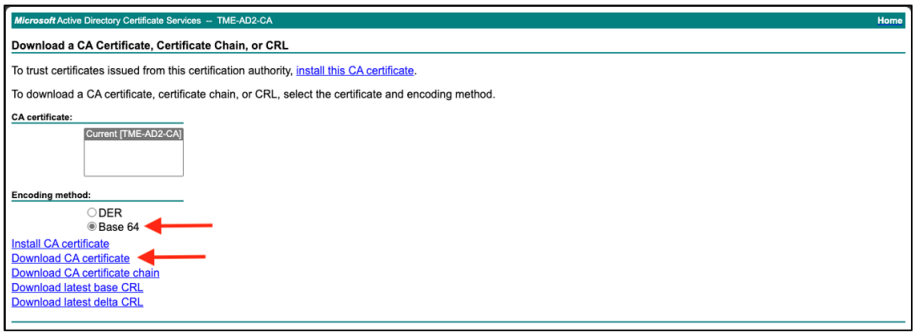
Windows Certificate Authority: Retrieve the CA (Root) Certificate

When setting up certificates in Extreme Platform ONE Security you must download the CA certificate also known as the root certificate from the certificate authority so that it can be uploaded into Extreme Platform ONE Security. Navigate to the domain controller certificate services site.

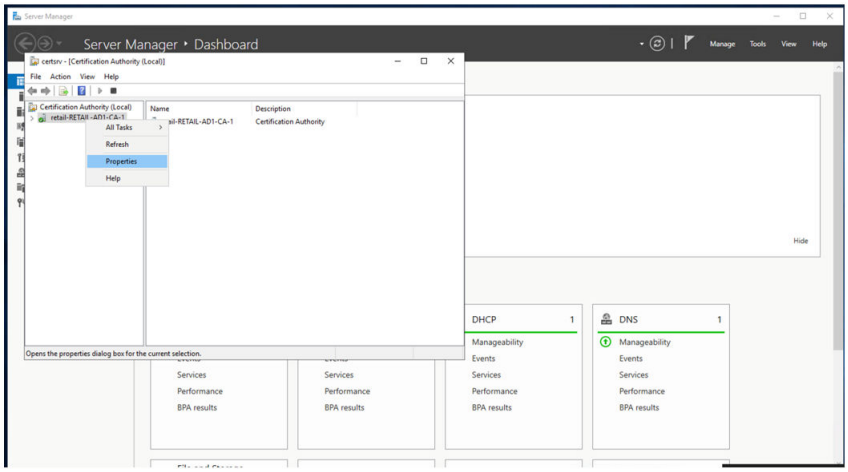
Note

CA management does not require Windows Certificate Authority. It can be managed anywhere.

1. Go to Microsoft Active Directory Certificate Services: **https://<certificatedomain>/certsrv**.
2. Select **Download a CA certificate, certificate chain, or CRL**.
3. Under **Encoding method**, select the **Base 64** option and select **Download CA certificate**.



4. If web-based certificate services are not enabled, you can open the Certification Authority window from Server Manager on the Active Directory machine, right-click on the CA and select **Properties**.



5. Under the **General** tab, select **View Certificate**.
6. Under the **Details** tab, select **Copy to File**.

   The system displays the **Certificates Export Wizard**.

7. In the **Export File Format** section, select the **Base-64 encoded X.509** option and select **Next**.
8. In the **File to Export** section, under **File name**, select **Browse**.
9. Navigate to a directory where the file will be saved, enter an appropriate name, and select **Save**.
10. To complete the process, select **Next**.

    The file will be downloaded with a **.cer** extension.

> **Note**
> Before the file can be uploaded you must rename the file with a **.pem** extension.

To upload the certificate to Extreme Platform ONE Security, go to Manage CA Trusted Root Certificates in Extreme Platform ONE Security on page 155.

Manage CA Trusted Root Certificates in Extreme Platform ONE Security

Retrieve the CA certificate also known as the root certificate from the certificate authority to upload into Extreme Platform ONE Security. For more information, see Windows Certificate Authority: Retrieve the CA (Root) Certificate on page 154.

> **Note**
> If intermediate CAs exist, they must be bundled with Root CA and the whole chain is required for upload in the root CA section.

Use this task to manage certificates.

1. Go to **Administration & Settings** > **Access Management** > **RADIUS & Certificates** > **Certificate Management**.
2. In the CA Trusted Root Certificates table from the  the following actions are available:
   - Select **Edit OCSP Responder URL**, enter an updated OCSP URL, and select **Save**.
   - Select **Download Certificate** and select **Delete** to confirm.
   - Select **Delete Root Certificate**.

> **Note**
> Root certificates associated to the RADIUS certificates cannot be deleted.

> **Note**
> After a successful validation and update of the CA certificate, active authentication sessions will continue to function. However, for all new connections, the handshake process will occur using the new CA certificate.

Once you have added the certificate within Extreme Platform ONE Security, go to Configure the Server Certificate on page 156.

Configure the Server Certificate

Before you configure the Server Certificate, you must Manage CA Trusted Root Certificates in Extreme Platform ONE Security on page 155.

Before a Server Certificate can be requested, a Certificate Signing Request (CSR) needs to be generated on behalf of Extreme Platform ONE Security to be signed by the Certificate Authority or Intermediate Certificate Authority.

Use this task to create a SAN configuration file, and execute a command against that file to create a new certificate file as well as a new private key file with no password.

Note
Along with the CN and SAN attributes, you must also get server the certificates uploaded in Extreme Platform ONE Security.

1. Access any Linux environment with OpenSSL installed using SSH.
2. After accessing the machine, generate a key file using the following comment.
   ```
   openssl genrsa -out serverkey.pem 2048
   ```
3. Use vi, vim, or another editor to create a file named **san.cnf**.
4. Edit the file and then copy in the sample text below with adjustments for your region.
   ```
   [ req ]
   default_bits = 2048
   prompt = no
   default_md = sha256
   distinguished_name = dn
   req_extensions = req_ext

   [ dn ]
   CN = radius.va2-uz.extremecloudiq
   emailAddress = remote_demo@extremenetworks.com
   O = Extreme Networks
   OU = Solutions Engineering
   L = Salem
   ST = New Hampshire
   C = US

   [ req_ext ]
   subjectAltName = @alt_names

   [ alt_names ]
   DNS.1=radius.va2-uz.extremecloudiq.com
   ```

   Note
   The above text is a sample, replace all **va2-uz** instances with the deployment region or RDC.

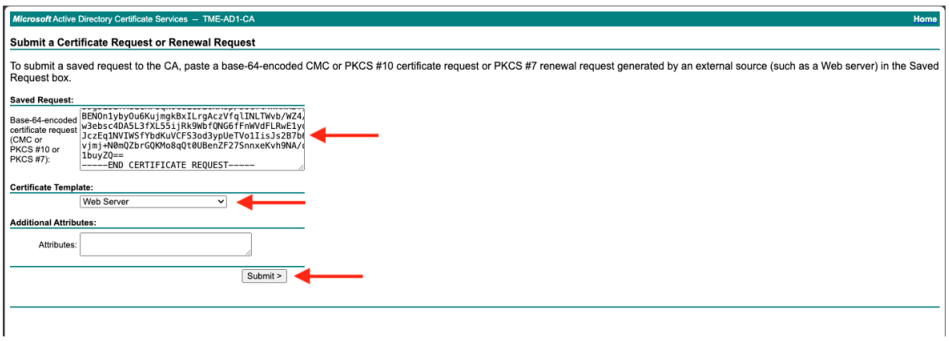
   Note
   The "CN" field is mandatory.

5. Save the file and then run an updated version of the following sample command:

   ```
   openssl req -new -key serverkey.pem -out va2-uz-server.csr -config san.cnf
   ```

   Note
   The above text is a sample, replace all **va2-uz** instances with the deployment region or RDC.

   This command will create a **.csr** file to be used to create a new server certificate to be used along with the **serverkey.pem** file to update the server certificate in Extreme Platform ONE Security.
6. Go back to Microsoft Active Directory Certificate Services: **https://<domain name>/certsrv**.
7. Select **Request a Certificate** and **advanced certificate request**.
8. Copy the contents of the CSR file and paste it into the **Save Request** field.



9. Select **Web Server** from the template drop-down and select **Submit**.
10. Once complete, select **Base 64 encoded** and **Download Certificate**.
11. The certificate request can also be made using powershell by issuing and updated version of the following sample command:

    ```
    certreq -submit -attrib "CertificateTemplate: WebServer" va2-uz-server.csr
    ```

    Note
    The above text is a sample, replace all **va2-uz** instances with the deployment region or RDC.

12. Go to Extreme Platform ONE Security, select **Access Management** > **RADIUS & Certificates** > **Certificate Management**.

    Note
    Note: If an intermediate certificate authority issues the certificate, the intermediate CA certificate needs to be bundled with the server certificate. In a text editor the files can be added sequentially.

13. Within the **RADIUS Server & Intermediate Certificates** section, select and select **Edit Certificate**.

    Note
    Both certificate and key files must be renamed using a **.pem** extension before being uploaded.

14. Select **Certificate with Embedded Key** or **Certificate with Separate Key**.
15. To upload the newly created certificate as well as the key file drag and drop or browse for the file.
16. Select **Save**.

    Validation of the certificate is instantaneous. Certificate deployment to freeradius will take upwards of two minutes to complete. Once this is accomplished, clients should be able to connect using 802.1X EAP-TLS.

17. To invalidate RADIUS server certificates, select and select **Invalidate Certificate** from the drop-down menu.

Match Criteria for Clients

Before you match criteria for clients, go to Configure the Server Certificate on page 156.

Currently Extreme Platform ONE Security will authenticate user certificates using one of two specific formats. Use this task to select the specify the client certificate attributes or key/value pairs that Extreme Platform ONE Security should examine in order to detect the username (an email address) and a device ID.

Note
The **Device ID** field is only available for devices synced from Intune via Mobile Device Management integration.

1. Go to **Access Management** > **RADIUS & Certificates** > **Certificate Management**.
2. From the **Certificate Attribute for Username** field, select one of the three options:

   Note
   Extreme Platform ONE Security expects the Username to be an email address or a User Principal Name (UPN). Other values will be rejected.

   - Subject Distinguished Name | Common Name - The **Subject** field of the certificate the **CN** or **Common Name** must contain the full email address of the client.
   - SAN | Email Address - The **SAN** or **Subject Alternative Name** must contain either an email attribute, or that attribute must contain the full email address of the client.
   - SAN | User Principal Name - The UPN must be the user's complete email address.

3. To choose the username value from the RADIUS Request, under **Fallback Criteria** select **Match with RADIUS Username**.

4. From the **Certificate Attribute for Device Identifier** select one of three options:
   - Subject Distinguished Name | Common Name
   - SAN | User Name Principal
   - SAN | DNS Name

   Note
   For Microsoft Intune synced devices, the Entra ID Device Identifier is used to match devices.

5. Select **Update**.

   Extreme Platform One Security first checks the valid username attribute selected in **Certificate Attribute for username**. If no valid email is found, then it move to **RADIUS Username** if the fallback criteria is enabled. If no valid email address is found in RADIUS username as well, then the system check the value for **Certificate Attribute for Device Identifier**.

Once you have matched the client criteria, go to Edit OCSP Responder URL on page 159.

Edit OCSP Responder URL

Use this provide the OCSP responder server's URL or endpoint for checking the validity or revocation status of a specific digital certificate.

1. Go to **Access Management** > **RADIUS & Certificates** > **Certificate Management**.
2. To validate certificates, select  and select **Edit OCSP Responder URL**.
3. In the **Enter URL** field, enter the responder server's URL or endpoint.
4. Select **Save**.

Configure Eduroam

Before you begin your Eduroam configuration you must:

- Install the RadSec Proxy.
- Register the Educational Institution with Eduroam federation.
- Ensure connectivity between RadSec Proxy and Eduroam federal-level servers.

To configure and deploy Eduroam:

- Configure Eduroam SSID in ExtremeCloud IQ (Classic).
- Manage SSID in Extreme Platform ONE Security.
- Enable Eduroam Integration.
- Configure EduroamVisitorPolicy.

- Deploy RadSec Proxy.
- Register your institution with Eduroam FLR.

Note
Your home institution requests from the FLR should be forwarded to the RadSec proxy IP and port number 3812.

For more information see:

- Eduroam Component Architecture on page 161
- Eduroam Authentication Flow on page 161

Extreme Platform ONE Security SSID

1. Go to **Configuration** > **Network** and select **SSID**.
2. From the 3-dot menu, select **Managed SSID** and select **Managed**.

Eduroam Integration

3. Go to **Access Management** > **RADIUS & Certificates**.
4. Select **Eduroam** and configure the settings in Table 75.

Table 75: Eduroam Configuration Settings

Field	Description
Domain	Enter your educational institution's domain. For example, myinstitution.edu.
Primary FLR and **Secondary FLR** (Optional)	
Federal Level RADIUS (FLR) Target IP	Enter the Federal Level RADIUS (FLR) Target IP.
Authentication Port	Enter the authentication port.
Accounting Port	Enter the accounting port.
RADIUS Share Secret	Enter the RADIUS Share Secret.
Enable Eduroam	Toggle the Eduroam feature to ON.

5. Select **Save**.

EduroamVisitorPolicy

When Eduroam is enabled, an **EduroamVisitorPolicy** is automatically created to manage authentication for visiting users from other institutions. Location condition as well as user group for Eduroam visitors are also created.

6. Select **Eduroam** and select **View Policy**.
7. Customize authentication rules and access controls, and select **Save** to apply the policy to all visiting Eduroam users.

Note
This policy governs network access for users from federated institutions. Ensure it aligns with your security and access requirements.

Eduroam Component Architecture

Figure 28 displays how different components interact in the authentication flow during deployment.

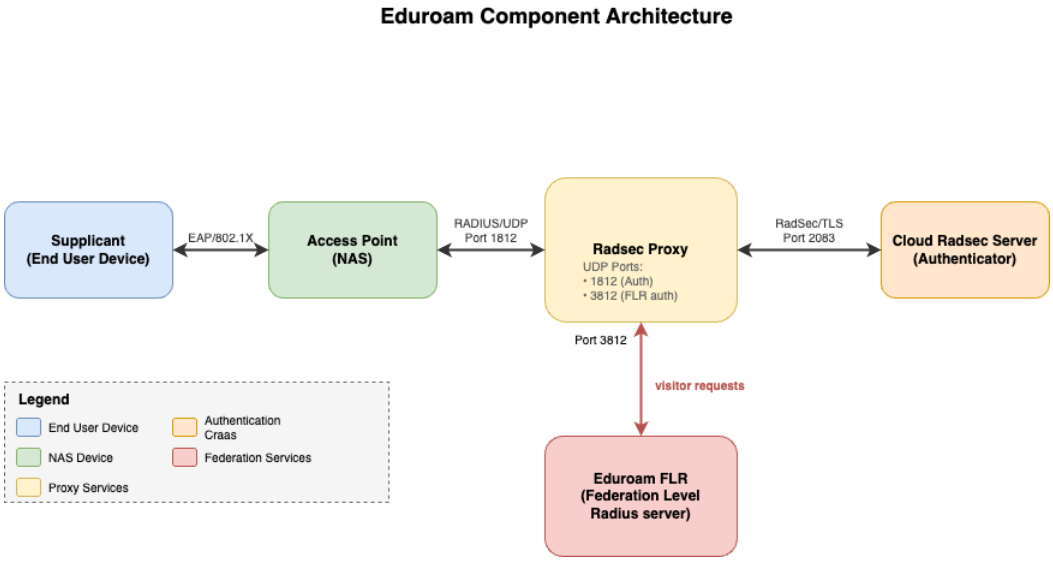


Figure 28: Eduroam Component Architecture

Table 76 provides an overview of the components.

Table 76: Components Overview

Component	Description	Protocol/Ports
Supplicant	End user device initiating 802.1X/EAP authentication	EAP over 802.1X
Access Point (NAS)	Network Access Server forwarding RADIUS requests	RADIUS
RadSec Proxy	Proxy service converting RADIUS to RadSec over TLS	UDP 1812, 3812 (in) / TCP 2083 (out)
RADIUS Server	Authentication Server validating credentials via TLS	TCP 2083
Eduroam FLR	Federation-level Router for inter-institution routing	Usually UDP 1812

For more information on Authentication flow, see Eduroam Authentication Flow on page 161.

Eduroam Authentication Flow

The following images outline authentication request flow scenarios. For more information on architecture components, see Eduroam Component Architecture on page 161.

Home User Initiates Connection to Eduroam SSID

In this scenario the user connects to their home institution.

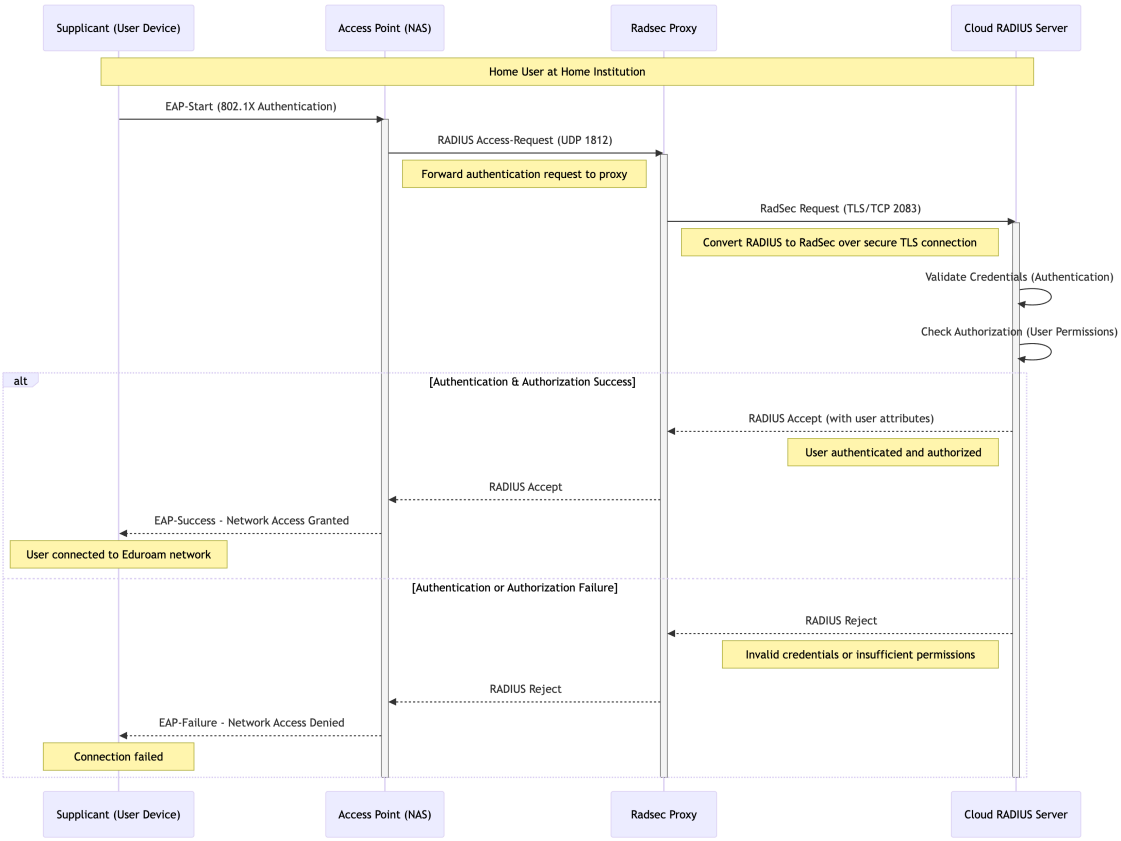


Figure 29: Home Institution Connection

Home User Initiates Connection to a Visiting Institution

In this scenario the home user is roaming at a different institution.

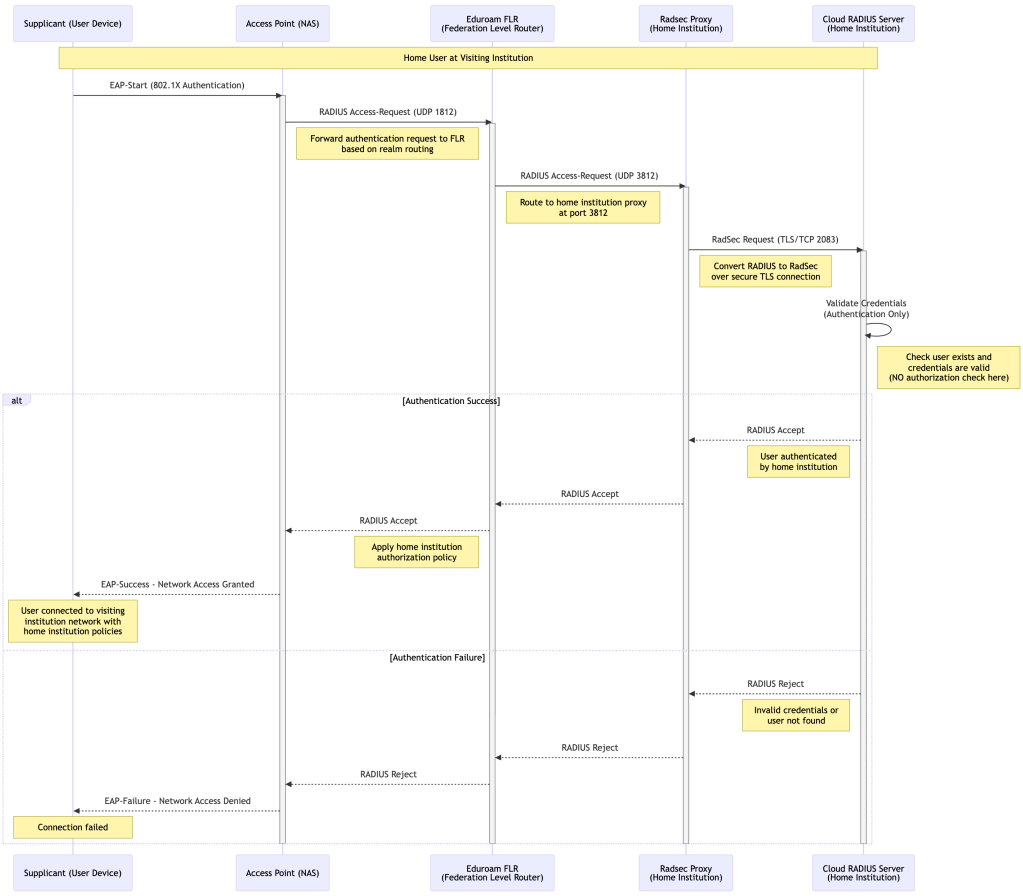


Figure 30: Visiting Institution Connection

Visiting User Initiates Connection to Eduroam at Home Institution

In this scenario a visiting user from another institution connects at your institution.

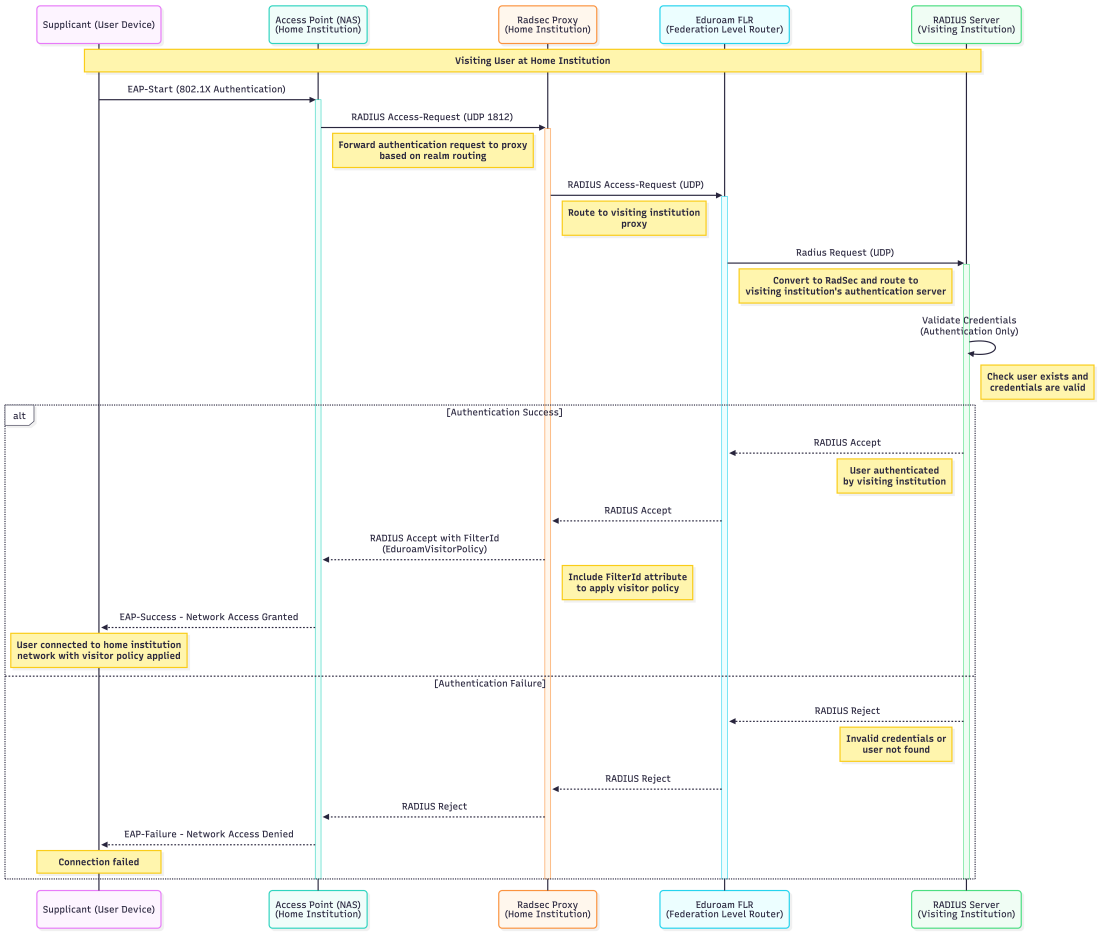


Figure 31: Visiting User Connection to Home Institution

Administration & Settings | Security Services

Deploy Service Connectors

Follow these recommendations:

Note
When Secure Socket Layer (SSL) decryption is in use, the traffic does not pass through the service connector.

- Packaged deployment:

  Recommended OS

  Ubuntu 22.04 or 24.04

  VMware OVA
- Dockerized deployment: compatible with multiple operating systems; requires only Docker to be installed.
- Port Availability (outbound)- The following ports must be allowed oubound from the Service Connector:
  - WireGuard Encryption Protocol: 51820, 51821(UDP)
  - IPsec Encryption Protocol: 4500 (UDP)
  - TURN Service Ports: 3478, 3479 (UDP)
- Port Availability (inbound) - If the connector and the user are in the same network, open the following ports for inbound requests:
  - WireGuard encryption Protocol: 51820 (UDP)
  - IPsec Encryption Protocol: 4500 (UDP)
- Minimum hardware requirements: CPU: 4 Ram: 16 GB

Use this task to deploy a service connector which:

- Connects to private, cloud-hosted application services and facilitates secure data exchange between the user and these application services

- Performs data transformation and routing between the user and application services
- Can be hosted in private data center or public cloud such as AWS, Entra ID, and GCP

1. If deploying a Service Connector outside of the onboarding process, go to **Administration & Settings** > **Security Services** > **Service Connectors**.
2. Select **Deploy Service Connector** > **Private Hosted** from the drop-down on the right.
   a. Read the Guidelines.
   b. For the **Connector Name**, enter at least three alphanumeric characters
   c. Select an existing site or add a site for **Associate Site**.
   d. Enter a size for **Set MTU** (Maximum Transmission Unit).
   The MTU value is the maximum size of a data packet that an internet-connected device can accept in bytes. The MTU size ranges from 1200 to 1400 bytes.
   e. Select **Deploy**.
   f. Choose a deployment method.
   g. Read Deployment instructions.
   h. Select **Done**.
3. Select **Deploy Service Connector** > **Multi-Cloud Hosted** from the drop-down on the right.
4. The following actions are available for existing Service Connectors:
   - To update an existing Service Connector deployment, select  and select **Edit**.
   - To scale instances, select  and select **Scale Instances**. See Scale Instances on page 166.
   - To enable debugging logs, select  and select **Enable Debugging Logs**. To confirm select **Enable**.
   - To deactivate an existing Service Connector deployment, select the instance number and in the **<connector name> instances** window select  and select **Deactivate**.
   - To delete a Multi-Cloud Service Connector, select  and select **Delete.**.
   - To delete a Private-Hosted Service Connector, see Delete a Private-Hosted Service Connector Entry on page 169.

   Note
   A Private-Hosted Service Connector entry can not be deleted until its individual instances are removed.

When deployment finishes, the service connector status turns green and displays **Up**.

Your enterprise applications and networks are now securely accessible to the service connector.

Scale Instances

Use this task to scale Service Connector Instances.

Considerations:

- Outbound requests from Service Connector Instances must be able to access the internet.
- In order to provide secure access to all applications within the private network, they must be reachable by the service connector and have internet connectivity.
- **System Requirements**:
  - Packaged Deployment: Recommended OS - Ubuntu 20.04 or above.
  - Dockerized Deployment: C-Supported Platform: amd64.

    Note
    Compatible with multiple operating systems; requires Docker to be installed.

- **Port Availability** - If connector and user are in the same network, the following ports are to be made open for the inbound requests:
  - Wireguard Encryption Protocol: 51820
  - IPSec Encryption Protocol: 500, 4500
- **Note**
  It is possible to replicate this command across numerous host machines, resulting in the installation of several Service Connector instances. The traffic load will be distributed evenly among these instances, providing high availability.

1. Go to **Administration & Settings** > **Security Services** > **Service Connectors**.
2. Select  and select **Scale Instances**.

3. Choose one of the following deployment methods and follow configurations instructions:
   a. **Containerized**

      Note
      Docker must be installed to run the container installation commands.

      i. Your service connector is ready to be installed. Copy the given command within the host machine where you would like it to be installed and rest can be taken care of by Extreme Platform One Security.
      ii. Create an Empty Config JSON File. On your host machine, navigate to the directory where you want to store the configuration for the Service Connector run the command on the screen.

      Note
      This empty JSON file will be used to persist the configurations for your Service Connector.

      iii. Start the Service Connector Container. Run the command on the screen to start the Service Connector within a docker container.

   a. **Packaged**
      i. Your service connector is ready to be installed. Copy the given command within the host machine where you would like it to be installed and rest can be taken care of by Extreme Platform One Security.
      ii. Download the package. Download the connector using the link or paste the command on the screen to your host machine to download the package directly.
      iii. Install the package and bring up the service connector. To install the package, run the command on the screen.

   a. **OVA**
      i. a. Download the OVA file and import it into your preferred appliance.
      ii. During the initial setup, you'll be prompted to enter credentials. Copy the details below and paste them into your host machine. Update these default credentials immediately for security purposes:
         - Username: localadmin
         - Password: localadmin
      iii. Once logged into the host machine, you'll receive a prompt to enter the authentication token. Copy the token provided and paste it into the machine.

      .

      If the Service Connector installation fails at any point, you can use the command on the screen to retry the installation.

Delete a Private-Hosted Service Connector Entry

Use this task to delete a service connector.

Note
A Private-Hosted Service Connector entry can not be deleted until its individual instances are removed.

1. Go to **Administration & Settings** > **Security Services** and select **Service Connectors**.
2. Select the value in the **Instances** column that applies to your connector.

   The **<connector name> Instances** window appears.
3. To delete an existing Service Connector deployment, in the **<connector name> Instances** window select and select **Delete**.
4. Select **Delete** to confirm.
5. Once all instances are deleted, close the **<connector name> Instances** window and select associated with your service connector entry and select **Delete**.

Deploy RadSec Proxies

A RadSec Proxy is only required when the network switch or AP does not support native RadSec. This is specifically applicable to 3rd party devices. Any Extreme Universal switch or Access Point supports native RadSec and should be connected in that way as a best practice.

Follow these recommendations:

- Packaged deployment:

  Recommended OS

  Ubuntu 22.04 or 24.04

  VMware OVA
- Port availability: The following ports need to be allowed outbound from the RadSec proxy:
  - RadSec Port: 2083, 443
  - RADIUS accounting and Authenticating ports: 1812, 1813
- Minimum hardware requirements: CPU: 2 Ram: 4 GB

This task shows you how to deploy RadSec Proxies to implement secure authentication on non-RadSec protocol compatible devices.

1. If deploying a RadSec Proxy during onboarding, select the **Deploy RadSec Proxy** tab.

   If deploying a RadSec Proxy outside of onboarding, select **Administration & Settings** > **Security Services** > **RadSec Proxy** from the navigation pane on the left.

2. Select **Deploy RadSec Proxy**.
   a. Read the Guidelines and configure the settings in Table 77.

Table 77: RadSec Proxy Configuration Settings

Field	Description
RadSec Proxy Name	Enter at least three alphanumeric characters.
Associate Site	Select an existing site or create one. **Note:** Site update takes 1 to 2 minutes.
Certificate Rotation Time	Enter the number of days until the next rotation.
Shared Secret	You can update the text field with a value between 3 and 32 characters in length. This shared secret will be used with network devices authenticating via RADIUS to the RadSec Proxy.

   b. Select **Next**.
   c. Select the deployment mode and follow the installation procedure shown.
   d. Read the information and follow the installation procedure for the host machine.
   e. Select **Done**.

   The new proxy displays in the RadSec Proxy list with the **Ready to Install** status.
3. Go to your host machine and perform the installation using the guidelines provided.

Your proxy should come into service after waiting a short period, and display the **UP** status.

To update an existing RadSec Proxy, select . From this menu you can do the following:

- Connect Devices
- Edit
- Sync Now
- Delete
- Enable Local Authentication

Integrate with the Public Cloud

There are three public cloud integration options:

- Amazon Workspace (AWS)
- Microsoft Azure

Use this task to add an integration to deploy and manage cloud service connectors.

1. Select **Security Services** > **Public Cloud**.

2. To add an AWS integration:
   a. Select the **AWS Integration** tab.
   b. Select **Add Integration** and update the following fields:
      - Integration Name
      - AWS Account ID
   c. Select **Next**.
   d. Update the following fields:
      - AWS Access Key ID
      - AWS Secret
      - Session Token
   e. Select **Save**.
   f. To edit an existing integration, from the 3-dot menu, select **Edit**. Make updates and select **Save**.
   g. To edit an existing integration, from the 3-dot menu, select **Delete**. To confirm select **Delete**.
3. To add an Azure integration:
   a. Select the **Azure Integration** tab.
   b. Select **Add Integration** and follow the instructions in the UI.
   c. Update the following fields:
      - Integration Name
      - Subscription ID
      - Tenant ID
      - Application Client ID
      - Object ID
      - Application Client Secret
   d. Select **Add**.
   e. To edit an existing integration, from the 3-dot menu, select **Edit**. Make updates and select **Save**.
   f. To edit an existing integration, from the 3-dot menu, select **Delete**. To confirm select **Delete**.

Manage DNS Servers

Use this task to add, update, or remove Domain Name Systems (DNS) servers.

1. Select **Resources** > **DNS**.

   The **DNS** window displays.

2. Select **Add DNS Server** and configure the settings in Table 78.

Table 78: DNS Configuration Settings

Field	Description
Server Name	Enter at least three alphanumeric characters.
IP Address	Enter an IP address.
Service Connector	Select a service connector from the drop-down list.

3. Select **Add**.

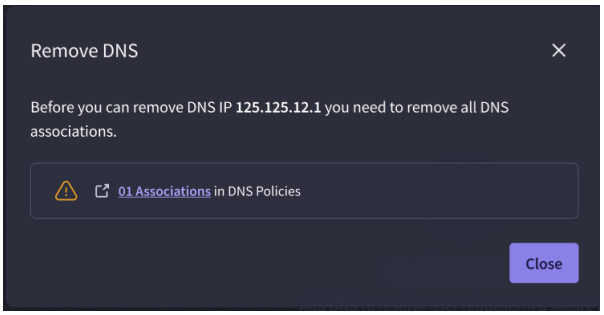
   Next, you will see a sequence of screen updates while Universal ZTNA works to bring the DNS server up.

   a. A connectivity test runs.
   b. If the test passes, a confirmation message displays at the top of the window.
   c. Your server displays in the server list.
   d. The **Status** column displays **Activating**.
   e. The **Status** changes to **Up** when the server is in service.

4. To update an existing DNS server, select ⋮ and select **Update** from the drop-down list.

5. To remove an existing DNS server, select ⋮ and select **Remove** from the drop-down list.

Note
Before removing a DNS server, you must remove all associations.



Add a DNS Policy

Use this task to add a DNS policy.

Note
You can add multiple policies, with and without location conditions. A location policy will have priority if it matches the users location.

Note

Multiple DNS policies are chosen at random. The tenant must ensure the services' domains are translatable from all the DNS servers.

1. Go to **Resources** > **DNS**.

   The **DNS** window displays.
2. Select the **DNS Policies** tab.
3. Select **Add DNS Policy** and configure the settings in Table 79.

Table 79: DNS Policy Configuration Settings

Field	Description
Policy Name	Enter between 3 and 250 alphanumeric characters.
Location-Based Conditions	Select a location-based conditions from the drop-down list.
Primary DNS	Select a **DNS Type**: • **Public** - Enter IP Address. • **Private** - Select a DNS Server from the drop-down list.
Secondary DNS (Optional)	

4. Select **Add**.
5. To edit or delete an existing DNS policy, from the 3-dot menu, select **Edit** or **Delete**.

Administration & Settings | Alert Policies

View Global Policies

Use the **Global Policy** screen to enable or disable **Alert Rules**, and edit alert rule parameters.

Note
The Observer role does not have access to Alert Policies.

Use this task to view global policies.

1. Go to **Administration & Settings** > **Alert Policies**, and select **Global Policy**.
2. Select one of the following rule categories to see Alert Rules for that type:

Table 80: Alert Rules by Category

Category	Alert Rules
ExtremeCloud IQ	The following alert rules are available: • Device • Security • AP Radio Usage • CPU & Memory Usage • Power Consumption • Switch PSU (Power Supply Unit) Usage • Wired Port Usage
Extreme Vendor Specific	The following alert rules are available: • Device

Table 80: Alert Rules by Category (continued)

Category	Alert Rules
Extreme Platform ONE Security	The following alert rules are available: • Application Access • Authentication • Device • Network Access • Local Failover Postgres CPU & Memory Usage • Local UZ Auth Service CPU & Memory Usage • Local UZ Network Rule Engine CPU & Memory Usage • RADSec Proxy CPU & Memory Usage • Service Connector CPU & Memory Usage
ExtremeCloud SD-WAN	The following alert rules are available: • EQS • Management • Overlay • Resources • Service • Underlay

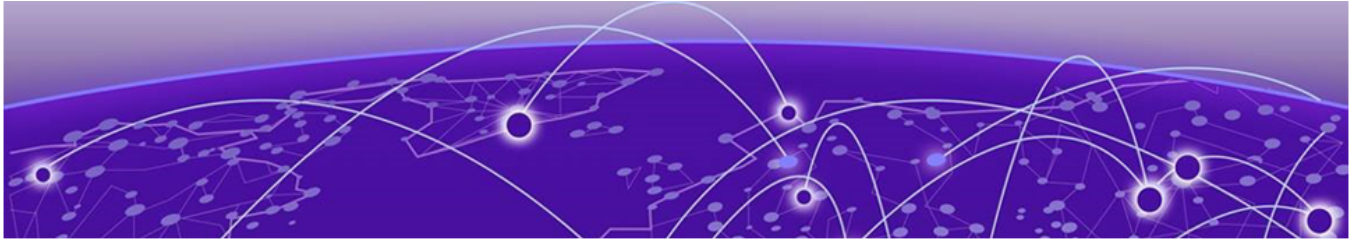
3. Alert rule parameters can be enabled or disabled by selecting the alert rule, then toggle the enable/disable radio button for the event or metric. To edit alert rule parameters, select  for the rule.

Add a Site Policy

Use this task to add a site policy.

Note
The Observer role does not have access to Alert Policies.

1. Go to **Administration & Settings** > **Alert Policies**, and select **Site Policies**.
2. Select **Add Site Policy**.
3. Complete the following:
   - Provide the **Alert Policy Name**.
   - Select **Sites**.
4. Select **Next**.
5. Select an **Alert Rule** and optionally edit, enable, or disable the rule parameters.
6. Select **Apply Rules**.
7. To edit or delete the site policy, from the 3-dot menu, select **Edit** or **Delete**.



Administration & Settings | External Notifications

Recipients

Go to **Administration and Settings** > **External Notifications** > **Recipients** to do the following:

- Add Email Recipient on page 176
- Add Webhook on page 178
- Add ServiceNow Account on page 177

Add Email Recipient

Use this task to add email recipients.

1. Go to **Administration and Settings** > **External Notifications** > **Recipients** select **Email Recipients**.

2. Select **Add Email Recipient** and configure the settings in Table 81.

Table 81: Email Recipient Configuration Settings

Field	Description
Business Email	Enter a valid email address.
Notification Type and Notification Rule	The following Notification Types and associated rules are available for email recipients: • Alert - Select one or more **Application**, **Severity**, and **Alert Policy** from the drop-down list. **Note:** By default, **Select All** is selected for severity, application, sites and policy drop down values. **Note:** To use global policy to generate an email notification when there is no site-specific policy, select **Global Policy**. If a site-specific policy exists, and you select Global Policy, the system does not send a notification. • Subscription - Select at least one **Subscription** fron the drop-down list. • Contract - Select at least one **Contract Rule** from the drop-down list.
Enable Notifications	Select the toggle to enable notifications.

3. Select **Save**.
4. Type in the **Search** field to view specific email recipients.
5. Apply the following filters for email recipients:
   - All
   - Verified
   - Not Verified

Add ServiceNow Account

Use this task to add a ServiceNow account.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **ServiceNow**:
2. Type in the **Search** field to view specific ServiceNow alerts.

3. To add a ServiceNow alert, select **Add Account** and configure the settings in Table 82.

Table 82: Add ServiceNow Alerts Configuration Settings

Field	Description
ServiceNow Email	Enter a valid email address
Sites	Select at least one site or all sites.
Applications	Select at least one application or all applications.
Severity	Select at least one severity or all severity levels.
Alert Policy	Select at least one alert policy or all alert policies.

   a. Select the **Enable Notifications** toggle.
   b. Select **Save**.

Add Webhook

Use this task to add Webhooks.

1. Go to **Administration and Settings** > **External Notifications.** > **Recipients** select **Webhooks**:
2. Type in the **Search** field to view specific Webhook alerts.
3. To add a webhook alert, select **Add Webhook** and configure the settings in Table 83.

Table 83: Webhook Alerts Configuration Settings

Field	Enter
POST URL	Enter a valid URL
Access Token (optional)	Provide access token details.
Sites	Select at least one site or all sites.
Applications	Select at least one application or all applications.
Severity	Select at least one severity or all severity levels.
Alert Policy	Select at least one alert policy or all alert policies.

   a. Select the **Enable Notifications** toggle.
   b. Select **Save**.

Rules

Go to **Administration and Settings** > **External Notifications** > **Rules** to do the following:

- Add a Rule for Subscriptions on page 179
- Add a Rule for Contracts on page 179

Add a Rule for Subscriptions

Use this task to add a rule for subscriptions.

1. Go to **Administration and Settings** > **External Notifications** > **Rules** select **Subscriptions**:
2. Select **Add Rule** and configure the settings in Table 84.

Table 84: Subscription Rule Configuration Settings

Field	Enter
Rule Name	Enter a rule name.
Applications	Select the checkboxes for the applications that apply from the drop-down menu.
Timeline Rules	Select the checkboxes for the timeline rules that apply from the drop-down menu.
Event Rules	Select the checkboxes for the event rules that apply from the drop-down menu.

3. Select **Save**.
4. Type in the **Search** field to view specific rules.

Add a Rule for Contracts

Use this task to add a rule for contracts.

1. Go to **Administration and Settings** > **External Notifications** > **Rules** select **Contracts**:
2. Type in the **Search** field to view specific rules.
3. Select **Add Rule** and configure the settings in Table 85.

Table 85: Contracts Rule Configuration Settings

Field	Enter
Rule Name	Enter a rule name.
Timeline Rules	Select the checkboxes for the timeline rules that apply.

4. Select **Save**.

Administration & Settings | Integrations

Add Event Collectors on page 180

Add Event Collectors

There are two options to add event connectors:

- Splunk
- API-based Log Collection

Use this task to add Splunk and use API to filter activity logs.

1. Select **Integrations** > **Event Collector**.
2. Select **Add Splunk Integration** and configure the settings in Table 86.

Table 86: Splunk Integration Configuration Settings

Field	Description
HTTP Event Collector Host	Enter an appropriate value based on your Splunk license (replace "host" with your Splunk server hostname).
Port	Specify a port number for the HEC to listen on.
Protocol	Select HTTP or HTTPS.
Verify server SSL Certificate	Enable this option if you are using a CA-signed certificate. If you are using a self-signed certificate, disable SSL verification.
Authentication Token	Enter the token you generated at Splunk to enable the integration.

3. Select **Save**
4. To edit an existing integration, select the 3-dot menu and select, **Edit**.
5. To delete an existing integration, select the 3-dot menu and select, **Delete**.
6. To use an API-based log collection:
   a. Follow instructions on the screen.
   b. Copy the API endpoint.
   c. Select **Generate Token**.

Administration & Settings | Logs

Logs

The following log captures are available from **Administration & Setting** > **Logs**:

Table 87: Log Configuration Settings

Log Type	Description
Audit	• 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.
GDPR	The General Data Protection Regulation (GDPR) audit log displays information about download tasks performed on client data, and deletion tasks performed on user, client, and admin data to support compliance with GDPR requirements for EU citizens. Use this log to track actions that are currently being processed, that are complete, or that have failed.
Authentication	The Authentication Logs table displays information about successful authentication attempts involving cloud-based PPSK and RADIUS users, and users authenticating through a cloud-hosted captive web portal using either social log in credentials or a PIN. The table includes authentication events for the time range that you define using the Start, End, and Time controls at the top of the page. Search for a specific client or user name in the Search field above the table.
Accounting	The Accounting Logs table displays information about cloud-based PPSK and RADIUS user sessions on your network. The table includes authentication events for the time range that you define using the Start, End, and Time controls at the top of the page. Use the Search field above the table to search for a specific client or user name.

Table 87: Log Configuration Settings (continued)

Log Type	Description
Credentials	The Credential Logs table displays information about cloud-based RADIUS user credentials that have expired. To set a time range to view expired user credentials, use the Start, End, and Time controls at the top of the page. Use the Search field above the table to search for a specific client or user name.
SMS	The SMS Logs table displays information about SMS notifications sent to users who request network access.
Email	The Email Logs table displays information about email notifications to users who requested network access.
KDDR	Kernel Diagnostic Data Recorder (KDDR) logs record failures or interruptions of ongoing processes. The KDDR log format is binary. Generally these logs are for more advanced troubleshooting. Extreme Networks support might ask for these logs for troubleshooting unexplained reboots or crashes.
Event	
Security	• System changes: Captures system activity. Audit logs must be compliant with all Extreme Network standards, for example, HIPPA, PCI, NIST. • End-user activity: For example, end-user login activity such as signing in and signing out. • Service access: Captures when an end-user starts or ends a service access activity.

Manage Logs

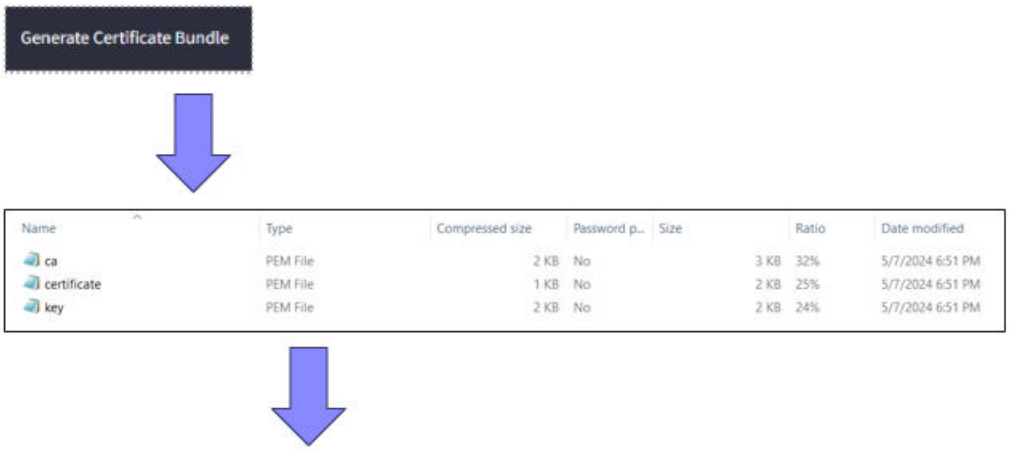
Use this task to search, schedule, and refresh logs.

1. Log into Extreme Platform ONE Security.
2. Go to **Administration and Settings** > **Logs.**
3. Select the **Log** and **Date** and **Time** pickers to do the following:
   a. View logs for up to 30 days.
   b. View logs for last week, last month or last quarter.
   c. Select an end time.
   d. Reset to default.
   e. Use arrows to select a specific month.
   f. To view a logs for a specific date, select the date directly from the calendar.
4. You can also search and filter by column heading.
5. Select the **Date/Time** column to sort in ascending or descending order.
6. Select **Column** to add, hide, and reposition columns on the screen.
7. To refresh the screen and get the latest audit logs, select  .

Appendices

Fabric Engine Locally Managed Sample Configuration

Generate and Download the Certificate Files




```
Directory of C:\Users\Radsec\Downloads\certificate-file-extreme


05/15/2024 10:06 AM <DIR> .

05/15/2024 10:06 AM <DIR> ..

05/13/2024 02:04 PM 2,427 ca.pem

05/13/2024 02:04 PM 1,244 certificate.pem

05/13/2024 02:04 PM 1,678 key.pem

3 File(s) 5,349 bytes

2 Dir(s) 43,057,008,640 bytes free
```

Upload Certificate Files to the Switch Using FTP

```
C:\Users\Radsec\Downloads\certificate-file-extreme>ftp 10.68.16.150

Connected to 10.68.16.150.

220 FTP server ready

530 USER and PASS required

User (10.68.16.150:(none)): rwa

331 Password required

Password:

230 User logged in

ftp> binary

200 Type set to I, binary mode

ftp> put ca.pem

200 Port set okay

150 Opening BINARY mode data connection

226 Transfer complete

ftp: 2427 bytes sent in 0.00Seconds 2427000.00Kbytes/sec.

ftp> put certificate.pem

200 Port set okay

150 Opening BINARY mode data connection

226 Transfer complete

ftp: 1244 bytes sent in 0.00Seconds 1244000.00Kbytes/sec.

ftp> put key.pem

200 Port set okay

150 Opening BINARY mode data connection

226 Transfer complete

ftp: 1678 bytes sent in 0.00Seconds 1678000.00Kbytes/sec.

ftp> quit

221 Bye...see you later
```

Note

files are uploaded in the default location **/intflash**

When running Enhanced Secure Mode (ESM) default location will be **/intflash/shared** directory

Apply the Certificate Files to the Switch Using Default RADIUS Secure-Profile

```
#radius secure-profile default ca-cert-file ca.pem

#radius secure-profile default cert-file certificate.pem

#radius secure-profile default key-file key.pem

#radius secure-profile default key-pwd radsec
```

Apply the RADIUS/RADIUS-Secure Configuration to the Switch

```
#radius server host 3.72.170.112 key radsec used-by eapol

#radius server host 3.72.170.112 used-by eapol secure-enable

#radius secure-flag

#radius enable
```

Optional Configuration

```
#radius secure-profile TestProfile -to use create custom Radius secure-
profile
```

```
#radius server host 3.72.170.112 used-by eapol secure-profile TestProfile -to link the
custom profile to a specific Radius
          server
```

```
#radius server host 3.72.170.112 used-by eapol acct-enable -to enable accounting for a
specific Radius
          server
```

```
#radius accounting enable -to enable the accounting globally
```

```
#radius server host 3.72.170.112 used-by eapol secure-log-level -to change log level for
the TCP/TLS
          session
```

```
#radius server host 3.72.170.112 used-by eapol secure-mode -to switch
between TLS and DTLS
```

802.1X NEAP Basic System and Port Configuration

```
#eapol enable

#interface gigabitEthernet 1/1

#(config-if)#eapol multihost radius-non-eap-enable

#(config-if)#eapol status auto
```

Optional Configuration

```
#interface gigabitEthernet 1/1

#(config-if)#eapol multihost non-eap-mac-max 10 -to change the max number of NEAP clients
allowed on that
          port

#(config-if)#eapol multihost mac-max 10 -to change the max Mac clients allowed on 802.1x
enabled
            ports

#(config-if)#eapol re-authentication enable -to enable
          re-authentication
```

802.1X NEAP on Ports Enabled for Auto-sense

```
Auto-sense is a port-based functionality to support zero touch capabilities on the VOSS
        switches. When you enable Auto-sense on a port, the system dynamically configures
the port based on the Link Layer Discovery Protocol (LLDP)
        events .

#interface gigabitEthernet 1/1
```

#(config-if)#auto-sense

Optional Configuration for Auto-sense Eapol

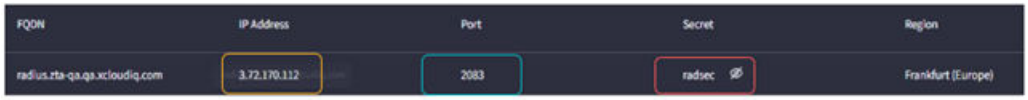
```
#auto-sense eapol multihost non-eap-mac-max 10 -to change the max number of NEAP clients
allowed on that
          port

#auto-sense eapol multihost mac-max 10 -to change maximum MAC clients supported on
              an Eapol enabled port
```

Switch Engine Locally Managed Sample Configuration

Generate, Download, and Apply the Certificate Files to the Switch


```
# download ssl <ip address> certificate trusted-ca ca.pem
# download ssl <ip address> certificate certificate.pem
# download ssl <ip address> privkey key.pem
```

Apply the RADIUS/RadSec configuration to the switch – RADIUS Accounting is optional but will help with immediate client disconnect notifications in Universal ZTNA




```
# config radius tls ocsp off
# configure radius netlogin 1 server 3.72.170.112 tls 2083 client-ip <switch ip> shared-secret radsec vr VR-Mgmt
# enable radius netlogin
# configure radius-accounting netlogin 1 server 3.72.170.112 tls 2083 client-ip <switch ip> shared-secret radsec vr VR-Mgmt
# enable radius-accounting netlogin
```

Apply Netlogin/Policy Configuration to the Switch

1. Configure the policy for dACL and VLAN authorization.

   ```
   # configure policy rule-model access-list

   # config policy vlanauth enable

   # config policy maptable response both

   # enable policy
   ```

2. Configure netlogin for dot1x or mac authentication/reauth (example on ports 1-5).

```
# enable netlogin dot1x mac

# configure netlogin authentication protocol-order dot1x mac web-based
          cep

# enable netlogin ports 1-5 dot1x mac

# configure netlogin add mac-list ff:ff:ff:ff:ff:ff 48

# configure netlogin mac ports 1-5 timers reauthentication on
```

Extreme Platform ONE Security Authentication

Extreme Platform ONE Security supports three authentication types: 802.1X EAP-TTLS, 802.1X EAP-TLS, and MAC Authentication.

Configuring the end client for any 802.1X authentication type depends on the operating system and how the client is managed.

To set up 802.1X in Extreme Platform ONE or ExtremeCloud IQ for Extreme Platform ONE Security authentication, you will use the native IDM server hosted by Extreme. Use this task to enable it.

1. Configure SSID.
   a. In ExtremeCloud IQ, go to one of the two SSID configuration sections.
      Go to **Configure** > **Network Policies** enter the policy name and select **Wireless Networks**.

      Or

      Go to **Configure** > **Common Objects** > **Policy** and select **SSID**.
2. For 802.1X, create or edit an SSID and select Enterprise as the authentication method.
   a. Under Authentication Settings, choose the option for Authentication with Extreme Platform ONE Security.
   b. Save the SSID and deploy the configuration to the relevant Access Points.
   c. In Extreme Platform ONE Security or Networking, go to **Configuration** > **Network** > **SSID**, select the SSID that was created in the previous step and select **Extreme Platform ONE Security Manage**.
   d. Once the configuration is successfully pushed, you can connect to the SSID that was pushed in the previous step.
3. For MAC Authentication, create or edit an SSID of Personal or Open, then select the MAC Authentication tab under SSID Usage.
   a. Enable the MAC Authentication option and select Authentication with Extreme Platform ONE Security.
   b. Save the SSID and deploy the configuration to the relevant Access Points.
   c. In Extreme Platform ONE Security or Networking, go to **Configuration** > **Network** > **SSID**, select the SSID that was created in the previous step and select **Extreme Platform ONE Security Manage**.
   d. Once the configuration is successfully pushed, you can connect to the SSID that was pushed in the previous step.

These steps will help you establish wireless authentication using IDM with EAP-TTLS for Extreme Platform ONE Security in ExtremeCloud IQ.