

Extreme Management Center® Release Notes Version 8.4.0

IMPORTANT: This release of Extreme Management Center version 8.4 is considered early access (EA) and should not be installed in production.



12/2019
9036572-00
Subject to Change Without Notice

Table of Contents

Extreme Management Center® Release Notes Version 8.4.0	1
Table of Contents	2
Extreme Management Center Version 8.4 Release Notes	5
1. Enhancements in Version 8.4	5
1.1 Engines	6
1.2 Extreme Management Center	6
1.3 ExtremeAnalytics	11
1.4 ExtremeCompliance	11
1.5 ExtremeConnect	12
1.6 ExtremeControl	12
1.7 ExtremeWireless	13
2. Deprecated Features	13
3. Known Issues and Vulnerabilities Addressed	13
3.1 Known Issues Addressed in 8.4.0.116	13
3.2 Vulnerabilities Addressed	29
4. Installation, Upgrade, and Configuration Changes	30
4.1 Installation Information	30
4.1.1 Installing Without an Internet Connection	31
4.1.2 Custom FlexViews	31
4.1.3 Custom MIBs and Images	31
4.2 Important Upgrade Considerations	31
4.2.1 License Renewal	33
4.2.2 Upgrading Hardware	33

4.2.3 Free Space Consideration	33
4.2.4 Legacy Java Applications Memory Usage	34
4.2.5 Site Discover Consideration	34
4.3 ExtremeAnalytics Upgrade Information	34
4.4 ExtremeControl Upgrade Information	35
4.4.1 General Upgrade Information	35
4.4.2 ExtremeControl Version 8.0 and newer	35
4.4.3 Other Upgrade Information	36
4.5 Fabric Configuration Information	36
4.5.1 Certificate	36
4.5.2 Authentication Key	37
4.5.3 Service Configuration Change	37
4.5.4 CLIP Addresses	37
4.5.5 Gateway Address Configuration Change	37
4.5.6 Upgrading VSP-8600	38
4.5.7 Removing Fabric Connect Configuration	38
4.5.8 Password Configuration	38
4.5.9 VRF Configuration	38
4.6 Device Configuration Information	38
4.6.1 VDX Device Configuration	38
4.6.2 VSP Device Configuration	39
4.6.3 ERS Device Configuration	39
4.6.4 SLX Device Configuration	40
4.6.5 ExtremeXOS Device Configuration	40
4.7 Firmware Upgrade Configuration Information	40

4.8 ExtremeWireless Upgrade Information	41
5. System Requirements	42
5.1 Extreme Management Center Server and Client OS Requirements	42
5.2 Extreme Management Center Server and Client Hardware Requirements	42
Extreme Management Center Server	43
Extreme Management Center Client	43
5.3 Virtual Engine Requirements	44
5.3.1 Extreme Management Center Virtual Engine Requirements	44
5.3.2 ExtremeControl Virtual Engine Requirements	45
5.3.3 ExtremeAnalytics Virtual Engine Requirements	45
5.3.4 Fabric Manager Requirements	46
5.4 ExtremeControl Agent OS Requirements	46
5.5 ExtremeControl Supported End-System Browsers	47
5.6 ExtremeControl Engine Version Requirements	48
5.7 ExtremeControl VPN Integration Requirements	48
5.8 ExtremeControl SMS Gateway Requirements	49
5.9 ExtremeControl SMS Text Messaging Requirements	49
5.10 ExtremeAnalytics Requirements	49
5.11 Ekahau Maps Requirements	49
5.12 Guest and IoT Manager Requirements	50
5.12.1 Guest and IoT Manager Server OS Requirements	50
5.12.2 Guest and IoT Manager Outlook Add-in Client Requirements	50
5.12.3 Guest and IoT Manager Virtual Engine Requirements	50
5.12.4 Guest and IoT Manager Supported Browsers	50
6. Getting Help	51

Extreme Management Center Version 8.4 Release Notes

8.4.0.116
December, 2019

IMPORTANT: This release of Extreme Management Center version 8.4 is considered early access (EA) and should not be installed in production.

The Extreme Management Center Release Notes provide information on the new features and enhancements included in version 8.4, as well as issues that have been resolved and configuration changes for this release.

IMPORTANT: For upgrade and installation requirements, as well as configuration considerations, please see [Extreme Management Center Configuration and Requirements](#).

The most recent version of these release notes, as well as the most recent firmware compatibility matrix, can be found on the Extreme Networks Documentation site: <https://www.extremenetworks.com/support/release-notes>. Follow this path to the document: Management and Orchestration > Extreme Management Center > Release 8.4.

For information regarding the features supported by specific devices, see the [Firmware Support Matrix](#). Version 8.4 of Extreme Management Center supports the devices listed in the matrix.

1. Enhancements in Version 8.4

New features and enhancements are added to the following areas in Extreme Management Center version 8.4:

- [Engines](#)
- [Extreme Management Center](#)
- [ExtremeAnalytics](#)
- [ExtremeCompliance](#)
- [ExtremeControl](#)
- [ExtremeWireless](#)

For additional information about each of the features listed in this guide, refer to the documentation posted online at ExtremeNetworks.com or the Help system included with the software.

1.1 Engines

- [Upgrades Accessible to Engines without Internet Connectivity](#)
- [Operating Systems Upgrade to Ubuntu 18.04](#)

Upgrades Accessible to Engines without Internet Connectivity

Upgrades for the Extreme Management Center server, the ExtremeAnalytics engine, and the ExtremeControl engine are now accessible without internet connectivity.

Operating Systems Upgrade to Ubuntu 18.04

The Extreme Management Center, ExtremeAnalytics, and ExtremeControl engine operating systems have been upgraded to Ubuntu 18.04.

1.2 Extreme Management Center

- [ExtremeCloud Appliance VE6125 Model Supported](#)
- [New Top Devices by Resources Report Created](#)
- [Enhancements to Generate Show Support View](#)
- [Enhancements to Multi Cloud Dashboard](#)
- [Introducing Fabric Assist](#)
- [Added Support for Additional Device Types](#)
- [Additional Device Types Can Now Be Managed via ZTP+](#)
- [Additional Trap Definitions Available](#)
- [Improvements to Add Device to Group View](#)
- [Ability to Display Port Extenders in Extreme Management Center](#)
- [JVM Runtime Memory Value Added to Server Report](#)
- [Ability to Add Identification Information to the Status Bar](#)
- [Enhancements to Inventory Dashboard and Reports](#)
- [Ability to Sort Multiple Columns in FlexViews Table](#)
- [Improvements to Extreme Management Center Filter Tool](#)

ExtremeCloud Appliance VE6125 Model Supported

Extreme Management Center now supports the ExtremeCloud Appliance VE6125 model.

New Top Devices by Resources Report Created

A new Top Devices by Resources report has been created, which combines the data from (and replaces) the former Top Host and Top Switches by Resource reports. Also, the temperature has been configured for Celsius and Fahrenheit degrees, and the maximum device count has been increased to 100 devices.

Enhancements to Generate Show Support View

A Show Support Lite ZIP file can now be generated from the **Administration > Diagnostics > Support > Generate Show Support** view. Additionally, a **Start Show Support** option has been added to the existing **Start** button, and a new **Start Show Support Lite** button has been added to the view.

Enhancements to Multi Cloud Dashboard

The **Network > Multi Cloud Dashboard** has been streamlined, and new data columns have been added to the Detail views on the **Private Cloud** tab.

Introducing Fabric Assist

Fabric Assist helps you migrate your existing VLAN-centric network to a Fabric Connect network. Missing port templates are now inherited through the device. Fabric Assist accomplishes the migration by enhancing VLAN provisioning using the following features:

- **VLAN Trunk Mode** – Identifies a port as a VLAN trunk and automatically adds all the device VLANs as tagged.
- **VLAN Range** - Imports many VLANs to the device all at once instead of manually adding and editing one entry at a time.
- **Layer 2 VSN Service Creation** - Automatically maps VLAN entries to Layer 2 VSNs.
- **VLAN Pruning** - Prevents the unnecessary configuration of VLANs that have no egress.

Added Support for Additional Device Types

Extreme Management Center now supports the following device types:

- ExtremeXOS X465
- AP505
- AP510

- AP560i
 - AP560u
 - AP560h
 - AP7632-680B30-TN
 - AP7632-680B40-TN
 - AP7662-680B30-TN
 - AP7662-680B40-TN
 - SLX 9030
 - SLX 9640
 - V300
 - VSP4900
 - VSP 7400
- Extreme Management Center now also supports LAG, MLAG, and Fabric Connect functionality for VSP-86x Tsunami devices.
- XA1480
 - XA1550
 - ExtremeCloud Appliance 4.56.02

Additional Device Types Can Now Be Managed via ZTP+

The following device types can now be managed via ZTP+:

- ExtremeXOS devices in a stacked configuration running ExtremeXOS Cloud Connector version 3.4.x or later.
- ERS3600 on which firmware version 6.4 or later is installed.
- ERS4900/5900 on which firmware version 7.8 or later is installed support discovery via ZTP+.

Additional Trap Definitions Available

Extreme Management Center now includes trap definitions for ERS and VSP devices.

Improvements to Add Device to Group View

Improvements to the Add Device to Group window include a larger window size, the addition of a search field, and better navigation via tree expansion and selection persistence.

Ability to Display Port Extenders in Extreme Management Center

You can now indicate which ports are included in a port extender and which ports are included in a controlling bridge. In releases prior to Extreme Management Center version 8.4, all ports that were included in an extended bridge displayed as a part of the device. Beginning in Extreme Management Center version 8.4, you can define the ports that are part of the controlling bridge and those that belong to the port extenders that are connected to that controlling bridge. Additionally, you can add your port extenders to maps you create to display the relationships between a controlling bridge and the port extenders to which it is connected.

JVM Runtime Memory Value Added to Server Report

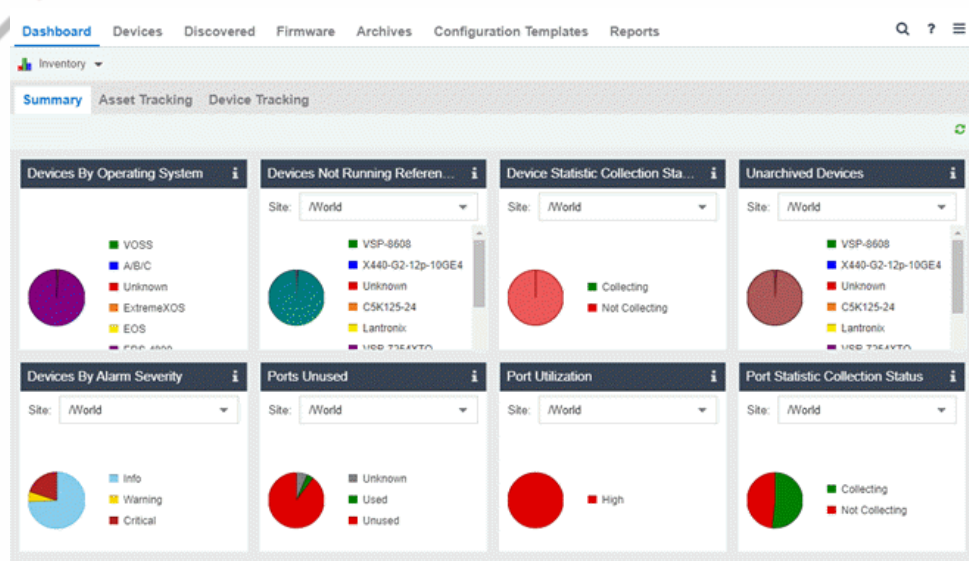
The JVM runtime maximum memory value has been added to the Server CPU/Memory report.

Ability to Add Identification Information to the Status Bar

The ability to add customized identifying information to the Status Bar in the footer of Extreme Management Center windows, via the **Administration > Options** tab has been added.

Enhancements to Inventory Dashboard and Reports

Enhancements to the [Inventory Dashboard](#) (accessible via the **Network** tab) include new pie charts and reports that enable you to view the activity and status of the devices and ports that comprise your network.



The following charts are included on the Inventory Dashboard:

Devices By Operating System - Categorizes devices by network operating systems.

Devices By Alarm Severity - categorizes the devices, at the site you select, based on the current alarms that they have.

Devices Not Running Reference Firmware - categorizes the devices by device type, at the site you select, that currently are not running reference firmware.

Ports Unused - categorizes the ports, at the site you select, that currently are and are not being used.

Device Statistic Collection Status - categorizes the devices, at the site you select, that currently are and are not collecting statistics.

Port Utilization - categorizes the number of ports, at the site you select, with moderate or high utilization.

Unarchived Devices - categorizes the devices, by device type, at the site you select, that have not been archived in the last 30 days.

Port Statistic Collection Status - categorizes the ports, at the site you select, that currently are and are not collecting statistics.

The criteria for each chart is configurable, and selecting each chart opens a report displaying details about the device and port activity.

The Inventory Dashboard also includes Asset and Device Tracking tabs. Use these tables to monitor changes made to assets and devices in your network.

Ability to Sort Multiple Columns in FlexViews Table

New functionality allows you to sort multiple columns in the FlexViews table via the **Network > Devices** tab.

Improvements to Extreme Management Center Filter Tool

Improvements to the filter tool include:

- The **Show Filters** button is always active.
- All active filters for a grid display when **Show Filters** button is selected.
- A message displays if there are no active filters.
- All active filters can be expanded (or collapsed) for a quick overview of what is being filtered.

- Any active filter can be modified by changing the values in the window. Changes are immediate.
- Any active filter can be removed by selecting the minus symbol to the right of the filter. Filter removal is immediate. The filter becomes available in the **Add Filters** field.
- New filters can be added to the grid by selecting the column title from the field in the top toolbar. Active filters do not appear in this field.

1.3 ExtremeAnalytics

- [Streaming Flow Data from ExtremeAnalytics into Splunk](#)
- [Improvements to Response Time Dashboard](#)

Streaming Flow Data from ExtremeAnalytics into Splunk

ExtremeAnalytics supports the ability to stream flow data from an ExtremeAnalytics engine into Splunk. This support includes instructions on how to configure IPFIX to work with Splunk and files that you can copy to the Splunk server to facilitate integration.

Improvements to Response Time Dashboard

The ExtremeAnalytics Response Time dashboard, when grouping by interface, displays only the device IP address for received Application Telemetry flow data when it is lacking sampled packet information.

1.4 ExtremeCompliance

The Information Governance Engine is now ExtremeCompliance. When you install Extreme Management Center 8.4, your version of the Information Governance Engine is automatically upgraded to ExtremeCompliance.

The new version supports the following device types:

- VSP4900
- VSP1440
- VSP1480
- VSP 7400-48Y
- AP560i

- AP560u
- AP560h

Regimes and audit tests created in versions 8.1, 8.2, and 8.3 are retained following the upgrade.

1.5 ExtremeConnect

- [New End-System and OS Fields Added](#)
- [Extreme Connect Configurations Included in Extreme Management Center Backups](#)

New End-System and OS Fields Added

New custom end-system data fields and additional operating system data fields have been added to Extreme Connect.

ExtremeConnect Configurations Included in Extreme Management Center Backups

Extreme Management Center backups now include ExtremeConnect configurations.

1.6 ExtremeControl

- [Enhanced Enforce Preview Functionality for ExtremeControl](#)
- [ExtremeCloud Appliance Uses CoA for Reauthentication](#)
- [NAC Rule Engine Table Includes Compact View of Rules](#)
- [Ability to Select Multiple Switches and Edit Switch Properties](#)
- [Improvements to the ExtremeControl Group Editor](#)

Enhanced Enforce Preview Functionality for ExtremeControl

The Enforce Preview functionality is enhanced for the ExtremeControl engine configuration, displaying additional details about the enforce.

ExtremeCloud Appliance Uses CoA for Reauthentication

ExtremeCloud Appliances now use Change-Of-Authorization (CoA) by default for reauthentication.

NAC Rule Engine Table Includes Compact View of Rules

The NAC Rule Engine table has been revised to provide a more compact view of the rules. Use the Expand Rule Details item in the View menu of the Rule table to show all Conditions and Actions for every rule.

Ability to Select Multiple Switches and Edit Switch Properties

The ability to select multiple switches on an ExtremeControl engine or an Engine Group and edit the switch properties individually is added in Extreme Management Center version 8.4.

Improvements to the ExtremeControl Group Editor

General improvements to the Group Editor include streamlined presentation of data, shorter load times, and better performance. Also, the editing functionality has been improved to allow administrators to save their changes without the need to lock other users out of the group, allowing more than one user to make changes at the same time.

1.7 ExtremeWireless**11ax Radio for AP5xx Models Supported**

ExtremeWireless now supports 11ax Radio for AP5xx models.

2. Deprecated Features

Beginning in Extreme Management Center version 8.4, the legacy Java applications (Console, MIB Tools, NAC Manager, and Policy Manager) are deprecated and disabled by default. These applications will no longer be available in version Extreme Management Center 8.5. To use the legacy Java applications in version 8.4, follow the instructions in the [GTAC knowledgebase article](#).

Beginning in Extreme Management Center version 8.5, the Extreme Management Center server will no longer support native installation for the Windows operating system.

3. Known Issues and Vulnerabilities Addressed**3.1 Known Issues Addressed in 8.4.0.116****Extreme Management Center Issues Addressed****ID**

3. Known Issues and Vulnerabilities Addressed

When setting the Global authentication configurations for a device, the default option was Disable authentication on Interswitch links . Now, for the Port Authentication Status window, the default option is now Disable authentication on all ports .	01883054
An error message was displayed when Ekahau maps with a customer wall type were imported.	01741222
In Fabric Manager, an unauthorized user entry was appearing in the .ssh->authorized_keys folder.	01909821
When using "Add Device" from the Devices tab when in the context of a group, the device was not being added to the group and could only be seen by switching to another device contest (for example, Sites).	01953687
Extreme Management Center was displaying unexpected error counts in the SNMP Details view. Also, "end of table" was being included as an error.	01863719
In Fabric Manager, the tree view refresh was deleting Topology Definition and Service Definition unsaved data.	1936883
Fabric Manager was not displaying FA links for devices that were enabled and then disabled for SPBM, and then configured for FA.	01861595
With Extreme Management Center's version 8.3, delay in IP Resolution to VOSS and BOSS devices was causing the IP Address Resolution queue to overflow.	01887823
Retrieving FlexViews against multiple devices was not logging status in the Operations panel.	-----
Extreme Management Center was not able to add the Guest and IoT (GIM) engine if Load Balancing was enabled.	-----
The Configuration Evaluation Tool window was not the correct size, based on Extreme Management Center's browser size. The tool field has been reconfigured to resize, based on the vertical view port. Additionally, a vertical scrollbar has been added to the User Input tab.	-----
Some changes to devices, made using the Add Devices function on the Discovered tab, were not being made.	-----
After adding VSensor licenses, Extreme Management Center had to be restarted manually for the licenses to be activated.	-----

3. Known Issues and Vulnerabilities Addressed

FlexViews retrieved for devices were not displaying an empty row for IPs when there was no response from the device. Now, there is a FlexView Option, Show Empty Row , which can be enabled so the FlexView will display an empty row for each device that does not respond to the FlexView query.	-----
Passwords that contained multiple dollar sign (\$) characters successively were being stripped in email and SMS notifications.	-----
When executing CLI commands, if some devices were not reachable, no exception was seen in the results.	-----
The Port Duplex mode was incorrect on VSP and Summit Series switches.	-----
Inventory Manager settings for SCP/SFTP had an incorrect default root path when Extreme Management Center was installed as non-root.	-----
Discovered devices were not being automatically added even though the Automatically Add Devices Action was selected.	-----
The Network > VPLS Summary on a site or map was unable to launch.	-----
Workflows that depended on the deviceIP variable (as opposed to the devices variable) for device selection were not working and caused activities within the workflow to be skipped.	-----
ExtremeCloud Appliance statistics collection was failing every collection cycle with IOOB exception.	-----
On the Tasks > Scheduled Tasks tab, the Weekly Scheduled Tasks were not displaying the correct days of the week.	-----
Extreme Management Center was discarding traps sent from VSP devices that were successfully configured with an SNMPv3 NoAuthNoPriv credential configuration.	-----
Adding a new device in the context of a User Device Group was not also adding that device to the group. Also, the User Device Group selection window was fully expanding the selection tree when opened.	-----
When attempting to save IP addresses to a site included in a map, an error caused the "Could Not Load Report" message to display.	1817029
V3 Traps registered for BOSS ERS devices were not being recognized by Extreme Management Center.	01819453

3. Known Issues and Vulnerabilities Addressed

No alert message displayed if changes were made, but not saved, to entries in the End-Systems Groups function in the Group Editor. Warnings that changes will be lost if not saved have been added.	1896149
IP Addresses or device names had to be entered manually when adding entries to a Location Group in the Group Editor panel. A new Select Devices button, which allows users to select from a list of network devices, has been added.	1738208 01868775
The flow collector was attempting to apply a port-based IDs to flows with no identification without checking if the matching port-based fingerprint was enabled.	01855275
Packet capture was being applied to all switches, regardless of whether the switches reported the flow selected for capture, causing a delay in responsiveness. Packet capture now only applies to those switches that reported the flow selected by the user, and multiple packet captures for a single IP address are processed simultaneously.	01849005
Creating a Location Group with an Interface of Wireless and all other options set to Any was matching wired end-systems.	-----
ZTP+ was unable to upgrade and onboard new devices when /world was configured to Updates = Never for configuration and firmware upgrades.	1941725
On ZTP+ image upgrades, special characters in the Extreme Management Center username or password caused the upgrade to fail.	-----
Custom time filters in Alarms and Events were discarded when new events occurred.	01937890 01919341
In the legacy console, the graphing function for Port Utilization in Percent was not rendering and the Utilization in Percent option was not displaying.	01923651
Some table columns in Extreme Management Center did not sort in numeric order.	01937793
In Extreme Management Center, when a map was exported as an SVG image, the device images did not render correctly.	-----

3. Known Issues and Vulnerabilities Addressed

For ZTP+, the Use Discovered checkbox did not allow customers to select whether to use the discovered IP or use both the discovered IP and management interface.	01925201
The Device Restart operation for VSP8606 reported a failure when the reset operation was successful.	-----
Users were not notified when VSP archive/restore was used with a non-admin CLI profile.	-----
The Archive option for VSP devices to download the device backup file did not include the full backup, it only included the text file.	-----
Extreme Management Center users with multipart usernames were incorrectly restricted from editing other users in the Authorized Users table.	-----
Extreme Management Center access of Juniper switches was not working. Enhancing the detection of Management Login authentications resolved the issue.	01196551 01706511 01706510 01737211
Extreme Management Center access of Bluecoat switches was not working. Enhancing the detection of Management Login authentications resolved the issue.	1200082
FlexViews created for a User Device Group that contained both Ports and Devices did not display the data for all of the selected ports and devices.	-----
Authorized Users added to an Authorization Group as a result of Automatic Member functionality were incorrectly able to be edited by other users.	1399058
The Tasks tab is showing up and reporting in the starting page for user profiles that may not include those features.	1553521
Traps were not displaying varbind information properly in the information column.	1550414
Attempting to log in to Extreme Management Center using a password that contained special (non-alphanumeric) characters was not successful.	01706905
Users were able to edit system scripts, which caused some features to stop working. The scripts are no longer editable.	-----

3. Known Issues and Vulnerabilities Addressed

Virtual Networks and SSIDs on an ExtremeCloud Appliance may not display on the Wireless > Network tab.	01907673 01918004 01918005
Dragging an AP icon outside of the floor map view caused odd results.	01752414
The Port Usage Details table was not displaying properly. To resolve the issue, the Collection status per port was added as this is also required to have a valid used percent statistic created.	01935642
Extreme Management Center does not allow for PVID to be a tagged vid.	-----
Searching for alarm history By Source was not showing alarms if a device has a nickname and the device tree option for Device Tree Name Format is set to Nickname .	01784068 01811444
Highlighting and deleting the Password field on the Administration > Profile > CLI Credentials tab was not allowing a save of the changes.	01908341
Port/VLAN data was not available (for example, in the VLANs column of the Ports tab of the DeviceView and via Northbound Interface queries) immediately after startup until Extreme Management Center reloaded the data from the device.	01864826
ExtremeXOS Configuration Archive/Restore scripts do not allow users to override configure file from default value of primary.	1786645
Launching WebView for an Extreme Wireless Controller uses the IP address rather than the name of the controller.	1788531
Attempting to synchronize Fabric Manager with Extreme Management Center failed because the root password contained special (non-alphanumeric) characters.	01818533
Real Capture on AP3805_ROW fails and displays an “Unknown name value” error message.	01820613
Because of security vulnerabilities, the JDK was migrated from Oracle Java to Amazon Corretto.	01854576 01879829
Changing the Inventory Settings to Disable the Firmware Download MIB and Configuration Download MIB overrides produced empty confirmation prompts and the settings were not saved.	01912457

3. Known Issues and Vulnerabilities Addressed

Scripts in Extreme Management Center were failing if the CLI output contained non-printable characters.	01849224
---	----------

To improve help, tooltips were added to all columns in the Administration > Diagnostics > SNMP Details table.	01863719
--	----------

Tracking SNMP PDU errors was confusing. To address this, the following changes were made:	01863719
---	----------

- Capture SNMP PDU error details by IP.
 - Use List of IPs and check SnmpTrace in Configure Network Monitor Diagnostics.
 - Reset the view to start.
-

The progress bar in the Operations panel remained at 0% for firmware downloads for ERS devices.	-----
---	-------

Alias information was missing from Endpoint Locations after importing them from a CSV file.	01874421 01936119
---	----------------------

Functions that heavily utilize SNMP, such as device statistics collection and policy enforcement, can take excessive time to complete.	1900346 1910244 1928480
--	-------------------------------

Links for VSP and ERS devices included in a map were not changing to red when the port had a Status of Down .	-----
---	-------

Adding a device to the Network > Device > User Device Groups was slow. Usability improvements were added to the User Device Groups selection dialog, including tree state persistence, search filtering, and a better initial layout.	-----
--	-------

VLANs in the Policy Egress tab that are not used in a role or rule were not displaying in the Role/Service Usage dialog.	1878530
---	---------

Selecting or deselecting the Enable Network Monitor Cache checkbox was not working properly and the Save button was not enabled after making changes to the options on the tab.	-----
---	-------

3. Known Issues and Vulnerabilities Addressed

ExtremeXOS devices running the following firmware versions were not displaying Fabric Attach settings correctly in Fabric Manager:

- 22.5.1.7-patch1-*
- 22.5.1.7-patch2-5 (last one – patch2-5 and later if any)
- 22.5.1.7-patch5-*
- 22.5.1.7-patch6-*
- 22.6.1.4-patch2-2 and later
- 22.6.1.4-patch3-*
- 22.7
- 30.*

Scheduling an inventory task (for example, creating a device archive) and then applying an Extreme Management Center license (for example, NMS Advanced) was causing Extreme Management Center to create an identical inventory task.	01941537 01944216
---	----------------------

Floor plan maps using rectangle objects to specify exterior walls were not displaying wireless coverage properly.	1914363
---	---------

Discovering potentially duplicate devices in a site with Automatically Add Device selected was automatically adding one of the devices to the site, instead of adding all of the potentially duplicate devices to the Discovered tab so the user could select the device to add to the site.	-----
--	-------

ExtremeXOS XMODs included in a patch release were not compatible for upgrade with existing devices that match the firmware release fields.	1937246
--	---------

Extreme Management Center did not support ExtremeCloud Appliance version 4.76.	-----
--	-------

An unnecessary server.log exception could be reported when a port element in a user device group no longer has its associated entity data.	1887304
--	---------

Special characters were not permitted in audit test names.	1908562
--	---------

The ExtremeXOS SNMP v1/v2 Disabled audit test appeared to fail.	1908562
---	---------

3. Known Issues and Vulnerabilities Addressed

Increasing the number of VRF configurations adversely affected VSP SNMP performance. This issue is resolved by upgrading to VSP release 8.1.1 or later and VSP 8600 Series release 6.3.3 or later.	-----
Sorting of a device's L2 Services table was not working.	-----
Enforcing site VLANs that have Multicast or IGMP settings to a device was incorrectly indicating differences between the device configuration and Extreme Management Center.	-----
Configuration validation was being performed during enforcement for features that the device does not support.	-----
Applying a port template is no longer a one-time import of settings to that port. Ports assigned a port template will always reflect that port template's settings. To override port settings, you must create a new template and assign it to the port or set the port's template value to Use Local Settings, which enables you to apply any setting to that port.	-----
Users were able to create an L3VSN service using either the MgmtRouter or GlobalRouter, which cannot support these services.	-----
After successful enforcement to an ExtremeXOS device, the enforcement preview panel still shows that there are VLAN differences.	-----
Users were able to create Switched UNI or Transparent UNI services in a Service Application that shares the same Service ID as an L3VSN service.	-----
When there was no Authorization Group Device Mapping for a device, the Contact Device by Group's Profile action was using NA. Now, the Device Mapping's "<*>" designation is respected, and the default Profile for the device is used.	-----

3. Known Issues and Vulnerabilities Addressed

Editing an inherited configuration from a Service Application or Site may change the Source ID of that edited item. -----

- Items that exactly match the inherited configuration will have their Source ID revert to the original location of that item.
- Items that do not exactly match the inherited configuration will have their Source ID marked as Local.

Users were unable to create L2 or L3 Services that did not have a name associated with them. -----

While editing a device, the CLIP Addresses table were not displaying all IPv4 and IPv6 addresses associated with a VSP device (CLIP, VLAN, BROUTER, MGMT). Now the user will be able to create, edit and delete CLIP addresses in this table, while the other address types (MGMT, VLAN, BROUTER) will not be editable by the user. -----

Creating a port template in a sub-site will potentially create a port template with the same name in /World with an invalid configuration. -----

Syslog or SNMP Trap messages received from a device that has a source IP address that is not the same as the primary management address for that device can cause Alarm Mail notifications to be sent without a Device ID. -----

Enforce preview was incorrectly detecting VLAN differences for devices for which VLAN provisioning is not supported. -----

Ports added to a Switched UNI or Transparent UNI service inherited from Service Application while editing a device can possibly be lost once that service is updated. -----

L2 and L3 Services defined in a Service Application were incorrectly defined as duplicates if they shared the same name. -----

ExtremeAnalytics Issues Addressed

ID

Virtual Sensor status updates occasionally would not display in the tree view. -----

3. Known Issues and Vulnerabilities Addressed

ExtremeAnalytics flow rate data was not available if unused Analytics Engines were configured.	01902842
The AppldMgrServer was failing to start and was displaying a java.lang.NullPointerException error when custom enterprise definitions missing names were defined.	-----
The Device Type Definitions view, on the Devices tab, was taking an inordinate amount of time to load.	-----
Live updates of the ExtremeAnalytics fingerprints were occasionally failing, and a No Files Found in Directory error displayed.	-----
Accessing the End-Systems Applications Summary for a client for which Extreme Management Center resolved the IP address was displaying a 0 for the Clients , Application , and Application Groups columns.	01877808
The ExtremeAnalytics engine was running out of storage space as a result of duplicate entries saved in the log.	01909813
After running the Configure VOSS App-Telemetry script, no status was displayed indicating whether the device was reachable.	01897718
During upgrades, the ExtremeAnalytics engine was changing the order of interfaces even if the user has customized the definition.	01910066
ExtremeAnalytics did not allow you to disable the Virtual Sensor integration. You can now disable this integration to improve performance.	-----
Devices managed using an SNMP Context String were causing a NumberFormatException error in the server.log.	-----
Workflow Signal Activity was not working correctly when triggered from an alarm/trap.	-----
Devices discovered via the ZTP+ process with a Poll Type of SNMP were occasionally automatically updated by Extreme Management Center to a Poll Type of ZTP+ .	01893092

3. Known Issues and Vulnerabilities Addressed

Security enhancements were requested for the Analytics Engine, 01937342 and implemented as follows:

- The server certificate has been regenerated with an improved hashing algorithm.
- The server responses now includes the X-Frame-Options HTTP header to protect against clickjacking.

Inventory override settings (for example, File Transfer Mode) for a device were changing to default values after a device refresh/rediscover or after a server restart. -----

Inventory configuration templates were occasionally not available in the **Restore Configuration** window. -----

Selecting the **Application Flows** tab when users did not have access to an Analytics engine that was modeled on their server resulted in an error message and a browser error message repeatedly displaying every few seconds. -----

Site collectors did not allow users to select countries and cloud provider regions to be tracked or not tracked. -----

ExtremeAnalytics engines could not interoperate with Extreme Management Center using a non-standard (8443) server port. 01800638

When the input/output interface was unavailable, Analytics was not showing any device information in the Response Time dashboard. 01846836

When uninstalling a virtual sensor, the Analytics Virtual Sensor grid was not marking it as Uninstalling, and there was no progress shown in the operation panel. -----

When installing a new virtual sensor, the tree panel was not getting updated as soon as the installation finished.

In the Analytics **Top Applications for Clients** window, the Bandwidth column was not sorting correctly. -----

The Search Criteria page on the **Analytics > Browser** tab was displaying duplicate choices from the drop-down lists for all fields that show the choices **All** and **Custom**, except the Application Groups field. -----

A GeoLocation error was sometimes logged after an enforce. -----

3. Known Issues and Vulnerabilities Addressed

The **Analytics > Application Flows** tab contained inconsistent menu selections for the Show types.

ExtremeControl Issues Addressed	ID
In ExtremeControl's End-System IP Groups, the presence of an IP mask entry was occasionally causing authentications to fail.	1890590
In the Rule configuration for ExtremeControl, it was sometimes possible to scroll past the end of the list of rules and see only blank space.	01931514
In the ExtremeControl engine's Captive Portal, if email domain names were stripped during authentication, a user could register more than their maximum allowed number of devices.	01834349
In the Rule configuration for ExtremeControl, individual rules were not remembering whether their details panel had been expanded, resulting in every rule being collapsed by default.	01897740
The ExtremeControl engine Rule Engine table was not displaying the full set of rules, when a large number of rules was configured. The table has been reworked to provide a more compact view of the rules.	01954420
802.1x authentication was occasionally allowing 0 length passwords to successfully authenticate.	01878461
In the Guest and IoT Manager (GIM), a username created using an email address was not authenticating in ExtremeControl.	01888057
Hexadecimal representations of integer type attributes were not encoded in Disconnect or CoA RADIUS frames.	-----
IP Addresses or device names had to be entered manually when adding entries to a Location Group in the Group Editor panel. A new Select Devices button, which allows you to select from a list of network devices, has been added.	1738208 01868775
No alert message was displayed if changes were made, but not saved, to entries in the End-Systems Groups function in the Group Editor. Warnings that changes will be lost if not saved have been added.	1896149
When the Display Welcome Page option in the ExtremeControl captive portal was disabled, the Welcome page still displayed briefly before the Login/Register page displayed.	-----

3. Known Issues and Vulnerabilities Addressed

The Enforce Preview option for the Access Control Engine (Control > Access Control > Access Control Engines > Enforce Selection > Preview) was showing changes that were previously enforced for custom DHCP fingerprints instead of showing just the new changes.	-----
A Provisioner was unable to log into GIM if the following occurred: <ol style="list-style-type: none">1. The Local Password Repository Password Hash Type in Extreme Management Center was changed from PKCS5 (the default) to SHA1 for the GIM Provisioner account.2. The Provisioner user's password was subsequently changed in GIM.	01897869
In the Guest and IoT Manager (GIM), when the LDAP Sponsor option was selected, the Sponsor's Email field was not editable. Now, all sponsor-related details auto-populate when the LDAP Sponsor option is selected.	01891727
Global services created using copy/paste and added to a role (in an Extreme Management Center policy domain) were not persisted in the role's services list when the domain was saved.	1934247
Inbound/outbound rate limits for Policy Manager CoS were not supported for ExtremeCloud Appliance.	-----
The End-System Application Details window would not populate with data when opened using Global Search for an end-system.	01877808
Access Control engines running assessment and remediation sometimes caused SQL exceptions in the Extreme Management Center sever log when accessing a deprecated database table.	01928578
A missing image in the captive portal style sheet (causing an HTTP 404) could have prevented registration from working.	-----
Invalid MAC addresses with more than one type of delimiter could be added to ExtremeControl end system MAC groups.	01923226
Captive Portal did not work when the ExtremeControl engine's captive portal interface was configured with an IPv6 address, but lacked an IPv6 hostname.	-----
The Access Control engine was making continuous and frequent SNMP requests to switches that are down or unreachable.	01559177 01811345 01890792

3. Known Issues and Vulnerabilities Addressed

Enhanced the detection of Management Login authentications. 01776798
01900232
01917707

Automatically generated ExtremeControl Groups were needlessly recreated at Extreme Management Center server startup: Access Points, Administrators, Printers, Servers, and VoIP Phones. 01783964

The attribute lookup feature, which is available when editing LDAP User and LDAP Host Groups in the ExtremeControl Group Editor, has moved from the **Add...** button to a new **Attribute Lookup...** button. -----

Sorting the Access Control End Systems table by the Switch Port column was not sorting correctly. 01838795

The **Access Control > End System Details > Health Results** table was not displaying the **Start Scan** and **End Scan** details. 01859542

Attempting to create a new ExtremeControl configuration was failing. 01866382
01869832
01878243

Creating unique Captive Portal registration buttons was not possible. To allow further customization the following CSS classes were added to the NAC Captive Portal buttons: 01861530

- portalButtonLogin
- portalButtonRegister
- portalButtonCompleteRegistration
- portalButtonAssessmentAcknowledge
- portalButtonReattemptAccess

The old 'portalButton' class can still be used to modify all of the above buttons.

If the old 'portalButton' class is used simultaneously with the above classes, the above classes will take precedence over the 'portalButton' class.

Repeated attempts to SNMP manage unresponsive devices from ExtremeControl was slowing down IP resolution and Enforce processes. -----

3. Known Issues and Vulnerabilities Addressed

Sponsor Links in GIM sponsor request emails were sent using the IP of GIM instead of the FQDN of the hostname present on the system or installed certificate.	01911889
Date/time display format options were not persisting and being reflected in UI when changed.	1868647 01883636
Selecting multiple switches and editing the switch properties was not allowed in the Access Control > Switches dialog. Now you can edit a select number of properties between multiple switches, which is like the Java Thick Client.	-----
Enforcing the PVI VLAN to an ExtremeXOS device failed when changing the VID associated to that VLAN in the device's PVI island, or when moving the device from one island to another with a different VID.	01916898
Simultaneously enforcing configuration to the NAC while configuring users on the Guest and IoT Manager sometimes resulted in the NAC returning an Internal Server Error message.	01916208
The Use RADIUS Accept Policy link in the Control authorization rules configuration opened an empty Edit Policy Mapping dialog.	-----
The Auth. Access Type for ExtremeControl engine devices was not set to Manual Radius Configuration .	-----
ExtremeControl was not using CTRON-ALIAS-MIB as the mechanism for MAC to IP resolution via SNMP for ExtremeControl engines.	01935200
The <i>invert</i> option for Authentication Method rule matching did not work properly in ExtremeControl.	1937075
The ExtremeControl Assessment agent for OSX did not fully support 64-bit operating systems.	01925944 01932152
Values in ExtremeControl location groups could not be greater than 512 characters.	01937960 01941399
For Guest and IoT Manager in ExtremeControl, the Record Enabled checkbox accessibility for users could not be managed by administrators.	01916229
The background, title, brand logo, font type and font color on the Provisioner Login page for Guest and IoT Manager were not customizable.	01916189

3.2 Vulnerabilities Addressed

This section presents the vulnerabilities addressed in Extreme Management Center 8.4:

- The following vulnerabilities were addressed in the Extreme Management Center, ExtremeControl, and ExtremeAnalytics engine images:
 - CVE-2018-0500, CVE-2019-5481, CVE-2019-5482, CVE-2018-18074, CVE-2019-17546, CVE-2019-14973, CVE-2018-10779, CVE-2018-12900, CVE-2019-7663, CVE-2018-17000, CVE-2018-19210, CVE-2019-6128, CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303, CVE-2019-18408, CVE-2018-17456, CVE-2019-16056, CVE-2019-16935, CVE-2019-14287, CVE-2019-6977, CVE-2019-6978, CVE-2019-1543, CVE-2018-0734, CVE-2018-0735, CVE-2018-12015, CVE-2018-20060, CVE-2019-11236, CVE-2019-11324, CVE-2018-14498, CVE-2019-2201, CVE-2018-6557, CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126, CVE-2019-1010305, CVE-2019-9893, CVE-2018-11574, CVE-2018-10844, CVE-2018-10845, CVE-2018-10846, CVE-2019-3829, CVE-2019-3836, CVE-2016-4429, CVE-2017-8779, CVE-2018-14622, CVE-2019-3842, CVE-2019-7307, CVE-2019-11481, CVE-2019-11482, CVE-2019-11485, CVE-2019-11483, CVE-2019-15790, CVE-2019-3462, CVE-2019-18218, CVE-2018-10903, CVE-2019-5094, CVE-2019-2745, CVE-2019-2762, CVE-2019-2766, CVE-2019-2769, CVE-2019-2786, CVE-2019-2816, CVE-2019-2818, CVE-2019-2821, CVE-2019-2842, CVE-2019-6129, CVE-2019-7317, CVE-2019-7304, CVE-2019-12749, CVE-2019-13012, CVE-2019-9924, CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7665, CVE-2019-13636, CVE-2019-13638, CVE-2015-9253, CVE-2018-14851, CVE-2018-14883, CVE-2016-6153, CVE-2017-10989, CVE-2017-13685, CVE-2017-2518, CVE-2017-2519, CVE-2017-2520, CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2019-8457, CVE-2019-9936, CVE-2019-9937, CVE-2017-13720, CVE-2017-13722, CVE-2019-6133, CVE-2019-11922, CVE-2017-5953, CVE-2019-12735, CVE-2019-11068, CVE-2018-20843, CVE-2016-7942, CVE-2016-7943, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600
- The following vulnerabilities were addressed in the Extreme Management Center and ExtremeControl engine images:
 - CVE-2019-7317
- The following vulnerabilities were addressed in the ExtremeControl engine image:
 - CVE-2019-10092, CVE-2019-10208, CVE-2019-10209

4. Installation, Upgrade, and Configuration Changes

4.1 Installation Information

When you purchased Extreme Management Center, you received a Licensed Product Entitlement ID that allows you to generate a product license key. Prior to installing Extreme Management Center, redeem your Entitlement ID for a license key. Refer to the instructions included with the Entitlement ID sent to you.

For complete installation instructions, refer to the [installation documentation](#) located on the Documentation web page:

<https://www.extremenetworks.com/support/documentation/>.

If you have requested an Extreme Management Center evaluation license, you received an Entitlement ID. This Entitlement ID allows you to generate a product evaluation license key. Refer to the instructions included with the Entitlement ID to generate the license key. Use the key when you install the product.

Evaluation licenses are valid for 30 days. To upgrade from an evaluation license to a purchased copy, contact your Extreme Networks Representative to purchase the software. Refer to the Upgrading an Evaluation License section of the *Extreme Management Center Installation Guide* for instructions on upgrading your evaluation license.

IMPORTANT: The NetSight Server service may not start after installing Extreme Management Center version 8.0 on a system on which a Windows Server operating system is installed. Restarting Windows corrects this issue.

The **Compliance** tab is available and supported by Extreme on an Extreme Management Center engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support ExtremeCompliance functionality, but python version 2.7 or higher must be installed. Additionally ExtremeCompliance functionality requires the git, python2, python mysql module, python setuptools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

4.1.1 Installing Without an Internet Connection

If your Linux system requires an operating system upgrade, you are prompted to upgrade using either an internet connection or locally (without an internet connection) if no additional Ubuntu packages need to be installed.

!!! ATTENTION !!!

We can attempt to upgrade the OS without using the internet if there were no extra Ubuntu packages installed. If there were extraneous packages installed, the upgrade will fail with this method.

Do you want to attempt a local in-place upgrade of the OS and reboot when complete? (Y/n)

4.1.2 Custom FlexViews

When reinstalling Extreme Management Center Console, the installation program saves copies of any FlexViews you created or modified in the `<install directory>` `\.installer\backup\current\appdata\System\FlexViews` folder.

If you are [deploying FlexViews](#) via the Extreme Management Center server, save them in the `appdata\VendorProfiles\Stage\MyVendorProfile\FlexViews\My FlexViews` folder.

4.1.3 Custom MIBs and Images

If you are deploying MIBs via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\MIBs` folder.

If you are deploying device images (pictures) via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\Images` folder.

4.2 Important Upgrade Considerations

Extreme Management Center 8.4 supports upgrades from Extreme Management Center version 8.2.x (except version 8.2.2) or 8.3.x. If you are

upgrading from version 8.1 or earlier of NetSight/Extreme Management Center, you must perform an intermediate upgrade. For example, if you are upgrading from NetSight 7.1, you must first upgrade to the latest Extreme Management Center 8.1 release, then upgrade to the latest Extreme Management Center 8.2 or 8.3 release, then to 8.4.

IMPORTANT: When performing an upgrade, be sure to back up the database prior to performing the upgrade, and save it to a safe location. Use the **Administration > Backup/Restore** tab to perform the backup.

The NetSight Server service may not start after upgrading Extreme Management Center to version 8.0 on a system on which the Windows Server 2008 operating system is installed. Restarting Windows corrects this issue.

- When upgrading the Extreme Management Center server, ExtremeAnalytics engine, or ExtremeControl engine to version 8.4, ensure the DNS server IP address is correctly configured.
- When upgrading to Extreme Management Center version 8.4, ensure the `-Xms` and `-Xmx` settings in the `nserver.cfg` file are set to the values defined in the [Requirements table](#) and then restart the server:
 - On a server running a Linux operating system, enter `service nserver restart` in the command line to restart the server.
 - On a server running a Windows operating system, right-click the **NetSightServices Manager** icon in the notification area of the task bar and select **NetSightServer > Restart Server** to restart the server.
- When upgrading a 64-bit Extreme Management Center server or when upgrading from a 32-bit to a 64-bit Extreme Management Center server, if the `-Xmx` setting is set below 1536m, it increases to 1536m.
- When upgrading to Extreme Management Center version 8.4, if you adjusted the Extreme Management Center memory settings and want them to be saved on upgrade, a flag (`-DcustomMemory`) needs to be added to the `/usr/local/Extreme_Networks/NetSight/services/nserver.cfg` file.

For example:

```
-Xms12g -Xmx24g -XX:HeapDumpPath=../..nsdump.hprof -
```



```
XX:+HeapDumpOnOutOfMemoryError -XX:MetaspaceSize=128m -  
DcustomMemory
```

NOTE: The `nserver.cfg` file is located in the `<install directory>\NetSight\services` folder.

- If your network is using ExtremeAnalytics or ExtremeControl engines, Fabric Manager, or another add-on feature, you must first perform the Extreme Management Center upgrade to version 8.4 and then add the feature.
- If you are running Data Center Manager (DCM), a Mobile Device Management (MDM) integration, or other ExtremeConnect or Fusion integration with Extreme Management Center, or are accessing Web Services directly or through ExtremeConnect, you need to install an Extreme Management Center Advanced (NMS-ADV) license. Contact your Extreme Networks Representative for information on obtaining this license.

4.2.1 License Renewal

Upgrading to Extreme Management Center version 8.4 requires you to [renew your NMS license](#) if generated prior to November 24, 2019. Licenses generated prior to November 24, 2019 expire 90 days after upgrading to Extreme Management Center version 8.4.

4.2.2 Upgrading Hardware

When attempting to upgrade the Extreme Management Center server, the ExtremeAnalytics engine, or the ExtremeControl engine to version 8.4, the upgrade might not complete successfully. If the upgrade is not successful, begin the upgrade again.

4.2.3 Free Space Consideration

When upgrading to Extreme Management Center version 8.4, a minimum of 15 GB of free disk space is required on the Extreme Management Center server.

To increase the amount of free disk space on the Extreme Management Center server, perform the following:

- Decrease the number of Extreme Management Center backups (by default, saved in the `/usr/local/Extreme_Networks/NetSight/backup` directory).
- Decrease the Data Persistence settings (**Administration > Options > Access Control > Data Persistence**).

- Remove unnecessary archives (**Network > Archives**).
- Delete the files in the `<installation directory>/NetSight/.installer` directory.

4.2.4 Legacy Java Applications Memory Usage

After upgrading to Extreme Management Center version 8.0 or later, the legacy Java applications might not open successfully when Extreme Management Center is managing a large number of devices due to the amount of Java heap memory configured on the Extreme Management Center server.

Increasing the amount of Java heap memory on the Extreme Management Center server corrects the issue, but limits the systems that are able to access the legacy Java applications to those that are 64-bit and include enough physical memory. If the Java heap memory setting on the Extreme Management Center server is too large for the system attempting to access the legacy Java application, the Java application will not open successfully and an error message for the user might not display.

NOTE: 64-bit Windows systems might use a 32-bit Java Web Start application, which you need to upgrade to 64-bit in order to use larger amounts of memory. Use the Windows Task Manager to determine which processes are 32-bit.

To configure the maximum Java heap memory, access **Administration > Options > Legacy Clients** and change the value in the **Maximum Java Heap Size (MB)** field in the Client JVM section of the tab. This value represents the `-Xmx` setting used by the client JVM launched by the Java Webstart application on the client system accessing Extreme Management Center.

4.2.5 Site Discover Consideration

Discovering devices via the **Site** tab using a **Range**, **Subnet**, or **Seed** discover might not successfully add all expected devices. To correct the issue, increase the **Length of SNMP Timeout** value on the **Administration > Options > Site** tab in the Discover First SNMP Request section.

4.3 ExtremeAnalytics Upgrade Information

Enabling or disabling the disk flow export feature might cause enforce operations to time out. Enforcing again resolves the issue.

When you delete an ExtremeXOS device that is configured as a flow source via the Flow Sources table of the **Analytics > Configuration > Engines > Configuration** tab from the Devices list on the **Network > Devices** tab, an error message is generated in the `server.log`. The message does not warn you that the device is in use as a flow source. Adding the device back in the Devices list on the **Network > Devices** tab or removing the device from the Flow Source table fixes the issue.

The Flow Sources table on the **Analytics > Configuration > engine > Configuration** tab may take a few minutes to load.

4.4 ExtremeControl Upgrade Information

4.4.1 General Upgrade Information

Before upgrading to Extreme Management Center 8.4, you are required to upgrade your ExtremeControl engine version to 8.2 or 8.3. Additionally, both Extreme Management Center and the ExtremeControl engine must be at version 8.4 in order to take advantage of the new ExtremeControl 8.4 features.

NOTE: ExtremeControl 8.4 is not supported on the 2S Series and 7S Series ExtremeControl Controllers.

You can download the latest ExtremeControl engine version at the Extreme Portal: <https://extremeportal.force.com>. Be sure to read the *Upgrading to ExtremeControl 8.4* document (available on the **Documentation** tab of the Portal) for important information.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 8.4 if you upgrade to the ExtremeControl engine 8.4. Version 8.4 of the assessment agent adapter requires an operating system with a 64-bit architecture.

4.4.2 ExtremeControl Version 8.0 and newer

Beginning in version 8.0, ExtremeControl may fail to join Active Directory when accessing as a **Standard Domain User with Descendant Computer Objects ("Reset password" permissions only)** group member.

To allow this functionality, add the following permissions:

- Reset Password
- Validated write to DNS host name
- Validated write to service principal
- Read and write account restrictions
- Read and write DNS host name attributes
- Write servicePrincipalName

4.4.3 Other Upgrade Information

Immediately after you install version 8.4 on the ExtremeControl engine, the date and time does not properly synchronize and the following error message displays:

```
WARNING: Unable to synchronize to a NTP server. The time might not be correctly set on this device.
```

Ignore the error message and the date and time automatically synchronize after a short delay.

Additionally, the following message might display during the ExtremeControl upgrade to version 8.4:

No domain specified

```
To stop domain-specific winbindd process, run /etc/init.d/winbindd stop {example-domain.com}
```

4.5 Fabric Configuration Information

4.5.1 Certificate

Fabric Manager might be unavailable via Extreme Management Center after upgrading if the certificate is missing in Extreme Management Center Trust store.

To ensure Fabric Manager is available, enter the Fabric Manager certificate in the Extreme Management Center Trust store using **Generate Certificate** option.

4.5.2 Authentication Key

When you provision authentication keys for Fabric Attach, the key cannot be read back for security reasons. When the key is read from the device, it always shows "****". For this reason, it might seem that there is a configuration mismatch when one does not exist.

4.5.3 Service Configuration Change

If you change a configured service via the **Configure Device** window that references one of the following, and then enforce those changes to the device, the configuration on the device might change unexpectedly:

- MLT
- SMLT
- Port-specific settings to a port belonging to an MLT or SMLT

To prevent this merge, change rows in the **Enforce Preview** window where MLT or SMLT are in use from **Current** to **Desired**.

To correct the issue after enforcement, modify the service on the device via the CLI.

4.5.4 CLIP Addresses

Using the CLIP Addresses table in the Configure Device window, you can enter addresses in both IPv4 and IPv6 formats. However, Extreme Management Center version 8.4 only supports applying a single address (either IPv4 or IPv6) to a Loopback Interface.

4.5.5 Gateway Address Configuration Change

In versions of Extreme Management Center prior to 8.4, the Default Gateway IP Address is configured as part of the VLAN. In 8.4, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 8.4, merge any **Default Gateway IP Addresses** from the device into the configuration of Extreme Management Center to prevent incorrect configuration of the device.

4.5.6 Upgrading VSP-8600

When upgrading from Extreme Management Center version 8.2 to version 8.3, manually reload previously discovered VSP-8600 devices to gain access to Fabric Connect features.

4.5.7 Removing Fabric Connect Configuration

Removing a device's Fabric Connect configuration by setting the **Topology Definition** to **<None>** may fail if the device has Logical Interfaces assigned to ISIS.

4.5.8 Password Configuration

Fabric Manager fails to onboard in Extreme Management Center if the root password includes an ampersand (&) character. Additionally, if the Administration > Inventory Manager > SCP tab contains a password that includes an ampersand (&) in Extreme Management Center, the Fabric Manager firmware does not download successfully.

Ensure you use a password without an ampersand (&) character.

4.5.9 VRF Configuration

VSP SNMP performance is adversely affected as the number of VRF configurations increases. This issue can be resolved by upgrading to VSP release 8.1.1 or later or VSP8600 series version 6.3.3 or later.

4.6 Device Configuration Information

4.6.1 VDX Device Configuration

To properly discover interfaces and links for VDX devices in Extreme Management Center, enable `three-tuple-if` on the device.

NOTE: To enable `three-tuple-if` on the device in Extreme Management Center:

1. Access the **Network > Devices** tab.
 2. Right-click on the device in the Devices table.
 3. Select **Tasks > Config > VDX Config Basic Support**.
-

Additionally, for Extreme Management Center to display VCS fabric, the NOS version must be 7.2.0a or later.

Rediscover VDX devices after upgrading to Extreme Management Center version 8.4.0.

4.6.2 VSP Device Configuration

Topology links from VSP devices to other VSP or ERS devices might not display in a topology map (or might display inconsistently). To ensure topology map links display correctly, verify that the VSP device is configured to publish its management IP address in the autotopology (SONMP) data.

Ensure that the output of `show sys setting` command shows:

```
autotopology : on
ForceTopologyIpFlag : true
clipId-topology-ip : 0
```

If the output values displayed are different, configure the VSP device to publish management IP address in SONMP data by executing the following CLI commands:

```
(config)# autotopology
(config)# sys force-topology-ip-flag enable
(config)# default sys clipId-topology-ip
```

The **Status** of LAG links in maps will start working after the next polling following an upgrade to Extreme Management Center version 8.4. You can initiate the polling of a device by performing a refresh/rediscovery of the device.

4.6.3 ERS Device Configuration

ERS devices might automatically change VLAN configurations you define in Extreme Management Center. To disable this, change the `vlan configcontrol` setting for ERS devices you add to Extreme Management Center by entering the following in the device command line:

```
CLI commands
enable
config term
vlan configcontrol flexible
```

Additionally, configure all VLANs on the port for an ERS device with the same tag status (tagged or untagged). If enforcing to an ERS device on which a port has at least one VLAN as tagged, Extreme Management Center adds all untagged VLANs to the tagged VLAN list and clears the untagged VLAN list.

Creating an archive for ERS devices using the **Network > Archives** tab does not complete successfully if Menu mode (cmd-interface menu) is used instead of CLI mode (cmd-interface cli). [Use CLI mode](#) to create the archive.

4.6.4 SLX Device Configuration

When creating a ZTP+ Configuration for an SLX 9240 on which firmware version 18s.01.01 or 18s.01.02 is installed, the ZTP+ process fails if the **Administration Profile** value uses SSH or Telnet CLI credentials. Extreme Management Center indicates that the SSH or CLI profile is not supported by the device.

To create a ZTP+ configuration for an SLX 9240:

1. Create a new Device Profile with the **CLI Credential** set to **< No Access >**.

NOTE: The SLX ZTP+ Connector does NOT support configuring CLI credentials on the device.

2. Create the ZTP+ Configuration and select the new **Device Profile** you created in Step 1 as the **Administration Profile**.
3. After the ZTP+ process successfully completes and the device is added to Extreme Management Center, select a **Device Profile** that uses the correct CLI credentials for the SLX device in the **Administration Profile**.

4.6.5 ExtremeXOS Device Configuration

ExtremeXOS devices on which firmware version 30.3.1.6 is installed do not download and install new firmware versions successfully via the ZTP+ process. To correct the issue, access the **Network > Firmware** tab in Extreme Management Center, select the ExtremeXOS device you are updating via ZTP+, and change the **Version** field in the Details right-panel from **builds/xos_30.3/30.3.1.6** to **30.3.1.6**.

4.7 Firmware Upgrade Configuration Information

Extreme Management Center supports firmware downloads and uploads to devices using TFTP, FTP, SCP, and SFTP. However, before firmware images can be downloaded or uploaded from the server, Extreme Management Center

needs the root path or directory for each of the protocols. The following default root paths for each protocol are configurable from the **Administration > Options > Inventory Manager** tab:

Protocol Root Path:

- TFTP: /tftpboot/firmware/images/
- FTP: /tftpboot/firmware/images/
- SCP: /root/firmware/images/
- SFTP: /root/firmware/images/

To upload firmware images that are 2 GB or less to the server, use the Extreme Management Center **Network > Firmware** tab. For files larger than 2 GB, use a third-party client (such as SCP, WinSCP, or FTP).

For example, to use SCP to upload a firmware image to the SCP root path on the server, enter the following:

- `scp <LOCAL_FIRMWARE_PATH> root@<Extreme Management Center_SERVER_IP>:/root/firmware/images`
- Where:
 - `<Extreme Management Center_SERVER_IP>`= IP Address to Extreme Management Center Server
 - `<LOCAL_FIRMWARE_PATH>`= fully qualified path to a firmware image on the client machine

4.8 ExtremeWireless Upgrade Information

An ExtremeWireless High Availability pair cannot be added as a flow source if the WLAN(s) selected are not in common with both wireless controllers.

Following a Wireless Manager upgrade, clear the Java Cache before starting the Extreme Management Center client.

5. System Requirements

IMPORTANT: Extreme Management Center version 8.4 only runs on a 64-bit engine image. Any Extreme Management Center or ExtremeControl engine currently running a 32-bit OS image must be upgraded to the newer 64-bit image prior to upgrading to 8.4. Contact [Global Technical Assistance Center \(GTAC\)](#) with any questions.

Wireless event collection is disabled by default in version 8.4 due to the increase in disk space usage required. To enable event collection, select **Enable Event Collection** on the **Administration > Options > Event Analyzer** tab.

Internet Explorer is not supported in Extreme Management Center version 8.4.

5.1 Extreme Management Center Server and Client OS Requirements

These are the operating system requirements for both the Extreme Management Center server and remote Extreme Management Center client machines.

Manufacturer	Operating System
Windows (qualified on the English version of the operating systems)	Windows Server® 2012 and 2012 R2 Windows Server® 2016 Windows® 7
Linux	Red Hat Enterprise Linux WS and ES v6 and v7 Ubuntu 16.04
Mac OS X® (remote Extreme Management Center client only)	El Capitan Sierra
VMware® (Extreme Management Center Virtual Engine)	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server VMware ESXi™ 6.7 server vSphere (client only)™
Hyper-V (Extreme Management Center Virtual Engine)	Hyper-V Server 2012 R2 Hyper-V Server 2016

5.2 Extreme Management Center Server and Client Hardware Requirements

These are the hardware requirements for the Extreme Management Center server and Extreme Management Center client machines.

NOTES: ExtremeControl and ExtremeAnalytics are not supported on Small Extreme Management Center servers.

Extreme Management Center Server

Specifications	Small	Medium	Enterprise	Large Enterprise
Total CPUs	1	2	2	2
Total CPU Cores	8	16	24	24
Memory	16 GB	32 GB	64 GB	64 GB
Memory allocated to Java:				
-Xms	4 GB	8 GB	16 GB	16 GB
-Xmx	8 GB	16 GB	32 GB	32 GB
Disk Size	240 GB	480 GB	960 GB	1.92 TB
IOPS	200	200	10,000	10,000
Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
ExtremeAnalytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

IMPORTANT: For optimal performance the CPU and Memory needs to reserved in the ESX Client and the virtual machine needs to be deployed using Thick Disk provisioning.

Extreme Management Center Client

Specifications	Requirements
CPU Speed	3.0 GHz Dual Core Processor
Memory	8 GB (4 GB for 32-bit OS)
Disk Size	300 MB (User's home directory requires 50 MB for file storage)
Java Runtime Environment (JRE) (Oracle Java only)	Version 8
Browser ¹ (Enable JavaScript and Cookies)	Microsoft Edge (version 41.16.199.10000.0 in compatibility mode) Mozilla Firefox (version 34 or later ²) Google Chrome (version 33.0 or later)

¹Browsers set to a zoom ratio of less than 100% might not display Extreme Management Center properly (for example, missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.

²When accessing Extreme Management Center using Firefox version 59.0.1 on a non-touchscreen system on which a Windows operating system is installed, the vertical scroll arrows do not display.

5.3 Virtual Engine Requirements

The Extreme Management Center, ExtremeControl, and ExtremeAnalytics virtual engines must be deployed on a [VMWare or Hyper-V server](#) with a disk format of VHDX.

- The VMWare Extreme Management Center virtual engines are packaged in the .OVA file format (defined by VMware).
- The Hyper-V Extreme Management Center virtual engines are packaged in the .ZIP file format.

IMPORTANT: For ESX and Hyper-V servers configured with AMD processors, the Extreme ExtremeAnalytics virtual engine requires AMD processors with at least Bulldozer based Opterons.

5.3.1 Extreme Management Center Virtual Engine Requirements

Specifications	Small	Medium	Large
Total CPU Cores	8	16	24
Memory	16 GB	32 GB	64 GB
Memory allocated to Java:			
-Xms	8 GB	12 GB	24 GB
-Xmx	12 GB	18 GB	36 GB
Disk Size	240 GB	480 GB	960 GB
IOPS	200	200	10,000

Recommended scale based on server configuration:

Maximum APs	250	2,500	25,000
Maximum Wireless MUs	2,500	25,000	100,000
Maximum Managed Devices	100	1,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000
Statistics Retention (Days)	90	180	180
ExtremeAnalytics	No	Yes	Yes
MU Events	No	Yes	Yes

IMPORTANT: For optimal performance the CPU and Memory needs to reserved in the ESX Client and the virtual machine needs to be deployed using Thick Disk provisioning.

5.3.2 ExtremeControl Virtual Engine Requirements

Specifications	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	16 GB	32 GB
Disk Size	40 GB	120 GB	120 GB
IOPS	200	200	200

Recommended scale based on server configuration:

ExtremeControl End-Systems	3,000	6,000	9,000/12,000 ¹
Authentication	Yes	Yes	Yes
Captive Portal	No	Yes	Yes/No ¹
Assessment	No	Yes	No

¹The Enterprise ExtremeControl engine configuration supports two different scale options:

- Up to 9,000 end-systems if your network uses Captive Portal functionality.
- Up to 12,000 end-systems if your network does not use Captive Portal functionality.

IMPORTANT: For optimal performance the CPU and Memory needs to reserved in the ESX Client and the virtual machine needs to be deployed using Thick Disk provisioning.

5.3.3 ExtremeAnalytics Virtual Engine Requirements

Specifications	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	32 GB	64 GB
Disk Size	40 GB	480 GB	960 GB
IOPS	200	10,000	10,000

Recommended scale based on server configuration:

Flows Per Minute	250,000	500,000	750,000
End-Systems	10,000	20,000	30,000

IMPORTANT: The ESXi free license supports a maximum of 8 CPU cores, and the medium and enterprise ExtremeAnalytics virtual engine installations require 16 CPU cores. Sixteen CPU cores are only available by purchasing a permanent license. To use the ExtremeAnalytics virtual engine with an ESXi free license, adjust the number of CPU cores to 8.

To reduce the possibility of impaired functionality, ensure at least 4 GB of swap space is available for flow storage on the ExtremeAnalytics virtual engine. To verify the amount of available RAM on your Linux system, use the `free` command

5.3.4 Fabric Manager Requirements

Specifications	Requirements
Total CPU Cores	4
Memory	9 GB
Memory allocated to Java:	
-Xms	4 GB
-Xmx	6 GB
Disk Size	60 GB

5.4 ExtremeControl Agent OS Requirements

The table below outlines the supported operating systems for end-systems connecting to the network through an ExtremeControl deployment that is implementing agent-based assessment. Additionally, the end-system must support the operating system disk space and memory requirements as provided by Microsoft® and Apple®.

Manufacturer	Operating System	Operating System Disk Space	Available/Real Memory
Windows¹	Windows Vista	80 MB	40 MB (80 MB with Service Agent)
	Windows XP		
	Windows 2008		
	Windows 2003		
	Windows 7		
	Windows 8		
	Windows 8.1		
	Windows 10		
Mac OS X	Catalina	10 MB	120 MB
	Tiger		
	Snow Leopard		
	Lion		
	Mountain Lion		
	Mavericks		
	Yosemite		
	El Capitan		
Sierra			

¹Certain assessment tests require the Windows Action Center (previously known as Windows Security Center), which is supported on Windows XP SP2+, Windows Vista, and Windows 7, Windows 8, and Windows 8.1 operating systems.

ExtremeControl Agent support for Antivirus or Firewall products includes, but is not limited to, the following families of products:

- McAfee
- Norton
- Kaspersky
- Trend Micro
- Sophos

ExtremeControl Agent operating system support for the above products includes the latest Windows or Mac OS X versions currently available at the time of product release. Some features of various products might not be supported. For additional information on specific issues, see [Known Issues and Limitations](#).

5.5 ExtremeControl Supported End-System Browsers

The following table outlines the supported desktop and mobile end-system browsers connecting to the network through the Mobile Captive Portal of Extreme Networks ExtremeControl.

Medium	Browser	Version
Desktop	Microsoft Edge	41 and later
	Microsoft Internet Explorer	11 and later
	Mozilla Firefox	34 and later
	Google Chrome	33.0 and later
Mobile	Internet Explorer Mobile	11 and later (Windows Phone)
	Microsoft Edge	All versions
	Microsoft Windows 10 Touch Screen Native (Surface Tablet)	N/A
	iOS Native	9 and later
	Android Chrome	4.0 and later
	Android Native	4.4 and later
	Dolphin	All versions
	Opera	All versions

NOTES: A native browser indicates the default, system-installed browser. Although this might be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection for a device. Typically, this is a non-configurable option for Wi-Fi Captive Network Detection, but default Android, Microsoft and iOS devices are tested for compatibility with the Mobile Captive Portal.

A mobile device can access the standard (non-mobile) version of the Captive Portal using any desktop-supported browsers available on a mobile device.

For other browsers, the Mobile Captive Portal requires the browser on the mobile device to be compatible with Webkit or Sencha Touch.

To confirm compatibility with Webkit or Sencha Touch, open `http://<ExtremeControl Engine IP>/mobile_screen_preview` using your mobile web browser.

- If the browser is compatible, the page displays properly.
- If the browser is not compatible with the Mobile Captive Portal, the following error displays:



5.6 ExtremeControl Engine Version Requirements

For complete information on ExtremeControl engine version requirements, see the [Extreme Management Center Version 8.4 Release Notes](#) section of these Release Notes.

5.7 ExtremeControl VPN Integration Requirements

VPN concentrators are supported for use in ExtremeControl VPN deployment scenarios.

- Supported Functionality: Authentication and Authorization (policy enforcement)
Cisco ASA
Enterasys XSR

- Supported Functionality: Authentication
Juniper SA (requires an S-Series Stand Alone (SSA) system in order to provide access control)

NOTE: For all ExtremeControl VPN Deployment scenarios, an S-Series Stand Alone (SSA) system is required to change authorization levels beyond the initial authorization, such as when using assessment.

5.8 ExtremeControl SMS Gateway Requirements

The following SMS Gateways have been tested for interoperability with ExtremeControl:

- Clickatell
- Mobile Pronto

5.9 ExtremeControl SMS Text Messaging Requirements

The following mobile service providers are supported by default for SMS text messaging in an ExtremeControl deployment. Additional service providers can be added:

AT&T	Sprint PCS
Alltel	SunCom
Bell Mobility (Canada)	T-Mobile
Cingular	US Cellular
Metro PCS	Verizon
Rogers (Canada)	Virgin Mobile (US and Canada)

5.10 ExtremeAnalytics Requirements

To use an ExtremeSwitching X440-G2 switch as an Application Telemetry source for ExtremeAnalytics, install firmware version 22.4.1.4-patch2-5 or higher.

5.11 Ekahau Maps Requirements

Extreme Management Center supports importing Ekahau version 8.x maps in .ZIP format.

5.12 Guest and IoT Manager Requirements

5.12.1 Guest and IoT Manager Server OS Requirements

These are the operating system requirements for Guest and IoT Manager server:

Manufacturer	Operating System
VMware® (Extreme Management Center Virtual Engine)	VMware ESXi™ 5.5 server VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server vSphere (client only)™

5.12.2 Guest and IoT Manager Outlook Add-in Client Requirements

These are the requirements for the Client Machines, which need to run Guest and IoT Manager Outlook Add-in.

Manufacturer	Operating System
Windows ¹	Windows 7 Windows 10
Mac OS X	Sierra High Sierra Mojave

¹Microsoft® Outlook® 2016 is needed on Windows/Mac clients for the add-in to operate.

5.12.3 Guest and IoT Manager Virtual Engine Requirements

The VMWare Guest and IoT Manager virtual engines are packaged in the .OVA file format (defined by VMware) and needs an x86, 64-bit capable environment

Specifications	Minimum	Recommended
Total CPU Cores	2	4
Memory	2 GB	4 GB
Disk Size	80 GB	80 GB
Interfaces	1 Physical NIC	3 Physical NICs

5.12.4 Guest and IoT Manager Supported Browsers

The following table outlines the supported desktop and mobile browsers that can be used to launch Guest and IoT Manager Admin and Provisioner Web Application:

Medium	Browser	Version
Desktop	Microsoft Internet Explorer	11 and later
	Mozilla Firefox	63 and later
	Google Chrome	65 and later
	Microsoft Edge	42 and later
	Safari	12 and later
Mobile ¹	iOS Native	9 and later
	Android Chrome	65 and later
	US Browser	11.5 and later
	Opera	40 and later
	Firefox	63 and later

¹Mobile Browsers are supported only for the Guest Self-Service Provisioning flow.

Notes:

- A mobile device can access the Guest and IoT Manager Application by using any desktop-supported browsers available on a mobile device. Before login, make sure to select the **Desktop site** option in the browser options.
- Browsers set to a zoom ratio of less than 100% might not display Guest and IoT Manager Application properly (for example, missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.
- Guest and IoT Manager Application is best viewed in 1920 x 1080 resolution or higher. Lower resolutions might result in improper layouts in some cases.
- If you are using self-signed certificates, they must be added in the Trusted Root Certificate store on the client machine or you might observe issues in the “print” use cases. This is only applicable for Microsoft Edge and Microsoft Internet Explorer browsers.

6. Getting Help

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](#)

Connect with other Extreme customers, ask or 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.

GTAC

For immediate support, call 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000.

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

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action 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 Return Material Authorization (RMA) numbers