ExtremeCloud™ IQ - Site Engine Release Notes

09/2022
22.06.13
PN: 9037543-02

Table of Contents

Release Notes for 22.06.13

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 22.06.13 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 22.06.13 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 onboardExtremeCloud 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

Changed the behavior of the Operations icon

The icon now indicates if there is a new update in the operations panel by the blue dot instead of a red counter.

Show Support available for Connection Loss and License Violation screens

Added the option to generate Show Support from both the License Violation screen and the Connection Loss screen.

Removed Auto Download Latest Cloud Connector from ZTP+ Options

Option to Auto Download Latest Cloud Connector was removed from Administration > Options > ZTP+. The Cloud Connector is now part of the switch firmware.

Channelized port range support for the 5720-24MXW Switch Engine added to ZTP+ Automated Templates

For EXOS and Switch Engine operating systems, the Port Template to Port Mapping for ZTP+ now requires the Slot:Port format. Existing EXOS and Switch Engine Port Mappings are updated during the upgrade to reflect the new format.

Beta support for Universal Platform 5720

Support for the 5720 platforms (Vendor Profiles) has been added.

Convert from Connected deployment to Air Gap deployment

Added the ability to convert from Connected deployment to Air Gap deployment (see Convert from Connected to Air Gap deployment.)

ExtremeCloud IQ - Site Engine

SNMP Wireless MIBs were updated to support new AP models.

New AP models

AP3000-WW	AP410C-1-IL
AP3000X-WW	AP305C-1-IL
AP410C-1-FCC	AP410C-1-EG
AP305C-1-FCC	AP305C-1-EG
AP410C-1-WR	AP3000-1-WW
AP305C-1-WR	AP3000X-1-WW
AP410C-1-CAN	AP4000-1-WW
AP305C-1-CAN	

Increase OpenSSH MaxStartups connections

New installs of ExtremeCloud IQ - Site Engine will have a default value of 40 simultaneous SSH connections. Existing installs can increase the previous default value of 10 to 40 by updating `/etc/ssh/sshd_config` and changing `Max Startups` from `10:30:100 to 40:30:100`. The change is required if ExtremeCloud IQ - Site Engine is configured to run more than 10 simultaneous SSH connections (for example archive backups).

ExtremeControl

Visualize Randomized MAC addresses in the End-Systems table

Implemented visualization of Randomized MAC addresses in the End-System table.

Modified the End-System Group and User Group details in the Access Control Event log

When End-System Group or User Group is modified, new and removed entries are now listed in the Access Control Event log message. Also addressed a parsing error for Client and User columns in Events.

Added Interface MTU/Jumbo Frames Support

Configuring MTU on Access Control interfaces is now supported. (This enhancement is associated with case numbers 02577639 and 02582742.)

NOTE	Configuring an MTU on an Access Control interface requires both ExtremeCloud IQ - Site Engine and ExtremeControl to be running 22.6.10 or higher.

ExtremeAnalytics

ExtremeAnalytics Fingerprints updates

Added 40+ fingerprints including Microsoft Teams.

Removed Threat Detection that remained from the SAN project

The XML reports were removed so SAN does not show up in the tree as a category.

- The categories may still show SAN if you have customized your reports. You will have to clean your MyReports.

The Threat column was removed from the flow grid.

- You may need to clear your browsing data if your data sorts by the threat column.

The checkboxes found in Sensor Module > Reputation Detector have been removed, and the default set to false.

The default SAN profile and CLI Credentials have been removed.

- This only applies to new installations.

Removed the Threat related targets from the Analytics > Browser.

FabricManager

ISIS Source IP Address validation has been removed

In VOSS firmware prior to release 8.2, the ISIS Source Address field could not be 0.0.0.0 when IP Shortcuts were enabled. If it was, the enforce failed and you would get an enforcement error. Starting in VOSS firmware 8.2, this restriction has been removed which allows the user to enable IP Shortcuts independent of what the ISIS Source Address field contains.

Enforcing the VOSS firmware prior to version 8.2 now triggers an enforcement error. The error message When SPBM IP shortcut is enabled, ISIS IP Source Address should be configured is displayed.

Customer Found Defects and Known Issues

Customer Found Defects Addressed in 22.06.12

ExtremeManagementCFDs Addressed	ID
Dell devices are accurately identified, so the correct license is allocated.	2610082

ExtremeManagementCFDs Addressed	ID
The Inventory Scripts `COMMANDREPEATUNTIL` macro will now abort the script if the string pattern is not found at the end of the retry attempts. This affects ERS devices with the menu mode enabled.	2619120
The `nstftpd` process crashing with buffer overflow that occurred when there was an error in the `tftp` process has been fixed.	2628313

Customer Found Defects Addressed in 22.06.10

ExtremeCloud IQ - Site Engine CFDs Addressed	ID
Analytics Engine no longer sends ICMP unreachable packets to the switches.	2500906
Adding multiple devices at the same time no longer results in some devices not being added.	2575395
Switch Engine/EXOS VLAN monitor cache data now use the webview url settings to determine if an HTTPS or HTTP call should be made.	2586087
Setting a non-default **MAC Hold Time** in the **Authentication Login Settings** failed if any Extreme XOS or Unified Switch Engine ports were selected.	2590103
Inventory Scripts for Switch Engine or EXOS VR's other than VR-Mgmt and VR-Default now work.	2608832

ExtremeAnalyticsCFDs Addressed	ID
The Analytics Flow table **Input Interface** and **Output Interface** columns were displaying `ifIndex` values instead of `ifName` values when the index values could be resolved on the server. Similarly, the **Client Address** and **Server Address** columns were displaying IP addresses instead of hostnames when the hostnames could be resolved on the ExtremeCloud IQ - Site Engine server.	2273609
Application-based graphs were not showing more than one Analytics graph at a time.	2431000
The Analytics engine status page now shows the correct needs enforce state of the appliances.	2437598
An intermittent issue with the **Analytics > Dashboard > Insights Dashboard > Application** response donut not displaying data when double-clicked.	2487802
A string search without a filter was causing the following error in the server.log: `getAggregateFlows: java.net.SocketTimeoutException: Read timed out`.	2560495
Analytics sometimes failed to add a VSP or Fabric Engine as an Application Telemetry Source (sFlow+). This occurred if the `shows sflow collector` CLI output displayed a next-hop node name instead of an IPv4 address in the `Reachable Via` column.	2569442
Removed the unnecessary check for a variable used to configure the Network Information Service. The check for this variable impacted the ability to proceed with the configuration.	2602424

ExtremeControlCFDs Addressed	ID
Authorization Groups Inventory advanced settings is now supported. The user can execute **Stamp New Version** if both the basic and advanced checks pass for that user group.	2600699
Delete Occurrences in Groups under **Control > End-Systems > Tools > Clean Up Data** now appears in red text. Also, a new confirmation dialog asking the user to confirm deletion of **End-Systems** appears after you select **Clean Up**.	2561455
Exporting Event Grids are now filtering events to the selected event log in device view and Alarm and Events.	2600270
Fixed licensing issue preventing Identity Management sourced end-systems from populating in ExtremeCloud IQ - Site Engine/ExtremeControl.	2590165
Fixed the issue with Fabric Manager generating the error `Could not find stateful bean` and not starting the GUI, was addressed.	2566268
Frozen port policy port selector will warn that frozen ports may be impacted if selected.	2589914
Impact Dashboard Historical Charts now show data.	2473085
Importing the preregistration CSV file with duplicate names caused the server to generate an exception issue. Duplicates are now ignored.	2556884
Removed unnecessary check for a variable used to configure NIS. The check for this variable impacted the ability to proceed with configuration.	2602424
The ability to drill down into Application Flows now work as expected.	2587430
The `cleanappidattributetable.sh` script now runs with location names up to 256 characters.	2569932
The client and user information were not presented correctly in the **Events** table when **Clean Up Data** was run.	2557028
The local authentication for MAC EAP-MD5 protocol was failing because it's incorrectly detecting the Authentication type. Now it's correctly validating the type and going through the local authentication successfully.	2610617 2590978
The misspelled word "Requred" in **Authentication Required (Active/Discard)** option for **Port Authentication Configuration** has been corrected.	2572984
Updated access control RADIUS server code to latest stable release to pick up crash fixes.	2560220
When distributed end-system cache was disabled, the end-system received the error page during registration. The end-system should now receive the correct registration page for this case and complete the registration.	2593762

ExtremeConnect CFDs Addressed	ID
Initializing ExtremeCloud IQ - Site Engine database not initializing ExtremeConnect configuration and data.	2556757

ExtremeManagementCFDs Addressed	ID
Access Control was matching the AAA rule incorrectly when the TLS user name was replaced with **TLS-Client-Cert-Common-Name** using **RADIUS_TLS_REPLACE_USERNAME** property. Now it's matching the correct AAA rule.	1853182

ExtremeManagementCFDs Addressed	ID
System workflows were incorrectly allowed to be executed by XIQ-SE Administrator user group. System workflows should be copied before use. System workflows are not executable by XIQ-SE Administrator users anymore.	2483350
The **Export End System Events** function has been modified to limit event exports to 1 million entries. For singularly selected end systems only, a thread lock issue when tens of millions of events were being exported for multiple end systems has been addressed.	2484014
Additional communication ports were added to the Ports List.	2473811
Under **Enforce Preview** for Services/L2 VSN, not all ports were displayed.	2487798
Inventory tree views now include access points for reference image support.	2490861
The additional prerequisite **Regex** field in Compliance Audit Test UI was not being saved.	2498187
Addressed inconsistency in lowercase and uppercase characters in the dialog box.	2498218
During a server restart, new subfamilies added in the Vendor tab will persist.	2500260
Site Engine now displays all groups in the **Access ControlGroup Editor**because the "At sign" (@) restriction in username has been removed.	2552502 2569702
Device View **Clear All Alarms** will only clear the alarms associated with that device.	2551441
Device View > Alarm > Alarm History grid now maps the source name to a known *hostname* (nickname) similar to the **Alarm Current** grid.	2560844
NBI Insufficient privileges responses for mutations were formatted without duplicate data.	2564433
The URL for downloading firmware will now launch the Extreme download page in a separate tab.	2568015
Addressed issue causing the following error in the `server.log: [java.lang.Class] class0 is invalid value for enumeration com.extreme.common.ezconfig.configblocks.PoePdClass. Supported values are: searching, class1, class2, class3, class4`	2569753
Device > Reports > Device Archives > Archive Events tabs displays filtered data by tab selection.	2596372
VOSS Configuration Templates are now working properly on a restore.	2571212
Added a checkbox to disable/enable map auto refresh to **Administration > Options > XIQ-SE General > Map**.	2571515
Interface views now filter tasks by the device Network OS selected in the view.	2574918
Renamed ExtremeCloud IQ option **Enable Sharing** to reflect **Enable connection to ExtremeCloud IQ** to better represent what this option does.	2576997
When adding multiple devices at the same time, the add action no longer runs multiple times on the same device.	2577615
Wireless Summary Report up/down/pending column widths have been increased to display five digit numbers.	2588568
SSH to EXOS switches running firmware versions 16.1 and older now works again. This issue affected scripting, workflows, configuration backup and restore, and firmware upgrades if EXOS was running version 16.1 and older and SSH and Site Engine version 21.11.11 and 22.3.10.	2574882
Clients were encountering 20 second login delays when there was no internet access.	2571555
The `nstftpd` service crashed on some systems running Ubuntu 18.04.	2571199

ExtremeManagementCFDs Addressed	ID
Inventory Scripts for Switch Engine or EXOS VR's other than VR-Mgmt and VR-Default now work.	2608832

ExtremeControlGuest and IoT Manager CFDs Addressed	ID
Host routes added to GIM (for example, 32 bit mask or 255.255.255.255) did not persist on reboot. All manually added routes — host and network — now persist after rebooting GIM.	2464026
Adding a certificate that contains spaces was failing through GIM certificate UI. Now certificates with spaces can be added.	2576600

Known Issues Addressed in 22.06.13

FabricManagerIssues Addressed
An error occurring during the initial onboarding of ZTP+ Add Archive.

ExtremeControl and ExtremeAnalytics Issues Addressed
ExtremeControl and ExtremeAnalytics alarms were not working.

Known Issues Addressed in 22.06.10

ExtremeCloud IQ - Site Engine Issues Addressed
Fixed missing scroll option in the Policy Rule Hit Counts window

Policy Issues Addressed
Fixed missing scroll option in the Policy Rule Hit Counts window

ExtremeControlIssues Addressed
Addressed issue when ZTP+ added VOSS/Fabric Engine device to Access Control Engine as Extreme Policy instead of Extreme VOSS - Fabric Attach or Extreme VOSS - Per-User ACL.
Added the ability to run a health check on joined domains using a customer defined health check user. This applies to LDAP configurations that are set up for NTLM authentication and used in AAA configuration rules .

ExtremeManagement Issues Addressed
Updated `oui.txt` from IEEE's latest at [`http://standards-oui.ieee.org|http://standards-oui.ieee.org/oui.txt`] This makes 494 changes to the prior file (includes add/updates/deletes)

FabricManager Issues Addressed
Configure > Enforce Preview > Fabric Topology > Topology now displays Enable RSMLT Edge Support. Enforce itself ignores the SPBM Origin to better address inline management scenarios. SPBM Dynamic NickName is handled properly in the background. AutoSense Onboarding ISID and VLANs are ignored by Enforce Preview because it is not a GUI configuration option.
Nessus picked up an Apache Log4j issue that is a false positive. The Log4j library in FabricManager does not process any untrusted data. Therefore, the FabricManager is not vulnerable to CVE-2019-17571. Path : `/usr/local/Extreme_Networks/NetSight/jboss/jboss-6.1.0.Final/server/all/tmp/vfs/automountb7b5a60dbcf9568c/log4j-1.2.13_CVE_2019_17571.jar-6b4b4124aed577b3/log4j-1.2.13_CVE_2019_17571.jar` Installed version : 1.2.13

Vulnerabilities Addressed

This section presents the vulnerabilities addressed in 22.6. If you need more information on vulnerability testing, see Security and Vulnerability Testing.

Vulnerabilities in 22.06.13

ExtremeCloud IQ - Site Engine, ExtremeControl, ExtremeAnalytics, and Application Analytics Traffic Sensor

CVE-2016-3709, CVE-2019-5815, CVE-2021-30560, CVE-2021-3155, CVE-2021-4120, CVE-2021-4209, CVE-2021-44730, CVE-2021-44731, CVE-2022-0494, CVE-2022-1048, CVE-2022-1195, CVE-2022-1652, CVE-2022-1679, CVE-2022-1729, CVE-2022-1734, CVE-2022-1974, CVE-2022-1975, CVE-2022-24805, CVE-2022-24806, CVE-2022-24807, CVE-2022-24808, CVE-2022-24809, CVE-2022-24810, CVE-2022-2509, CVE-2022-2586, CVE-2022-2588, CVE-2022-28893, CVE-2022-33981, CVE-2022-34918, CVE-2022-37434

ExtremeControl

CVE-2022-2625

Vulnerabilities in 22.06.12

ExtremeCloud IQ - Site Engine, ExtremeControl, ExtremeAnalytics, and Application Analytics Traffic Sensor

CVE-2015-20107, CVE-2022-2068, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315, CVE-2022-29187, CVE-2021-46790, CVE-2022-30783, CVE-2022-30784, CVE-2022-30785, CVE-2022-30786, CVE-2022-30787, CVE-2022-30788, CVE-2022-30789, CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-27404, CVE-2022-27405, CVE-2022-27406, CVE-2022-31782, CVE-2022-1304, CVE-2022-21125, CVE-2022-21166, CVE-2022-21123, CVE-2022-28388, CVE-2022-1353, CVE-2022-1205, CVE-2022-2380, CVE-2022-28389,

CVE-2022-1011, CVE-2022-1516 , CVE-2022-1204, CVE-2021-4197, CVE-2022-1198, CVE-2022-1199, CVE-2022-34903, CVE-2022-34480, CVE-2022-22747, CVE-2021-44730, CVE-2021-44731, CVE-2021-4120, CVE-2021-3155

ExtremeControl

CVE-2022-28738, CVE-2022-28739, CVE-2022-28614, CVE-2022-29404, CVE-2022-28615, CVE-2022-26377, CVE-2022-30522, CVE-2022-30556, CVE-2022-31813, CVE-2022-31626, CVE-2022-31625

Vulnerabilities in 22.06.10

ExtremeCloud IQ - Site Engine

CVE-2022-23218, CVE-2022-23219, CVE-2021-3998, CVE-2016-10228, CVE-2021-3326, CVE-2020-6096, CVE-2020-29562, CVE-2020-27618, CVE-2021-3999, CVE-2021-27645, CVE-2021-35942, CVE-2019-25013, CVE-2021-31873, CVE-2021-31872, CVE-2021-31871, CVE-2021-31870, CVE-2022-29155, CVE-2021-25220, CVE-2022-0396, CVE-2022-0391, CVE-2021-4189, CVE-2021-3426, CVE-2022-21716, CVE-2022-21712, CVE-2018-25032, CVE-2022-25308, CVE-2022-25310, CVE-2022-25309, CVE-2018-16301, CVE-2020-8037, CVE-2022-1271, CVE-2022-29800, CVE-2022-29799, CVE-2022-1473, CVE-2022-1343, CVE-2022-1434, CVE-2022-1292, CVE-2021-36690, CVE-2022-24903, CVE-2020-35512, CVE-2022-0934, CVE-2020-25648, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-0561, CVE-2022-0891, CVE-2022-0562, CVE-2020-35522, CVE-2022-0865, CVE-2022-23308, CVE-2022-29824, CVE-2019-20838, CVE-2020-14155, CVE-2022-28656, CVE-2022-28657, CVE-2022-28658, CVE-2021-3899, CVE-2022-28655, CVE-2022-28652, CVE-2022-28654, CVE-2022-1242, CVE-2022-0435, CVE-2021-44733, CVE-2021-43976, CVE-2021-3506, CVE-2021-45095, CVE-2022-0492, CVE-2022-27666, CVE-2022-26490, CVE-2022-23039, CVE-2022-23037, CVE-2022-24958, CVE-2022-25258, CVE-2022-26966, CVE-2022-27223, CVE-2022-25375, CVE-2022-23036, CVE-2022-23042, CVE-2022-23038, CVE-2022-23040, CVE-2021-26401, CVE-2022-30594, CVE-2022-29581, CVE-2021-20193, CVE-2022-0617, CVE-2022-24448, CVE-2021-43975, CVE-2022-24959, CVE-2022-0001, CVE-2022-25636, CVE-2022-23960, CVE-2022-0002, CVE-2021-28713, CVE-2021-28712, CVE-2021-28711, CVE-2021-28715, CVE-2021-28714, CVE-2021-45480, CVE-2021-4135, CVE-2022-0516, CVE-2022-1055, CVE-2022-20008, CVE-2022-1016, CVE-2020-27820, CVE-2022-1116, CVE-2022-1664, CVE-2019-13050,CVE-2022-24765, CVE-2017-9525, CVE-2019-9705, CVE-2019-9706, CVE-2019-9704, CVE-2020-10001, CVE-2019-8842, CVE-2022-26691, CVE-2022-21413, CVE-2022-21478, CVE-2022-21435, CVE-2022-21437, CVE-2022-21417, CVE-2022-21425, CVE-2022-21438, CVE-2022-21462, CVE-2022-21460, CVE-2022-21414, CVE-2022-21440, CVE-2022-21454, CVE-2022-21451, CVE-2022-21412, CVE-2022-21415, CVE-2022-21459, CVE-2022-21436, CVE-2022-21423, CVE-2022-21452, CVE-2022-21457, CVE-2022-21444, CVE-2022-21418, CVE-2022-21427

ExtremeAnalytics images:

CVE-2022-23218, CVE-2022-23219, CVE-2021-3998, CVE-2016-10228, CVE-2021-3326, CVE-2020-6096, CVE-2020-29562, CVE-2020-27618, CVE-2021-3999, CVE-2021-27645, CVE-2021-35942, CVE-2019-25013, CVE-2021-31873, CVE-2021-31872, CVE-2021-31871, CVE-2021-31870,

CVE-2022-29155, CVE-2021-25220, CVE-2022-0396, CVE-2022-0391, CVE-2021-4189, CVE-2021-3426, CVE-2022-21716, CVE-2022-21712, CVE-2018-25032 CVE-2022-25308, CVE-2022-25310, CVE-2022-25309, CVE-2018-16301, CVE-2020-8037, CVE-2022-1271, CVE-2022-29800, CVE-2022-29799, CVE-2022-1473, CVE-2022-1343, CVE-2022-1434, CVE-2022-1292, CVE-2021-36690, CVE-2022-24903, CVE-2020-35512, CVE-2022-0934, CVE-2020-25648, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-0561, CVE-2022-0891, CVE-2022-0562, CVE-2020-35522, CVE-2022-0865, CVE-2022-23308, CVE-2022-29824, CVE-2019-20838, CVE-2020-14155, CVE-2022-28656, CVE-2022-28657, CVE-2022-28658, CVE-2021-3899, CVE-2022-28655, CVE-2022-28652, CVE-2022-28654, CVE-2022-1242, CVE-2022-0435, CVE-2021-44733, CVE-2021-43976, CVE-2021-3506, CVE-2021-45095, CVE-2022-0492, CVE-2022-27666, CVE-2022-26490, CVE-2022-23039, CVE-2022-23037, CVE-2022-24958, CVE-2022-25258, CVE-2022-26966, CVE-2022-27223, CVE-2022-25375, CVE-2022-23036, CVE-2022-23042, CVE-2022-23038, CVE-2022-23040, CVE-2021-26401, CVE-2022-30594, CVE-2022-29581, CVE-2022-0617, CVE-2022-24448, CVE-2021-43975, CVE-2022-24959, CVE-2022-0001, CVE-2022-25636, CVE-2022-23960, CVE-2022-0002, CVE-2021-28713, CVE-2021-28712, CVE-2021-28711, CVE-2021-28715, CVE-2021-28714, CVE-2021-45480, CVE-2021-4135, CVE-2022-0516, CVE-2022-1055, CVE-2022-20008, CVE-2022-1016, CVE-2020-27820, CVE-2022-1116, CVE-2022-1664, CVE-2019-13050, CVE-2021-20193, CVE-2022-24765, CVE-2017-9525, CVE-2019-9705, CVE-2019-9706, CVE-2019-9704, CVE-2020-10001, CVE-2019-8842, CVE-2022-26691

ExtremeControl images:

CVE-2022-23218, CVE-2022-23219, CVE-2021-3998, CVE-2016-10228, CVE-2021-3326, CVE-2020-6096, CVE-2020-29562, CVE-2020-27618, CVE-2021-3999, CVE-2021-27645, CVE-2021-35942, CVE-2019-25013, CVE-2021-31873, CVE-2021-31872, CVE-2021-31871, CVE-2021-31870, CVE-2022-29155, CVE-2017-9118, CVE-2017-8923, CVE-2021-21707, CVE-2017-9120, CVE-2017-9119, CVE-2021-25220, CVE-2022-0396, CVE-2022-22720, CVE-2022-23943, CVE-2022-22721, CVE-2022-22719, CVE-2022-0391, CVE-2021-4189, CVE-2021-3426, CVE-2022-21716, CVE-2022-21712, CVE-2018-25032, CVE-2022-25308, CVE-2022-25310, CVE-2022-25309, CVE-2018-16301, CVE-2020-8037, CVE-2022-1271, CVE-2022-29800, CVE-2022-29799, CVE-2022-1473, CVE-2022-1343, CVE-2022-1434, CVE-2022-1292, CVE-2021-36690, CVE-2022-24903, CVE-2020-35512, CVE-2022-0934, CVE-2020-25648, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-0561, CVE-2022-0891, CVE-2022-0562, CVE-2020-35522, CVE-2022-0865, CVE-2022-23308, CVE-2022-29824, CVE-2019-20838, CVE-2020-14155, CVE-2022-28656, CVE-2022-28657, CVE-2022-28658, CVE-2021-3899, CVE-2022-28655, CVE-2022-28652, CVE-2022-28654, CVE-2022-1242, CVE-2022-0435, CVE-2021-44733, CVE-2021-3506, CVE-2021-45095, CVE-2022-0492, CVE-2022-27666, CVE-2022-26490, CVE-2022-23039, CVE-2022-23037, CVE-2022-24958, CVE-2022-25258, CVE-2022-26966, CVE-2022-27223, CVE-2022-25375, CVE-2022-23036, CVE-2022-23042, CVE-2022-23038, CVE-2022-23040, CVE-2021-26401, CVE-2022-30594, CVE-2022-29581, CVE-2021-20193, CVE-2022-0617, CVE-2022-24448, CVE-2021-43975, CVE-2022-24959, CVE-2022-1552, CVE-2022-0001, CVE-2022-25636, CVE-2022-23960, CVE-2022-0002, CVE-2021-43976, CVE-2021-28713, CVE-2021-28712, CVE-2021-28711, CVE-2021-28715, CVE-2021-28714, CVE-2021-45480, CVE-2021-4135, CVE-2022-0516, CVE-2022-1055, CVE-2022-20008, CVE-2022-1016, CVE-2020-27820, CVE-2022-

1116, CVE-2022-1664, CVE-2019-13050, CVE-2022-24765, CVE-2017-9525, CVE-2019-9705, CVE-2019-9706, CVE-2019-9704, CVE-2020-10001, CVE-2019-8842, CVE-2022-26691

Application Analytics Traffic Sensor images:

CVE-2022-23218, CVE-2022-23219, CVE-2021-3998, CVE-2016-10228, CVE-2021-3326, CVE-2020-6096, CVE-2020-29562, CVE-2020-27618, CVE-2021-3999, CVE-2021-27645, CVE-2021-35942, CVE-2019-25013, CVE-2021-31873, CVE-2021-31872, CVE-2021-31871, CVE-2021-31870, CVE-2022-29155, CVE-2021-25220, CVE-2022-0396, CVE-2022-0391, CVE-2021-4189, CVE-2021-3426, CVE-2022-21716, CVE-2022-21712, CVE-2018-25032, CVE-2022-25308, CVE-2022-25310, CVE-2022-25309, CVE-2018-16301, CVE-2020-8037, CVE-2022-1271, CVE-2019-18276, CVE-2022-29800, CVE-2022-29799, CVE-2022-1473, CVE-2022-1343, CVE-2022-1434, CVE-2022-1292, CVE-2021-36690, CVE-2022-24903, CVE-2020-35512, CVE-2022-0934, CVE-2020-25648, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-23308, CVE-2022-29824, CVE-2019-20838, CVE-2020-14155, CVE-2022-28656, CVE-2022-28657, CVE-2022-28658, CVE-2021-3899, CVE-2022-28655, CVE-2022-28652, CVE-2022-28654, CVE-2022-1242, CVE-2022-0435, CVE-2021-44733, CVE-2021-43976, CVE-2021-3506, CVE-2021-45095, CVE-2022-0492, CVE-2022-27666, CVE-2022-26490, CVE-2022-23039, CVE-2022-23037, CVE-2022-24958, CVE-2022-25258, CVE-2022-26966, CVE-2022-27223, CVE-2022-25375, CVE-2022-23036, CVE-2022-23042, CVE-2022-23038, CVE-2022-23040, CVE-2021-26401, CVE-2022-30594, CVE-2022-29581, CVE-2021-20193, CVE-2022-0617, CVE-2022-24448, CVE-2021-43975, CVE-2022-24959, CVE-2022-0001, CVE-2022-25636, CVE-2022-23960, CVE-2022-0002, CVE-2021-28713, CVE-2021-28712, CVE-2021-28711, CVE-2021-28715, , CVE-2021-28714, CVE-2021-45480, CVE-2021-4135, CVE-2022-0516, CVE-2022-1055, CVE-2022-20008, CVE-2022-1016, CVE-2020-27820, CVE-2022-1116, CVE-2022-1664, CVE-2019-13050, CVE-2022-24765, CVE-2017-9525, CVE-2019-9705, CVE-2019-9706, CVE-2019-9704, CVE-2020-10001, CVE-2019-8842, CVE-2022-26691

FabricManager images:

CVE-2022-1292, CVE-2022-1343, CVE-2022-1434, CVE-2022-1473, CVE-2019-18276, CVE-2019-18276, CVE-2021-3506, CVE-2021-43976, CVE-2021-44733, CVE-2021-45095, CVE-2022-0435, CVE-2022-0492, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315, CVE-2020-35512, CVE-2020-35512, CVE-2022-23308, CVE-2022-29824, CVE-2021-3426, CVE-2021-4189, CVE-2022-0391, CVE-2021-43975, CVE-2022-0617, CVE-2022-24448, CVE-2022-24959, CVE-2021-26401, CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23042, CVE-2022-24958, CVE-2022-25258, CVE-2022-25375, CVE-2022-26490, CVE-2022-26966, CVE-2022-27223, CVE-2017-9525, CVE-2022-27666, CVE-2021-20193, CVE-2021-3899, CVE-2022-1242, CVE-2022-28652, CVE-2022-28654, CVE-2022-28655, CVE-2022-28656, CVE-2022-28657, CVE-2022-28658, CVE-2022-24903, CVE-2022-2257, CVE-2022-27774, CVE-2022-27775, CVE-2022-27776, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-1664, CVE-2022-29799, CVE-2022-29800, CVE-2021-25220, CVE-2022-0396, CVE-2022-25308, CVE-2022-2530, CVE-2022-25310, CVE-2022-1271, CVE-2022-21712, CVE-2022-21716, CVE-2022-1271, CVE-2022-23308, CVE-2018-25032, CVE-2018-16301, CVE-2020-8037, CVE-2022-0778, CVE-2017-9525, CVE-2019-9704, CVE-2019-9705, CVE-2019-9706, CVE-2019-13050, CVE-2021-36690, CVE-2022-0001, CVE-2022-0002, CVE-2021-36084, CVE-2021-36085, CVE-2021-36086, CVE-2021-36087

Guest and IoT Manager images:

CVE-2022-26377,CVE-2022-28330,CVE-2022-28614,CVE-2022-28615,CVE-2022-29404,CVE-2022-30522,CVE-2022-30556,CVE-2022-31813,CVE-2022-26377,CVE-2022-28330,CVE-2022-28614,CVE-2022-28615,CVE-2022-29404,CVE-2022-30522,CVE-2022-30556,CVE-2022-31813

Installation, Upgrade, and Configuration Changes

Installation Information

There are two supported scenarios for onboarding ExtremeCloud IQ - Site Engine toExtremeCloud 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 22.06.13 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 running in Air Gap deployment.
- Connected mode supports upgrades from Extreme Management Center versions 8.4.4 or 8.5.7, or ExtremeCloud IQ - Site Engine running in Connected deployment.

NOTE: Changing deployment mode from air gap to connected is available after the upgrade.

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 22.06.13.

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 22.6 (connected)	Upgrade to ExtremeCloud IQ - Site Engine version 22.6 (air gap)
	8.1.7	8.3.3	8.4.4	8.5.7		
ExtremeCloud IQ - Site Engine 22.3, 22.1 & 22.11 (air gap)						X

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 22.6 (connected)	Upgrade to ExtremeCloud IQ - Site Engine version 22.6 (air gap)
	8.1.7	8.3.3	8.4.4	8.5.7		
ExtremeCloud IQ - Site Engine 22.3, 22.1 & 22.11 (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
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 or 8.5.7 and then to ExtremeCloud IQ - Site Engine version 22.06.13.

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 22.06.13, 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 22.06.13 and then add the feature.
- The 4.xx version of the NAC Request Tool is not compatible with the 22.06.13 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 22.06.13.
- 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.
- If ExtremeControl is using an intermediate certificate used by the Access Control Engine Radius certificate, you must also add the Root CA certificate. The complete certificate chain is needed to prevent the EAP-TLS authentication from being rejected.

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, ExtremeAnalyticsengine, or ExtremeControlengine to version 22.06.13, ensure the DNS server IP address is correctly configured.
- When upgrading to ExtremeCloud IQ - Site Engine version 22.06.13, 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 ExtremeControlengines, Fabric Manager, or another add-on feature, you must first perform the ExtremeCloud IQ - Site Engine upgrade to version 22.06.13 and then add the feature.

License Renewal

Upgrading to ExtremeCloud IQ - Site Engine version 22.06.13 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 22.06.13, 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 22.06.13 on the ExtremeControlengine, 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 22.06.13:

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 22.06.13 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 22.06.13, the Default Gateway IP Address is configured as part of the VLAN. In 22.06.13, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 22.06.13, 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 EngineNetwork > 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.

Server and Client System Requirements

IMPORTANT: Wireless event collection is disabled by default in version 22.06.13 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 22.06.13.

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
Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000

	Small	Medium	Enterprise	Large Enterprise
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000 air gap 8,000 connected	10,000 air gap 8,000 connected
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 ExtremeExtremeAnalytics 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 air gap 8,000 connected
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 ExtremeControlengine 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 NetworksExtremeControl.

Medium	Browser	Version
Desktop	Microsoft Edge Microsoft Internet Explorer Mozilla Firefox Google Chrome	41 and later 11 and later 34 and later 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://<ExtremeControlEngine 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 ExtremeControlengine version requirements, see Release Notes for 22.06.13.

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	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.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

ExtremePortal
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