Extreme Platform ONE™ Security v25.6.0 Release Notes

Enhancements, Fixes, and Supported Devices

9041068-00 Rev AA
April 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/

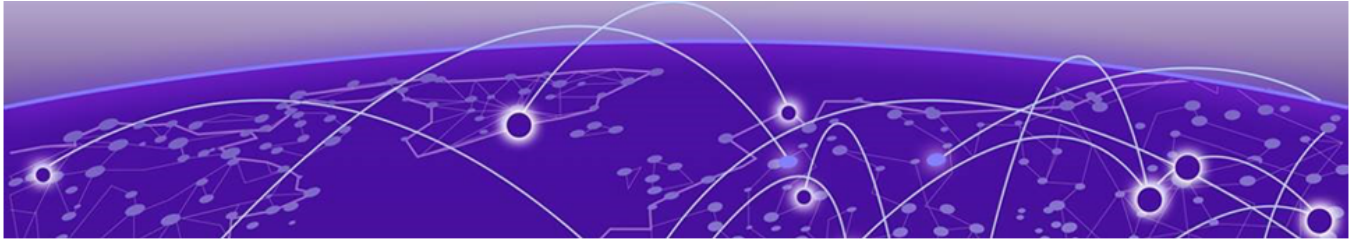
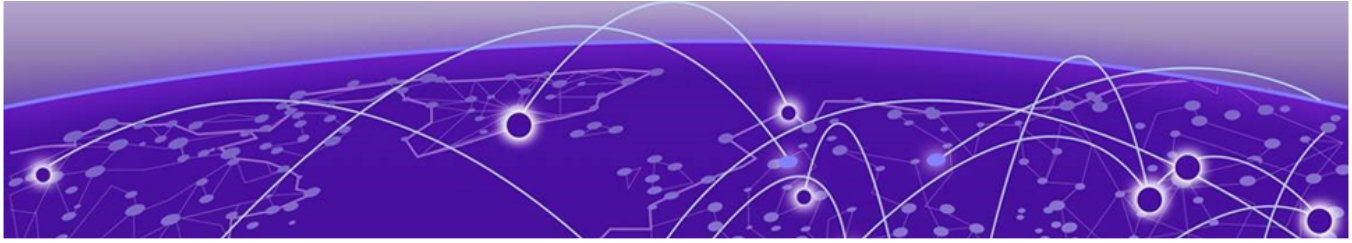


Table of Contents



Abstract

These release notes for Extreme Platform ONE Security version 25.6.0 provide a technical summary of new capabilities, addressed defects, known limitations, and supported hardware for identity-based network and application access security across campus and remote environments. The release introduces enhanced certificate lifecycle management, including client certificate deployment, CSR support for EAP-TLS, global user and device block lists, expanded security logging for network access activity, containerized RadSec proxy deployment, support for HENNGE One as an identity provider, multiple location selection within security policies, and improvements to client, posture, and application visibility. Updates also include refinements to MDM integration workflows, Eduroam configuration documentation, Fabric Engine L2 fingerprint support, and backend API refactoring in preparation for upcoming releases. The notes detail resolved issues affecting UI behavior, authentication workflows, RadSec proxy status, macOS SSO, Ubuntu service connector installation, and SSID synchronization, while documenting known constraints such as iOS tunnel limitations, application connector dependencies, and performance considerations at scale. Supported access points and switching platforms, along with minimum software versions and onboarding models, are specified, providing operational guidance for experienced network and security administrators planning or upgrading production deployments.

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.

Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

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

Table 1: Notes and warnings (continued)

Icon	Notice type	Alerts you to...
	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.

Table 3: Command syntax (continued)

Convention	Description
...	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.

Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by Switch Engine software, which are the following:

- ExtremeSwitching® switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the Switch Engine command documentation (see the Extreme Documentation page at www.extremenetworks.com/documentation/). In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines sections.

Terminology

When features, functionality, or operation is specific to a device family, such as ExtremeSwitching, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the *device*.

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.

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:

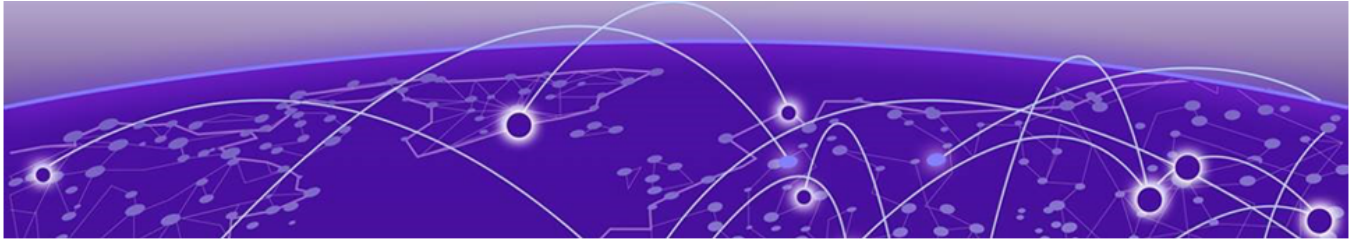
- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental 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.



Extreme Platform ONE Security General Release Information

Overview

Extreme Platform ONE Security integrates network, application, and device access security within a single solution to bolster security organization wide. Establish and maintain a consistent security policy across your network with a single solution to manage and enforce an identity-level zero trust policy for all users. You can also manage user networks, applications, and Internet of Things (IoT) device access independent of the user's location.

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

Switch Onboarding Options

Option 1 – Managed

- Supported NOSs: Switch Engine and Fabric Engine
- Supported Switches: 4120, 4220, 5320, 5420, 5520, 5720, x435, 7520, 7720
- Minimum NOS version: Fabric Engine 9.0.2, Switch Engine 33.2.1
- Summary: Switch configuration is fully managed by ExtremeCloud IQ. The Instant Secure Port workflow is used to provision RADIUS/authentication and Extreme Platform ONE Security policy is provisioned via static policy.

Option 2 – Locally Managed

- Supported NOSs: Fabric Engine and Switch Engine
- Supported Switches: 5320, 5420, 5520, 5720, 7520, 7720, x435
- Minimum NOS version: Fabric Engine 9.0.2, Switch Engine 33.2.1
- Summary: Switch is onboarded but switch must be manually configured to use RadSec Proxy or native RadSec to the cloud RADIUS server. Extreme Platform ONE Security network policy is provisioned by dACLs by RADIUS VSAs.

Note
Extreme Networks provides support for many other Extreme and non-Extreme devices with additional manual configuration.

Firewall Considerations

Outbound access to the following IP Addresses are required in any firewall configurations:

- 13.248.199.77
- 76.223.79.155

New Features for 25.6.0

Table 4: New Features in 25.6.0

Feature ID	Feature	Description
UZ-2156	API Refactor for upcoming release	APIs in the following categories have been refactored for use in the DevPortal for release 25.7.0. • User/Device Group Management • Access Control • Client & Endpoint Visibility
UZ-2157	Client Certificate Deployment	**Client Management** tab added to Extreme Platform ONE Security to manage the following: • Certificate Authorities • Issued Certificates (Beta) • Self-Enrollment
UZ-2939	RadSec Proxy Containerized Deployment	New "Containerized" RadSec Proxy deployment option that runs all RadSec Proxy services in Docker containers using a single-command install.
UZ-3582	Allow more certificate file extension types	Certificate uploads are no longer restricted to .pem extensions. All certificate file types are inspected for validity.
UZ-3585	Multiple location section within Policies.	When adding an Application, Network, or Hybrid Security policy, you can now select multiple locations from the drop-down list.
UZ-3635	CSR Support for EAP-TLS	Admins can now create certificate signing requests directly within the system giving them more control over the certificate lifecycle and deployment security.
UZ-9950	HENNGE One IdP support	HENNGE One is now supported for user and group synchronization and application access.

Table 4: New Features in 25.6.0 (continued)

Feature ID	Feature	Description
UZ-12104	Global Block List Management	Two groups are automatically created per tenant: • User Group: Global Block List (users) • Device Group: Global Block List (devices / MAC addresses) When added to the list by an admin, those user or device authentication attempts are denied access.
UZ-12105	Network Access Activity Logging	New Security log captures all RADIUS authentication events, including success, failure, method (EAP-TLS, PEAP, MAC Auth), and user/device identifiers.
UZ-15398	Support for Wired MAC Address	Support for MDM synced second ethernet MAC address for wired.
UZ-16240	API-Based Log now collection sending Cloud NAC logs to SIEM	Extreme Platform ONE Security is now receiving logs for Cloud NAC.
UZ-16793	Eduroam Documentation	Eduroam configuration information, component architecture, and authentication flow are now available within the Extreme Platform ONE Security User Guide.
UZ-17324	Mobile Device Management Microsoft Entra ID Prerequisites link	Added a **Prerequisites** link to the **Connect Mobile Device Management** screen within MDM to facilitate configuration without leaving the workflow.
UZ-18133	Service Connector Token Rotation	Service Connection instances now use separate access keys that will rotate before they expire. Users can update the lifetime of the connector key and the number of hours before expiration.

Addressed Issues in 25.6.0

Table 5: Addressed Issues in 25.6.0

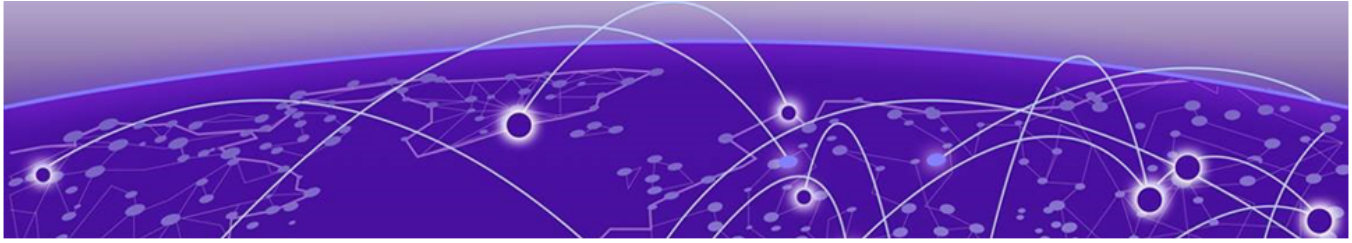
Issue ID	Issue	Description
CFD-15869	RadSec proxy status indication is showing as grayed-out within Extreme Platform ONE Security.	This defect is caused by an issue in the code, where a script automatically added all the translations for static strings, statuses are static strings but there is logic based on that string (status). This affected the translations. Indicators are now working as intended.
CFD-15921	UI issue when trying to configure MAC authentication condition in the Security Policy.	When MAC Authentication is selected within the policy creation screen, the UI displays a message and then goes blank. This appears to be only affecting the Safari Browser. This issue has now been resolved.
CFD-16807	Error when installing packaged installer on an Ubuntu environment.	When running the Extreme Platform ONE Security Service Connector packaged installer on an Ubuntu environment and executing the packaged installer on Ubuntu 24.04, the installation fails with the following error: "Is not a supported architecture." Language support has now been added to the Connector installation script.
CFD-16883	Certificate information deleted during upgrade. Unable to generate an Extreme managed certificate.	All existing certificate authority information was deleted from Extreme Platform ONE Security due to the PEEPs upgrade. This has been corrected. We are now able to generate an Extreme Managed Certificate.
UZ-20399	SSO (Pass-through Authentication) is not working for certain macOS users	For certain macOS users, the system displayed an error after enabling SSO on Extreme Platform ONE Security. The error was "This device isn't Entra ID joined. Select **Login with Credentials** to proceed." This error no longer appears.
UZ-15494	Unregistered devices and network location conditions both show up stale SSIDs in the desktop agent and Extreme Platform ONE Security, respectively.	This issue has been addressed as part of the new SSID sync implementation and migration script.

Known Issues in 25.6.0

The following table lists Extreme Platform ONE Security known product issues. Issues are grouped according to ID prefix and sorted within their group with the most recently logged issue listed first. Issue IDs are in descending order.

Table 6: Known Issues in 25.6.0

Issue Name	Description
UZ-3129	Device login or posture failures are not reported on the insights table.



Supported Devices

The following devices are support for Extreme Platform ONE Security.

Access Points

Note
Extreme Networks supports all 3rd party Access Points. For unlisted devices, refer to 3rd party process.

Device Model Series	Minimum Version
AP5020	IQ Engine 10.7.3
AP5050D/U	IQ Engine 10.7.3
AP5010	IQ Engine 10.7.3
AP302W	IQ Engine 10.7.3
AP4000	IQ Engine 10.7.3
AP3000/X	IQ Engine 10.7.3
AP460C	IQ Engine 10.7.3
AP410C	IQ Engine 10.7.3
AP510C/CX	IQ Engine 10.7.3
AP305C/CX	IQ Engine 10.7.3

Switches

Note
Extreme Networks supports all 3rd party Switches. For unlisted devices, refer to 3rd party process.

Note
Fabric Engine references in the following table apply to locally-managed devices only. For more information, see Switch Onboarding Options on page 9.

Device Model Series	Minimum NOS Version
4120	Switch Engine 33.2.1
4220	Switch Engine 33.2.1

Device Model Series	Minimum NOS Version
5320	Fabric Engine 9.0.2, Switch Engine 32.6.3
5420	Fabric Engine 9.0.2, Switch Engine 32.6.3
5520	Fabric Engine 9.0.2, Switch Engine 32.6.3
5720	Fabric Engine 9.0.2, Switch Engine 32.6.3
7520	Fabric Engine 9.0.2, Switch Engine 32.6.3
7720	Fabric Engine 9.0.2, Switch Engine 32.6.3
x435	Switch Engine 32.6.3