ExtremeCloud™ IQ - Site Engine Release Notes

04/2022
22.3.10
PN: 9037432-00

Table of Contents

Release Notes for 22.3.10

ExtremeCloud IQ - Site Engine includes all the features and functionality of Extreme Management Center as well as issues that have been resolved and configuration changes for this release.

If you are an existing Extreme Management Center customer, contact your representative to have your Extreme Management Center license migrated to an ExtremeCloud IQ - Site Engine license. The ExtremeCloud IQ - Site Engine license also includes licensing for ExtremeAnalytics.

IMPORTANT:

- For upgrade and installation requirements, as well as configuration considerations, see ExtremeCloud IQ - Site Engine Configuration and Requirements.
- ExtremeCloud IQ - Site Engine version 22.3.10 consumes licenses from ExtremeCloud IQ in a connected deployment mode or from a license file in air gap deployment mode. ExtremeCloud IQ - Site Engine is a subscription-based -only licensing model. Existing NMS licenses do not provide access to ExtremeCloud IQ - Site Engine. You can view the status of your license by accessing Administration > Licenses after the installation is complete.
- ExtremeCloud IQ - Site Engine is not compatible with ExtremeCloud IQ Connect level account. Either the Evaluation or Pilot level is mandatory.
- In Connected mode, ports statistics are shared with ExtremeCloud IQ only for ports that are enabled to Collect Port Statistics.
- Onboarding ExtremeCloud IQ - Site Engine devices using an ExtremeCloud IQ HIQ account is not supported. You must use a VIQ Account to onboard ExtremeCloud IQ - Site Engine devices.

For the most recent version of these release notes, see ExtremeCloud IQ - Site Engine Release Notes.

For information regarding the features supported by specific devices, see the Firmware Support Matrix. Version 22.3.10 of ExtremeCloud IQ - Site Engine supports the devices listed in the matrix.

Devices that do not have serial numbers or MAC addresses in Extreme Management Center must be rediscovered after you upgrade to ExtremeCloud IQ - Site Engine before they can be onboarded to ExtremeCloud IQ.

Connected mode only - If your number of devices exceeds your licenses available, ExtremeCloud IQ - Site Engine transitions to a license violation state and your access to ExtremeCloud IQ - Site Engine is locked. To resolve the license shortage you need to access the Extreme Networks portal or ExtremeCloud IQ to evaluate the quantities of available Pilot and Navigator licenses versus the number of licenses required by ExtremeCloud IQ - Site Engine.

Licensing Changes

Beginning with ExtremeCloud IQ - Site Engine version 21.04.10, your ExtremeAnalytics license is included as part of your ExtremeCloud IQ Pilot license. Separate licenses are no longer required.

For users upgrading from Extreme Management Center to ExtremeCloud IQ - Site Engine, note that the XIQ-NAC subscription must be used instead of IA-ES- license. For new users that complete an initial install of ExtremeCloud IQ - Site Engine, ExtremeControl licensing does not include end-system capabilities.

Onboarding ExtremeCloud IQ - Site Engine from ExtremeCloud IQ in Connected Deployment Mode

After installing or upgrading to ExtremeCloud IQ - Site Engine, you need to onboard ExtremeCloud IQ - Site Engine to ExtremeCloud IQ. When the onboarding is complete, you can then access ExtremeCloud IQ - Site Engine.

Entering your ExtremeCloud IQ name and password are required during the first-time login to ExtremeCloud IQ - Site Engine.

NOTE: If Extreme Management Center is onboarded to ExtremeCloud IQ, when you upgrade to ExtremeCloud IQ - Site Engine, you need to remove Extreme Management Center from ExtremeCloud IQ before onboarding ExtremeCloud IQ - Site Engine.

Enhancements

The following enhancements were made to ExtremeCloud IQ - Site Engine in this release. For additional information about each of the enhancements listed in the release notes, refer to the documentation posted online at ExtremeCloud IQ - Site Engine Documentation or the Help system included with the software.

ExtremeManagement

Enhancement to the Welcome window
A link to the database backup restore procedure has been added.

New critical severity alarm
This alarm is added by default to the Alarm Configuration to detect the device license expiration.

API enhancement
The ability to add and remove entries from the location group has been added to the API.

New CLI import command
Modules located in `appdata/scripting/extensions` can import `emc_results` by using the command **`import emc_results from xmcbase`**.

Support of Universal Series Platform 5320
This support has been added to Fabric Engine and Switch Engine.

New Network Operating Systems (Network OS)
Added support for Fabric Engine and Switch Engine. Areas impacted by this change are:

- Options tab (Administration > Options)
- System scripts
- Compliance tests
- FlexView categories VOSS and XOS
- System workflows

ExtremeControl

Add Device to the Access Control Engine Group
For switches running VOSS or Fabric Engine, when "Run Site's Add Actions" is executed (manually or through ZTP+) the correct "RADIUS Attributes to Send" will be assigned automatically based on Add Device to Policy Domain setting.

The correct "RADIUS Attributes to Send" will not be assigned for devices added to the database before version 22.3.10

New NBI calls added
The new NBIs are for the manipulation of the LDAP/RADIUS user groups and LDAP Host group.

```
addUserGroupEntryToGroup
removeUserGroupEntryFromGroup
```

ExtremeAnalytics, ExtremeControl, ExtremeManagement, and FabricManager

Automatic log out from the console for STIG compliance
After 15 minutes of inactivity, the console will automatically log out.

Automatic log out from SSH for STIG compliance
After 10 minutes of inactivity, SSH will automatically log out.

Weak ciphers in the SSHd configuration disabled
Only the strong ciphers are now available for SSH access to the appliance.

Customer Found Defects, Known Issues, and Vulnerabilities Addressed

Customer Found Defects Addressed in 22.3.10

ExtremeAnalytics CFDs Addressed	ID
Loading speed of the Application dashboards has been improved.	2217570
Insights dashboard not displaying analytical data.	2263077
Addressed the Analytics issue for reports not displaying all applications in the graphs.	2431000
Added the ability to set the Maximum Transmission Unit (MTU) size from the management interface.	2454882
Alerts are now more descriptive and contain the time the alert occurred. Chart X-axis now displays the time.	2487802

ExtremeControl CFDs Addressed	ID
During the captive portal registration process, the error page showed the incorrect MAC Address and could not proceed with the registration.	1837039 1973048
In the Events table, if an `and/or` filter was done and left active, it could hinder the display of the access control group editor and possibly other areas. The performance has been enhanced in this area so that it does not cause the display issue.	2405659
If you have multiple policy mapping names and rename one of them, then ExtremeControl will update all of the NAC profiles which causes confusion. A confirmation dialog now appears when editing or saving a policy mapping name to a new name.	2418338
Addressed the issue of ExtremeControl using the incorrect LDAP configuration when the LDAP was specifically selected from the AAA Join AD Domain list.	2430733
If ExtremeCloud IQ - Site Engine manages the ExtremeControl SNMP, it caused the `nacconfig` script summary to display the incorrect SNMP configuration.	2435541
A backslash (\) is no longer allowed in the SNMP credentials because it caused files to be written incorrectly.	2455425
The **Authorization** column size is increased so the RADIUS attributes are not truncated anymore in **End-System Events** table.	2464361
The **Move** button has been added to the **End-System Group** editor. One or more entries can now be moved to a different end-system groups.	2474882
If the username and MAC address are the same, ExtremeControl detected the authentication type incorrectly for 802.1X TLS in the **End-Systems** table.	2484541
The ExtremeControl rule list was getting out of order when grouped by label.	2560207

ExtremeManagement CFDs Addressed	ID
Configure Device now reloads more than one device at a time.	2291146
Notification queued email actions stopped getting processed when previous email connections fail to close. A new monitor was added to close connections on timeout.	2373900 2409779 2415656 2418164 2562926
ExtremeCloud IQ - Site Engine LLDP map links are no longer disappearing between 200 series and EXOS after being drawn following the initial recovery.	2455054

ExtremeManagement CFDs Addressed	ID
ExtremeManagement no longer generates alerts or alarms if the certificate in the internal communication Truststore chain has expired. Other Keystore or Truststore checks will continue to run and generate alarms as before.	2463716
The `nsdevicedata` table was getting corrupted when attempting to create a device without any available licenses. Northbound Interface (NBI) is now displaying an error when attempting to create a device without a license.	2464583
The maximum accepted value for the controller wireless statistics (TotalBwKbps) has been increased to allow the reporting of high bandwidth throughput.	2465351
Added additional error checks in the firmware upgrade scripts for the Ethernet Routing Switches (ERS) products.	2472141
Addressed the issue where the capability to configure Multi (Chassis) Link Aggregation Group (MLAG) with Link Aggregation Control Protocol (LACP) on devices running Fabric Engine and VOSS where not working.	2473891
Addressed the issue when sysName, sysContact, and sysLocation did not update properly when changed on the switch via CLI.	2484783
Addressed the issue when ExtremeManagement failed to backup the configuration file from VSP when VSP uses the VOSS sys priv-exec-password. The command has been added to the script engine.	2484872
Used values in Port Capacity FlexReport were not being set correctly for ports that have started collection within the last month.	2485737
Non-automatic users who were also not authorized via RADIUS were allowed to log into ExtremeCloud IQ - Site Engine. The new system property `extreme.admin.user.attributes.check=true` can be now added in `NSJBoss.properties` so that a non-automatic user is not allowed to login to ExtremeCloud IQ - Site Engine unless the automatic membership matching criteria is provided and properly configured. The user will now see a message that explains the behavior if they complete the deletion.	2490075
During the onboarding of ExtremeCloud IQ - Site Engine to ExtremeCloud IQ it was not clear to the user that the Proxy Server had to be a valid IP address or Fully Qualified Domain Name (FQDN). Invalid formats made the onboarding fail. To address this issue, a tooltip has been added for clarification.	2493263
Authentication in Policy could not be configured with Access OneView Administration being disabled.	2495594
When the NBI got a list of workflows that used "starts with" for string matching, the wrong workflow was being added because it was using the first workflow in the list. NBI mutation for custom actions now matches the exact name of the workflow.	2497349
The support Map image formats are PNG, GIF, and JPG (without transparency).	2498218
Status Poller was not detecting the boot prom version changes in sysDescription for ERS 5952 series.	2507622

Policy CFDs Addressed	ID
On the End Systems tab, End System Events tab, and Policy Mappings Preview, some RADIUS attributes that usually display in the Authorization column were missing. This caused users to be concerned that the NAC Engine was not working properly. There was not an issue with the NAC Engine. So, this fix addressed the NAC misconception by always displaying the Policy Mapping names.	2456485
The Site Engine was using port 80 instead of 443 by default for REST calls when the WebView URL was configured for HTTPS without a specific port. If the WebView URL is configured for HTTP, the Site Engine now uses port 80. Otherwise, port 443 is used.	2471556
Saving a policy domain with other policy domains open in a different browser tab sometimes resulted in all devices being removed from the domain.	2482785
The Site Engine was not configuring the Netlogin number of allowed users for Link Aggregation (LAG) Master ports on ExtremeXOS devices even though the configuration was supported.	2486028

Known Issues Addressed in 22.3.10

ExtremeAnalytics Issues Addressed
Addressed the issue when adding a device to Analytics Engine failed with error message : `Failed to add device to home engine null: Unable to get configure sflow sources even if the home engine was defined.`
Updated Vendor Profiles to reflect the official name of Application Analytics Traffic Sensor
The selectors in Analytics > Application Flows are now persistent and will survive if the user navigates to other menus and returns back.
Addressed the installation issue of Traffic Sensor from the ISO image when Traffic Sensor failed to start.

ExtremeControl Issues Addressed
Show Advancedin Edit/Add Policy Mapping did not display all the properties.
Access Control supports RADIUS configuration and Reauthentication (CoA) for the 5420, 5520, and 5320 devices running ExtremeXOS/Switch Engine or VOSS/Fabric Engine operating systems.
There are improvements to Policy Mapping: • The screen loading speed has been improved when adding a new policy. • Sorting is no longer case-sensitive (aA - zZ). • Map to Location in Create Policy Mapping has been enhanced to allow the user to type letters.
New buttons have been added to Edit User Group: Zone group: • Select All Groups • Deselect All Groups

ExtremeManagement Issues Addressed

Fixed NBI Mutation call to create network device with `pollType MONITOR_SNMP`.
Legacy Java clients were deprecated inExtremeCloud IQ - Site Engine. Removed Legacy Clients from Administration > Options.
Addressed an issue when the replacement devices were not processed based on the site mapping during the ZTP+ and followed the /World site.
Sorting of Start Date and End Date columns are now working properly on the Licenses tab (Administration > Licenses.).
Fixed the Enforce Preview issue where the current settings of both edited devices were merged with the desired settings. The correct behavior is only the selected device's settings are merged.
Vendor profile now supports Cisco 2900S-Stack.
The AutoSense Port Template can now be used with the VSP-4900 version 8.3 and newer.
The Serial Number(Locking ID)has been added to the Licenses screen (Administration > Licenses).
The license file drag and drop capability can now only be done from the Licenses tab (Administration > Licenses).
Removed duplicate information from the License Diagnostics report in the Diagnostics tab (Administration > Diagnostics > System > License Diagnostics).
All three licenses types (Pilot, Navigator, and NAC) will now appear in the Licenses tab (Administration > Licenses) even when the license quantity is zero.
Product family *Unified Switching EXOS* was renamed to *Universal Platform EXOS*. Product family *Unified Switching VOSS* was renamed to *Universal Platform VOSS*. If you use custom workflows or custom scripts, update the product names accordingly.
Fixed the CVE-2021-4034 vulnerability by removing the -s bit in the polkit.
Fixed the issue when Authentication property inside the Port Template could not be configured once opened is Subsite.
For ZTP+ for VOSS devices when the DVR Domain ID was not specified, then error `java.lang.NullPointerException` was reported.
Fixed issue when Authentication property inside the Port Template was not configurable.
In connected mode only, implemented cache in case of temporary ExtremeCloud IQ connectivity outage. Messages for ExtremeCloud IQ are cached into the database for the period of connectivity outage. Once the connectivity is restored, the information in ExtremeCloud IQ is updated.

Management Server Issues Addressed

The L2 VSN area under Network > Devices > Service Definitions has been enlarged.

Policy Issues Addressed

The Policy Service ID tooltip now includes I-SID and NSI.
Bilateral rules in the Policy definitions are now supported in Per User ACLs for VOSS platforms.

Wireless Issues Addressed

The integration of ExtremeCloud IQ - Site Engine and legacy ExtremeWireless Controller (EWC) versions 10.01, 10.11, and 10.21 have been removed.

When IPv6 DHCP Relay addresses are configured on a VOSS/Fabric Engine device, errors occur in `server.log` and causes unknown port states. This configuration is no longer supported.
"Unable to lookup short form for AP of serial number" log message (server.log) is no longer produced when the AP does not have a channel selected.

Vulnerabilities Addressed

This section presents the vulnerabilities addressed in 22.3.10

ExtremeCloud IQ - Site Engine

CVE-2017-12424,CVE-2018-7169,CVE-2021-3155,CVE-2021-3640,CVE-2021-3752,CVE-2021-3973,CVE-2021-3974,CVE-2021-3984,CVE-2021-4019,CVE-2021-4034,CVE-2021-4069,CVE-2021-4083,CVE-2021-4120,CVE-2021-4155,CVE-2021-4202,CVE-2021-20322,CVE-2021-22600,CVE-2021-28711,CVE-2021-28712,CVE-2021-28713,CVE-2021-28714,CVE-2021-28715,CVE-2021-39685,CVE-2021-42739,CVE-2021-43975,CVE-2021-44730,CVE-2021-44731,CVE-2021-45960,CVE-2021-46143,CVE-2022-0185,CVE-2022-0330,CVE-2022-21245,CVE-2022-21249,CVE-2022-21253,CVE-2022-21254,CVE-2022-21256,CVE-2022-21264,CVE-2022-21265,CVE-2022-21270,CVE-2022-21301,CVE-2022-21302,CVE-2022-21303,CVE-2022-21304,CVE-2022-21339,CVE-2022-21342,CVE-2022-21344,CVE-2022-21348,CVE-2022-21351,CVE-2022-21358,CVE-2022-21362,CVE-2022-21367,CVE-2022-21368,CVE-2022-21370,CVE-2022-21372,CVE-2022-21374,CVE-2022-21378,CVE-2022-21379,CVE-2022-22822,CVE-2022-22823,CVE-2022-22824,CVE-2022-22825,CVE-2022-22826,CVE-2022-22827,CVE-2022-22942,CVE-2022-23852,CVE-2022-23990,CVE-2022-25235,CVE-2022-25236

ExtremeAnalytics images:

CVE-2017-12424,CVE-2018-7169,CVE-2021-3155,CVE-2021-3640,CVE-2021-3752,CVE-2021-3973,CVE-2021-3974,CVE-2021-3984,CVE-2021-4019,CVE-2021-4034,CVE-2021-4069,CVE-2021-4083,CVE-2021-4120,CVE-2021-4155,CVE-2021-4202,CVE-2021-20322,CVE-2021-22600,CVE-2021-28711,CVE-2021-28712,CVE-2021-28713,CVE-2021-28714,CVE-2021-28715,CVE-2021-39685,CVE-2021-42739,CVE-2021-43975,CVE-2021-44730,CVE-2021-44731,CVE-2021-45960,CVE-2021-46143,CVE-2022-0185,CVE-2022-0330,CVE-2022-21249,CVE-2022-21256,CVE-2022-21264,CVE-2022-21265,CVE-2022-21301,CVE-2022-21302,CVE-2022-21303,CVE-2022-21304,CVE-2022-21339,CVE-2022-21344,CVE-2022-21351,CVE-2022-21362,CVE-2022-21367,CVE-2022-21368,CVE-2022-21370,CVE-2022-21374,CVE-2022-21379,CVE-2022-22822,CVE-2022-22823,CVE-2022-22824,CVE-2022-22825,CVE-2022-22826,CVE-2022-22827,CVE-2022-22942,CVE-2022-23852,CVE-2022-23990,CVE-2022-25235,CVE-2022-25236

ExtremeControl images:

CVE-2017-12424,CVE-2018-7169,CVE-2021-3155,CVE-2021-3640,CVE-2021-3752,CVE-2021-3973,CVE-2021-3974,CVE-2021-3984,CVE-2021-4019,CVE-2021-4034,CVE-2021-4069,CVE-2021-4083,CVE-2021-4120,CVE-2021-4155,CVE-2021-4202,CVE-2021-20322,CVE-2021-22600,CVE-2021-28711,CVE-2021-28712,CVE-2021-28713,CVE-2021-28714,CVE-2021-28715,CVE-2021-39685,CVE-2021-41816,CVE-2021-41817,CVE-2021-41819,CVE-2021-42739,CVE-2021-43975,CVE-2021-44224,CVE-2021-44730,CVE-2021-44731,CVE-2021-44790,CVE-2021-

45960,CVE-2021-46143,CVE-2022-0185,CVE-2022-0330,CVE-2022-21249,CVE-2022-21256,CVE-2022-21264,CVE-2022-21265,CVE-2022-21301,CVE-2022-21302,CVE-2022-21303,CVE-2022-21304,CVE-2022-21339,CVE-2022-21344,CVE-2022-21351,CVE-2022-21362,CVE-2022-21367,CVE-2022-21368,CVE-2022-21370,CVE-2022-21374,CVE-2022-21379,CVE-2022-22822,CVE-2022-22823,CVE-2022-22824,CVE-2022-22825,CVE-2022-22826,CVE-2022-22827,CVE-2022-22942,CVE-2022-23852,CVE-2022-23990,CVE-2022-25235,CVE-2022-25236

Application Analytics Traffic Sensor images:

CVE-2017-12424,CVE-2018-7169,CVE-2021-3155,CVE-2021-3640,CVE-2021-3752,CVE-2021-3973,CVE-2021-3974,CVE-2021-3984,CVE-2021-4019,CVE-2021-4034,CVE-2021-4069,CVE-2021-4083,CVE-2021-4120,CVE-2021-4155,CVE-2021-4202,CVE-2021-20322,CVE-2021-22600,CVE-2021-28711,CVE-2021-28712,CVE-2021-28713,CVE-2021-28714,CVE-2021-28715,CVE-2021-39685,CVE-2021-42739,CVE-2021-43975,CVE-2021-44730,CVE-2021-44731,CVE-2021-45960,CVE-2021-46143,CVE-2022-0185,CVE-2022-0330,CVE-2022-21249,CVE-2022-21256,CVE-2022-21264,CVE-2022-21265,CVE-2022-21301,CVE-2022-21302,CVE-2022-21303,CVE-2022-21304,CVE-2022-21339,CVE-2022-21344,CVE-2022-21351,CVE-2022-21362,CVE-2022-21367,CVE-2022-21368,CVE-2022-21370,CVE-2022-21374,CVE-2022-21379,CVE-2022-22822,CVE-2022-22823,CVE-2022-22824,CVE-2022-22825,CVE-2022-22826,CVE-2022-22827,CVE-2022-22942,CVE-2022-23852,CVE-2022-23990,CVE-2022-25235,CVE-2022-25236

Guest and IoT Manager

CVE-1999-0524,CVE-1999-0632,CVE-2004-0230,CVE-2019-0199,CVE-2019-10072,CVE-2019-12418,CVE-2019-17563,CVE-2019-17569,CVE-2020-1935,CVE-2020-1938,CVE-2020-9484,CVE-2020-11996,CVE-2020-13934,CVE-2020-13935,CVE-2020-13943,CVE-2020-17527,CVE-2021-24122,CVE-2021-25329,CVE-2021-30640,CVE-2021-33037

Fabric Manager images:

CVE-2022-0330,CVE-2021-4083,CVE-2021-4104,CVE-2021-4155,CVE-2021-4202,CVE-2020-14145,CVE-2020-15778,CVE-2021-22600,CVE-2021-22959,CVE-2021-28711,CVE-2021-28712,CVE-2021-28713,CVE-2021-28714,CVE-2021-28715,CVE-2021-39685,CVE-2021-45960,CVE-2021-46143,CVE-2022-21248,CVE-2022-21271,CVE-2022-21277,CVE-2022-21282,CVE-2022-21283,CVE-2022-21291,CVE-2022-21293,CVE-2022-21294,CVE-2022-21296,CVE-2022-21299,CVE-2022-21305,CVE-2022-21340,CVE-2022-21341,CVE-2022-21349,CVE-2022-21360,CVE-2022-21365,CVE-2022-21366,CVE-2022-22822,CVE-2022-22823,CVE-2022-22824,CVE-2022-22825,CVE-2022-22826,CVE-2022-22827,CVE-2022-22942,CVE-2022-23852,CVE-2022-23990,CVE-2022-25235,CVE-2022-25236

Installation, Upgrade, and Configuration Changes

Installation Information

There are two supported scenarios for onboarding ExtremeCloud IQ - Site Engine to ExtremeCloud IQ:

- After upgrading to ExtremeCloud IQ - Site Engine from Extreme Management Center version 8.4.4, 8.5.5, or 8.5.6.
- After Initial Installation of ExtremeCloud IQ - Site Engine.

There are three tiers of licenses for ExtremeCloud IQ - Site Engine and devices:

- Pilot
- Navigator
- No License

As you begin to onboard ExtremeCloud IQ - Site Engine and your devices, ExtremeCloud IQ will determine if you meet or exceed the license limits for each license type.

For complete installation instructions, refer to the Documentation web page: ExtremeCloud IQ - Site Engine Suite Installation.

IMPORTANT: The Compliance tab is available and supported by Extreme on an 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.

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)
```

Custom FlexViews

When reinstalling ExtremeCloud IQ - Site Engine 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 ExtremeCloud IQ - Site Engine server, save them in the `appdata\VendorProfiles\Stage\MyVendorProfile\FlexViews\My FlexViews` folder.

Custom MIBs and Images

If you are deploying MIBs via the ExtremeCloud IQ - Site Engine server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\MIBs\` folder.

If you are deploying device images (pictures) via the ExtremeCloud IQ - Site Engine server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\Images\` folder.

Important Upgrade Information

ExtremeCloud IQ - Site Engine version 22.3.10 supports two different upgrade strategies.

- Air Gap mode supports upgrades from Extreme Management Center versions 8.4.4, 8.5.7 or ExtremeCloud IQ - Site Engine 21.11.
- Connected mode supports upgrades from ExtremeCloud IQ - Site Engine versions 21.04.10, 21.09.10, 21.11.10 or Extreme Management Center versions 8.4.4 or 8.5.7.

NOTE: Changing deployment modes from connected to air gap or air gap to connected is not currently supported.

The following table details which upgrades are needed for each NetSight, Extreme Management Center or ExtremeCloud IQ - Site Engine version prior to upgrading to ExtremeCloud IQ - Site Engine version 22.3.10.

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 22.3 (connected)	Upgrade to ExtremeCloud IQ - Site Engine version 22.3 (air gap)
	8.1.7	8.3.3	8.4.4	8.5.7		
ExtremeCloud IQ - Site Engine 21.11 (air gap)						X

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 22.3 (connected)	Upgrade to ExtremeCloud IQ - Site Engine version 22.3 (air gap)
	8.1.7	8.3.3	8.4.4	8.5.7		
ExtremeCloud IQ - Site Engine 21.11 (connected)					X	
ExtremeCloud IQ - Site Engine version 21.04 and version 21.09					X	
Extreme Management Center version 8.5.5, 8.5.6 , or 8.5.7					X	X
Extreme Management Center version 8.5.0-8.5.4				X*	X	X
Extreme Management Center version 8.4.4					X	X
*Extreme Management Center version 8.4.0-8.4.3			X*	X*	X	X
*Extreme Management Center version 8.2.x or 8.3.x			X*	X*	X	X

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 22.3 (connected)	Upgrade to ExtremeCloud IQ - Site Engine version 22.3 (air gap)
	8.1.7	8.3.3	8.4.4	8.5.7		
Extreme Management Center version 8.0.x or 8.1.x		X		X	X	X
NetSight version 7.1 or older	X	X		X	X	X

*These versions can be updated to either version 8.4.4, 8.5.5, 8.5.6, or 8.5.7 and then to ExtremeCloud IQ - Site Engine version 22.3.10.

IMPORTANT: When performing an upgrade, be sure to backup the Extreme Management Center 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 22.3.10, ensure the DNS server IP address is correctly configured.

During the installation (if upgrading using the user interface installer), you have the option to backup additional user files by selecting a checkbox on the Previous Installation Detected screen. This option lets you backup user files such as Inventory Manager archive files not automatically backed up during the install because the backup could take several minutes.

Important Upgrade Considerations

- If your network is using ExtremeAnalytics or ExtremeControl engines, Fabric Manager, or another add-on feature, you must first perform the ExtremeCloud IQ - Site Engine upgrade to version 22.3.10 and then add the feature.
- The 4.xx version of the NAC Request Tool is not compatible with the 22.3.10 ExtremeCloud IQ - Site Engine server. If you are using the NAC Request Tool you need to upgrade the version of NAC Request Tool to version 22.3.10.
- To upgrade Traffic Sensor from version 21.x, a fresh installation is recommended. If the fresh installation cannot be used, then please check Knowledge Base for a special procedure.

Upgrading ExtremeControl Engine to Version 22.3.10

General Upgrade Information

You are not required to upgrade your ExtremeControl engine version to 22.3.10 when upgrading to ExtremeCloud IQ - Site Engine version 22.3.10. However, both ExtremeCloud IQ - Site Engine and ExtremeControl engine must be at version 22.3.10 in order to take advantage of the new ExtremeControl version 22.3.10 features. ExtremeCloud IQ - Site Engine version 22.3.10 supports managing ExtremeControl engine versions 8.4, 8.5, 21.4, 21.9, 21.11, and 22.3.10.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, you should also upgrade your assessment agent adapter to version 22.3.10 if you upgrade to ExtremeControl version 22.3.10.

You can download the latest ExtremeControl engine version at the Extreme Portal.

Agent Version for NAC Agent-Based Assessment

If you are using onboard agent-based assessment, be aware that the agent version is upgraded during the ExtremeControl engine software upgrade. If you would like end-systems to update their agent to the new version, you must configure your assessment test set to test for the new agent version. Refer to the Upgrade Information section in the ExtremeCloud IQ - Site Engine Release Notes or the agent version included in the ExtremeControl engine software.

Upgrading to Policy Manager 22.3.10

- Policy Manager 22.3.10 only supports ExtremeWireless Controller version 8.01.03 and higher. If you upgrade to ExtremeCloud IQ - Site Engine 22.3.10 prior to upgrading your controllers, then Policy Manager does not allow you to open a domain where the controllers already exist or add them to a domain. A dialog is displayed indicating your controllers do not meet minimum version requirements and that they must be upgraded before they can be in a domain.
- Following an upgrade to Wireless Controller version 8.31 and higher, a Policy Manager enforce fails if it includes changes to the default access control or any rules that are set to contain. To allow Policy Manager to modify the default access control or set rules to contain, you must disable the **"Allow" action in policy rules contains to the VLAN assigned by the role** checkbox accessed from the Wireless Controller's web interface on the Roles > **Policy Rules** tab. This will allow the enforce operation to succeed.

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 ExtremeCloud IQ - Site Engine server, ExtremeAnalytics engine, or ExtremeControl engine to version 22.3.10, ensure the DNS server IP address is correctly configured.
- When upgrading to ExtremeCloud IQ - Site Engine version 22.3.10, if you adjusted the ExtremeCloud IQ - Site Engine 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/nsserver.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 ExtremeCloud IQ - Site Engine upgrade to version 22.3.10 and then add the feature.

License Renewal

Upgrading to ExtremeCloud IQ - Site Engine version 22.3.10 requires you to transition from perpetual to subscription-based license model. Existing NMS licenses do not provide access to ExtremeCloud IQ - Site Engine. If your perpetual licenses were not transitioned to subscription-based licenses, contact your Extreme Networks Representative for assistance.

Free Space Consideration

When upgrading to ExtremeCloud IQ - Site Engine version 22.3.10, a minimum of 15 GB of free disk space is required on the ExtremeCloud IQ - Site Engineserver

To increase the amount of free disk space on the ExtremeCloud IQ - Site Engine server, perform the following:

- Decrease the number of ExtremeCloud IQ - Site Engine 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.

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.

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/Switch Engine 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.

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

Other Upgrade Information

Immediately after you install version 22.3.10 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 22.3.10:

No domain specified

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

Fabric Configuration Information

Certificate

Fabric Manager might be unavailable via ExtremeCloud IQ - Site Engine after upgrading if the certificate is missing in ExtremeCloud IQ - Site Engine Trust store.

To ensure Fabric Manager is available, enter the Fabric Manager certificate in the ExtremeCloud IQ - Site Engine Trust store using **Generate Certificate** option.

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.

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.

CLIP Addresses

Using the CLIP Addresses table in the Configure Device window, you can enter addresses in both IPv4 and IPv6 formats. However, ExtremeCloud IQ - Site Engine version 22.3.10 only supports applying a single address (either IPv4 or IPv6) to a Loopback Interface.

Gateway Address Configuration Change

In versions of ExtremeCloud IQ - Site Engine prior to 22.3.10, the Default Gateway IP Address is configured as part of the VLAN. In 22.3.10, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 22.3.10, merge any **Default Gateway IP Addresses** from the device into the configuration of ExtremeCloud IQ - Site Engine to prevent incorrect configuration of the device.

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.

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.

Password Configuration

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

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

VRF Configuration

VOSS/Fabric Engine SNMP performance is adversely affected as the number of VRF configurations increases. This issue can be resolved by upgrading toVOSS/Fabric Engine release 8.1.1 or later or VSP-8600 series version 6.3.3 or later.

Device Configuration Information

VDX Device Configuration

To properly discover interfaces and links for VDX devices in ExtremeCloud IQ - Site Engine, enable `three-tuple-if` on the device.

NOTE: To enable `three-tuple-if` on the device in ExtremeCloud IQ - Site Engine:

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 ExtremeCloud IQ - Site Engine to display VCS fabric , the NOS version must be 7.2.0a or later.

Rediscover VDX devices after upgrading to ExtremeCloud IQ - Site Engine version 8.4.2.

VOSS/Fabric Engine Device Configuration

Topology links from VOSS/Fabric Engine devices to other VOSS/Fabric Engine or ERS devices might not display in a topology map (or might display inconsistently). To ensure topology map links display correctly, verify that the VOSS/Fabric Engine 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 VOSS/Fabric Engine 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 ExtremeCloud IQ - Site Engine version 8.4. You can initiate the polling of a device by performing a refresh/rediscovery of the device.

ERS Device Configuration

ERS devices might automatically change VLAN configurations you define in ExtremeCloud IQ - Site Engine. To disable this, change the `vlan configcontrol` setting for ERS devices you add to ExtremeCloud IQ - Site Engine 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, ExtremeCloud IQ - Site Engine 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.

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. ExtremeCloud IQ - Site Engine 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 ExtremeCloud IQ - Site Engine, select a **Device Profile** that uses the correct CLI credentials for the SLX device in the **Administration Profile**.

ExtremeXOS Device Configuration

ExtremeXOS/Switch Engine 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 ExtremeCloud IQ - Site Engine, 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.

Firmware Upgrade Configuration Information

ExtremeCloud IQ - Site Engine 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, ExtremeCloud IQ - Site Engine 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 ExtremeCloud IQ - Site Engine 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@<ExtremeCloud IQ - Site Engine_SERVER_IP>:/root/firmware/images`
- Where:
  - *<ExtremeCloud IQ - Site Engine_SERVER_IP>*= IP Address to ExtremeCloud IQ - Site Engine Server
  - *<LOCAL_FIRMWARE_PATH>*= fully qualified path to a firmware image on the client machine

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.

System Requirements

IMPORTANT: Wireless event collection is disabled by default in version 22.3.10 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 ExtremeCloud IQ - Site Engine version 22.3.10.

ExtremeCloud IQ - Site Engine Server and Client OS Requirements

ExtremeCloud IQ - Site Engine Server Requirements

Manufacturer	Operating System
Linux	Red Hat Enterprise Linux WS and ES v6 and v7 Ubuntu 18.04
VMware® (ExtremeCloud IQ - Site Engine Virtual Engine)	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server VMware ESXi™ 6.7 server VMware ESXi™ 7.0 server vSphere (client only)™
Microsoft® Hyper-V (ExtremeCloud IQ - Site Engine Virtual Engine)	Windows® Server 2012 R2 Windows® Server 2016

These are the operating system requirements for the ExtremeCloud IQ - Site Engine server.

ExtremeCloud IQ - Site Engine Client Requirements

These are the operating system requirements for remote ExtremeCloud IQ - Site Engine 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

ExtremeCloud IQ - Site Engine Server and Client Hardware Requirements

These are the hardware requirements for the ExtremeCloud IQ - Site Engine server and ExtremeCloud IQ - Site Engine client machines.

NOTES: ExtremeControl and ExtremeAnalytics are not supported on Small ExtremeCloud IQ - Site Engine servers.

ExtremeCloud IQ - Site Engine Server Requirements

	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

	Small	Medium	Enterprise	Large Enterprise
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.

ExtremeCloud IQ - Site Engine Client Requirements

	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 ExtremeCloud IQ - Site Engine properly (for example, missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.

[2]When accessing ExtremeCloud IQ - Site Engine 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.

Virtual Engine Requirements

The ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics virtual engines must be deployed on a VMWare or Hyper-V server with a disk format of VHDX.

- The VMWare ExtremeCloud IQ - Site Engine virtual engines are packaged in the .OVA file format (defined by VMware).
- The Hyper-V ExtremeCloud IQ - Site Engine 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.

ExtremeCloud IQ - Site Engine Virtual Engine Requirements

Specifications	Small	Medium	Enterprise
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
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.

ExtremeControl Virtual Engine Requirements

Specifications	Small	Medium	Enterprise	Large Enterprise
Total CPU Cores	8	16	16	20
Memory	12 GB	16 GB	32 GB	48 GB
Disk Size	40 GB	120 GB	120 GB	120 GB
IOPS	200	200	200	200
Recommended scale based on server configuration:				
ExtremeControl End-Systems	3,000	6,000	9,000/12,000[1]	12,000/24,000[2]
Authentication	Yes	Yes	Yes	Yes
Captive Portal	No	Yes	Yes/No[1]	Yes/No[2]
Assessment	No	Yes	No	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.

[2] The Large Enterprise ExtremeControlengine configuration supports two different scale options:

- Up to 12,000 end-systems if your network uses Captive Portal functionality.
- Up to 24,000 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.

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

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

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	Catalina 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. The ExtremeControl Agent running on MAC Operating Systems requires Java Runtime Environment (JRE) support. Some features of various products might not be supported. For additional information on specific issues, see Known Issues and Limitations.

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

Medium	Browser	Version
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

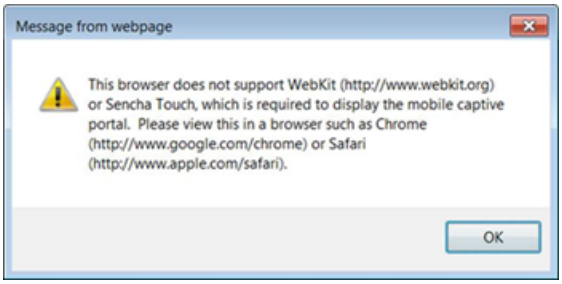
NOTES: A native browser indicates the default, system-installed browser. Although this might be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection for a device. Typically, this is a non-configurable option for Wi-Fi Captive Network 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:



ExtremeControl Engine Version Requirements

For complete information on ExtremeControl engine version requirements, see the Release Notes for 22.3.10 section of these Release Notes.

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.

ExtremeControl SMS Gateway Requirements

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

- Clickatell
- Mobile Pronto

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)

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.

Ekahau Maps Requirements

ExtremeCloud IQ - Site Engine supports importing Ekahau version 8.x maps in .ZIP format.

Guest and IoT Manager Requirements

Guest and IoT Manager Server OS Requirements

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

Manufacturer	Operating System
VMware® (ExtremeCloud IQ - Site Engine Virtual Engine)	VMware ESXi™ 5.5 server VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server vSphere (client only)™

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.

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

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 Mozilla Firefox Google Chrome Microsoft Edge Safari	11 and later 63 and later 65 and later 42 and later 12 and later
Mobile[1]	iOS Native Android Chrome US Browser Opera Firefox	9 and later 65 and later 11.5 and later 40 and later 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.

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