Extreme Management Center® Release Notes
Version 8.3.3

11/2019
9036258-03 Rev. AA

Table of Contents

Extreme Management Center Version 8.3 Release Notes

8.3.3.11
November, 2019

The Extreme Management Center Release Notes provide information on the new features and enhancements included in version 8.3, 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 8.3.

For information regarding the features supported by specific devices, see the Firmware Support Matrix. Version 8.3 of Extreme Management Center supports the devices listed in the matrix.

1. Enhancements in Version 8.3

New features and enhancements are added to the following areas in Extreme Management Center version 8.3:

- Engines
- Extreme Management Center
- ExtremeControl
- ExtremeAnalytics
- Information Governance Engine
- 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

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

1.2 Extreme Management Center

Additions to the Device View

There are two new tabs on the Device View of the Network > **Devices** tab. These tabs, called **MAC Address** and **VLAN**, are for Enterasys OS switches.

Enhancement to Devices Discovered in Extreme Management Center

A newly discovered device is no longer automatically added to a Site if it is a potential duplicate of another device. During discovery, Extreme Management Center automatically adds the first discovered device to the site (if the Site's Action is set to **Automatically Add**), and subsequent potentially duplicate devices are added to the **Discovered** tab, instead of to the site. A column display option in the

Discovered tab groups the devices by Serial Number (or by MAC Address if the Serial Number is blank) or by IP Address when the same IP is discovered by different Profiles. This grouping helps determine which device IP should be added to the Site for polling, configurations and to receive syslog and trap messages. If duplicates have already been added to Sites, the Device Potential Duplicates Report identifies the potential duplicates to help the Extreme Management Center Administrator resolve which devices to remove/add from Sites. This is especially useful for devices (such as those in the VSP Device Family) which use multiple IP Addresses for management, CLIP and VLAN/port interfaces. The Add Device feature does not evaluate potentially duplicate devices – devices (potentially duplicate or not) are added to the site.

Added Support for Additional Device Types

Extreme Management Center now supports the following device types:

- ExtremeXOS X465
- AP505
- AP510
- AP560
- SLX 9030
- SLX 9640
- VSP 7400

Extreme Management Center now also supports LAG, MLAG, and Fabric Connect functionality for VSP-86x Tsunami devices.

Enhancements to the Impact Analysis Dashboard

The Impact Analysis dashboard contains the following charts:

- AP Site Quality — Indicates the ratio of ExtremeCloud sites with applications that meet the required RFQI (Radio Frequency Quality Indicator) standards to the total number of sites.
- AP Quality — Indicates the ratio of applications that meet the required RFQI (Radio Frequency Quality Indicator) standards to the total number of APs.

Ability to Authenticate to Extreme Management Center Using TACACS+ Servers

Users with access to Extreme Management Center can now authenticate using up to three TACACS+ servers by selecting TACACS+ as the Authentication Type on the Administration > Users tab.

Compatibility with VMware HA Environments

Extreme Management Center version 8.3.0 is compatible with VMware High Availability environments and can be activated using vSphere configurations.

Device Menu Usability Improvement

The usability of the Device menu on the Network > Devices tab is improved.

Enhancements to Terminal

The device terminal, accessible from the Network > Devices tab, now includes the following functionality:

- Ability to copy and paste
- Ability to log device terminal session

Enhancement to Enforce for Devices that Support Fabric Connect

Extreme Management Center now performs additional validation when enforcing a configuration to a device that supports Fabric Connect. The validation is done after the user clicks the Enforce button from the Compare Device Configuration window. Any configuration errors Extreme Management Center detects are displayed in the Enforce Validation Errors window, which allows the user to cancel or enforce the configuration with errors. The additional validation is only performed if Fabric Services or All is selected in the Enforce drop-down list in the Compare Device Configuration window.

Fabric Support for Additional Device Types

The VSP-8600 device type supports fabric connect functionality. The level of support depends on the firmware version installed on the device:

- Firmware version 6.2 — Basic support, Layer 2 VSN, Layer 3 VSN, IPv4 shortcuts, SPB multicast.
- Firmware version 6.3 — All of the above features plus Fabric Attach, Switched UNI, and Transparent UNI.

NOTE: IPv6 shortcuts are not supported on VSP-8600 devices.

Additionally, Fabric Manager now supports VSP74xx and VOSS 8.0 devices.

New Device Poll Type

You can select the Status Only poll type for devices for which you only need to monitor status. You can add a maximum of 10,000 Status Only devices in Extreme Management Center, and those devices do not count against your licensed device limit.

NOTE: Status Only devices cannot be configured in the legacy Java Console application; they must be configured in Extreme Management Center. Additionally, you can configure the Status Only Poller interval only in Extreme Management Center.

Additional Functionality Added to the Northbound Interface

Because the Northbound Interface now includes Fabric Connect and ExtremeConnect queries and mutations, you can read and write Fabric and ExtremeConnect information from third-party applications.

Enhancement to Licensing

Beginning in Extreme Management Center version 8.3, Extreme APs, Virtual Sensors, and third-party devices with fewer than 10 ports are counted as 1/10 of a device towards your XMC license. You can view the devices included in XMC as 1/10 of a device in Administration > Diagnostics > System > License Diagnostics.

1.3 ExtremeControl

Enhanced Enforce Preview Functionality for ExtremeControl

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

Ability to Redirect Wired Users to ExtremeGuest Captive Portal

You can now configure ExtremeControl to redirect wired guest users to ExtremeGuest. This allows both wired and wireless users to achieve a unified guest experience. This feature is supported with ExtremeXOS switches, which provide centralized guest management, including multiple guest onboarding methods and guest analytics for wired and wireless deployments.

Regular Expressions Supported in Group Entries

Entries in most ExtremeControl Groups now support regular expression matching, in addition to the previously supported asterisk (*) and question mark (?) wildcards. Entries that begin with a caret (^) and end with a dollar sign ($) are compiled as regular expressions with the standard Java syntax.

NOTE: LDAP User, LDAP Host, and RADIUS User groups do not support regular expression matching.

Ability to Modify the Case and Spacing in RADIUS Attributes

When creating RADIUS attributes via the Edit RADIUS Attribute Configuration window, you can remove spaces and change the case of strings of text.

GIM Enhancements in Extreme Management Center

Extreme Management Center added the following enhancements to improve Guest and IoT Manager functionality:

- The Guest and IoT Managers tab in Control > Access Control > Engine Groups contains a Name field where you can specify the name of your Guest and IoT Managers.
- End-System Groups added by Guest and IoT Manager in Extreme Management Center now include the Device Name in the Description field.
- User Groups added by Guest and IoT Manager in Extreme Management Center now include the user's first and last name in the Description field.

Ability to Use CSV File to Onboard Devices and Users in GIM

To onboard a large number of devices or Guest User accounts at one time, use the Voucher/CSV Type Onboarding Template to upload a CSV file. You can also create a large number of Guest User accounts in Guest and IoT Manager by specifying the number of Vouchers GIM generates with a random username and password.

Enhancement to Backups in GIM

In version 8.3, the Backup screen contains a Scheduled Backup section where you can configure backups to occur on a scheduled basis.

Housekeeping in GIM

A new section for housekeeping is introduced in Guest and IoT Manager that has some predefined tasks, which enables the admin to delete Guest Users/Devices that have never logged into the system and have their first login pending.

Swagger for APIs Included in GIM

Using the Swagger tool included in Guest and IoT Manager Administrator application, the administrator can use REST APIs directly from the application.

Change in LDAP Sponsor in GIM

The LDAP Sponsor configuration setting has changed in release 8.3. In the earlier releases, the admin specifies the User Search Root for the Sponsor LDAP config (for example, OU=Gim,CN=Users,DC=SponsorGroup,DC=com). This is now changed and the admin should specify the LDAP Group instead (for example, CN=Gim,CN=Users,DC=SponsorGroup,DC=com).

SMS Gateway Visibility Option

In the Administration section under notifications the SMS gateways are present. Admin now has the choice to specify if these gateways are visible to Provisioners. If a gateway is not marked as visible then the Provisioner does not see it while onboarding guest users. This is applicable to both Provisioner and Self Service flow.

Ability to Resend Details and Password in GIM

The provisioner can use the Resend Details and Resend Password buttons to resend the details and password, respectively, to a Guest User.

Enhancement to Number of Languages in GIM

GIM now includes five languages in Locales:

- English
- French
- Italian
- Dutch
- Swedish

Improvement to Sponsor Tab in GIM

In releases prior to version 8.3, the Sponsor tab in the Provisioner application displays regardless of the presence of any records on the screen. In version 8.3, the

tab displays on the left panel of the screen only if there are records to view.

Improvement to Administration Idle Timeout Setting

The Administrator login uses the idle timeout setting configured in Extreme Management Center. You can configure a different idle timeout setting value for the Administrator and Provisioner applications.

1.4 ExtremeAnalytics

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.

Streaming Flow Data from ExtremeAnalytics into Elastic Stack

ExtremeAnalytics supports the ability to stream flow data from an ExtremeAnalytics engine into Elastic Stack (aka ELK stack). This support includes instructions on how to add the open-source “Elastiflow” module to an ELK server and how to update this deployment to make Elastiflow aware of Extreme’s IPFIX format. We also included files that you can copy to the ELK server to assist with the customization.

Introducing the Virtual Sensor

Beginning in version 8.3, you can monitor flows in your network across virtual environments using the ExtremeAnalytics Virtual Sensor. The Virtual Sensor works with your existing ExtremeAnalytics engine to collect flow data and display it in Extreme Management Center. The virtual sensors status is also included on the Insights dashboard on the Analytics tab.

New Devices Support Application Telemetry

Application Telemetry is supported on the following device types:

- ExtremeXOS devices using V400 port extenders
- VSP 7400-32C

- Summit X465-G2 switches
- SLX9140

NOTE: SLX9140 is the only SLX device that supports Application Telemetry.

Improved Location Performance

Data from the Analytics > Configuration > Locations window now displays on the Network > Devices > Sites > Endpoint Locations tab, which improves performance, allowing up to 20,000 locations to display.

1.5 ExtremeConnect

ExtremeConnect Configurations Included in Extreme Management Center Backups

Extreme Management Center backups now include ExtremeConnect configurations.

VMWare vSphere Module Enhancements

The VMWare vSphere module includes the following enhancements:

- Ability to import the Management MAC address into Extreme Management Center.
- Ability to filter based on DataCenter name.

Ability to Integrate ExtremeConnect with Microsoft SCVMM

ExtremeConnect now includes a Microsoft System Center Virtual Machine Manager module that allows you to integrate Extreme Management Center with Microsoft System Center Virtual Machine Manager.

1.5 Information Governance Engine

When you install Extreme Management Center 8.3, your version of the Information Governance Engine (IGE) is automatically upgraded. The new version supports the following device types:

- ExtremeXOS X465 with firmware version 30.2 or later
- VSP7400
- SLX 9030

- SLX 9640
- AP505i
- AP505e
- AP510i
- AP510e
- WiNG 7

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

1.6 ExtremeWireless

11ax Radio for AP5xx Models Supported

ExtremeWireless now supports 11ax Radio for AP5xx models.

2. Deprecated Features

There are no deprecated features in Extreme Management Center version 8.3.

3. Known Issues and Vulnerabilities Addressed

3.1 Known Issues Addressed in 8.3.3.11

Extreme Management Center Issues Addressed	ID
ExtremeXOS XMODs included in a patch release were not compatible for upgrade with existing devices that match the firmware release fields.	1937246
Links for VSP and ERS devices included in a map were not changing to red when the port had a Status of Down.	------
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
Extreme Management Center did not support ExtremeCloud Appliance version 4.76.	------

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

ExtremeControl Issues Addressed	**ID**
ExtremeCloud Appliances were not using Change-Of-Authorization (CoA) by default for reauthentication.	01887597 01941407
ExtremeControl was not sending RADIUS Change of Authorization (CoA) messages to ExtremeCloud Appliance devices.	------
Values in ExtremeControl location groups could not be greater than 512 characters.	01937960 01941399
The ExtremeControl Assessment agent for OSX did not fully support 64-bit operating systems.	01925944 01932152
The "invert" option for Authentication Method rule matching did not work properly in ExtremeControl.	1937075
ExtremeControl was not using CTRON-ALIAS-MIB as the mechanism for MAC to IP resolution via SNMP for ExtremeCloud Appliances.	01935200
The Auth. Access Type for ExtremeCloud Appliance devices was not set to Manual Radius Configuration.	------

3.2 Known Issues Addressed in 8.3.2.11

Extreme Management Center Issues Addressed	**ID**
Scripts in Extreme Management Center were failing if the CLI output contained non-printable characters.	01849224
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.	------
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
Virtual Networks and SSIDs on an ExtremeCloud Appliance may not display on the Wireless > Network tab.	01907673 01918004 01918005

Upgrading an Extreme Management Center server, an ExtremeAnalytics engine, or an ExtremeControl engine from version 8.1.6 to version 8.2 or 8.3 was causing the system to boot into Emergency mode.	------
Installing or upgrading an Extreme Management Center server, an ExtremeAnalytics engine, or an ExtremeControl engine to version 8.3 without an internet connection caused dependency errors for various linux packages.	------
The NTP daemon was not starting properly if it was initially disabled and enabled after installation or upgrade.	------
NTP may fail when upgrading to 8.3.1.	------
Functions that heavily utilize SNMP, such as device statistics collection and policy enforcement, can take excessive time to complete.	1900346 1910244 1928480
ExtremeXOS devices running with RESTCONF version 2.0.1.5 or later are not displaying Fabric Attach settings correctly in Fabric Manager.	------
Using a GSIS integration to collect Extreme Management Center reporting data for a custom duration was generating reports with an incorrect time stamp.	------
ExtremeAnalytics Issues Addressed	**ID**
Accessing the End-Systems Applications Summary for a client for which Extreme Management Center resolved the IP address was displaying a 0 for Clients, Application, and Application Groups.	01877808
ExtremeControl Issues Addressed	**ID**
Global rules allowed the HTTP Redirect action to be configured even though the HTTP Redirect action is not supported.	01896871

3.3 Known Issues Addressed in 8.3.1.9

Extreme Management Center Issues Addressed	**ID**
A cursor did not display in the WebShell when a Terminal session was opened for a device in Extreme Management Center version 8.3.0.	01891075
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.	------

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.	------
Extreme Management Center was not processing SNMPv3 informs from devices configured to use a NoAuthNoPriv credential.	------
Attempting to delete multiple firmware images from the Network > Firmware tab right-panel was not completing successfully and displayed an Uncaught TypeError.	------
Extreme Management Center was failing to send emails when an SMTP server was configured for AUTH/LOGIN and Extreme Management Center was configured to send the email anonymously.	01888358 01888890 01889722 01889949 01889965 01890369 01892555
Statistics collected from ExtremeCloud Appliances were slow (or occasionally failed) to display in Extreme Management Center.	------
Extreme Management Center was displaying the server IP address instead of the device IP address when the device's sysName contained a hyphen character (-) and the sysName before the hyphen character is also included in the Extreme Management Center domain name. For example, the issue would occur if the device sysName was commonname-device and the Extreme Management Center domain name was commonname-xmc.	01832176 01823739 01896889
Workflow Signal Activity was not working correctly when triggered from an alarm/trap.	------
Upgrading the firmware on an ExtremeXOS via SCP was taking an excessive amount of time (up to 10 minutes).	01889226 01889760 01882603
Workflows that included the devicesIP variable were not working and activities within the workflow were skipped.	------
ExtremeAnalytics Issues Addressed	**ID**

Attempting to update ExtremeAnalytics fingerprints via the **Analytics** > **Configuration** > **Fingerprints** tab was occasionally failing and a No Files found in directory error displayed.	------
The Top Clients by Interface report was not displaying data after upgrading to Extreme Management Center version 8.3.0.	01868265
The ExtremeAnalytics engine was unresponsive after upgrading to Extreme Management Center version 8.3.0.	01887990
ExtremeAnalytics allows you to disable the Virtual Sensor integration to improve performance.	------
Valid values in the **Target** drop-down list on the Analytics > **Browser** tab were occasionally not available.	------
The AppIdMgrServer was failing to start and displaying a java.lang.NullPointerException error when custom enterprise definitions missing names were defined.	------
ExtremeControl Issues Addressed	**ID**
ExtremeControl IP address resolution for end-eystems on VOSS/BOSS devices was taking an excessive amount of time, resulting in ExtremeControl performance issues.	01887823
Guest & IoT Manager password email notifications may have removed dollar symbols ($) for passwords if the password contained two or more successive dollar symbols ($$). The original password is stored as entered by the user.	01880231
Users provisioned by Guest & IoT Manager using an email-based username were not appropriately matching ExtremeControl authentication and authorization rules that used Username groups as criteria.	01888057
ExtremeConnect Issues Addressed	**ID**
The MGMT and VMKernal MAC addresses were not populating in the ExtremeConnect vCenter module from VMware vCenter.	------

3.4 Known Issues Addressed in 8.3.0.111

Extreme Management Center Issues Addressed	**ID**
With the exception of ExtremeAnalytics 8.2.4.x, the local console port for 8.2.x installed on Extreme Management Center / Access Control engines was inoperable after initial use.	01856232

On the Network > Devices > Device Tree, when a selection other than Sites was chosen from the left-panel menu, the File Transfer Settings tab was missing from the Archives menu. Now, the “File Transfer Settings” tab has been renamed “Inventory Settings” and has been added to the Archives menu.	------
After upgrading to Extreme Management Center version 8.2, the Extreme Management Center server was running slowly and using excessive memory and CPU, or became unresponsive, when Wireless Controllers were in use.	------
The launch point for Fabric Topology was unclear and hard to locate. Now, the Fabric Topology tab has been relocated to the Sites > Maps > More Views tab in the Device tree menu.	------
The “More Views” and “More Actions” selections on the Network > Devices > Device tree were missing.	------
Device Grid reference images and impact analysis for devices running a reference image were incorrect for ERS devices.	------
The Execute Command Script tool was taking a long time to load, and browsers were sometimes timing out. Now, when the Execute Command Script view is launched, the user is informed that the screen is awaiting retrieval of the device information.	01847499
On the Devices > Maps tab, clicking the Add Device button would not add “Ping Only” devices directly to a map.	------
Canceling a map edit sometimes resulted in the map remaining in edit mode.	------
The Inventory Dashboard for references images was not reflecting ERS devices that matched the reference images.	------
On the Tasks > Workflows tab, workflow executions failed when a Shell Script Activity took more than 15 seconds to complete. The timeout has now been increased from 15 seconds to three minutes.	1849857
The Valid Values field for an input with a Display Type of ComboBox in the Manage Inputs window (Tasks > Workflows > Inputs > Manage Inputs) was not allowing special characters.	------
Adding a device to a site with Enable Collection selected on the Site > Actions tab was not collecting port information on the device after the device was discovered.	------

Changing the selection of the left-panel drop-down list on the Network > Devices tab with a large number of devices caused a Could Not Load Report error to display.	------
Fabric Manager was installing two network adapters when only one adapter could be configured during IP deployment. Now, only one adapter is installed.	01819550
Fabric Manager failed to sync with Extreme Management Center if the root password included an ampersand (&) character.	01818533
Validation errors in port collection were causing SNMP timeouts.	01781720
Saving a Service Application that has 10 or more Switched UNI services defined was taking longer than expected to complete.	------
Setting the Fabric Enable value for a port to FABRIC_ATTACH was leading to incorrectly identified configuration mismatches during configuration enforcement.	------
Performing a reload while editing the configuration of a device was not properly refreshing all the CLIP addresses configured on that device.	------
On the Alarms & Events > Alarm Configuration tab, the Save button was being disabled when an interval time other than “Days” was selected.	01825612
The option to change LAG and MLAG Provisioning log settings was not included on the Server Diagnostics tab.	------
Applying an IP address to a VLAN was causing errors during enforcement.	------
VLAN and port details were not displaying for VDX devices in the Network > Devices > Device View.	01825809
VSP Syslog messages were not being mapped to the Device Name in Events if the messages used a different CLIP IP than what was used to add the device to Extreme Management Center.	------
Selecting Register Trap Receiver for a VSP device was not registering the VSP device as a trap receiver.	01842123
VSP and ERS devices were reporting trap registration at 50% and were not completing.	------
Links displayed on maps were attached to the wrong port on a device.	01837871

When the end-system had moved from one engine to another, agent-based device type detection failed to update the end-system Device Type.	01842162
Creating a user-defined port template with a name that starts with the name of a built-in template caused aberrant operation.	01833254
The Firmware Minimum Version on the Administration > Vendor Profiles tab for the X465-24MU-24W device was incorrectly labeled Firmware Maximum Version, which prevented the newest firmware version from being downloaded.	------
The server was not starting if the Device Type, Device Family, or Device Subfamily fields on the Vendor Profiles or New Vendor Profile tabs were not populated with unique values.	1841823 1848426
Opening the Interface History report from the Port Tree on the Network > Devices tab caused an Invalid Target error.	1783878
Installing Extreme Management Center with the user "netsight" was incorrectly setting the file permissions, and caused an exception issue with the trap registration process.	1856419
Novell E-directory Extended LDAP API requests were causing a java.io.IOException.	01410626 01845907 01814218 01868151
The TACACS+ shared secret was too long at eight characters. The minimum shared secret length is now six characters.	------
After restarting the Extreme Management Center server, scheduled archives and firmware upgrades no longer started automatically.	------
Restarting the Extreme Management Center server might not complete successfully. Additionally, attempting to access a site or perform actions to a site might not complete successfully.	------
Creating a scheduled task to upgrade firmware on a device with Restart Devices After Upgrade selected was upgrading the firmware, but not restarting the device.	1336886
Authorized Users who are added to an Authorization Group as a result of Automatic Member functionality were incorrectly able to be edited by other users.	1399058
Devices in the Device list on the Network > Devices tab occasionally indicated they were running the reference image when they were not.	------

The Backup Configuration for VSP devices was including changes in the comments that were not configuration-related (for example, timestamp changes).	01732915
Sorting the values in a column that includes a blank value on the Wireless > Clients > Clients tab was causing the other values in the column to not sort properly.	1749184
After filtering FlexViews by Device Type, FlexViews for other Device Types were still available.	------
Extreme Management Center could not display the contents of an archive from a Fabric Manager device. Attempting to read the archive was causing an exception in the server log.	------
Changing the **Status** column for a device to **Not Polled** was not updating correctly and did not send device updates when polling was restored.	01409445
TCL scripts were using the “error” command, which was not stopping the script.	1405601
Extreme Management Center was not returning search results when searching for user names that consist of numbers.	01802028
Compass Search was not validating MAC Address, IP Address, and Subnet search parameters.	1548747
Using the Compass Search feature with a blank **Address** field were failing.	1521490
Performing a Compass Search was allowing users without device access to view the device in the results.	1376919
Devices discovered with **Use Discovered IP** functionality enabled and configured with a non-default VLAN were incorrectly applying the default VLAN.	01840128
The **Alias** and **Display Name** fields on Port Statistic reports occasionally did not display correctly.	1829952
EXOS .xmod files were not properly selected when firmware was upgraded.	------
Inventory Manager for Extreme Management Center was not supporting all .xmod file formats. Inventory Manager firmware upgrade functionality now supports all .xmod file formats.	------

SNMP Set events were not correctly setting the client and user name in the event log.	------
Inventory Dashboard for reference images now reflects the ERS devices that match the reference image.	------
Adding a device with a **Poll Type** of **Ping Only** was slow to indicate **Status**.	
Passwords were visible for some users with Read-only access and who did not have access rights to view passwords.	------
On the Network > Devices > Configure Device tab, the Frozen Port Status was not displaying appropriately. The Frozen Port Status was also being cleared when Reload Device was selected or if data was configured on the frozen port. It was also possible to set a port with a Frozen Port Status. Improvements include the following:	1831245
The Traps Server Path and Poll Interval fields were not editable.	01855665
Enforcing large Fabric Connect configurations to a device was failing due to timeouts.	------
Creating a Configuration Template for an ERS devices was causing Extreme Management Center to become unresponsive and required a restart of the session.	------
ZTP+ enabled devices on the Discovered panel were resetting the IP to N/A when saving the configuration.	------
The ZTP+ process was creating duplicate operation panel entries.	------
Fabric Manager was not displaying an error message when attempting to process a telnet profile that is not supported by Fabric Manager.	------
The source for VRF or VLAN configuration would occasionally be shown as being inherited from a Site or Service Application, when there was identical configuration locally defined for that device.	------
Issues were occurring with SLX devices:	------
ExtremeAnalytics Issues Addressed	**ID**
An error message on the server log was generated every 15 minutes when Application Telemetry was added to an Extreme Management Center engine.	01823783

Disabling Automatic Syslog Configuration was preventing the script from running on the switches.	1783878
The License tool was not displaying the fpm value rates on per-hour intervals.	01840383 01843395 01832694
Flow-based and end-system-based license charts were not displaying data when the 6-hour, 8-hour, or 12-hour time spans were selected.	------
Generating an application report via the Analytics > Browser tab with a Display Format of Chart over Time was not displaying properly.	------
The End System Applications Summary report (in the Client Address view on the Analytics > Application Flows tab) was failing to open and was displaying browser exceptions.	------
The default Flow Collection Type for an ExtremeAnalytics engine is changed from NetFlow to Both.	------
When running the `dnetconfig` script on the ExtremeAnalytics engine more than once, the default option might not display the selection you made the last time `dnetconfig` was run.	------
ExtremeAnalytics was not indicating when an ExtremeXOS device did not possess sufficient resources to be added as an Application Telemetry source on the Analytics > Configuration > Engines > {Engine Name} > Configuration tab.	01745243
The Site > Endpoint Locations tab now displays 20K locations without significant load-time delay.	------
ExtremeControl Issues Addressed	**ID**
Default profiles that were deleted were not recreated when enabling features in the Captive Portal Configuration that require those profiles to exist.	01849002
In the ExtremeControl engine Captive Portal's Pre-Registration portal, setting the expiration time for a user via the calendar tool was logging the administrator out.	01848122 01849784 01857419 01869761
When upgrading an ExtremeControl engine or an ExtremeAnalytics engine using the Upgrade Firmware feature with the Restart Devices After Upgrade option selected, the engine was not restarted and the upgrade task failed on the restart step.	------

Guest and IoT Management (GIM) Active Directory Sponsor Lookup was not searching using the User Search Root in the LDAP Configuration, and was not comparing the "memberOf" attributes returned to what was configured in the GIM application.	01816454
The FreeRADIUS debug tool was rejecting the management login password for the ExtremeControl engine.	01842653
The ExtremeControl engine was not attempting to use ipNetToPhysicalTable unless the target device it identified was a router. ExtremeControl engines will now use IP-MIB:ipNetToPhysicalTable (RFC4293) for MAC-to-IP address resolution.	------
After upgrades to Extreme Management Center versions 8.2.4 and 8.2.5, end-systems in the Trusted Domain server were not being authenticated by the ExtremeControl engine.	01841156 01842605
ExtremeControl registration emails were failing when the SMTP server did not respond to the Send request.	01855345
The initial System Group Request on the Site > Discover tab was improperly displaying the following default values: `timeout: 3` and `retries: 0`. Using new Site Options, you can control initial SNMP Timeouts and Retries and set them to best match your network configuration.	------
The **Port Info Raw** and **Switch Port** columns in the Control > End-Systems table were displaying inaccurate AP Name and AP Zone information.	01780216
Failed attempts to authenticate to Extreme Management Center were not showing the correct **Client** in the Event Log.	------
The details of a device or end-system on the Overview tab after searching the network were obscured by other details after clicking the arrow icons to view additional information.	01426781
ExtremeControl registration email processing was stopping if the SMTP server failed to respond to email requests.	01855345
Multiple ExtremeControl Policy Mapping entries with the same name (but differing Locations) were repeating the name multiple times in various Policy drop-down lists in the ExtremeControl Profile editor.	01851596
Adding, deleting, or editing supplemental locales now retains the existing message and any custom strings for other locales.	------

Novell E-directory Extended LDAP API requests were causing a java.io.IOException.	01410626 01845907 01814218
The French translation in the GIM Terms of Use was not displaying properly.	1857611
IP Addresses in AccessControl tables were not being ordered correctly after the IP Address column was sorted.	01821535
End-Systems in the End-system table had a value of 0 for assessment scores when assessment was not used.	01821535
The End-system Configuration Evaluation tool was not importing SSID, AP Name, AP MAC, AP Serial, AP Zone/Group, and RADIUS values for wireless devices.	
ExtremeControl now supports up to eight proxy RADIUS servers to be configured per AAA configuration.	01263396
The Name field for a policy Role (Control > Policy > Roles/Services > Roles > Create Role) was incorrectly not allowing special characters.	01848955

3.5 Vulnerabilities Addressed

This section presents the vulnerabilities addressed in Extreme Management Center 8.3:

- The following vulnerabilities were addressed in the Extreme Management Center, ExtremeControl, and Extreme ExtremeAnalytics engine images:
    - CVE-2018-10779, CVE-2018-12900, CVE-2018-17000, CVE-2018-19210, CVE-2019-6128, CVE-2019-7663, CVE-2011-5325, CVE-2014-9645, CVE-2015-9261, CVE-2016-2147, CVE-2016-2148, CVE-2017-15873, CVE-2017-16544, CVE-2018-1000517, CVE-2018-20679, CVE-2019-5747, CVE-2019-8904, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907, CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024, CVE-2019-6133, CVE-2019-3842, CVE-2019-11068, CVE-2019-7303, CVE-2018-20483, CVE-2019-5953
- The following vulnerabilities were addressed in the Extreme Management Center and ExtremeControl engine images:
    - CVE-2018-10915, CVE-2018-10925, CVE-2018-1058

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 Governance tab is available and supported by Extreme on an Extreme Management Centerengine running the Linux operating system supplied by Extreme. Other Linux operating systems can support Governance functionality, but python version 2.7 or higher must be installed. Additionally Governance 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 8.3 supports upgrades from Extreme Management Center version 8.0.x, 8.1.x, or 8.2.x (except version 8.2.2). If you are upgrading

from version 7.1 or earlier of NetSight/Extreme Management Center, you must perform an intermediate upgrade. For example, if you are upgrading from Extreme Management Center 7.0, you must first upgrade to the latest Extreme Management Center 7.1 release, then upgrade to the latest Extreme Management Center 8.0 or 8.1 release, then to 8.3.

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 8.3, ensure the DNS server IP address is correctly configured.
- When upgrading to Extreme Management Center version 8.3, ensure the -Xms and -Xmx settings in the `nsserver.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 nsserver 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.

  NOTE: The `nsserver.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 8.3 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 8.3 requires you to renew your NMS license if generated prior to November 30, 2018. Licenses generated prior to November 30, 2018 expire 90 days after upgrading to Extreme Management Center version 8.3.

4.2.2 Upgrading Hardware

When attempting to upgrade the Extreme Management Center server, the ExtremeAnalytics engine, or the ExtremeControl engine to version 8.3, 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 8.3, 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 Persistance).
- 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

When upgrading to Extreme Management Center 8.3, you are required to upgrade your ExtremeControl engine version to 8.1 or 8.2. Additionally, both Extreme Management Center and the ExtremeControl engine must be at version 8.3 in order to take advantage of the new ExtremeControl8.3 features.

NOTE: ExtremeControl 8.3 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 8.3* 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 8.3 if you upgrade to the ExtremeControlengine8.3. Version 8.3 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 8.3 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 8.3:

No domain specified

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

4.5 Fabric Manager 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 8.3 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 8.3, the Default Gateway IP Address is configured as part of the VLAN. In 8.3, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 8.3, 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.

4.6 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.

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
```

Additionally, the Status of LAG links in maps will start working after the next polling following an upgrade to Extreme Management Center version 8.3.3. 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.

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.

4.7 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

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

5. System Requirements

IMPORTANT: Extreme Management Center version 8.3 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 8.3. Contact Global Technical Assistance Center (GTAC) with any questions.

Wireless event collection is disabled by default in version 8.3 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 8.3.

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 -Xmx	8 GB 12 GB	12 GB 16 GB	24 GB 36 GB	24 GB 36 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)

[1]Browsers 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.

[2]When 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	16
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

[1]The 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
Windows[1]	Windows Vista Windows XP Windows 2008 Windows 2003 Windows 7 Windows 8 Windows 8.1 Windows 10	80 MB	40 MB (80 MB with Service Agent)
Mac OS X	Tiger Snow Leopard Lion Mountain Lion Mavericks Yosemite El Capitan Sierra	10 MB	120 MB

[1]Certain 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 8.3 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

[1]Microsoft® 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

[1]Mobile 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