



Extreme Management Center[®] Release Notes Version 8.5.1

9/2020
9036781-01 Rev. AB
Subject to Change Without Notice

Table of Contents

Extreme Management Center® Release Notes Version 8.5.1	1
Table of Contents	2
Extreme Management Center Version 8.5 Release Notes	5
1. Enhancements in Version 8.5.1	5
1.1 Customer Feature Requests Addressed in 8.5.1	6
1.1.2 Customer Feature Requests Addressed in 8.5.0	12
1.2 Engines	13
1.3 Extreme Management Center	13
1.4 ExtremeAnalytics	18
1.5 ExtremeCompliance	19
1.6 ExtremeControl	19
2. Deprecated Features	21
3. Known Issues and Vulnerabilities Addressed	22
3.1 Known Issues Addressed in 8.5.1	22
3.1.1 Known Issues Addressed in 8.5.0	23
3.2 Vulnerabilities Addressed	28
4. Installation, Upgrade, and Configuration Changes	31
4.1 Installation Information	31
4.1.1 Installing Without an Internet Connection	32
4.1.2 Custom FlexViews	32
4.1.3 Custom MIBs and Images	32
4.2 Important Upgrade Considerations	33
4.2.1 License Renewal	34
4.2.2 Upgrading Hardware	34

4.2.3 Free Space Consideration	34
4.2.4 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 later	35
4.4.3 Other Upgrade Information	36
4.5 Fabric Configuration Information	36
4.5.1 Certificate	36
4.5.2 Authentication Key	36
4.5.3 Service Configuration Change	36
4.5.4 CLIP Addresses	37
4.5.5 Gateway Address Configuration Change	37
4.5.6 Upgrading VSP-8600	37
4.5.7 Removing Fabric Connect Configuration	37
4.5.8 Password Configuration	37
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	38
4.6.3 ERS Device Configuration	39
4.6.4 SLX Device Configuration	39
4.6.5 ExtremeXOS Device Configuration	40
4.7 Firmware Upgrade Configuration Information	40
4.8 Wireless Manager Upgrade Information	41
5. System Requirements	41

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

Extreme Management Center Version 8.5 Release Notes

8.5.1

September 2020

The Extreme Management Center Release Notes provide information on the new features and enhancements included in version 8.5.1, 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](#).

IMPORTANT: Upgrading to Extreme Management Center version 8.5 requires you to [renew your NMS license](#) if generated prior to July 31, 2020. Licenses generated prior to July 31, 2020 expire 90 days after upgrading to Extreme Management Center version 8.5.

You can view the status of your license by accessing **Administration > Diagnostics > Server > Server Licenses**.

For the most recent version of these release notes, see [Extreme Management Center Release Notes](#).

For information regarding the features supported by specific devices, see the [Firmware Support Matrix](#). Version 8.5 of Extreme Management Center supports the devices listed in the matrix.

1. Enhancements in Version 8.5.1

New features and enhancements are added to the following areas in Extreme Management Center version 8.5.1:

- [Customer Feature Requests](#)
- [Engines](#)
- [Extreme Management Center](#)
- [ExtremeAnalytics](#)

- [ExtremeCompliance](#)
- [ExtremeControl](#)

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 Customer Feature Requests Addressed in 8.5.1

Extreme Management Center CFRs Addressed	ID
<p>DvR Functionality Supported in Extreme Management Center Extreme Management Center now supports DvR functionality to provide routing redundancy in a fabric-connect network.</p> <p>NOTE: VOSS devices support a new "dvr-one-ip" feature in the 8.2 release that allows you to share an IP address between a VLAN and its DvR interface. XMC currently does not support the "dvr-one-ip" feature and cannot read or enforce configurations of this type. Configure VOSS device IP addresses on VLANs and their DvR interfaces through the VLAN Definition tab.</p>	----
<p>New Warning For NMS-EVAL License Expiry No warning was issued when an NMS-EVAL license was about to expire. New notifications have been added to alert users prior to NMS-EVAL license expiry.</p>	----
<p>Extreme Management Center Now Supports Unified Series 5520 Devices</p> <p>NOTE: Changing unified series devices from EXOS to VOSS or vice versa is not supported in Extreme Management Center. We recommend the following steps when changing a unified series to a different operating system.</p> <ol style="list-style-type: none"> 1. Delete the device from Extreme Management Center (make sure the check box is checked to delete from database). 2. Manually change the device to the different operation system ("EXOS to VOSS" or "VOSS to EXOS" or use ExtremeCloud IQ to perform this action). 3. Add the device back into Extreme Management Center. 	----

Remove From Device Group Available When Multiple Devices Selected	01709827 01971882
The Remove From Device Group menu action was available only when a single device listed under a User Device Group was selected. It is now available when one or more devices listed within the Devices table are selected.	
Overview Tab Functionality for Imported Scripts Corrected	02216199
Overview tab functionality has been corrected so that scripts that are imported or edited via the Overview tab are no longer corrupted.	
Support for RADIUS ERS-CoA-Reauthenticate Attribute Added	02200420
Support for RADIUS ERS-CoA-Reauthenticate attribute has been added for Extreme ethernet routing switches.	
RADIUS Servers Now Configurable on Several Tabs	02219510
Extreme Management Center is now able to configure RADIUS servers in Administration, Users, Manage SSH Configuration tabs.	
MIB Not Supported Error Not Improperly Reported	01932839 02190132
3rd party devices were reporting a "MIB Not Supported" error even though they had a valid script associated to them for archives. This error is no longer being reported in these cases.	
Schedule Options Properly Displayed	01917452
The Device Reset screen was displaying the schedule option when devices in the group did not support scheduled operations (for example, VOSS and EWC devices). Now the schedule box does not display if at least one of the devices in the group does not support the scheduled reset.	
New Capability to Rediscover Added	02177860
The capability for executing a "Rediscover" of a device has been moved from the NetSight OneView>Access OneView Administration capability and is now included with the NetSight Suite > Devices > Add, Discover, Import capability.	

New Capability to Launch WebView Added	02177860
The capability for executing a "WebView" of a device has been moved from the NetSight OneView > Access OneView Administration capability to a new capability: NetSight Suite > Devices > Launch WebView .	
NOTE: If you are upgrading to Extreme Management Center Version 8.5.1 (and future versions), the "Launch WebView" capability is enabled by default for new Authorization Groups. For Extreme Management Center Versions 8.5.0 or earlier, the "Launch WebView" capability is DISABLED by default. After upgrading to version 8.5.1, you must review and modify your Administrative Groups and configure them for "Launch WebView" individually.	
Message Added to Warn of Impact to Tasks When Deleting User Profile	01930813 01931694
A new message warns that, when deleting a user profile, the scheduled firmware and archived tasks created by the user being deleted are impacted.	
Standby Units Identified for Archiving EXOS Devices	02230235 02229333
EXOS stacks with backups but no standby units were failing to archive the configuration. Standby units have been identified to successfully archive EXOS devices.	
Password Updates and Prompts Improved	01918709 01977127
Changes have been made to properly update passwords and ensure password change prompts occur.	
Loading Icon Introduced to DeviceView	1987849
A loading icon has been introduced for the DeviceView that remains visible until all the grids of the tab are loaded to prevent an empty view from displaying if there is a delay in the rendering of one grid.	
ZTP+ Onboarding for VOSS Devices Added	----
VOSS devices can now be configured using the ZTP+ onboarding process.	
Message to Use System Workflow Added	1869524
A new message to use a System Workflow instead of using Legacy Inventory scripts when attempting to upgrade VDX devices has been added.	
Alarm Refresh Interval Updated	01992245
An additional Refresh interval of 5 seconds has been added to Alarms in Extreme Management Center.	

Warning Message for Port Settings Added	01910126
A warning message has been added that alerts you if an HTTP/HTTPS port was set to a value less than 1024, and Extreme Management Center was installed as non-root user, the setting is ignored and not saved.	
Ability to Access Scheduled Tasks Improved	01883066
If the (legacy) Access OneView Administration option was disabled, the Access Scheduled Tasks option was also being improperly disabled. Now, if the Access OneView Administration option is disabled, the Access Scheduled Tasks option is no longer disabled.	
Export to CSV Button Added to Ports Tabs	1926242
A new Export to CSV button has been added to Extreme Management Center's Device View > Ports and More Views > Port Tree tabs that provides the ability to export port details to a .csv file.	
Ability to View Configuration Options for Archived Devices Added	02234207
Two new options to View Configuration have been added to the Device and DeviceView tabs:	
<ul style="list-style-type: none"> • DeviceView > Archives > Select a Config file > View Configuration • Right-click a Device > Archives > View Last Configuration 	
In addition, you can now select View Configuration File from the Archives tab to view archive information for ERS8600 series devices.	
Ability to Add Tagged and Untagged VLANs for LAG / MLAG Added	-----
You can now add Tagged & Untagged VLANs for LAG/MLAG on the Configuration > Ports tab.	
Maximize Feature Added to Tasks Windows	1889058
The Maximize feature has added to several Tasks > Scripts and Tasks > Workflows windows.	
ExtremeAnalytics CFRs Addressed	ID

New Titles and Data Added to ExtremeAnalytics Reports 1783081

Additional data has been added for several ExtremeAnalytics reports, which are accessible on the **Analytics > Reports and Reports > Reports > Application Analytics** tabs.

The enhanced reports (with new titles) are:

- Analytics Events
- Bandwidth for a Client Over Time
- Most Popular Applications
- Most Used Applications for a Client
- Most Used Applications for a User Name
- Network Activity by Cloud Region and Site
- Network Activity by Site
- Network Activity for a Client
- Network Activity for an Application
- Sites Using the Most Bandwidth
- Slowest Applications by Site

Insights Dashboard Drill Down Displays Correct Data 01854859

The **ExtremeAnalytics > Insights Dashboard Response Time** ring chart often displayed error data (in red); however, if you select the error data to drill down for details, no errors displayed on the Tracked Applications Dashboard. Now the Tracked Applications Dashboard displays the appropriate error data.

Dashboard Response Time Results Now Consistent 01846024

The ExtremeAnalytics Dashboards were displaying inconsistent Response Time results. The **Insights, Network Service, and Tracked Application Dashboards** now all display consistent Response Time results.

Disable and Enable Options for Web Applications Fingerprints Functioning Properly 01978971

The Disable function for fingerprints was improperly continuing to display data. The Disable and Enable options are now functioning properly for Web Application fingerprints.

False Data From Exports No Longer Seen	02000756
ExtremeAnalytics was showing incorrect data when processing records exported from FortiGate firewalls. The issue has been corrected and false data is no longer seen.	
Flow Collection Process Corrected to Discontinue Continual Issuing of SNMP Requests	2161359
The ExtremeAnalytics engine was constantly issuing SNMP requests for switch port data. The flow collection process has been corrected to prevent performing any unneeded SNMP on the engine and should significantly reduce the load on the engine.	
ExtremeControl CFRs Addressed	ID
New ExtremeControl Engine Property Added	01937405
A new ExtremeControl engine property, "AAA_STRIP_USERNAME_USE_LDAP_CONFIG" allows AAA auth requests using LDAP configuration to strip or preserve the domain name in usernames for auth request from the LDAP configuration being used.	
Option to Skip EAP-Message Check Added	01414443
ExtremeControl engine settings now allow you to skip the EAP-Message check when determining if a request is administrative.	
Web View Rendering Process Improved	01938001
Large configurations and rules in ExtremeControl were causing the web view to lag and load slowly. Pagination has been introduced for the Rules table and for the Groups tab, and page size has been set to 100, to speed the rendering process for the web view.	
Ability to Override RADIUS Shared Secret Via NBI	----
ExtremeControl northbound interface (NBI) now allows you to override a RADIUS shared secret when creating or updating a switch on an Access Control engine group.	
SNMP Profile Changes Cause Enforce Flag	02168972
Changing switch SNMP profile in either the ExtremeControl configuration or the Network > Devices view now causes an enforce flag.	
WebView and Terminal Features Added to End System Table	1926229
WebView and Terminal features were included on the ExtremeControl > Access Control > End System table. Webview and Terminal options have been added to the End System table menu.	

GIM Sponsor Retrieval Advanced Configuration Feature Added	01978498
A new feature in Extreme Management Center and GIM (Guest and IoT Manager) enables you to choose how you configure the method of retrieving sponsors in the GIM Domain.	01898456 01816454

1.1.2 Customer Feature Requests Addressed in 8.5.0

Extreme Management Center CFRs Addressed	ID
<p>Port Template Enhancement</p> <p>In addition to User-configured Port Templates, Extreme Management Center now supports Vendor-configured Automated Port Templates. After Extreme Management Center discovers devices via ZTP+ and asks for configuration, the automated port templates are automatically assigned to the ports on the device.</p>	----
<p>Policy ACL Rule Management Support</p> <p>Extreme Management Center version 8.5.1 allows you to manage ACL rules on ExtremeXOS devices on which version 30.5 or later is installed. By using ACLs, the access control entries (ACEs) can be ordered by the administrator, allowing for more flexibility in the configuration and better utilization of hardware resources on the device.</p> <p>ExtremeXOS uses the IETF YANG data model for ACLs (ietf-access-control-list) defined in RFC- 8519.</p>	----
<p>New FlexView for BOSS Power Supply Information</p> <p>Serial Numbers and Power Supply information were not included in the BOSS Chassis Components FlexView for ERS devices on which BOSS 7.8.x or later was installed. The information is now in a new FlexView called BOSS Power Supply Information.</p>	1943390
<p>Enhancement to Alarms in Extreme Management Center</p> <p>Beginning in Extreme Management Center version 8.5.0, you can open the map to which a device belongs from the Alarms tab.</p>	1709802
<p>VRRP Provisioning Support Added for VSP Devices</p> <p>Extreme Management Center now supports VRRP (Virtual Router Redundancy Protocol) provisioning. Using the Configure Device > VLAN Definitions tab, you can configure your VSP devices to form a virtual router interface to act as a redundant forwarding element for the network.</p>	----

ExtremeCloud Appliance Versions 4.56.02 and 5.06 Now Supported	-----
Extreme Management Center 8.5.0 now supports ExtremeCloud Appliance versions 4.56.02 and 5.06.	
ExtremeControl CFRs Addressed	ID
Functions Added to LDAP Mappings	01912554
The Add, Edit, and Delete functions, as well as Import and Export functions, for LDAP Mappings have been added to the Configuration > AAA tab and Configuration > Access Control > Profiles tab.	01979187
Filter Enhancements to Rules Tab Added	01889129
Columns on the ExtremeControl Configuration > Rules tab now can be filtered by criteria you define.	

1.2 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.

1.3 Extreme Management Center

- [Ability to Export Filtered Events Added](#)
- [New Alarms Added in Extreme Management Center](#)
- [WebAccess Added to Authorization Groups User Capabilities](#)
- [Ping Device Feature Added](#)
- [Devices Now Supported by Extreme Management Center](#)
- [Discover Now Allowed for Sites Based on Add Device Capability](#)
- [Clarification of Port Type Column on Device View > Port Tab](#)
- [Enhancement to Extreme Management Center Backups](#)

- [Failed to Join Domain Alarm Added](#)
- [REST API Added to GIM](#)
- [Fabric Authentication Type Enhancement](#)
- [Fabric Attach and Switched UNI Enhancement](#)
- [Enhancements to VPEX](#)
- [Improvements to Server Certificates](#)
- [11ax Radio for AP5xx Models Supported](#)
- [Enhancements to Network Status Summary](#)
- [New Wireless FloorPlans Summary Added](#)
- [Enhancements to ExtremeConnect](#)

Ability to Export Filtered Events Added

The ability to export filtered events to a .csv file has been added to Extreme Management Center.

New Alarms Added In Extreme Management Center

The following alarms are available in Extreme Management Center version 8.5.1:

- Port RX % Utilization Threshold Alarm
- Port TX % Utilization Threshold Alarm

WebAccess Added to Authorization Group Capabilities

WebAccess has been added to the **Administration > Users > Group Authorization > Capabilities** tab.

Ping Device Feature Added

You can now send a Ping (ICMP or TCP Echo Request) to determine if a device is reachable. The timeout value for the request is configured in **Administration > Options > Status Polling > Ping > Length of Ping Timeout**, and the result of the request is displayed in a pop-up dialog. Extreme Management Center installations that are configured to run as root issue ICMP Requests, while installations that are configured to run as users other than root will use a TCP Echo Request.

NOTE: Firewalls and server configurations can block ICMP and/or TCP requests, which can result in an Unsuccessful Ping, even though SNMP, SSH, Telnet and other protocols are successful.

Devices Now Supported by Extreme Management Center

The following devices are now supported by Extreme Management Center version 8.5:

- AP310i-FCC
- AP310i-CAN
- AP310i-IL
- AP310e-FCC
- AP310e-WR
- AP310e-CAN
- Ap310e-IL
- AP360i-WR
- AP360i-CAN
- AP360i-IL
- AP360e-FCC
- AP360e-WR
- AP360e-CAN
- AP360e-IL
- AP360i-FCC
- AP310i-WR
- SLX 9740
- SLX-9740-40C
- SLX-9740-80C
- VSP-4900-24XE
- VSP-4900-12MXU
- VSP-4900-24S

Discover Now Allowed for Sites Based on Add Device Capability

Discover is now allowed for valid sites based on Add Device capability. The capability for "Sites Read/Write Access" is not necessary for Site Discover, but it is necessary for adding or editing sites.

Clarification of Port Type Column in Device View > Port Tab

The Port Type column on the Device View > Port tab has been renamed Neighbor Capabilities and shows all advertised capabilities of the neighbor, instead of displaying "Interswitch" or "Access."

Enhancement to Extreme Management Center Backups

A new checkbox on the Administration > [Backup/Restore tab](#) allows you to select whether alarm, end-system event, and reporting are included in Extreme Management Center backups.

Failed to Join Domain Alarm Added

A “Failed to Join Domain” alarm is now automatically generated in Extreme Management Center when an engine is unable to join a domain and an event is generated.

REST API Added to GIM

REST API has been added to GIM to increase the .CSV import level for devices from 200 to 5000, and to improve the time to provision these devices.

Fabric Authentication Type Enhancement

Fabric Enable in NNI mode now supports the SHA-256 Fabric Auth Type.

Fabric Attach and Switched UNI Enhancement

Extreme Management Center now supports Fabric Attach (FA) and Switched User Network Interface (S-UNI) on the same port at the same time.

This feature is supported by VSP firmware version 8.1.1 and later, and on all platforms currently supported by Extreme Management Center with two exceptions: XA1400 and VSP-8600.

Enhancements to VPEX

Extreme Management Center now supports the following Virtual Port Extender (VPEX) configurations:

- VPEX Ring Topologies - When two VPEX cascades are linked together, they form a VPEX ring. This type of ring provides a redundant connection from any bridge port extender (BPE) in the ring to the controlling bridge (CB). Extreme Management Center requires the controlling bridge to have ExtremeXOS 30.6 or later.
- One-Armed MLAGs - In this dual control configuration, the first tier BPEs are only connected to one of the two controlling bridges, which leaves more trusted ports available. In some applications, BPEs are limited to only two links for forming the ring, and the use of one-armed MLAGs is required.

Improvements to Server Certificates

The following improvements to server certificates are included in Extreme Management Center version 8.5:

- PKCS#12/PFX keystores without a keystore password can be imported
- Unencrypted RSA private keys containing a "BEGIN RSA PRIVATE KEY" header can be imported
- Error messages are more descriptive

11ax Radio for AP5xx Models Supported

Extreme Management Center now supports 11ax Radio for AP5xx models.

Enhancements to Network Status Summary Report

The Network Status Summary PDF report has been updated to include the following enhancements:

- Reports display Top 10 instead of Top 5 statistics.
- New "Top 10 WLANs by Clients" and "Top 10 Clients by Bandwidth" reports have been added.
- Enhanced color and graphic resolution for all reports.
- Ability to select a site and generate a Network Status Summary based on the activity for that site.
- Scheduling capability to generate the Network Status Summary on an hourly, daily, weekly, or monthly basis.

The Network Status Summary reports are now also available in the **Reports Catalog** under the **Network** option in the left-panel tree.

New Wireless FloorPlans Summary Added

A new **FloorPlans Summary** report, which displays AP, WLAN and Client data based on selected floorplans, has been added to Extreme Management Center's **Reports Catalog** under the **Wireless** option in the left-panel tree. You can also schedule the FloorPlan Summary to generate hourly, daily, weekly or monthly reports.

Enhancements to ExtremeConnect

Several enhancements have been made to ExtremeConnect, including:

- New custom end-system data fields and additional operating system data fields have been added to ExtremeConnect.
- Extreme Management Center backups now include ExtremeConnect configurations.
- Beginning with Extreme Management Center version 8.5, the following ExtremeConnect modules are hidden by default:

- FiberlinkMaaS360
- FntCommand
- Intune
- McAfee Dxl
- McAfee EPO
- MobileIron
- MSLync SDN
- OpenStack
- Sophos Mdm
- Xen Desktop
- Xen Server
- Xen Mobile
- Domain Portal (cross-XMC search - has no UI anymore)
- Eset Security
- Nutanix
- VWClever RDC

If you have enabled one or more of these modules, it should not be hidden in your network; however, ExtremeConnect may hide the module if it is disabled at any time. Hidden modules are still fully functional, but cannot be configured automatically by ExtremeConnect. To enable a hidden module, modify the configuration file manually.

1.4 ExtremeAnalytics

- [Streaming Flow Data from ExtremeAnalytics into Splunk](#)
- [Improvements to Response Time Dashboard](#)
- [Additional Devices Support Application Telemetry](#)

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.

Additional Devices Support Application Telemetry

Application Telemetry is supported on the following device types:

- SLX9740
- ERS4900
- ERS5900
- ERS devices running firmware versions later than 7.7.0
- BOSS devices running firmware versions later than 7.7.0

1.5 ExtremeCompliance

ExtremeCompliance now supports the following device types (as of Extreme Management Center Version 8.5):

- VSP4900-12MXU12XE
- VSP4900-24S
- VSP4900-24XE
- SLX9740-40C
- SLX9740-80C
- AP310i/e
- AP360i/e

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

1.6 ExtremeControl

- [Enhancements to DCHP Fingerprint Functionality](#)
- [Ability to Configure RADSec and TCP on Proxy RADIUS Servers](#)
- [Export of End-System Table Data Now Supports HTML Format](#)
- [New Option to Remove End-Systems via the End-Systems Tab](#)
- [Advanced Location-Based Registration and Web Access Configuration Available](#)

- [Ability to Create Helpdesk Provisioners in Guest & IoT Manager](#)
- [Preview with RADIUS Attributes Added](#)
- [Enhancement to Variables in RADIUS Attribute Configurations](#)
- [Enhanced Enforce Preview Functionality for ExtremeControl](#)

Enhancements to DHCP Fingerprint Functionality

Several enhancements to the **Detection and Profiling table** on the **Administration > Device Types** tab have been made to improve DHCP fingerprint functionality.

- Add or edit DHCP device type profiles directly to the table. If a system fingerprint is edited, a custom fingerprint is created that overrides the system fingerprint.
- Delete custom fingerprints directly from the table. If the custom fingerprint was overriding a system fingerprint, the system fingerprint becomes active once again.
- Import a custom DHCP fingerprint xml definitions file to Extreme Management Center.
- The Detection and Profiling table now supports additional operations, including the Group by this Field option, which groups the data in the table by the selected column heading, and the Show in Groups option, which displays the fingerprints grouped by the field you selected.

NOTE: Fingerprints are now applied to all ExtremeControl engines and are no longer engine-specific.

Ability to Configure RADSec and TCP on Proxy RADIUS Servers

You can now select TCP and RADSec setting options when configuring RADIUS Server authentication and accounting ports. RADSec adds TLS (Transport Layer Security) over TCP. For versions prior to Extreme Management Center version 8.5, TCP/TLS settings are not supported and cannot be enforced to ExtremeControl engines.

Export of End-System Table Data Now Supports HTML Format

Export of ExtremeControl end-systems and end-system events from the respective tables now supports HTML format.

New Option to Remove End-Systems via the End-Systems Tab

A new Cleanup Data option has been added to the Tools menu in the End-Systems Table on the **Access Control > End-Systems tab**, which enables you to easily remove end-systems from the tables and charts on the End-Systems tab.

Advanced Location-Based Registration and Web Access Configuration Available

Advanced location-based registration and web access enables you to configure different access features for end users based on the location of a connecting end-system. Using the **Rules** tab, you can define a location-based access configuration, which specifies the access method and portal used by the end user to register or log in, and the access levels assigned to the end user following registration or login.

Ability to Create Helpdesk Provisioners in Guest & IoT Manager

You can now create a Helpdesk Provisioner user in Guest & IoT Manager with the ability to view and edit all the Guest user and Device records of the Onboarding Templates to which they are assigned. Helpdesk Provisioners can add records of assigned Onboarding Templates; edit, delete and extend user expiration; and perform resend password, resend details, renew password, and print operations on accessible records.

Preview with RADIUS Attributes Added

A new **Preview with RADIUS Attributes** option, which allows you to preview your policy with a given RADIUS Attribute configuration, has been added to **Access Control > Policy Mappings**.

Enhancement to Variables in RADIUS Attribute Configurations

Custom substitution variables can now contain other variables and are resolved up to three times in RADIUS Attribute configurations.

Enhanced Enforce Preview Functionality for ExtremeControl

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

2. Deprecated Features

In Extreme Management Center version 8.5, the following legacy Java applications (Console, MIB Tools, NAC Manager, and Policy Manager) are disabled by default. To use the legacy Java applications in version 8.5, follow the instructions in the [GTAC knowledgebase article](#).

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

Additionally, beginning in version 8.5, Extreme Management Center no longer supports restoring legacy backups. You can access legacy backups by upgrading to Extreme Management Center version 8.5.

3. Known Issues and Vulnerabilities Addressed

3.1 Known Issues Addressed in 8.5.1

Extreme Management Center Issues Addressed	ID
The Add Device to Access Control Engine Group option on the Site > Actions panel and the Add/Configure Device > Actions panel was not completing for ExtremeControl engines during ZTP+ process.	2183833
Moving maps within the left-panel navigation tree on the Sites tab did not always move the devices properly and, sometimes, associated submaps did not move with the maps.	2172986
A tooltip message was improperly displaying for the Neighboring Capabilities field on the DeviceView > Ports and Port Tree views. The message no longer displays.	02211816
The ICX-MLX Backup Configuration System Workflow was assigning different directories for a single archive configuration, which was causing an unusable backup organization for the archive.	2184831
Selecting Stamp New Version on the Network > Archives tab did not complete successfully if the user's name contained an "at sign" character (@).	01807646
XML fields with greater than 2048 characters were causing the LDAP Configuration to stop responding.	1222245
Attempting to create a manual link for devices in a map was unsuccessful.	2241955
The Archived Devices ring chart on the Impact Analysis dashboard could not be configured to display the number of archives created for devices over a duration of more or less than 30 days. Users can now configure the duration from which the total number of device archives is calculated and displayed on the Impact Analysis dashboard via the Administration > Options > Impact Analysis tab.	1940347
Additionally, when an archive was not created successfully, alarms did not clearly explain the issue. Events that indicate a device archive failure are now prepended with Failed to more clearly indicate the issue.	
Administrator-selected options were sometimes being ignored when the list of Archived devices was updated.	----

3. Known Issues and Vulnerabilities Addressed

An improperly implemented base collector class support was creating a memory leak in the Trap Receiver.	-----
Enforce/Verify failures were occasionally occurring after changing the VLAN or NSI mapping of Policy Roles or Rules and enforcing to a Wireless Controller.	-----

ExtremeAnalytics Issues Addressed	ID
IPFIX parsing was potentially ignoring flow set data, resulting in some flow sets not being processed. Now, flows in every flow set in an IPFIX packet are processed.	-----
The appid process was crashing when it encountered certain ERSPAN packets.	02192534

ExtremeControl Issues Addressed	ID
On the Access Control tab, column settings were not persisting in the End Systems table when navigating away from the page and back again, and when the Refresh button was selected.	2178542
When adding a secondary device modeled with non-default SNMPv3 credentials to the ExtremeControl engine, the device would lose or alter the <code>/etc/snmpd.conf</code> file and fail to be modeled thereafter. This is no longer happening.	01880374
The AUP for Guest Registration was improperly preventing guests from being able to register. The issue has been addressed and is no longer interfering with guest registration.	01889261
On the Access Control tab, end-systems were displaying in the wrong ExtremeControl engine End-System table. Now, end-systems display in the appropriate end-system table	02190793
Policy enforcement failure with "ArrayIndexOutOfBounds" exceptions in the server.log were occasionally occurring when enforcing to an X435 on which ExtremeXOS version 30.5 or later was installed.	-----

3.1.1 Known Issues Addressed in 8.5.0

Extreme Management Center Issues Addressed	ID
---	-----------

3. Known Issues and Vulnerabilities Addressed

The <code>watchdog.log</code> and <code>appmonitor.log</code> files could not be configured to remove the oldest files. Now the <code>cleanLogs</code> script is included with Extreme Management Center so that only the latest 10 files are saved.	01981039
Devices with a Poll Type of Maintenance no longer periodically issue SNMP requests in order to check for component changes.	----
SNMP timeouts were occurring when Extreme Management Center was communicating with third-party devices.	----
Extreme Management Center options for displaying MAC addresses with an OUI prefix were not available.	----
Discover was not being allowed for valid Sites based on the "Add Device" capability. The capability for "Sites Read/Write Access" is not necessary for Site Discover, but it is necessary for adding or editing sites.	----
QoS and EAPs fields were required fields to create VLAN scripts for EXOS in Extreme Management Center. Now, the <code>Create_VLAN</code> scripts for EXOS have been updated to treat QoS and EAPs as optional fields.	1813187
The default <code>TransferProtocol</code> setting for the Cisco Vendor Profile database was previously set incorrectly.	01985239
The Archive Restore function was not displaying a warning if the archive was from a different model type.	----
The Scheduled Task Name, Description, and Subject values were reverting back to default values after being changed during editing.	1782136
NMS-BASE license now allows you to enable, disable and add a port to a group via the right-click Port drop-down list in the Devices > Device view.	01837802
The Interface History PDF was unclear because it was missing titles on three area charts and multi-line charts were using the same colors for each line.	01709514
The Generate Show Support feature was not showing the current status when navigating away and back.	----
The MLAG Summary report was displaying information from more than one MLAG pair when devices had identical MLAG configurations.	1946635
Attempting to set an EXOS device's restart time to a date more than a month ahead would fail, indicating that the proposed reboot time was in the past.	1784366

3. Known Issues and Vulnerabilities Addressed

Extreme Management Center was indicating that devices had exceeded device memory usage on EXOS and was generating alarms, although the devices appeared to have plenty of memory available.	1958668
The Mgmt [4095] VLAN for ExtremeXOS devices was incorrectly able to be added to the Tagged list for a port in Extreme Management Center. Now, the Mgmt [4095] VLAN is no longer selectable in the Tagged list for a port.	-----
Archives were being sorted incorrectly because they were being sorted alphabetically, which doesn't respect numerical date formats properly.	01946495
The temperature graph for certain VOSS devices was not displaying on the Device View > Historical Performance tab.	01994534
The maximum SNMP Compass search time has been expanded from 2 minutes to 10 minutes to support larger deployments.	-----
Workflow paths with a conditional expression were not working for device specific variables, causing Workflows to fail.	-----
Firmware upgrades were not allowed for devices set to Maintenance / Remove from Service.	1944261
netSNMP log messages were being merged with the device trap message in the Extreme Management Center > Event view.	1942303
Archive menu options were hidden when permission for firmware upgrade was removed from user permissions.	01940887
EXOS 8 Stacks were sometimes timing out before completing archive backup.	01973463
The ICX-7450 stacks with 2 units were mapping as one single system in Extreme Management Center.	01877301
In the Devices table, the Firmware column was displaying the Boot ROM version for Aruba 2930F.	1968881
Workflows triggered by an alarm/event were only working for devices that existed in the Extreme Management Center database, but not for missing or unknown devices.	-----
The Manage SSH Configuration > Create/Edit/Delete functionality was not working properly on the Administration > Users tab.	01982920 01992095 01984146
Logical ports on third-party devices were counting against the license limit.	1974488

3. Known Issues and Vulnerabilities Addressed

The MLAG Summary report, generated from the Network > Devices tab, was displaying unnecessary MLAG information.	1946635
End-system groups that were deleted or renamed in Extreme Management Center were being deleted from GIM Onboarding Templates. Now, when end system groups are deleted in Extreme Management Center, a warning message is shown in GIM when the Onboarding Template is opened for editing.	01934063
The Diagnostics > Server> Server License > Add License window did not include IA-GIM.	01991124
The Devices > Device > Ports view was not displaying Cisco Fabric Extender ports correctly.	01981119
A message was displaying that a VLAN name could not be modified when it was assigned to a port. That message no longer displays because names of VLANs that are assigned to ports can be changed.	1155260 1718693
The Syslog and Trap "Ignore IP List" filter was not being applied to new trap or syslog messages.	-----
The Archive Compare File Swap feature was not swapping the displayed files.	1404408
Deleting an Extreme wireless controller that shares a WLAN or VNS with another Extreme wireless controller was displaying a ConstraintViolationException error in the System log.	01964545
ExtremeAnalytics Issues Addressed	ID
In ExtremeAnalytics, the Application Server compound collector was not respecting the limit of top 100 apps and top 100 servers per app.	01851795
The ExtremeAnalytics > Engine License Rates chart was incorrectly displaying significantly less unique end-system counts than were observed.	01992118 02161641
ExtremeControl Issues Addressed	ID
In the Control> Dashboard> Overview Report page, Authentication Type wasn't launching the filtered end-systems table correctly, and in the Control> Dashboard> Health Report pane, Risk Level wasn't launching the filtered end-systems table correctly.	-----
End systems were displaying as "MAC" authenticated on the Control > End System tab when an X session was active on the switch.	01801463 01827905 01932037

3. Known Issues and Vulnerabilities Addressed

The value of sysObjectID was being incorrectly set for ExtremeControl engines.	01983768
Resetting End-System diagnostics by MAC or IP address was not completely disabling diagnostics.	01522146 01982359
The AAA Rule Configuration> Supported RADIUS Type incorrectly included PAP and EAP-TTLS with tunneled PAP as options for NTLM authentication. Those options have been removed to clarify this field.	-----
End-System table live updates were not being filtered by zone when viewed with view access limited to specified zones.	01955995
Sorting some Access Control > Policy Mapping table columns was throwing exceptions if any values were empty.	01956869
In ExtremeControl, the live end-system count was increasing in the End-system table when end-systems were updating and not newly added. Now, only newly added end-systems are counted, and updated end-systems are not counted again.	-----
The Access Control evaluate tool was not launching from the Configurations table.	-----
The Access Control > End Systems > End System table was not displaying port alias information.	01981206
ExtremeControl engine was incorrectly running the snmpconfig script to change SNMP.	01983768
The ExtremeControl > Guest Web Access > Customize Fields > Edit window was lagging in the "Loading" state.	01916225
The "Start Packet Capture" option is no longer available in any ExtremeControl end-system tables.	-----
ExtremeConnect Issues Addressed	ID
Using ExtremeConnect with a large number of end-systems connected (for example, 50,000) was causing significant performance issues for the Extreme server.	01937179

3.2 Vulnerabilities Addressed

This section presents the vulnerabilities addressed in Extreme Management Center 8.5.1:

- The following vulnerabilities were addressed in the Extreme Management Center, ExtremeControl, and ExtremeAnalytics engine images:
 - CVE-2018-0500, CVE-2018-8740, CVE-2019-19603, CVE-2019-19645, CVE-2020-11655, CVE-2020-13434, CVE-2020-13435, CVE-2020-13630, CVE-2020-13631, CVE-2020-13632, CVE-2020-13790, CVE-2020-0543, CVE-2020-0548, CVE-2020-0549, CVE-2019-1547, CVE-2019-1549, CVE-2019-1551, CVE-2019-1563, CVE-2017-11109, CVE-2017-5953, CVE-2017-6349, CVE-2017-6350, CVE-2018-20786, CVE-2019-20079, CVE-2019-12387, CVE-2019-12855, CVE-2019-9512, CVE-2019-9514, CVE-2019-9515, CVE-2020-10108, CVE-2020-10109, CVE-2020-10531, CVE-2020-1700, CVE-2019-13734, CVE-2019-13750, CVE-2019-13751, CVE-2019-13752, CVE-2019-13753, CVE-2019-19880, CVE-2019-19923, CVE-2019-19924, CVE-2019-19925, CVE-2019-19926, CVE-2019-19959, CVE-2019-20218, CVE-2020-9327, CVE-2020-8130, CVE-2019-19221, CVE-2020-9308, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2020-8597, CVE-2019-19956, CVE-2020-7595, CVE-2018-16888, CVE-2019-20386, CVE-2019-3843, CVE-2019-3844, CVE-2020-1712, CVE-2019-19906, CVE-2017-16808, CVE-2018-10103, CVE-2018-10105, CVE-2018-14461, CVE-2018-14462, CVE-2018-14463, CVE-2018-14464, CVE-2018-14465, CVE-2018-14466, CVE-2018-14467, CVE-2018-14468, CVE-2018-14469, CVE-2018-14470, CVE-2018-14879, CVE-2018-14880, CVE-2018-14881, CVE-2018-14882, CVE-2018-16227, CVE-2018-16228, CVE-2018-16229, CVE-2018-16230, CVE-2018-16300, CVE-2018-16451, CVE-2018-16452, CVE-2018-19519, CVE-2019-1010220, CVE-2019-15166, CVE-2019-15167, CVE-2019-5188, CVE-2019-15795, CVE-2019-15796, CVE-2019-20367, CVE-2019-13627, CVE-2019-15165, CVE-2019-15845, CVE-2019-16201, CVE-2019-16254, CVE-2019-16255, CVE-2019-14866, CVE-2019-12290, CVE-2019-18224, CVE-2019-13117, CVE-2019-13118, CVE-2019-18197, CVE-2019-6111, CVE-2019-10222, CVE-2019-13012, CVE-2019-12450, CVE-2019-8457, CVE-2019-12735, CVE-2019-19377, CVE-2019-19769, CVE-2020-11494, CVE-2020-11565, CVE-2020-11608, CVE-2020-11609, CVE-2020-11668, CVE-2020-12657, CVE-2020-12826, CVE-2020-8616, CVE-2020-8617, CVE-2020-11669, CVE-2020-12762, CVE-2020-3810, CVE-2019-20795, CVE-2020-12243, CVE-2018-5383, CVE-2020-2759, CVE-2020-2760, CVE-2020-2762, CVE-2020-

2763, CVE-2020-2765, CVE-2020-2780, CVE-2020-2804, CVE-2020-2812, CVE-2020-2892, CVE-2020-2893, CVE-2020-2895, CVE-2020-2896, CVE-2020-2897, CVE-2020-2898, CVE-2020-2901, CVE-2020-2903, CVE-2020-2904, CVE-2020-2921, CVE-2020-2922, CVE-2020-2923, CVE-2020-2924, CVE-2020-2925, CVE-2020-2926, CVE-2020-2928, CVE-2020-2930, CVE-2019-16234, CVE-2019-19768, CVE-2020-10942, CVE-2020-11884, CVE-2020-8648, CVE-2020-9383, CVE-2019-2228, CVE-2020-3898, CVE-2019-18348, CVE-2020-8492, CVE-2020-11008, CVE-2020-5260, CVE-2020-8428, CVE-2020-8834, CVE-2020-8992, CVE-2018-14553, CVE-2019-11038, CVE-2020-8831, CVE-2020-8833, CVE-2020-8835, CVE-2018-14498, CVE-2018-19664, CVE-2018-20330, CVE-2019-2201, CVE-2018-11574, CVE-2019-19046, CVE-2020-8428, CVE-2020-15709, CVE-2020-12400, CVE-2020-12401, CVE-2020-6829, CVE-2020-15704, CVE-2020-11936, CVE-2020-15701, CVE-2020-15702, CVE-2020-14539, CVE-2020-14540, CVE-2020-14547, CVE-2020-14550, CVE-2020-14553, CVE-2020-14559, CVE-2020-14568, CVE-2020-14575, CVE-2020-14576, CVE-2020-14586, CVE-2020-14591, CVE-2020-14597, CVE-2020-14619, CVE-2020-14620, CVE-2020-14623, CVE-2020-14624, CVE-2020-14631, CVE-2020-14632, CVE-2020-14633, CVE-2020-14634, CVE-2020-14641, CVE-2020-14643, CVE-2020-14651, CVE-2020-14654, CVE-2020-14656, CVE-2020-14663, CVE-2020-14678, CVE-2020-14680, CVE-2020-14697, CVE-2020-14702, CVE-2019-17514, CVE-2019-20907, CVE-2019-9674, CVE-2020-14422, CVE-2017-12133, CVE-2017-18269, CVE-2018-11236, CVE-2018-11237, CVE-2018-19591, CVE-2018-6485, CVE-2019-19126, CVE-2019-9169, CVE-2020-10029, CVE-2020-1751, CVE-2020-1752, USN-4377-1, CVE-2020-14309, CVE-2020-15707, CVE-2020-10713, CVE-2020-15706, CVE-2020-14311, CVE-2020-14310, CVE-2020-15705, CVE-2020-14308, CVE-2020-10711, CVE-2020-10751, CVE-2020-12768, CVE-2020-12770, CVE-2020-13143, CVE-2020-5963, CVE-2020-5967, CVE-2020-5973, CVE-2020-8169, CVE-2020-8177, CVE-2020-12049, CVE-2019-17023, CVE-2020-12399, CVE-2019-7303

- Extreme Management Center and ExtremeControl engine images:
 - CVE-2019-7317, CVE-2020-13820, CVE-2020-13819, CVE-2019-11599, CVE-2019-9503, CVE-2019-3842, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-3874, CVE-2019-3882, CVE-2019-6133, CVE-2018-5743, CVE-2019-0136, CVE-2019-10207, CVE-2019-11487, CVE-2019-13631, CVE-2019-15211, CVE-2019-15215, CVE-2018-21008, CVE-2019-14816, CVE-2019-14821, CVE-2019-15117, CVE-2019-15118, CVE-2019-15505, CVE-2019-15902, CVE-2018-20784, CVE-

2019-10638, CVE-2019-13648, CVE-2019-14283, CVE-2019-14284, CVE-2019-3900

- Extreme Management Center and ExtremeAnalytics engine images:
 - CVE-2019-14895, CVE-2019-14896, CVE-2019-14897, CVE-2019-14901, CVE-2019-16231, CVE-2019-18660, CVE-2019-19045, CVE-2019-19052, CVE-2019-19524, CVE-2019-19534, CVE-2019-19529
- Extreme Management Center engine image:
 - CVE-2019-18813, CVE-2019-19051, CVE-2019-19055, CVE-2019-19072, CVE-2019-11190, CVE-2019-11191, CVE-2019-11810, CVE-2019-11815, CVE-2016-3189, CVE-2019-12900, CVE-2019-10126, CVE-2019-1125, CVE-2019-12614, CVE-2019-13272, CVE-2019-3846, CVE-2016-10743, CVE-2019-9495, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499, CVE-2019-9893, CVE-2019-11477, CVE-2019-11478, CVE-2018-20836, CVE-2019-10142, CVE-2019-11833, CVE-2019-11884, CVE-2019-2054, CVE-2019-5435, CVE-2019-5436, CVE-2019-9924, CVE-2019-11555, CVE-2018-20843, 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-2019-9936, CVE-2019-9937, CVE-2019-13057, CVE-2019-13565, CVE-2019-11479, CVE-2019-16056, CVE-2019-16935, CVE-2019-14615, CVE-2019-15291, CVE-2019-18683, CVE-2019-18885, CVE-2019-19057, CVE-2019-19062, CVE-2019-19063, CVE-2019-19227, CVE-2019-19332, CVE-2018-3639, CVE-2018-3640, CVE-2018-3646, CVE-2019-3462, CVE-2018-16890, CVE-2019-3822, CVE-2019-3823, CVE-2018-20685, CVE-2019-6109, CVE-2019-1559, CVE-2015-9383, CVE-2018-20406, CVE-2018-20852, CVE-2019-10160, CVE-2019-5010, CVE-2019-9636, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948, CVE-2019-5481, CVE-2019-5482, CVE-2019-15903, CVE-2019-14287, CVE-2016-10905, CVE-2017-18509, CVE-2018-20961, CVE-2018-20976, CVE-2019-15926, CVE-2019-14835, CVE-2019-15030, CVE-2019-15031, CVE-2016-5195, CVE-2019-5094, CVE-2018-12207, CVE-2019-0154, CVE-2019-0155, CVE-2019-11135, CVE-2019-15098, CVE-2019-16746, CVE-2019-17052, CVE-2019-17053, CVE-2019-17054, CVE-2019-17055, CVE-2019-17056, CVE-2019-17666, CVE-2019-2215, CVE-2019-16275, CVE-2019-17075, CVE-2019-17133, CVE-2019-0155, CVE-2019-11135, CVE-2019-11139, CVE-2019-18218, CVE-2019-18218, CVE-2016-10906, CVE-2017-18232, CVE-2019-14814, CVE-2019-16168, CVE-2019-19242, CVE-2019-19244, CVE-2019-5018, CVE-2019-5827, CVE-2018-20856, CVE-2018-10844, CVE-2018-10845, CVE-2018-10846, CVE-2019-3829, CVE-2019-3836, CVE-2016-7076, CVE-2017-1000368, USN-4038-3, USN-4049-3

- The following vulnerabilities were addressed in the ExtremeControl engine image:
 - CVE-2019-10092, CVE-2019-11234, CVE-2019-11235, CVE-2018-16884, CVE-2019-9500, CVE-2018-14678, CVE-2018-18021, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-6974, CVE-2019-7221, CVE-2019-7222, CVE-2019-7308, CVE-2019-8912, CVE-2019-8980, CVE-2019-9213, CVE-2018-18397, CVE-2018-19854, CVE-2019-6454, CVE-2019-14814, CVE-2019-14815, CVE-2019-15918, CVE-2018-19985, CVE-2019-10639, CVE-2019-14763, CVE-2019-15090, CVE-2019-15212, CVE-2019-15214, CVE-2019-15216, CVE-2019-15218, CVE-2019-15220, CVE-2019-15221, CVE-2019-15292, CVE-2019-3701, CVE-2019-3819, CVE-2019-9506, USN-4115-2
- The following vulnerabilities were addressed in the ExtremeAnalytics engine image:
 - CVE-2019-16233, CVE-2019-19083, CVE-2019-19807

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 **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 8.5.x supports upgrades from Extreme Management Center version 8.3.x or 8.4.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 8.1, you must first upgrade to the latest Extreme Management Center 8.3 or 8.4 release, then to 8.5.1.

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.

- When upgrading the Extreme Management Center server, ExtremeAnalytics engine, or ExtremeControl engine to version 8.5.1, ensure the DNS server IP address is correctly configured.
- When upgrading to Extreme Management Center version 8.5.1, 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
```

- 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 8.5 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 8.5 requires you to [renew your NMS license](#) if generated prior to July 31, 2020. Licenses generated prior to July 31, 2020 expire 90 days after upgrading to Extreme Management Center version 8.5.

4.2.2 Upgrading Hardware

When attempting to upgrade the Extreme Management Center server, the ExtremeAnalytics engine, or the ExtremeControl engine to version 8.5, 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 8.5, 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 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 8.5, upgrade your ExtremeControl engine version to 8.2 or 8.3. Additionally, both Extreme Management Center and the ExtremeControl engine must be at version 8.5 in order to take advantage of the new ExtremeControl 8.5 features.

NOTE: ExtremeControl 8.5 functionality is not supported on the 2S Series and 7S Series ExtremeWireless 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 8.5* 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 8.5 if you upgrade to the ExtremeControl engine 8.5. Version 8.5 of the assessment agent adapter requires an operating system with a 64-bit architecture.

4.4.2 ExtremeControl Version 8.0 and later

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 8.5 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 8.5:

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 8.5 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 8.5, the Default Gateway IP Address is configured as part of the VLAN. In 8.5, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 8.5, 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 8.4.2.

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 Wireless Manager Upgrade Information

A 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: Wireless event collection is disabled by default in version 8.5 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 8.5.

5.1 Extreme Management Center Server and Client OS Requirements

5.1.1 Extreme Management Center Server Requirements

These are the operating system requirements for the Extreme Management Center server.

Manufacturer	Operating System
Linux	Red Hat Enterprise Linux WS and ES v6 and v7 Ubuntu 18.04
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

5.1.2 Extreme Management Center Client Requirements

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

Manufacturer	Operating System
Windows (qualified on the English version of the operating systems)	Windows® 10
Linux	Red Hat Enterprise Linux WS and ES v6 and v7 Ubuntu 18.04
Mac OS X®	El Capitan Sierra

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.

5.2.1 Extreme Management Center Server Requirements

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
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.

5.2.2 Extreme Management Center Client Requirements

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
Disk Size	240 GB	480 GB	960 GB
IOPS	200	200	10,000

Specifications	Small	Medium	Large
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

Specifications	Small	Medium	Enterprise
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
Windows ¹	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		

Manufacturer	Operating System	Operating System Disk Space	Available/Real Memory
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 8.5 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
Mobile¹	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