ExtremeCloud™ Universal ZTNA v25.1.0 Release Notes

Enhancements, Fixes, and Supported Devices

9039170-00 Rev AB
February 2025

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/

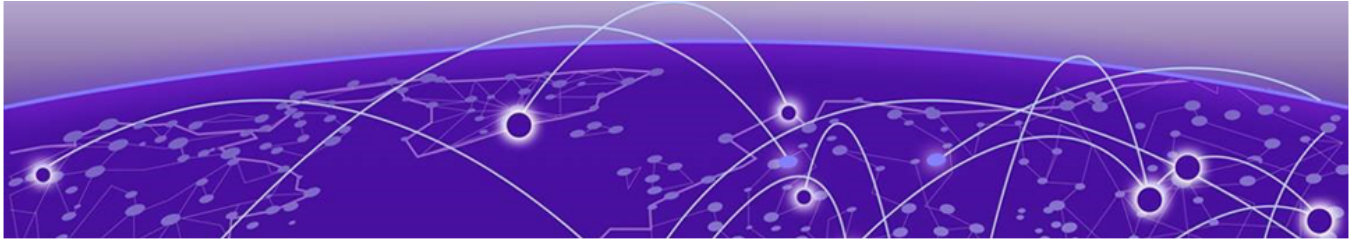
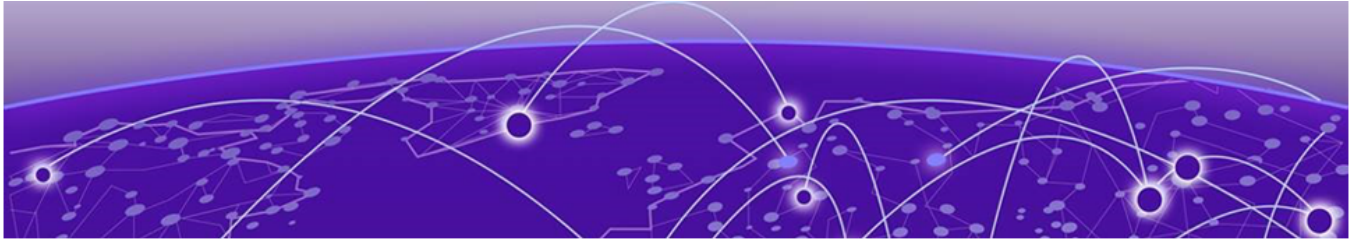


Table of Contents



Abstract

The ExtremeCloud™ Universal ZTNA Release Notes for version 25.1.0 provide detailed information on new features, addressed issues, and known issues. Key technical points include the integration of network, application, and device access security within a single solution, supporting both remote and campus access with continuous authentication and NAC capabilities. The document highlights new features such as Azure support and significant changes to the ZTA Authentication system, including enhanced user lifecycle event handling and improved status tracking. Addressed issues cover various fixes, including VLAN assignment logic updates and device registration improvements. Known issues are also listed, providing insights into current limitations, and troubleshooting tips. The document is intended for technical readers and provides comprehensive guidance on configurations, supported devices, and browser compatibility.

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 SLX 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 *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 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: 32.6.3
- 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 32.6.3
- 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 25.1.0

Table 4: New Features in 25.1.0

Feature ID	Feature	Description
UZ-2892	Azure Support	This release now supports Universal ZTNA deployment on Microsoft Azure.
UZ-2927	New Release Notification	This feature notifies the end user via push notification and in-app notifications for the end user agent on every platform including Android, iOS, MacOS, Windows, and Chrome Book when there is a new release.

Addressed Issues in 25.1.0

Table 5: Addressed Issues in 25.1.0

Issue ID	Issue	Description
CFD-12779	AP Aware does not assign a VLAN.	AP Aware was enabling "auth-override" on the policy, with no ability to specify VLAN egress on the port for the Access Point. All traffic was mapped to the existing VLAN ID on the port or the untagged VLAN that was configured in the policy. To resolve this issue VLAN assignment logic has been updated for better reliability. To allow additional VLAN IDs to be tagged in an AP Aware policy, add the following RADIUS Attributes to the Advanced Section of the Network Policy: FA-VLAN-ISID=1:1, 10:10, 13:13 In this example VLAN 1 is the Untagged VLAN assigned in the policy. This should match what is assigned above. The rest of the VLAN IDs, i.e. 10 and 13, will be added as tagged VLANs. Fabric mode is not required for this functionality to work.
CFD-13097	When adding 4000+ new mac addresses to the devices and then adding them to a group, the authentications are not matching in the group.	Within the device group, editing by adding or removing devices (mac addresses) works. However, within the Identities table, when you select **Add to Device Group** there is an issue. In this case, the event sends down only the selected device ID, that ID is added and all others are deleted. The fix is for the UI to send down the entire updated list, or we need a new event so policy can handle it correctly when it is an incremental add only.

Table 5: Addressed Issues in 25.1.0 (continued)

Issue ID	Issue	Description
UZ-3897	When Universal ZTNA policies are created and deleted continuously through automation, Dynamic Policy push to the access point freezes.	Creating a Network Service with a Custom IP in ExtremeCloud IQ causes Universal ZTNA enforcement to fail for ExtremeCloud IQ Wireless devices with an "UNKNOWN" reason in the Activity Log. **Note:** It is not likely that a customer will create a Custom IP Network Service in ExtremeCloud IQ if Universal ZTNA is managing Network Policies for ExtremeCloud IQ Wireless devices. However, if such a case occurs then CloudOps could apply the following SQL patch to the database. UPDATE hm_base_serv SET port_number = 0 WHERE service_type = 'NETWORK' AND ip_protocol = 'CUSTOM';
UZ-4085	Issue with DNS server status.	Configured DNS servers/policies require a manual Disconnect & Connect of the tunnel when updated or when a DNS server's status changes.
UZ-4393	Wireless authentication fails via BYOD in Linux for a slider enabled SSID.	In a future release of IDM, all eap-ttls requests will be proxied over to a RaaS FR server, which should eliminate this issue. Until then, BYOD with UZ-Slider turned ON is not supported.
UZ-4827	Peers fluctuating on Service Connector Recovery mechanism: user can disconnect/connect to recover.	Certain peers are not being created on Service Connector due to an error in the IPsec logs, which is preventing connections from being established.

Table 5: Addressed Issues in 25.1.0 (continued)

Issue ID	Issue	Description
UZ-4904	The unique together constraint on the devices table was preventing another entry for the same MAC address and user ID.	When a user installs the ZTNA agent on their machine and later changes the OS on that same machine, it causes an issue. After installing the ZTNA agent on the new OS, the device registration fails because the API tries to create a new entry in the database as the unique identifier was different. An entry already exists in the database with that Mac address and user ID, causing a database error as we currently have a unique together constraint for mac_address and created_by_id in the devices table. Removing this constraint allows the creation of another entry for that device in the database when the device registration API is called. **Note:** Currently this solution is not supported on dual-boot systems (any system with more than 1 OS partially or completely installed on it). In the event that the ZTA agent is run on such a system the results will be unpredictable.
UZ-4987	Synced user removed from local user group when using JIT provisioning.	When using Just-In-Time (JIT) provisioning, adding a synced user to a local user group may lead to an unexpected behavior. If the user logs into the agentless portal, they are automatically removed from the local user group.
UZ-5501	Default certificates deployment has failed when creating new workspaces.	When a workspace is created, if the default certificates transition to a failed state as noticed in some environments. The user can use the reset option on UI to activate the default certificates again or upload their own CA and server certificate, including the private key. Same issue occurred on SE RDC as well.

Table 5: Addressed Issues in 25.1.0 (continued)

Issue ID	Issue	Description
UZ-5941	Linux agent troubleshooting is failing for applications even though the applications are accessible.	The troubleshooting process on the Linux agent occasionally fails with a timeout error. **Note:** Before executing the solution, upgrade connectors across all the workspaces. Existing Limitations once a DNS policy is updated or DNS server's status changes, you need to Disconnect & Connect the tunnel again. Tenant administrators can set two DNS servers, both should resolve all authorized application FQDNs.
UZ-5942	Tunnel disconnects when accessing Remote Desktop Applications.	When a user accesses a remote desktop app (RDP/VNC), our app goes to the background, and the RDP/VNC app comes to the foreground. Due to iOS limitations, the socket connection is terminated when our app is in the background. Upon returning to our app, the tunnel reconnects. However, during the reconnection process, the UI remains accessible, and if the user quickly tries to access the RDP app again, the connection fails because the tunnel is not yet reestablished. This background-to-foreground transition disrupts the connection, which is not immediately reflected in the UI. While the DNS feature introduced in version 25.1.0 partially addresses this scenario, this is the case with every aws and non aws environment

Table 5: Addressed Issues in 25.1.0 (continued)

Issue ID	Issue	Description
UZ-6361		• Same IP with different port but same domain case is handled in app discovery implementation. • Same IP with different domains on different ports is not supported in existing implementation. • For this when apps will be discovered it will show 1st discovered app's domain in other apps but with different ports for those apps whose IP will be same
ZTNA-27150 & ZTNA-27145	Wireless authentication fails on SSIDs that have 'UZTNA Managed' and BYOD Enabled' enabled.	Wireless authentication fails on SSIDs that have 'UZTNA Managed' and BYOD Enabled' enabled.

Known Issues in 25.1.0

The following table listsUniversal 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 25.1.0

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-3566	Application Discovery will not work on first attempt. Attempt will timeout. A second attempt is required.
UZ-4081	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.
XCD-677	If Universal ZTNA is set as the default application on the applications page, XCD redirects to the wrong URL. Workaround: Don't select the Universal ZTNA application as the default application.
XCD-679	License SKU description is not displayed on XCD user interface.
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.

Note
For unlisted devices, refer to 3rd party process.

Table 7: Access Points

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

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

Table 8: Switches

Device Model Series	Minimum NOS Version
4120	Switch Engine 32.7.1
4220	Switch Engine 32.7.1
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

Table 8: Switches (continued)

Device Model Series	Minimum NOS Version
7720	Fabric Engine 9.0.2, Switch Engine 32.6.3
x435	Fabric Engine 9.0.2, Switch Engine 32.6.3