ExtremeCloud™ IQ - Site Engine Release Notes
Version 21.11.10

12/2021
9037048-02 Rev AA

Table of Contents

ExtremeCloud IQ - Site Engine Version 21.11.10 Release Notes

21.11.10
December 2021

Welcome to ExtremeCloud IQ - Site Engine

ExtremeCloud IQ - Site Engine includes all the features and functionality of Extreme Management Center.

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 21.11.10 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 21.11.10 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 version 21.11.10, the licensing and capabilities of ExtremeControl does not change. Note that the XIQ-NAC subscription must be used instead of IA-ES- license. For new users that complete an initial install of ExtremeCloud IQ - Site Engine, ExtremeControl licensing does not include end-system capabilities.

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

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

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

NOTES:	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.

1. Enhancements in Version 21.11.10

New features and enhancements are added to the following areas in ExtremeCloud IQ - Site Engine version 21.11.10:

- ExtremeCloud IQ - Site Engine
- ExtremeAnalytics
- ExtremeControl

For additional information about each of the features listed in this guide, refer to the documentation posted online at ExtremeNetworks.com or the Help system included with the software.

1.1 ExtremeCloud IQ - Site Engine

Site discover should include ping only choice]

ExtremeCloud IQ - Site Engine has ability to schedule and perform discovery with "Ping Only" profile.

Support for XCC appliance E2122

Added support for Extreme Campus Controller type E2122.

Do not update ExtremeCloud IQ

Sharing Stats and Alarms with ExtremeCloud IQ is now optional.

Subscription NAC, Pilot, and Navigator license input in air gapped mode

A new place to see and insert licenses has been added. License keys and License Files can be inserted by selecting **Administration > Licenses**.

Topology Configuration for VOSS 8.5

The Topology Configuration on VOSS platforms has been enhanced.

Resolve Serial numbers for new versions of XCC

Added ability to resolve the serial number of Extreme Campus Controller

Certificate replacement event

When a certificate is updated or deleted on Access Control Engine, a replacement event is now generated.

Beta Support for 5320 EXOS

Beta support for the 5320 running EXOS products in new devices is now supported with the exception of Fabric Manager.

Support for XCC appliances VE6125K and VE6120K

Added support for Extreme Campus Controller type VE6125K and VE6120K.

EXOS 31.4 = VPEX and Stacking

Added support for the Stack unit being a Controlling Bridge at the same time.

Operations Panel - persist expanded items on refresh

Event in the Operations panel has been expanded, it will now stay expanded when the Operations panel is updated.

ADD device: Remove "No Access" option

The option to add a new device to the database as "No Access" was removed from the GUI because there is not a use case for the option and it was only for internal use.

Systemd and kernel update

Kernel and systemd were updated to address reported vulnerabilities.

Update JRE in the XIQ-SE OS

The latest Java Corretto 18.0_302 for the ExtremeCloud IQ - Site Engineplatform products and the corresponding Zulu Java for the FM appliance have been packaged.

1.4 ExtremeAnalytics

Systemd and kernel update

Kernel and systemd were updated to address reported vulnerabilities

1.3 ExtremeControl

Radius configuration on VOSS 8.3

The ability to configure VOSS platforms as RADIUS clients to use Access Control Engine as RADIUS server has been added.

Edit Policy Mapping is missing "Switch to Advanced"

The Access Control Policy Mapping editor can now be expanded to show advanced fields from within the editor while in basic mode.

Certificate replacement event

When a certificate is updated or deleted on Access Control Engine the event is generated (Type: Access Control, Category: Configuration)

Update the CoA for XIQ Native

ExtremeControl now uses the correct CoA methods for ExtremeCloud APs (IQE) automatically.

Systemd and kernel update

Kernel and systemd were updated to address reported vulnerabilities.

MAC OUI Vendor List: Update for 21.11

OUI list was updated based on the latest IEEE. This makes 1307 changes to prior file (includes add/ updates/ deletes).

3. Customer Found Defects, Known Issues, and Vulnerabilities Addressed

3.1 Customer Found Defects Addressed in 21.11.10

ExtremeCloud IQ - Site Engine CFDs Addressed	ID
Counting interface discards as an error can be controlled by a Site Engine - Collector option on the Administration page.	02332127
Adding a device via the Discover tab will no longer override the add actions configured during the add process.	02355799
Device tracking now include "s/n" and asset tag information for devices that previously reported it as "N/A".	02372480
Feature "Register/Export Serial Numbers > Register device" has been removed and is no longer supported.	02372518
Add Device Window now allows the ability to not run add actions from Sites when adding a device.	02375522
Scripts and Workflows were failing to detect the shell prompt for Cisco Nexus and Aerohive AP devices resulting in timeout failures.	02371250
Configuration of the Fabric Enable field may only be done in /World site upon a Port Template in which the source is Global.	02372726
Addressed the issue of the Compliance engine freezing periodically.	02382078
Corrupted Vendor Profile does not prevent the product from starting.	02384433
Corrected issue displaying Interface History report when ifAlias contained a double dash (-)	02389778
Occasionally, devices were not being polled by ExtremeCloud IQ - Site Engine in environments where SNMPv3 is heavily used.	02389786
Set Port(s) Frozen and Clear Port(s) Frozen were not checking if the policy enforce/verify capability was enabled.	02392900
Port Utilization in Percent updated to support third party devices that have sparse interface support.	02394562
Scripting UI now warns if frozen ports are included in the list of selected ports.	02402814

XCC snmpv3 traps will no longer cause "Cannot deserialize instance of " errors.	02405366
Corrected a sorting issue with the Top 100 Interfaces by Bandwidth Daily report. All columns should now sort as expected.	02409186
Fixed an issue where nested RADIUS attributes to send variable values can get lost on auth requests due to exceptions on multi-threaded access of the attribute token list.	02420144
Addressed vulnerability reported by Nessus Plugin ID 42424 - CGI Generic SQL Injection (blind).	02439830
Information Criteria in Custom Criteria Alarms now correctly displays the selected information phrases.	02441764
Corrected a sorting issue with the Top APs panel on the Wireless Dashboard. All columns should now sort as expected.	02451951
NBI pre-registration useDiscoveredIP has been added back in. If set, ZTP+ will use the discovered IP and management interface for configuration.	02455391
ERS devices no longer show an alert for archive configurations that are different when there is no change.	02457903
Addressed issue with compliance never running. EXOS File transfers had a 2 hour timeout for each file being transferred in the configuration backup. The timeout has been reduced to 10 minutes per file being requested to transfer which is configurable in the EXOS scripts.	02458061 02474298

ExtremeControl CFDs Addressed	**ID**
The "User Name" column in the "User Sessions" table was not displaying the value read from the switch via SNMP if there was no End-System associated with the session in the Access ControlEnd-System Cache.	02250584
Access Control portal and admin web pages now include X-Frame-Options in response headers to prevent clickjacking attacks.	02280709
TCP/ UDP port rules, which also include an IP subnet, were being enforced to devices with the incorrect CIDR prefix bits.	02380479

Import entries to Access Control rule component groups fail if import file references existing groups that are not the same type as the import.	02400374
Single port TCP/UDP rules with the same type and direction (e.g. TCP Destination) within the same policy were collapsed to one rule when enforced to a device.	02403536
New Access Control profiles are created with quarantine policy disabled and unchecked until assessment is enabled.	02409737
Deleting user group to end-system group mapping in the captive portal caused exceptions and failures to save changes.	02410842
LDAP connections test fails if URL contains uppercase letters such as LDAP://<IP_Address>:389	02434205
Fixed failure to display advanced locations in Access Control when the associated captive portal configuration is missing.	02436336
Upgrades or a database import/restore prevents displays of the Access Control UI due to missing type data in the captive portals.	02437531
Addressed issue when unsupported NTP timezone were selected for Access Control Engine	02452914
Fixed issue where editing custom fields in the captive portal caused the portal UI to hang.	02468666
Filtering on the Access Control end-system table Authorization column with table in Live mode threw exceptions in the server log.	02475657
AAA rule evaluation used wrong LDAP Configuration for Registration (Auth & Admin)	02412769 02420742
Windows 11 Operating System fingerprint detection has been added.	02456240 02455032

3.2 Known Issues Addressed in 21.11.10

ExtremeCloud IQ - Site Engine Issues Addressed
XIQ-SE did not support VPEX ports on with slot numbers above 128.
Addressed an issue when the workflow or script was executed by Netsight Server (e.g. through scheduler) the NBI calls returned empty response.

Limitation: If a user name happen to have string "@" in it, it will be incorrectly replaced with '@' character. This could cause unintended behavior.
Legacy landing page with legacy java applications was removed. The https://<Server>:8443/Clients/index.jsp redirects to current GUI
When Site Engine is onboarded to ExtremeCloud IQ, the VIQ ID is now added to the `server.log`
The link to start FlexView Editor is now called FlexView Editor / MIB Tools to reflect the fact that MIB Tools and FlexView editor features are merged and available at Administration --> Diagnostics --> Server --> Server Utilities

ExtremeControl Issues Addressed
The Filter-Id was added to "Extreme VOSS - Per-User ACL". The Policy column in the End Systems table will display the Policy name if the "Extreme VOSS - Per-User ACL" is used

3.3 Vulnerabilities Addressed

This section presents the vulnerabilities addressed in ExtremeCloud IQ - Site Engine 21.11.10

The following vulnerabilities were addressed in the ExtremeCloud IQ - Site Engine images:

- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5073-1)**

  CVE-2021-3653, CVE-2021-3612, CVE-2021-3656, CVE-2021-38160, CVE-2021-34693

- **Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5071-2)**

  CVE-2021-3612, CVE-2021-22543, CVE-2020-36311, CVE-2021-3653, CVE-2021-3656

- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5091-1)**

  CVE-2021-38199, CVE-2021-3679, CVE-2021-38160, CVE-2021-33624, CVE-2021-38204,CVE-2021-37576

- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5094-1)**

  CVE-2021-3679, CVE-2021-37576, CVE-2021-38205, CVE-2021-3732, CVE-2021-22543, CVE-2021-38204

- **Ubuntu Security Notification for Squashfs-Tools Vulnerability (USN-5057-1)**
  CVE-2021-40153
- **Ubuntu Security Notification for GNU cpio Vulnerability (USN-5064-1)**
  CVE-2021-38185
- **Ubuntu Security Notification for Git Vulnerability (USN-5076-1)**
  CVE-2021-40330
- **Ubuntu Security Notification for Apport Vulnerabilities (USN-5077-1)**
  CVE-2021-3709, CVE-2021-3710
- **Ubuntu Security Notification for Squashfs-Tools Vulnerability (USN-5078-1)**
  CVE-2021-41072
- **Ubuntu Security Notification for curl Vulnerabilities (USN-5079-1)**
  CVE-2021-22946, CVE-2021-22947, CVE-2021-22945
- **Ubuntu Security Notification for Vim Vulnerabilities (USN-5093-1)**
  CVE-2021-3778, CVE-2021-3796, CVE-2021-3770
- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5044-1)**
  CVE-2021-3587, CVE-2021-3573, CVE-2021-3564
- **Ubuntu 18.04 LTS / 20.04 LTS / 21.04: OpenSSL vulnerabilities (USN-5051-1)**
  CVE-2021-3711, CVE-2021-3712
- **Ubuntu 18.04 LTS / 20.04 LTS: GNU binutils vulnerabilities (USN-5124-1)**
  CVE-2020-16592, CVE-2021-3487
- **Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 21.04: GD library vulnerabilities (USN-5068-1)**
  CVE-2017-6363, CVE-2021-38115, CVE-2021-40145
- **Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-5114-1)**
  CVE-2020-3702, CVE-2021-38198, CVE-2021-40490
- **Ubuntu 18.04 LTS / 20.04 LTS / 21.04: Libgcrypt vulnerabilities (USN-5080-1)**
  CVE-2021-33560, CVE-2021-40528

- **Ubuntu 18.04 LTS / 20.04 LTS: Linux kernel vulnerabilities (USN-5116-1)**

  CVE-2020-3702, CVE-2021-3732, CVE-2021-38198, CVE-2021-38205, CVE-2021-40490

- **Ubuntu 18.04 LTS: OpenSSL vulnerability (USN-5051-3)**

  CVE-2021-3712

The following vulnerabilities were addressed Fabric Manager:

- **Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 / 21.04: libxml2 vulnerabilities (USN-4991-1)**

  CVE-2017-8872, CVE-2019-20388, CVE-2020-24977, CVE-2021-3516, CVE-2021-3517, CVE-2021-3518, CVE-2021-3537, CVE-2021-3541

- **Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-4907-1)**

  CVE-2018-13095, CVE-2021-3347, CVE-2021-3348

- **Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-4916-1)**

  CVE-2021-3493, CVE-2021-29154

- **149410 - Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-4946-1)**

  CVE-2021-20292, CVE-2021-26930, CVE-2021-26931, CVE-2021-28038, CVE-2021-28688, CVE-2021-29264, CVE-2021-29265, CVE-2021-29650, CVE-2021-30002

- **150155 - Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-4979-1)**

  CVE-2020-25670, CVE-2020-25671, CVE-2020-25672, CVE-2020-25673, CVE-2021-3428, CVE-2021-3483, CVE-2021-28660, CVE-2021-28964, CVE-2021-28971, CVE-2021-28972, CVE-2021-29647, CVE-2021-31916, CVE-2021-33033

- **Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-5018-1)**

  CVE-2020-24586, CVE-2020-24587, CVE-2020-26139, CVE-2020-26147, CVE-2020-26558, CVE-2021-0129, CVE-2021-23134, CVE-2021-31829, CVE-2021-32399, CVE-2021-33034, CVE-2021-33200, CVE-2021-33909

- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5073-1)**

  CVE-2021-3653, CVE-2021-3612, CVE-2021-3656, CVE-2021-38160, CVE-2021-34693

- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5094-1)**
  CVE-2021-3679, CVE-2021-37576, CVE-2021-38205, CVE-2021-3732, CVE-2021-22543, CVE-2021-38204
- **Ubuntu 18.04 LTS / 20.04 LTS / 20.10 / 21.04: LZ4 vulnerability (USN-4968-1)**
  CVE-2021-3520
- **Ubuntu 18.04 LTS / 20.04 LTS / 20.10 / 21.04: libx11 vulnerability (USN-4966-1)**
  CVE-2021-31535
- **Ubuntu 18.04 LTS / 20.04 LTS / 21.04: OpenSSL vulnerabilities (USN-5051-1)**
  CVE-2021-3711, CVE-2021-3712
- **Ubuntu 18.04 LTS / 20.04 LTS: GNU binutils vulnerabilities (USN-5124-1)**
  CVE-2020-16592, CVE-2021-3487
- **Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 / 21.04: Intel Microcode vulnerabilities (USN-4985-1)+**
  CVE-2020-24489, CVE-2020-24511, CVE-2020-24512, CVE-2020-24513
- **Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10: Nettle vulnerability (USN-4906-1)+**
  CVE-2021-2030
- **Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10: curl vulnerabilities (USN-4898-1)+**
  CVE-2021-22876, CVE-2021-22890
- **Ubuntu Security Notification for Vim Vulnerabilities (USN-5093-1)**
  CVE-2021-3778, CVE-2021-3796, CVE-2021-3770
- **Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-4883-1)+**
  CVE-2021-27363, CVE-2021-27364, CVE-2021-27365
- **Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-5003-1)+**
  CVE-2021-3600, CVE-2021-3609, CVE-2021-23133
- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5044-1)**
  CVE-2021-3587, CVE-2021-3573, CVE-2021-3564
- **Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-5114-1)+**
  CVE-2020-3702, CVE-2021-38198, CVE-2021-40490

- **Ubuntu 18.04 LTS / 20.04 LTS / 20.10 / 2104: systemd vulnerabilities (USN-5013-1)+**
  CVE-2020-13529, CVE-2021-33910
- **Ubuntu 18.04 LTS / 20.04 LTS / 20.10 : OpenSSL vulnerability (USN-4891-1)+**
  CVE-2021-3449
- **Ubuntu Security Notification for Apport Vulnerabilities (USN-5077-1)**
  CVE-2021-3709, CVE-2021-3710
- **Ubuntu Security Notification for GNU cpio Vulnerability (USN-5064-1)**
  CVE-2021-38185
- **Ubuntu 18.04 LTS / 20.04 LTS / 2104: Libgcrypt vulnerabilities (USN-5080-1)**
  CVE-2021-33560, CVE-2021-40528
- **Ubuntu 18.04 LTS / 20.04 LTS / 2104: curl vulnerabilities (USN-5021-1)+**
  CVE-2021-22898, CVE-2021-22924, CVE-2021-22925
- **Ubuntu Security Notification for curl Vulnerabilities (USN-5079-1)**
  CVE-2021-22946, CVE-2021-22947, CVE-2021-22945
- **Ubuntu 18.04 LTS / 20.04 LTS / 2104: OpenSSL vulnerabilities (USN-5051-1)**
  CVE-2021-3711, CVE-2021-3712

The following vulnerabilities were addressed in the ExtremeControl engine image:

- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5073-1)**
  CVE-2021-3653, CVE-2021-3612, CVE-2021-3656, CVE-2021-38160, CVE-2021-34693
- **Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5071-2)**
  CVE-2021-3612, CVE-2021-22543, CVE-2020-36311, CVE-2021-3653, CVE-2021-3656
- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5091-1)**
  CVE-2021-38199, CVE-2021-3679, CVE-2021-38160, CVE-2021-33624, CVE-2021-38204, CVE-2021-37576
- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5094-1)**
  CVE ID: CVE-2021-3679, CVE-2021-37576, CVE-2021-38205, CVE-2021-3732, CVE-2021-2254, CVE-2021-38204

- **Ubuntu Security Notification for Apache HTTP Server vulnerabilities (USN-4994-1)**
  CVE-2021-26690, CVE-2020-13950, CVE-2020-35452, CVE-2021-30641, CVE-2021-26691
- **Ubuntu Security Notification for Squashfs-Tools Vulnerability (USN-5057-1)**
  CVE-2021-40153
- **Ubuntu Security Notification for GNU cpio Vulnerability (USN-5064-1)**
  CVE-2021-38185
- **Ubuntu Security Notification for Git Vulnerability (USN-5076-1)**
  CVE-2021-40330
- **Ubuntu Security Notification for Apport Vulnerabilities (USN-5077-1)**
  CVE-2021-3709, CVE-2021-3710
- **Ubuntu Security Notification for Squashfs-Tools Vulnerability (USN-5078-1)**
  CVE-2021-41072
- **Ubuntu Security Notification for curl Vulnerabilities (USN-5079-1)**
  CVE-2021-22946, CVE-2021-22947, CVE-2021-22945
- **Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5090-1)**
  CVE-2021-36160, CVE-2021-40438, CVE-2021-34798, CVE-2021-33193, CVE-2021-39275
- **Ubuntu Security Notification for Vim Vulnerabilities (USN-5093-1)**
  CVE-2021-3778, CVE-2021-3796, CVE-2021-3770
- **Ubuntu Security Notification for PostgreSQL vulnerabilities (USN-5038-1)**
  CVE-2021-3677, CVE-2021-3449
- **Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5044-1)**
  CVE-2021-3587, CVE-2021-3573, CVE-2021-3564
- **Ubuntu 18.04 LTS / 20.04 LTS / 2104: OpenSSL vulnerabilities (USN-5051-1)**
  CVE-2021-3711, CVE-2021-3712
- **Ubuntu 18.04 LTS / 20.04 LTS: GNU binutils vulnerabilities (USN-5124-1)**
  CVE-2020-16592, CVE-2021-3487

- **Ubuntu 16.04 LTS / 18.04 LTS: Linux kernel vulnerabilities (USN-5114-1)**
  CVE-2020-3702, CVE-2021-38198, CVE-2021-40490
- **Ubuntu 18.04 LTS / 20.04 LTS / 21.04: Libgcrypt vulnerabilities (USN-5080-1)**
  CVE-2021-33560, CVE-2021-40528
- **Ubuntu 18.04 LTS / 20.04 LTS: Linux kernel vulnerabilities (USN-5116-1)**
  CVE-2020-3702, CVE-2021-3732, CVE-2021-38198, CVE-2021-38205, CVE-2021-40490
- **Ubuntu 18.04 LTS: OpenSSL vulnerability (USN-5051-3)**
  CVE-2021-3712

4. Installation, Upgrade, and Configuration Changes

4.1 Installation Information

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

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

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

- Pilot
- Navigator
- No License

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

For complete installation instructions, refer to the Documentation web page:XIQSE_21.11.10_Installation_Guide.pdf

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.

4.1.1 Installing Without an Internet Connection

If your Linux system requires an operating system upgrade, you are prompted to upgrade using either an internet connection or locally (without an internet connection) if no additional Ubuntu packages need to be installed.

```
!!! ATTENTION !!!

We can attempt to upgrade the OS without using the internet if
there were no extra Ubuntu packages installed. If there were
extraneous packages installed, the upgrade will fail with this
method.

Do you want to attempt a local in-place upgrade of the OS and
reboot when complete? (Y/n)
```

4.1.2 Custom FlexViews

When reinstalling 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.

4.1.3 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.

4.2 Important Upgrade Considerations

ExtremeCloud IQ - Site Engine version 21.11.10 supports two different upgrade strategies.

- Air Gap mode supports upgrades from Extreme Management Center versions 8.4.4, 8.5.6.
- Connected mode supports upgrades from ExtremeCloud IQ - Site Engine versions 21.04.10, 21.09.10, or Extreme Management Center versions 8.4.4 or 8.5.6.

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 21.11.10.

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 21.11	Upgrade to ExtremeCloud IQ - Site Engine version 21.11
	8.17	8.3.3	8.4.4	8.5.6		
ExtremeCloud IQ - Site Engine version 2104 and version 2109					X	
Extreme Management Center version 8.5.5, 8.5.6					X	X

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 21.1	Upgrade to ExtremeCloud IQ - Site Engine version 21.1
	8.1.7	8.3.3	8.4.4	8.5.6		
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 8.1x		X		X	X	X
NetSight version 7.1or older	X	X		X	X	X

*These versions can be updated to either version 8.4.4, 8.5.5, or 8.5.6, and then to ExtremeCloud IQ - Site Engine version 21.11.10.

IMPORTANT: When performing an upgrade, be sure to back up the database prior to performing the upgrade, and save it to a safe location. Use the **Administration** > **Backup/ Restore** tab to perform the backup.

- When upgrading the ExtremeCloud IQ - Site Engine server, ExtremeAnalytics engine, or ExtremeControl engine to version 21.11.10, ensure the DNS server IP address is correctly configured.
- When upgrading to ExtremeCloud IQ - Site Engine version 21.11.10, if you adjusted the ExtremeCloud IQ - Site Engine memory settings and want them to be saved on upgrade, a flag (`-DcustomMemory`) needs to be added to the `/usr/local/Extreme_Networks/NetSight/services/nsserver.cfg` file.

  For example:
  ```
  -Xms12g -Xmx24g -XX:HeapDumpPath=../../nsdump.hprof -XX:+HeapDumpOnOutOfMemoryError -XX:MetaspaceSize=128m -DcustomMemory
  ```
- If your network is using ExtremeAnalytics or ExtremeControl engines, Fabric Manager, or another add-on feature, you must first perform the ExtremeCloud IQ - Site Engine upgrade to version 21.11.10 and then add the feature.

4.2.1 License Renewal

Upgrading to ExtremeCloud IQ - Site Engine version 21.11.10 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.

4.2.2 Free Space Consideration

When upgrading to ExtremeCloud IQ - Site Engine version 21.11.10, a minimum of 15 GB of free disk space is required on the ExtremeCloud IQ - Site Engine server.

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.

4.2.3 Site Discover Consideration

Discovering devices via the **Site** tab using a **Range**, **Subnet**, or **Seed** discover might not successfully add all expected devices. To correct the issue, increase the **Length of SNMP Timeout** value on the **Administration** > **Options** > **Site** tab in the Discover First SNMP Request section.

4.3 ExtremeAnalytics Upgrade Information

Enabling or disabling the disk flow export feature might cause enforce operations to time out. Enforcing again resolves the issue.

When you delete an ExtremeXOS device that is configured as a flow source via the Flow Sources table of the **Analytics** > **Configuration** > **Engines** > **Configuration** tab from the Devices list on the **Network** > **Devices** tab, an error message is generated in the `server.log`. The message does not warn you that the device is in use as a flow source. Adding the device back in the Devices list on the **Network** > **Devices** tab or removing the device from the Flow Source table fixes the issue.

The Flow Sources table on the **Analytics** > **Configuration** > ***engine*** > **Configuration** tab may take a few minutes to load.

4.4 ExtremeControl Upgrade Information

4.4.1 General Upgrade Information

You are not required to upgrade your ExtremeControl engine version to 21.11.10 when upgrading to ExtremeCloud IQ - Site Engine 21.11.10. However, both ExtremeCloud IQ - Site Engine and ExtremeControl engine must be at version 21.11.10 in order to take advantage of the new ExtremeControl 21.11.10 features. ExtremeCloud IQ - Site Engine 21.11.10 supports managing ExtremeControl engine versions 8.4, 8.5, 21.4.10, 21.09.10, and 21.11.10.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, you should also upgrade your assessment agent adapter to version 21.11.10 if you upgrade to ExtremeControl version 21.11.10.

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

4.4.2 ExtremeControl Version 8.0 and later

Beginning in version 8.0, ExtremeControl may fail to join Active Directory when accessing as a **Standard Domain User with Descendant Computer Objects ("Reset password" permissions only)** group member.

To allow this functionality, add the following permissions:

- **Reset Password**
- **Validated write to DNS host name**
- **Validated write to service principal**
- **Read and write account restrictions**
- **Read and write DNS host name attributes**
- **Write servicePrincipalName**

4.4.3 Other Upgrade Information

Immediately after you install version 21.11.10 on the ExtremeControl engine, the date and time does not properly synchronize and the following error message displays:

```
WARNING: Unable to synchronize to a NTP server. The time might
not be correctly set on this device.
```

Ignore the error message and the date and time automatically synchronize after a short delay.

Additionally, the following message might display during the ExtremeControl upgrade to version 21.11.10:

No domain specified

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

4.5 Fabric Configuration Information

4.5.1 Certificate

Fabric Manager might be unavailable via 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.

4.5.2 Authentication Key

When you provision authentication keys for Fabric Attach, the key cannot be read back for security reasons. When the key is read from the device, it always shows "****". For this reason, it might seem that there is a configuration mismatch when one does not exist.

4.5.3 Service Configuration Change

If you change a configured service via the **Configure Device** window that references one of the following, and then enforce those changes to the device, the configuration on the device might change unexpectedly:

- MLT
- SMLT
- Port-specific settings to a port belonging to an MLT or SMLT

To prevent this merge, change rows in the **Enforce Preview** window where MLT or SMLT are in use from **Current** to **Desired**.

To correct the issue after enforcement, modify the service on the device via the CLI.

4.5.4 CLIP Addresses

Using the CLIP Addresses table in the Configure Device window, you can enter addresses in both IPv4 and IPv6 formats. However, ExtremeCloud IQ - Site Engine version 21.11.10 only supports applying a single address (either IPv4 or IPv6) to a Loopback Interface.

4.5.5 Gateway Address Configuration Change

In versions of ExtremeCloud IQ - Site Engine prior to 21.11.10, the Default Gateway IP Address is configured as part of the VLAN. In 21.11.10, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 21.11.10, merge any **Default Gateway IP Addresses** from the device into the configuration of ExtremeCloud IQ - Site Engine to prevent incorrect configuration of the device.

4.5.6 Upgrading VSP-8600

When upgrading from Extreme Management Center version 8.2 to version 8.3. manually reload previously discovered VSP-8600 devices to gain access to Fabric Connect features.

4.5.7 Removing Fabric Connect Configuration

Removing a device's Fabric Connect configuration by setting the **Topology Definition** to **<None>** may fail if the device has Logical Interfaces assigned to ISIS.

4.5.8 Password Configuration

Fabric Manager fails to onboard in 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.

4.5.9 VRF Configuration

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

4.6 Device Configuration Information

4.6.1 VDX Device Configuration

To properly discover interfaces and links for VDX devices in 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.

4.6.2 VOSS Device Configuration

Topology links from VOSS devices to other VOSS 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 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 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.

4.6.3 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.

4.6.4 SLX Device Configuration

When creating a ZTP+ Configuration for an SLX 9240 on which firmware version 18s.01.01 or 18s.01.02 is installed, the ZTP+ process fails if the **Administration Profile** value uses SSH or Telnet CLI credentials. 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**.

4.6.5 ExtremeXOS Device Configuration

ExtremeXOS devices on which firmware version 30.3.1.6 is installed do not download and install new firmware versions successfully via the ZTP+ process. To correct the issue, access the **Network** > **Firmware** tab in 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**.

4.7 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

4.8 Wireless Manager Upgrade Information

A High Availability pair cannot be added as a flow source if the WLAN(s) selected are not in common with both wireless controllers.

5. System Requirements

IMPORTANT: Wireless event collection is disabled by default in version 21.11.10 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 21.11.10.

5.1 ExtremeCloud IQ - Site Engine Server and Client OS Requirements

5.1.1 ExtremeCloud IQ - Site Engine Server Requirements

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

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 vSphere (client only)™
Microsoft®Hyper-V (ExtremeCloud IQ - Site Engine Virtual Engine)	Windows®Server 2012 R2 Windows®Server 2016

5.1.2 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

5.2 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.

5.2.1 ExtremeCloud IQ - Site Engine Server Requirements

Specifications	Small	Medium	Enterprise	Large Enterprise
Total CPUs	1	2	2	2

Specifications	Small	Medium	Enterprise	Large Enterprise
Total CPU Cores	8	16	24	24
Memory	16 GB	32 GB	64 GB	64 GB
Disk Size	240 GB	480 GB	960 GB	192 TB
IOPS	200	200	10,000	10,000
Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
ExtremeAnalytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

IMPORTANT: For optimal performance the CPU and Memory needs to reserved in the ESX Client and the virtual machine needs to be deployed using Thick Disk provisioning.

5.2.2 ExtremeCloud IQ - Site Engine Client Requirements

Specifications	Requirements
CPU Speed	3.0 GHz Dual Core Processor
Memory	8 GB (4 GB for 32-bit OS)
Disk Size	300 MB (User's home directory requires 50 MB for file storage)
Java Runtime Environment (JRE) (Oracle Java only)	Version 8
Browser[1](Enable JavaScript and Cookies)	Microsoft Edge (version 41.16.199.10000.0 in compatibility mode) Mozilla Firefox (version 34 or later[2]) Google Chrome (version 33.0 or later)

[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.

5.3 Virtual Engine Requirements

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

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

IMPORTANT: For ESX and Hyper-V servers configured with AMD processors, the Extreme ExtremeAnalytics virtual engine requires AMD processors with at least Bulldozer based Opterons.

5.3.1 ExtremeCloud IQ - Site Engine Virtual Engine Requirements

Specifications	Small	Medium	Large
Total CPU Cores	8	16	24
Memory	16 GB	32 GB	64 GB
Disk Size	240 GB	480 GB	960 GB
IOPS	200	200	10,000

Recommended scale based on server configuration:			
Maximum APs	250	2,500	25,000
Maximum Wireless MUs	2,500	25,000	100,000
Maximum Managed Devices	100	1,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000
Statistics Retention (Days)	90	180	180
ExtremeAnalytics	No	Yes	Yes
MU Events	No	Yes	Yes

IMPORTANT: For optimal performance the CPU and Memory needs to reserved in the ESX Client and the virtual machine needs to be deployed using Thick Disk provisioning.

5.3.2 ExtremeControl Virtual Engine Requirements

Specifications	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	16 GB	32 GB
Disk Size	40 GB	120 GB	120 GB
IOPS	200	200	200

Specifications	Small	Medium	Enterprise
Recommended scale based on server configuration:			
ExtremeControl End-Systems	3,000	6,000	9,000/ 12,000[1]
Authentication	Yes	Yes	Yes
Captive Portal	No	Yes	Yes/ No[1]
Assessment	No	Yes	No

[1]The Enterprise ExtremeControl engine configuration supports two different scale options:

- Up to 9,000 end-systems if your network uses Captive Portal functionality.
- Up to 12,000 end-systems if your network does not use Captive Portal functionality.

IMPORTANT: For optimal performance the CPU and Memory needs to reserved in the ESX Client and the virtual machine needs to be deployed using Thick Disk provisioning.

5.3.3 ExtremeAnalytics Virtual Engine Requirements

Specifications	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	32 GB	64 GB
Disk Size	40 GB	480 GB	960 GB
IOPS	200	10,000	10,000
Recommended scale based on server configuration:			
Flows Per Minute	250,000	500,000	750,000
End-Systems	10,000	20,000	30,000

IMPORTANT: The ESXi free license supports a maximum of 8 CPU cores, and the medium and enterprise ExtremeAnalytics virtual engine installations require 16 CPU cores. Sixteen CPU cores are only available by purchasing a permanent license. To use the ExtremeAnalytics virtual engine with an ESXi free license, adjust the number of CPU cores to 8.

To reduce the possibility of impaired functionality, ensure at least 4 GB of swap space is available for flow storage on the ExtremeAnalytics virtual engine. To verify the amount of available RAM on your Linux system, use the `free` command

Extreme Application Sensor Engine Virtual Engine Requirements

OVA	CPUs	Memory (GB)	Disk (GB)	Maximum Number of Monitoring Interfaces Supported
Small	8	12	40	1
Medium	16	24	440	2
Large	24	36	960	3

5.3.4 Fabric Manager Requirements

Specifications	Requirements
Total CPU Cores	4
Memory	9 GB
Memory allocated to Java:	
-Xms	4 GB
-Xmx	6 GB
Disk Size	60 GB

5.4 ExtremeControl Agent OS Requirements

The table below outlines the supported operating systems for end-systems connecting to the network through an ExtremeControl deployment that is implementing agent-based assessment. Additionally, the end-system must support the operating system disk space and memory requirements as provided by Microsoft® and Apple®.

Manufacturer	Operating System	Operating System Disk Space	Available/ Real Memory
Windows[1]	Windows Vista Windows XP Windows 2008 Windows 2003 Windows 7 Windows 8 Windows 8.1 Windows 10	80 MB	40 MB (80 MB with Service Agent)
Mac OS X	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.

5.5 ExtremeControl Supported End-System Browsers

The following table outlines the supported desktop and mobile end-system browsers connecting to the network through the Mobile Captive Portal of Extreme Networks ExtremeControl.

Medium	Browser	Version
Desktop	Microsoft Edge	41and later
	Microsoft Internet Explorer	11and later
	Mozilla Firefox	34 and later
	Google Chrome	33.0 and later
Mobile	Internet Explorer Mobile	11and later (Windows Phone)
	Microsoft Edge	All versions
	Microsoft Windows 10 Touch Screen Native (Surface Tablet)	N/A
	iOS Native	9 and later
	Android Chrome	4.0 and later
	Android Native	4.4 and later
	Dolphin	All versions
	Opera	All versions

NOTES: A native browser indicates the default, system-installed browser. Although this might be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection for a device. Typically, this is a non-configurable option for Wi-Fi Captive Network Detection, but default Android, Microsoft and iOS devices are tested for compatibility with the Mobile Captive Portal.

A mobile device can access the standard (non-mobile) version of the Captive Portal using any desktop-supported browsers available on a mobile device.

For other browsers, the Mobile Captive Portal requires the browser on the mobile device to be compatible with Webkit or Sencha Touch.

To confirm compatibility with Webkit or Sencha Touch, open `http://<ExtremeControl Engine IP>/mobile_screen_preview` using your mobile web browser.

- If the browser is compatible, the page displays properly.
- If the browser is not compatible with the Mobile Captive Portal, the following error displays:

5.6 ExtremeControl Engine Version Requirements

For complete information on ExtremeControl engine version requirements, see the ExtremeCloud IQ - Site Engine Version 21.11.10 Release Notes section of these Release Notes.

5.7 ExtremeControl VPN Integration Requirements

VPN concentrators are supported for use in ExtremeControl VPN deployment scenarios.

- Supported Functionality: Authentication and Authorization (policy enforcement)
  Cisco ASA
  Enterasys XSR
- Supported Functionality: Authentication
  Juniper SA (requires an S-Series Stand Alone (SSA) system in order to provide access control)

NOTE: For all ExtremeControl VPN Deployment scenarios, an S-Series Stand Alone (SSA) system is required to change authorization levels beyond the initial authorization, such as when using assessment.

5.8 ExtremeControl SMS Gateway Requirements

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

- Clickatell
- Mobile Pronto

5.9 ExtremeControl SMS Text Messaging Requirements

The following mobile service providers are supported by default for SMS text messaging in an ExtremeControl deployment. Additional service providers can be added:

AT&T	Sprint PCS
Alltel	SunCom
Bell Mobility (Canada)	T-Mobile
Cingular	US Cellular
Metro PCS	Verizon
Rogers (Canada)	Virgin Mobile (US and Canada)

5.10 ExtremeAnalytics Requirements

To use an ExtremeSwitching X440-G2 switch as an Application Telemetry source for ExtremeAnalytics, install firmware version `22.4.1.4-patch2-5` or higher.

5.11 Ekahau Maps Requirements

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

5.12 Guest and IoT Manager Requirements

5.12.1 Guest and IoT Manager Server OS Requirements

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

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

5.12.2 Guest and IoT Manager Outlook Add-in Client Requirements

These are the requirements for the Client Machines, which need to run Guest and IoT Manager Outlook Add-in.

Manufacturer	Operating System
Windows[1]	Windows 7 Windows 10
Mac OS X	Sierra High Sierra Mojave

[1]Microsoft® Outlook® 2016 is needed on Windows/Mac clients for the add-in to operate.

5.12.3 Guest and IoT Manager Virtual Engine Requirements

The VMWare Guest and IoT Manager virtual engines are packaged in the .OVA file format (defined by VMware) and needs an x86, 64-bit capable environment

Specifications	Minimum	Recommended
Total CPU Cores	2	4
Memory	2 GB	4 GB
Disk Size	80 GB	80 GB
Interfaces	1Physical NIC	3 Physical NICs

5.12.4 Guest and IoT Manager Supported Browsers

The following table outlines the supported desktop and mobile browsers that can be used to launch Guest and IoT Manager Admin and Provisioner Web Application:

Medium	Browser	Version
Desktop	Microsoft Internet Explorer Mozilla Firefox Google Chrome Microsoft Edge Safari	11and 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.

6. Getting Help

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

Extreme Portal
: Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.

The Hub
: Connect with other Extreme customers, ask or answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

GTAC
: For immediate support, call 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products

- A description of the failure
- A description of any action already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers