ExtremeCloud™ IQ - Site Engine Release Notes

10/2022
22.09.10
PN: 9037634-00
Subject to Change Without Notice

Table of Contents

Release Notes for 22.09.10

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 22.09.10 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 22.09.10 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 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

License revocation in Air Gap mode

In air gap deployment mode the Pilot , Navigator, and NAC licenses can be revoked and returned to the license pool.

Air Gap to Connected mode

If you have configured your system in Air Gap mode, you can now change it to Connected mode.

Launching a WebShell/Terminal audit

Four new event types were created (Event Type: Console, Event Category: CLI Session):

- CLI terminal session started via SSH
- CLI terminal session started via TELNET
- CLI terminal session ended
- CLI terminal session authentication error

When the Terminal is executed (right-click on the device and select **Terminal**), the event is generated for auditing purposes.

AP5010 support

Access Point AP5010 is supported.

AP305C-1 and AP410C-1 support

Access Points AP305C-1 and AP410C-1 are supported.

Update Rapid_City MIB to contain rcVirtualService

Added rcVirtualService MIBs for VOSS/Fabric Engine to support Integrated Application Hosting.

ZTP+ Image supports EXOS

ZTP+ now supports upgrading EXOS devices using `.lst` files.

Downloadable Show Support and NAC Failure handling in Show Support

Updated the **Show Support** functionality to support the download of `.zip` files from UI. Enhanced error reporting on completion is also included in this change.

Consolidation of installation/upgrade files into one

Consolidated three installation/upgrade files into one. This new file is called `XIQ-SE Install and Upgrade`. The file can be used for the following use cases:

- New installation of ExtremeCloud IQ - Site Engine on the supported OS
- Upgrade the virtual appliance
- Upgrade the physical appliance
- Upgrade the installation running on the supported OS

Check the Important Upgrade Information and Server and Client System Requirements sections for details regarding the upgrade path and supported platforms.

ExtremeControl

New NBI for Policy Mapping

- NBI query for Network Access Control to read a policy mapping.
- NBI query for Network Access Control to read all policy mappings.
- NBI mutation for Network Access Control to create a policy mapping.
- NBI mutation for Network Access Control to delete a policy mapping.
- NBI mutation for Network Access Control to manipulate policy mappings.

New NBI API calls for NAC Radius configuration

- NBI mutation for Network Access Control to manipulate upstream radius servers, enforce network access control settings.
- NBI queries for Network Access Control to check the need for configuration enforcement.

NAC Trusted Certificate Authorities & intermediate CA

Implemented a warning when a new certificate is updated:

If an intermediate certificate is used by the Access Control Engine, you must also add the Root CA certificate. The complete certificate chain is needed to prevent the EAP-TLS authentication from being rejected.

Customer Found Defects and Known Issues

Customer Found Defects Addressed

ExtremeCloud IQ - Site Engine CFDs Addressed	ID
In port selection, all ports will be displayed. Guest VM ports are no longer hiden from the user.	2580520
The **Connect Intune** module failed to retrieve all managed devices via Graph API calls.	2594155
SNMP Credential not displaying all created profiles.	2604590
Vendor scans picked up Amazon Correta JDK/JRE after updating to a new version.	2608008
Archiving failed when devices that do not support archiving were inadvertently added to the archive. The devices are added when **Add to Archive** under **Network > Devices** is enabled by default. Access Control Engine, Purview, Traffic Sensor, and Site Engine now ignore **Add to Archive**.	2610785
Incorrect directory paths caused long firmware refresh cycles and added 1000s of files. The option **Max Files Parsed** has been added to the **Firmware Refresh Settings** in **Inventory Manager** to control the maximum number of files to parse for the firmware refresh. The default is 1000.	2612088
NAC audit event displayed `Server` as the username in the audit log event when the Notification configuration was changed. The correct *username* now appears in the log.	2616897
Workflows executable by the restricted user are not allowed.	2617139
The ability to change the CLIP Address Interface Number at any time caused duplicate entries. Changing the number is no longer allowed once the update of the row completes.	2617196
The HP SFTP inventory script was not working. The HP switch rebooted before the firmware upgrade completed. An HP SFTP script has been added and the other HP scripts updated for error checking.	2620608
Pre-staged devices could not be saved when configuring in **Discovered** tab.	2646497

ExtremeAnalytics CFDs Addressed	**ID**
Passwords containing the **$** symbol caused the scripting engine to not working properly.	2608033
Tracked **Applications** were not showing up in various queries when selecting **All**.	2610241
Adding or removing a telemetry source was not saving the telemetry configuration change on the device.	2609137

ExtremeControlCFDs Addressed	**ID**
When you do not clear the search/filter in the **Events** table, the Access Control group editor and other areas are intermittently hindered. This issue is addressed by allowing only the Information, Source, and User fields to be used as the criteria, however, you can expand the criteria. Client, Event, and Source Host Name can be included by selecting each one in **Administration > Alarms/Event Logs and Tables** under **Event Search Scope by Field**.	2405659
High NAC transaction per second rate caused web GUI experiences to be slower.	2408846
When running scheduled tasks (**Task > Scheduled Tasks**), it is possible for a task to end up in an infinite wait time (freeze) situation. To prevent this from happening, enter timeout values for **SSH Key Exchange Timeout** and **SessionTimeout** in **Administration > Options > Tasks**. The default is 30 seconds.	2474298
Expiring certificate reports are no longer cleared immediately when other certificates in the chain are not expiring.	2549716
ServiceB did not allow traffic on all other interfaces except port 8445. It is recommended that you disconnect the ServiceB interface in the Hypervisor if the ServiceB interface in not being used.	2552429
The print page could not contain the $usercustom1-6 variables.	2556018
Memory leaks and file descriptor exhaustion are fixed in the Connect Clearpass and many other modules which can impact ExtremeCloud IQ - Site Engine performance.	2568026
Access control returned an incorrect policy attribute when using nested attribute variables in policy mapping. The nested attributes are now being returned correctly.	2595787
ExtremeCloud IQ - Site Engine with larger databases were rebooting before all of these services started. To address this issue, the services start-up timer has been increased from a from 30 minute default to a 90 minute default.	2599402
In some cases, the proxy authentication failed but showed as accepted. An engine property setting was added to configure the nac-proxy-failed module to prevent this scenario.	2603872
The North Bound Interface was not validating the switch IP addresses field in addLocationEntryToGroup. Wrong entries are now rejected.	2615348
The CA certificates were not easily identified in **Update AAA Trusted Certificate Authorities** because there was not enough information displayed. Fields **Serial Number**, **Valid From**, and **Valid To** were added to **Update AAA Trusted Certificate Authorities** to make CAs easier to identify.	2617151
The ability to manually set **Distributed Cache Enable** was removed in a previous release making cache distribution permanently active. However, this function did not survive updates. Now you must run the **Enforce** command on the updated engine to ensure that cache distribution works after an update, .	2617452
If a temporary connection issue occurred during a policy refresh, devices were removed from the policy domain.	2618875

ExtremeControlCFDs Addressed	**ID**
Access Control generated an error when the **Description** contained an ampersand(&).	2623522
The broken **Show Keywords Help** URL in **Access Control> Notification> Override Content**.	2624542

ExtremeManagementCFDs Addressed	**ID**
Mobile devices getting stuck on the Captive Portal registration screen .	2420426 2443140 2576704
Some of the ExtremeAnalytics Insight Dashboard gauges were slow to process their data. A `Loading...` message now displays so the user will not think there is an issue.	2433608 2444423 2435428 2581076
If the same username as the MAC address was used, Access Control detected the authentication type incorrectly for 802.1X TLS . The end system is properly detected now with the correct authentication type in the **End-Systems** table.	2484541
Connect was randomly sending RADIUS Accounting frames to the Fortigate device. This caused issues with the Fortigate device and should not be allowed. Connect/FortiGate accounting requests now uses incrementing packet ID numbers.	2609484

Known Issues Addressed in 22.09.10

ExtremeControlIssues Addressed
Added out-of-the-box support for Reauthentication (RFC 3576) for wireless controllers E2122, VE6120K, VE6125K, and VE6120H.
Per User ACLs for VOSS/Fabric Engine used bit reverse mask.
ExtremeControl and ExtremeAnalytics alarms not working.

ExtremeManagement Issues Addressed
The script *Factory script to update app-telemetry policy file* was enhanced to support the Universal Switch series.
The Network OS for XIQ Native APs is now officially defined as IQ Engine. This may impact custom workflows and scripts.

ExtremeAnalytics Issues Addressed
The Analytics Engine MTU setting was not configurable in the GUI.
ExtremeAnalytics reported applications as Undefined-XX and application group as Undefined.
Deleting S-Series devices from flow sources produced a message that the DWR was successful and to enforce the device. This message has been removed because the S-Series devices do not have their Netflow configured by ExtremeCloud IQ - Site Engine.

Vulnerabilities Addressed in 22.09.10

This section presents the vulnerabilities addressed in 22.9.10. If you need more information on vulnerability testing, see Security and Vulnerability Testing.

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

CVE-2020-35525, CVE-2021-20223, CVE-2020-35527, CVE-2022-31676, CVE-2022-2526, CVE-2022-35252, CVE-2021-33656, CVE-2021-33061, CVE-2021-33656, CVE-2022-1420, CVE-2022-1620, CVE-2022-1616, CVE-2022-1621, CVE-2022-0943, CVE-2022-1154, CVE-2022-1619

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 22.09.10 supports upgrades from Extreme Management Center versions 8.4.4, 8.5.7 or ExtremeCloud IQ - Site Engine.

NOTE: You can change deployment modes from air gap to connected or from connected to air gap 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 22.09.10.

Current Version				Upgrade to ExtremeCloud IQ - Site Engine version 22.9
	8.3.3	8.4.4	8.5.7	
ExtremeCloud IQ - Site Engine (all versions)				X
Extreme Management Center version 8.5.5, 8.5.6 , or 8.5.7				X
Extreme Management Center version 8.5.0-8.5.4			X*	X
Extreme Management Center version 8.4.4				X
*Extreme Management Center version 8.4.0-8.4.3		X*	X*	X
*Extreme Management Center version 8.2.x or 8.3.x		X*	X*	X
Extreme Management Center version 8.0.x or 8.1.x	X		X	X
NetSight version 7.1 or older	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 22.09.10.

IMPORTANT: A backup (**Administration >** Backup/Restore) of the database must be performed prior to the upgrade and saved to a safe location.

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 22.09.10 and then add the feature.
- The 4.xx version of the NAC Request Tool is not compatible with the 22.09.10 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 22.09.10.
- 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.

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 22.09.10, ensure the DNS server IP address is correctly configured.
- When upgrading to ExtremeCloud IQ - Site Engine version 22.09.10, 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 ExtremeControlengines, Fabric Manager, or another add-on feature, you must first perform the ExtremeCloud IQ - Site Engine upgrade to version 22.09.10 and then add the feature.

License Renewal

Upgrading to ExtremeCloud IQ - Site Engine version 22.09.10 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 22.09.10, 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 22.09.10 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 22.09.10:

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 22.09.10 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 22.09.10, the Default Gateway IP Address is configured as part of the VLAN. In 22.09.10, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 22.09.10, 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.

Server and Client System Requirements

IMPORTANT: Wireless event collection is disabled by default in version 22.09.10 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 22.09.10.

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
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)

	Requirements
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 -Xmx	4 GB 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
Mobile	Internet Explorer Mobile Microsoft Edge Microsoft Windows 10 Touch Screen Native (Surface Tablet) iOS Native Android Chrome Android Native Dolphin Opera	11 and later (Windows Phone) All versions N/A 9 and later 4.0 and later 4.4 and later All versions All versions

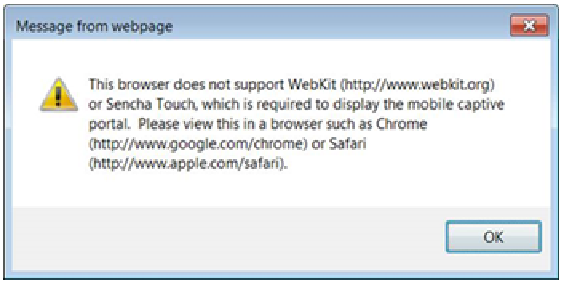
NOTES: A native browser indicates the default, system-installed browser. Although this might be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection for a device. Typically, this is a non-configurable option for Wi-Fi Captive Network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



This browser does not support WebKit (http://www.webkit.org) or Sencha Touch, which is required to display the mobile captive portal. Please view this in a browser such as Chrome (http://www.google.com/chrome) or Safari (http://www.apple.com/safari).

ExtremeControlEngine Version Requirements

For complete information on ExtremeControlengine version requirements, see Release Notes for 22.09.10.

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

Specifications	Minimum	Recommended
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:

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