



ExtremeCloud™ Universal ZTNA v25.2.0 Release Notes

Enhancements, Fixes, and Supported Devices

9039248-00 Rev AA
March 2025



Copyright © 2025 All rights reserved.

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses.

End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Abstract.....	iv
Preface.....	5
Conventions.....	5
Text Conventions.....	5
Platform-Dependent Conventions.....	7
Terminology.....	7
Send Feedback.....	7
Help and Support.....	8
Subscribe to Product Announcements.....	8
Universal ZTNA General Release Information.....	9
Overview.....	9
Switch Onboarding Options.....	9
Firewall Considerations.....	10
New Features for 25.2.0.....	11
Addressed Issues in 25.2.0.....	12
Known Issues in 25.2.0.....	14
Supported Devices.....	16
Access Points.....	16
Switches.....	16



Abstract

The release notes for ExtremeCloud™ Universal ZTNA version 25.2.0 provide comprehensive information on enhancements, fixes, and supported devices. This document details new features such as Ubuntu 24.04 support and a new option for the Network Evaluation tool to upload certificates for EAP-TLS authentication testing. Addressed issues include profile picture uniqueness across accounts, macOS Sequoia 15.0.1 failing to configure SSID, and discovered applications becoming inaccessible. Known issues involve device login or posture failures not reported on the insights table, applications with SSO enabled not accessible through agentless web access, and high Kafka memory usage in a GCP cluster. Supported devices include several access point and switch models, with specific minimum NOS versions required. The document also includes troubleshooting tips, frequently asked questions, and important configurations or settings.



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 or routers, the product is referred to as *the switch* or *the router*.

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 <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> 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 <i>type</i> .
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
<i>Words in italicized type</i>	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.
<i>italic text</i>	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, <i>member[member...]</i> .
\	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 <https://www.extremenetworks.com/documentation-feedback/>.

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

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.



Universal ZTNA General Release Information

Overview

Universal ZTNA 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.

Universal ZTNA 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 only
- Supported Switches: 4120, 4220, 5320, 5420, 5520, 5720, x435
- Minimum NOS version: 33.2.1
- Summary: Switch configuration is fully managed by ExtremeCloud IQ. The Instant Secure Port workflow is used to provision RADIUS/authentication and Universal ZTNA 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. Universal ZTNA 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 25.2.0

Table 4: New Features in 25.2.0

Feature ID	Feature	Description
UZ-3555	Ubuntu 24.04 support	Ubuntu 24.04 is now compatible with RadSec proxy, Service Connector, and End-user Agent.
UZ- 5931	New option for Network Evaluation tool to upload certificates for EAP-TLS authentication testing.	Go to Monitor > Troubleshooting , the Upload Certificate field is now available on the Network Evaluation for EAP-TLS authentication testing.



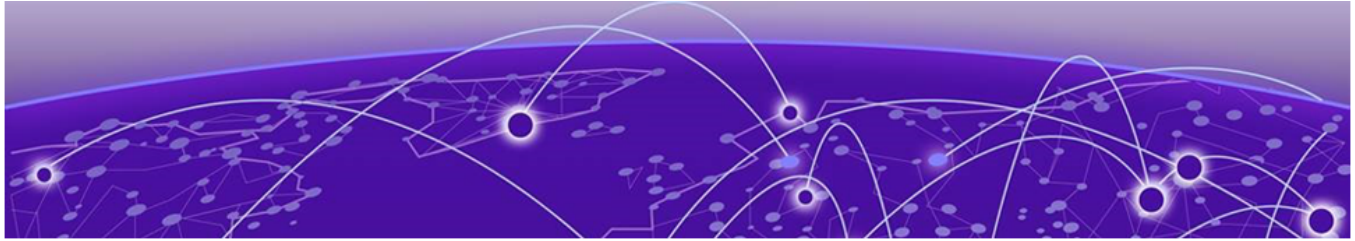
Addressed Issues in 25.2.0

Table 5: Addressed Issues in 25.2.0

Issue ID	Issue	Description
CFD-13103	Profile picture uniqueness across accounts issue	Previously, updating a profile picture in Universal ZTNA resulted in the same image being applied to all accounts. Resolution: A new endpoint /iam-service/myaccount/avatar is now used to fetch and update profile pictures for all tenant roles except End User. This ensures profile pictures remain user-specific.
UZ-3533	Getting Service Connector (SC) "Up Event" if redundant SC instance gets to UP state.	Redundant Service connector "UP Event" if a particular instance comes up if the SC is already in UP state.
UZ-4081	macOS Sequoia 15.0.1 fails with error "Failed to configure SSID".	macOS Sequoia 15.0.1 fails with error "Failed to configure SSID" when 'Click to Configure' is selected in the networks section of the Agent.
UZ-5221	Applications are being discovered in Application Discovery, but some become inaccessible and have false statuses.	The issue was caused due to web-socket connection break, the message to add discovered app rules on connector nftable dropped due to this discovered application was not accessible. Restart the Service Connector to add missed rules. If the Service Connector is unable to restart, the discovered app will be visible on UI but won't be accessible.
UZ-5450	In Hybrid policy, the default Service Connector group is not added by default.	Workaround: Clear the cache of browser and refresh or open the browser in a incognito window.

Table 5: Addressed Issues in 25.2.0 (continued)

Issue ID	Issue	Description
UZ-6686	Application Discovery: No. of Users count is incrementing for the unique user even though the application is not accessed	On Windows, the Telnet application is not getting discovered. The issue was tested and reproduced on two different Windows devices. The user count does not increment for Telnet when accessed from Windows and Chromebook, but it increments correctly when accessed from Linux and Mac. This issue is specific to telnet on Windows and Chromebook. We have logged a bug for the next release (25.2.0) to address the problem of the telnet application port not being discovered on Windows.
UZ-7365	UZTNA Version 25.1.0-7 for Mac Breaks Web Browser Keychain	After a new update is deployed with MDM, the Universal ZTNA Desktop Agent app does not automatically launch due to context issues. Users can manually start the app from Launchpad on macOS or the desktop shortcut on Windows.
UZ-8912	For Mac Universal ZTNA Desktop Agent in-app login feature, users see a prompt stating: "ExtremeCloud Universal ZTNA wants to export key 'Microsoft Workplace Join Key' from your keychain."	For Mac Universal ZTNA Desktop Agent in-app login feature, the in app browser is treated as new browser for system, prompting Microsoft login to import/export keys in Keychain Access. Users see a prompt stating: "ExtremeCloud Universal ZTNA wants to export key 'Microsoft Workplace Join Key' from your keychain." To avoid multiple password prompts and potential request timeouts, users should select "Always Allow." This permission is granted once and will not be requested again.
XCD-677	If Universal ZTNA is set as the default application redirection issue	If Universal ZTNA is set at the default application on the Application page, XCD is now redirecting to the correct URL.
XCD-679	License SKU description is not displayed on XCD user interface.	This has now been correct on XCD.



Known Issues in 25.2.0

The following table lists Universal ZTNA 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 25.2.0

Issue Name	Description
CFD-12203	FQDN Applications are only retrieving the first A record of the application.
UZ-3129	Device login or posture failures are not reported on the insights table.
UZ-3171	Applications with SSO enabled are not accessible through agentless web access.
UZ-3716	Under Insights > Identities , connected user and hostname of device are incorrect.
UZ-4405	When Universal ZTNA managed SSID is renamed the "State" changes to "N/A".
UZ-6553	The application cannot be added with two different connectors due to technical limitations on the WireGuard/IPSec tunnel side. If an application is configured with two connectors and access is granted for both, the application access will fail to function correctly on all platforms.
UZ-6732	When the Service Connector is down, in Application Discovery , the application status remains in "Activating" until the Service Connector is up again. The Service Connector can be activated from the UI if it was deactivated or by turning on the Service connector if it was turned off from the machine.
UZ-7277	When syncing a device from Intune Mobile Device Management (MDM), only the wireless MAC address is displayed on the MDM page within Universal ZTNA. The Ethernet MAC address is not shown, which may impact wired authentication workflows.
UZ-8434	During device and device group synchronization from Microsoft Intune, the expected default device groups "MDM Corporate Owned" and "Employee Owned" are not automatically created. As a result, devices are not dynamically categorized based on their ownership status, which may impact policy enforcement and access control.

Table 6: Known Issues in 25.2.0 (continued)

Issue Name	Description
UZ-8471	Site list takes 10 seconds to load with 1000 sites.
UZ-8773	On IPSec/ Android, DNS cannot be unset without turning off the tunnel. On network switch there is slight disruption in network causing tunnel to break but DNS remain set. Therefore, once internet is back the DNS resolution will be failing and apps remain in connecting state.
UZ-8899	Updating an existing Hybrid or Network Policy to remove the I-ISID will fail to remove the NSI from the corresponding policy-profile on ExtremeCloud IQ Managed Switch Engine devices. The following message may be seen in the Activity Log; "update with defaultNsi not allowed unless defaultVlan and defaultAction specified or already configured". The workaround is to delete the Hybrid or Network Policy and re-create it with the new configuration.
ZTNA-15224	No entries in activity log are created for actions performed in Device Posture admin screen.
ZTNA-21536	Unregistered devices and network location conditions both show up stale SSIDs in the desktop agent and Universal ZTNA, respectively.



Supported Devices

The following devices are support for Universal ZTNA.

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