ExtremeCloud™ IQ - Site Engine
Release Notes
Version 21.09.10

10/2021
9037048-01 Rev AA

Table of Contents

ExtremeCloud IQ - Site Engine Version 21.09.10 Release Notes

21.09.10.00
October 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 21.09.10 consumes licenses from ExtremeCloud IQ. 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.
- 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 21.09.10 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.

NOTES: If you re-initialize the database, then a new serial number is created and you need to onboard the new ExtremeCloud IQ - Site Engine to ExtremeCloud IQ. The serial number is part of the database backup.

If you restore your database, using the Administration > Backup/Restore > Restore Initial Database feature, after the database was reinitialized, then ExtremeCloud IQ - Site Engine will use the serial number from the backup. The ExtremeCloud IQ - Site Engine with not used serial number can be deleted from ExtremeCloud IQ.

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 21.09.10, the licensing and capabilities of ExtremeControl does not change. For new users that complete an initial install of ExtremeCloud IQ - Site Engine, ExtremeControl licensing does not include end-system capabilities.

NOTES: Access to ExtremeCloud IQ - Site Engine requires access to https://extremecloudiq.com and its subdomains, and an ExtremeCloud IQ account is required.

Air gapped mode (where ExtremeCloud IQ - Site Engine is not connected to ExtremeCloud IQ) is not supported for ExtremeCloud IQ - Site Engine version 21.09.10.

Onboarding ExtremeCloud IQ - Site Engine from ExtremeCloud IQ

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 21.09.10

New features and enhancements are added to the following areas in ExtremeCloud IQ - Site Engine version 21.09.10:

- ExtremeCloud IQ - Site Engine
- ExtremeConnect
- 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

- Ability to Log In to ExtremeCloud IQ - Site Engine via Single Sign On from ExtremeCloud IQ
- Additional Filtering and Reporting for Devices Onboarded to ExtremeCloud IQ
- Enhancements to Authorization Capabilities
- New APs Now Supported
- Enhancements to Port Templates
- ZTP+ Enhancements

Ability to Log In to ExtremeCloud IQ - Site Engine via Single Sign On from ExtremeCloud IQ

You can now access ExtremeCloud IQ – Site Engine to manage devices from the ExtremeCloud IQ Devices list without needing to log in to ExtremeCloud IQ – Site Engine. The Authorization Group in ExtremeCloud IQ – Site Engine for the user is inherited from the User Role in ExtremeCloud IQ. ExtremeCloud IQ - Site Engine creates corresponding User Roles automatically when it is onboarded to ExtremeCloud IQ. After the roles are automatically created, they can be modified.

Additional Filtering and Reporting for Devices Onboarded to ExtremeCloud IQ

When a device is onboarded to ExtremeCloud IQ, it is automatically added to a Cloud Configuration Group in ExtremeCloud IQ for each Device Group the device is a member of in ExtremeCloud IQ - Site Engine. A Cloud Configuration Group is also created for all devices onboarded from the specific ExtremeCloud IQ - Site Engine. This Cloud Configuration Group is prefixed with "XIQSE-" and is denoted by the hostname of ExtremeCloud IQ - Site Engine. Cloud Configuration Groups are updated when devices are added to User Device Groups (either by user action or by API call). Cloud Configuration Groups are also updated when devices are removed from a User Device Group or deleted from ExtremeCloud IQ - Site Engine.

Enhancements to Authorization Capabilities

Capabilities in ExtremeCloud IQ - Site Engine are enhanced in the following ways:

- Via the Basic Category, ExtremeCloud IQ - Site Engine can now resolve dependencies in capabilities when you create Authorization Groups.
- Authorization Group capabilities for the Northbound Interface are reorganized to give more granularity for Administration, Inventory, Network, and Workflows queries and mutations.

- You can now configure capabilities in Authorization Groups for Authentication and RADIUS Configuration functionality.
- You can now configure capabilities in Authorization Groups for Administration > Certificates tab functionality.
- You can now configure capabilities in Authorization Groups to view and configure Device Types.

IMPORTANT: After upgrading from a previous version of Extreme Management Center or ExtremeCloud IQ - Site Engine, verify the capabilities enabled for your Authorization Groups are properly configured.

New APs Now Supported

ExtremeCloud IQ - Site Engine now supports the following APs:

- AP4000/U
- AP302W

Enhancements to Port Templates

A new global port template, AutoSense, is available and automatically mapped through ZTP+ Automated Templates to all ports for 5x00 series switches on which the VOSS operating system is installed. Additionally, port templates now support SLPP, SLPP Guard, LSPP Guard Timer, and Span Guard for devices on which the VOSS operating system is installed.

ZTP+ Enhancements

The following features were added to ZTP+ device defaults for VOSS version 8.4 and later:

- Telnet
- SSH (Feature is always enabled on the switch regardless of Device Protocol > SSH option value.)
- HTTP
- HTTPS (Feature is enabled on the switch when the HTTP feature is enabled.)
- LACP
- FTP

Additionally, VOSS devices now also support the ZTP+ RMA feature.

Ability to Align Collection Interval with ExtremeCloud IQ

ExtremeCloud IQ collects data points at a 10 minute interval to create graphical displays of Port and Device statistics. If ExtremeCloud IQ - Site Engine is currently collecting data at an interval longer than 10 minutes, you can now align the collection interval with ExtremeCloud IQ via the Administration > Diagnostics > System > ExtremeCloud IQ Summary > Align Collection Interval feature. Selecting this feature improves the appearance of the ExtremeCloud IQ graphs, but it also increases the SNMP traffic on your network and requires more disk space for your ExtremeCloud IQ - Site Engine database.

Additional Trap Definitions Available

ExtremeCloud IQ - Site Engine version 21.9.10 includes 235 new SNMP trap definitions for MLXe, VDX, SLX devices.

Ability to Configure Routed Split Multi-Link Trunking on VLANs

You can now configure Routed Split Multi-Link Trunking (RSMLT) as the Routing Redundancy Method on a VLAN. RSMLT is only supported on VOSS devices.

Ability to Configure DHCP Snooping and ARP Inspection on VLANs

DHCP snooping and ARP Inspection can now be configured on VOSS devices.

Improvement to VOSS I-SID and Fabric Attach FlexViews and DeviceViews

VOSS I-SID and Fabric Attached FlexViews and DeviceViews are updated with improved Name columns.

Push Fabric Attach Proxy (static ISID VLAN bindings) to ExtremeXOS Devices

L2VSN Services can be configured on ExtremeXOS version 31.4 and later.

Client API Functionality Enhancements

The following enhancements are included in ExtremeCloud IQ - Site Engine version 21.09.10 for users added via the Administration > Client API Access tab:

- A menu is added to specify the Authorization Group when adding or editing clients. In previous releases, the only capabilities available are Client API and Northbound Interface API.
- When adding clients, an Authorized User in the Administration > Users tab is automatically created and ExtremeCloud IQ - Site Engine assigns it to the Authorization Group you specify.

NOTE: When upgrading from a previous version of ExtremeCloud IQ - Site Engine, any client that was added to **Administration** > **Client API Access**, but which was not added as an authorized user in **Administration** > **Users**, will not be automatically assigned an Authorization Group. To add the client to an Authorization Group, access the **Administration** > **Client API Access**, edit the client, and select an Authorization Group from the menu. Clients in the **Client API Access** tab that were added as authorized users in the **Administration** > **Users** tab retain the Authorization Group assigned in the **Administration** > **Users** tab prior to upgrade.

Java Version Upgraded

The version of Java included with ExtremeCloud IQ - Site Engine is upgraded to 1.8.0.282.

1.2 ExtremeConnect

Intune Connect Module Now Available

The Intune Connect module is again available in ExtremeCloud IQ - Site Engine after being deprecated in a previous release.

1.3 ExtremeControl

Ability to Filter by Values Not Present in End-System Table

The End-System table can now be filtered to display only values that do not contain or does not match a value you specify. For example, you can filter the table to display all end-systems that do not contain the word "Windows" in the **Device Family** column.

End-System Zone Configuration Now Available on the Access Control Tab

The ability to configure End-System Zones, previously only available in the NAC Manager legacy java application, can now be configured via the Access Control tab. End-system zones allow you to limit an ExtremeCloud IQ - Site Engine user's access to end-system information and configuration based on end-system zone membership. Users are only authorized to view or control a subset of end-systems, delimited by zones.

RADIUS Monitor Client Functionality Now Available on the Access Control Tab

The RADIUS Monitor Client configuration, previously only available in the NAC Manager legacy java application, can now be configured via the Access Control tab. The RADIUS Monitor Client enables you to add a RADIUS monitor client server IP address and configure a server shared secret.

Ability to Collapse and Expand Rules in the Rules Table

Rules listed in ExtremeControl Configurations can now be collapsed and expanded to hide or view additional conditions, end-systems, profile, and portal details. This enables users to view more rules at once.

Advanced Rule Ordering Available for Access Control Configuration Rules

ExtremeCloud IQ - Site Engine version 21.9.10 includes the ability to change the order of Access Control Configuration Rules.

Per-User ACLs Supported for VOSS Devices

Per-User ACLs (also known as Downloadable ACLs) are now supported for VOSS platforms 8.3 or later. The policy profile and rules can be transformed to Vendor Specific Attributes in the RADIUS Access Accept message, the policy definition is now applied to the end system connected to the VOSS device.

Agent-Based Assessment Configuration Now Available in ExtremeCloud IQ - Site Engine

The ability to configure Agent-Based Assessment, previously only available in the NAC Manager legacy java application, can now be configured via the Access Control tab.

New RADIUS Attributes to Send Available for VOSS Devices

New profiles are introduced in ExtremeCloud IQ - Site Engine version 21.09.10 for VOSS Devices: Extreme VOSS - Fabric Attach and Extreme VOSS - Fabric Attach - EPT.

2. Deprecated Features

IA-ES Enterprise NAC licenses are no longer supported for Access Control engines in ExtremeCloud IQ - Site Engine version 21.9.10. Only XIQ-NAC-S licenses are supported.

Additionally, the legacy Java applications NAC Manager, Policy Manager, Inventory Manager, Console, and MibTools are deprecated.

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

3.1 Customer Found Defects Addressed in 21.09.10

ExtremeCloud IQ - Site Engine CFDs Addressed	ID
Attempting to access the **Wireless** tab was not successful and displayed a "Could not load report" error when configured as the initial view and the ExtremeCloud IQ - Site Engine license is NMS or NMS_BASE.	02385940 02335769 02406887
Authorization Group capabilities were not properly verified. Capabilities are enhanced in this release to provide users with more granularity and resolve dependencies. See the Enhancements section of the Release Notes for additional details.	02373764
If the logged in user selects the **Force reauthentication and scan (assess) End-Systems** capability, the **Force Reauthentication** and the **Force Re-authentication and Scan** capabilities were not automatically selected by ExtremeCloud IQ - Site Engine. These capabilities are now automatically selected when **Force reauthentication and scan (access) End-Systems** is selected, regardless of whether the **Access OneView Access Control Reports** capability is selected.	02369723
Creating multiple SNMP Profiles via the **Administration** > **Profiles** tab and then changing the Default Profile multiple times occasionally did not change the Default Profile to the selected Profile.	02337178
Occasionally, devices were no longer being polled by ExtremeCloud IQ - Site Engine in environments where SNMPv3 is heavily used.	02389786

The table on the **Administration** > **Profiles** tab was not paginating properly.	2399261
Changing the **Auto Group Delimeter** on the **Administration** > **Options** > **Site Engine - General** tab was not saving successfully.	02355150
The **In/Out Bandwidth** values in the Top 100 Interfaces by Bandwidth Daily report were not formatted properly.	2380003
The FlexView limit was improperly being reached and the FlexView was failing to load. To correct this issue, beginning in version 21.9.10, the cache will be cleared of oldest FlexViews and the dialog does not appear.	02366012
Changing a custom report component when a report is configured to display as a Grid was changing the display to a Chart.	2381674
FlexReports and Maps occasionally incorrectly refreshed.	2358402
A Port Template that was previously deleted and then was added back with a new template was not properly added.	2358680 2406713 2434566
System-defined port templates were able to be removed from ExtremeCloud IQ - Site Engine. They are no longer allowed to be removed.	02446435
Map Links with a Name containing more than 64 characters were unable to be saved to a map.	2367449
Attempting to change the Network Profile for multiple devices via the Configure Device window was not successful.	02351409
Power supplies for ExtremeXOS devices were not displayed in the DeviceView and the Northbound Interface.	02334994
ExtremeCloud IQ - Site Engine was not validating if the User currently logged in had "Site Write Access" Capability when performing Endpoint Location actions (for example, Add, Edit, Delete).	2308935
The Interface Details PortView values for TX, RX, and Total Utilization percent were incorrect.	02350211
Ports on which Collection Mode is configured as **Historical** were occasionally no longer configured after restarting the ExtremeCloud IQ - Site Engine server.	2350844
Map links were occasionally not displayed for Cisco devices.	2351417

Executing a CLI command via the **Execute CLI Commands** window (Tasks > CLI Commands in the Device list menu) was having timeout and timeout override issues.	02350223 02330372
The **Configure** menu option was not available on the Network > Devices tab if the Firmware/Boot PROM Upgrade Wizard capability was not selected for a user. To fix this issue, a new Configure Devices capability is added to ExtremeCloud IQ - Site Engine.	02345920
When selecting the **On** filter for the Date/Time column in a table was not displaying any results from the selected day.	2305113
Occasionally, Access Control engines incorrectly appeared down in ExtremeCloud IQ - Site Engine due to memory errors as the result of Notify Engine Timer threads accumulating.	2307751

ExtremeControl CFDs Addressed	**ID**
ExtremeControl Group pages (Control > Access Control > Group Editor) were not sorting correctly.	02341978
Sorting in the End Systems table on the **Control** tab was not consistent. To ensure consistency, the **MAC OUI VENDOR** and **SWITCH NICKNAME** columns in the End Systems table can no longer be sorted. Additionally, when the table is **Live** and the End Systems table is sorted on a column other than **Last Seen Time**, then the table changes to **Paused** to allow sorting. If you select **Live**, the table sorts on the **Last Seen Time** column in descending order.	02363512
End-systems authenticating via 802.1x were having their Username cleared if it is the MAC address.	02332925
Access Control Captive Portal custom header image files containing parentheses may fail to display in the portal pages.	02381464
Policy was failing to enforce Ethertype, IP Protocol, ICMP, ICMPv6 range rules correctly to ExtremeXOS switches.	2422608
CoS Transmit Queue configuration problems were being flagged as errors in the Enforce Preview window even when **Transmit Queue / TxQ Shaper** management was disabled in the CoS Components panel.	02384163
The DHCP discovered hostname was overwriting the DNS resolved hostname if the IP address changed for the end-system but the hostname hasn't changed.	1759185

Access Control engines had unnecessary ports open by default when Captive Portal and Assessment were not configured.	02183938
Configuring an Access Control engine to use SHA/AES for the Authentication Protocol and enforcing the engine was occasionally changing the Authentication Protocol to MD5/DES.	02227916
Access control was not timing out pooled LDAP connections. Pooled LDAP connections now have a default timeout of 5 minutes (300000 milliseconds) and can be configured on the Access Control engine in the config.properties files using the com.sun.jndi.ldap.connect.pool.timeout=<time in milliseconds> property.	01957077
Provisioner Templates in the Guest and IoT Manager Onboarding list were not sorted alphabetically.	02371257

ExtremeConnect CFDs Addressed	**ID**
The FNT Command module was not processing the end-systems connecting to an ExtremeXOS device in a stacked configuration when the Options tab was not configured.	02369490
User Names of Chrome devices were unable to be retrieved via the Google GSuite ExtremeConnect module.	2235976

ExtremeAnalytics CFDs Addressed	**ID**
After deactivating WebApp fingerprints, the Analytics engine was occasionally becoming unresponsive.	02366151
ERS devices added via application telemetry with a DHCP IP address did not appear in application flows.	02260996
Analytics dashboards were not displaying data.	02263077

3.2 Known Issues Addressed in 21.09.10

ExtremeCloud IQ - Site Engine Issues Addressed	**ID**
Changing windows and tabs in ExtremeCloud IQ - Site Engine without allowing the window or tab to fully load can cause ExtremeCloud IQ - Site Engine to become unresponsive.	-----

Adding and deleting devices occasionally caused the server to become unresponsive. This may cause unintended behavior in ExtremeCloud IQ - Site Engine and required a server reset to resolve the problem.	-----
After upgrading to ExtremeCloud IQ - Site Engine, the initial license agreement page may display incorrectly if the browser has cached the old license pages. Perform a hard refresh in your browser to correct the issue.	-----
The RMA feature was not working properly for VOSS devices using ZTP+.	-----
The Administration > Diagnostics > System > XIQ Device Message Details is renamed to ExtremeCloud IQ Device Message Details and Administration > Diagnostics > System > XIQ Summary is renamed to ExtremeCloud IQ Summary.	-----
User Device Group Names could include special characters (for example, !, #, and $) when using Mozilla Firefox, but not when using Google Chrome or Microsoft Edge. User Device Group Names can now only include alphanumeric characters as well as dash (-), underscore (_) and period (.) on all browsers. If Group Names contain other special characters, the special characters will be removed from the User Device Group Name when upgrading to version 21.9.10.	-----
The Device Group ID column was misleading as devices can be members of more than one User Device Group. The column is removed from the device grid and it no longer appears in exports of the device grid.	-----
Selecting Only server certificates matching the recorded certificate are accepted for the Certificate Trust Mode (Administration > Certificates) may result in the disconnection of ExtremeCloud IQ and certificate errors in the ExtremeCloud IQ - Site Engine server.log. As a workaround, set the Server Trust Mode to All server certificates are accepted and recorded and restart the server. On the next connection, all certificates during established connections will be accepted and recorded (retained). Accepted SSL Certificate requests will be logged in the server.log. You can then set the Server Trust Mode back to Only server certificates matching the recorded certificate are accepted and the connections succeed.	-----

When a device changes from Unmanaged to Managed after adding licenses, there was no way to apply a site's actions to the device. You can now run the Site's Add Actions for a device using the Device menu (More Actions > Run Site's Add Actions).	-----
User-defined Workflows could exist with a role of NetSight Administrator, which does not exist in ExtremeCloud IQ - Site Engine. Workflows with a role of NetSight Administrator are updated to XIQ-SE Administrator. The version is not incremented. User-defined Workflows with imported scripts with role(s) mapped to NetSight Administrator need to be updated to XIQ-SE Administrator manually.	-----
ExtremeCloud IQ - Site Engine now only onboards itself and not other instances of ExtremeCloud IQ - Site Engine in ExtremeCloud IQ. If additional instances of ExtremeCloud IQ - Site Engine were onboarded in ExtremeCloud IQ - Site Engine version 21.4.10.99, they are not automatically removed when upgrading to version 21.9.10. The additional instances need to be manually removed from ExtremeCloud IQ - Site Engine and then added again in order to remove them from ExtremeCloud IQ.	-----

ExtremeAnalytics Issue Addressed	**ID**
VOSS devices were unable to be added as Application Telemetry devices. VOSS devices now require the user to select a valid exporter IP from IPs configured on the device when adding as an Analytics Flow Source.	-----

ExtremeControl Issue Addressed	**ID**
Access Control engines no longer configure RADIUS during enforce on unmanaged switches.	-----

3.3 Vulnerabilities Addressed

This section presents the vulnerabilities addressed in ExtremeCloud IQ - Site Engine 21.09.10

- The following vulnerabilities were addressed in the ExtremeCloud IQ - Site Engine, ExtremeControl, and ExtremeAnalytics engine images:

    - CVE-2021-3449, CVE-2021-3450, CVE-2020, CVE-2021-28038, CVE-2021-29650, CVE-2021-30002, CVE-2021-28660, CVE-2021-29265, CVE-2021-28375, CVE-2020-25639, CVE-2018-25014, CVE-2020-36331, CVE-2020-36329, CVE-2018-25009, CVE-2018-25011, CVE-2020-36330, CVE-2018-25012, CVE-2018-25013, CVE-2018-25010, CVE-2020-36328, CVE-2020-36332, CVE-2020-25672, CVE-2021-31916, CVE-2021-28964, CVE-2020-25670, CVE-2021-3483, CVE-2021-3428, CVE-2020-25671, CVE-2021-33033, CVE-2021-28971, CVE-2021-29647, CVE-2021-28660, CVE-2020-25673, CVE-2021-28972, CVE-2021-31916, CVE-2021-28950, CVE-2021-29264, CVE-2021-28971, CVE-2021-28964, CVE-2021-28972, CVE-2021-3483, CVE-2020-25672, CVE-2021-29647, CVE-2020-25671, CVE-2020-25670, CVE-2021-28688, CVE-2020-25673, CVE-2017-8779, CVE-2021-3517, CVE-2021-3518, CVE-2021-3516, CVE-2021-3541, CVE-2017-8872, CVE-2019-20388, CVE-2021-3537, CVE-2020-24977, CVE-2021-31829, CVE-2021-23134, CVE-2020-26147, CVE-2021-3506, CVE-2020-26145, CVE-2020-24586, CVE-2020-24587, CVE-2020-26139, CVE-2021-33034, CVE-2020-24588, CVE-2020-26141, CVE-2021-32399, CVE-2021-33200, CVE-2021-23133, CVE-2021-3609, CVE-2020-35523, CVE-2020-35524, CVE-2021-27218, CVE-2021-27219, CVE-2021-24031, CVE-2021-24032, CVE-2021-21300, CVE-2021-28153, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2020-27170, CVE-2020-27171, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2021-3444, CVE-2020-27170, CVE-2020-27171, CVE-2021-22876, CVE-2021-22890, CVE-2021-20305, CVE-2021-3348, CVE-2021-3347, CVE-2018-13095, CVE-2021-20194, CVE-2021-3348, CVE-2021-26930, CVE-2021-26931, CVE-2021-3493, CVE-2021-29154, CVE-2021-3492, CVE-2021-25214, CVE-2021-25215, CVE-2021-25216, CVE-2021-32550, CVE-2021-32555, CVE-2021-32552, CVE-2021-32554, CVE-2021-32547, CVE-2021-32548, CVE-2021-32551, CVE-2021-32549, CVE-2021-32556, CVE-2021-32557, CVE-2021-32553, CVE-2021-31535, CVE-2021-3520, CVE-2021-25217, CVE-2020-24489, CVE-2020-24512, CVE-2020-24513, CVE-2020-24511, CVE-2021-23133, CVE-2021-3609, CVE-2021-3600, CVE-2021-29264, CVE-2021-20292, CVE-2021-29650, CVE-2021-26930, CVE-2021-28688, CVE-2021-29265, CVE-2021-30002, CVE-2021-28038, CVE-2021-26931, CVE-2021-3448, CVE-2020-8696, CVE-2020-8695, CVE-2020-8698, CVE-2018-16869, CVE-2021-3580, CVE-2021-3502, CVE-2021-3468

- The following vulnerabilities were addressed in the ExtremeControl and ExtremeAnalytics engine images:
    - CVE-2019-7303, CVE-2020-11933, CVE-2020-11934, CVE-2020-27352

- ExtremeCloud IQ - Site Engine engine image:
    - USN-4719-1, CVE-2021-2203, CVE-2021-2308, CVE-2021-2208, CVE-2021-2154, CVE-2021-2307, CVE-2021-2193, CVE-2021-2171, CVE-2021-2215, CVE-2021-2169, CVE-2021-2179, CVE-2021-2232, CVE-2021-2278, CVE-2021-2172, CVE-2021-2293, CVE-2021-2299, CVE-2021-2201, CVE-2021-2166, CVE-2021-2301, CVE-2021-2146, CVE-2021-2194, CVE-2021-2196, CVE-2021-2212, CVE-2021-2300, CVE-2021-2217, CVE-2021-2230, CVE-2021-2304, CVE-2021-2162, CVE-2021-2164, CVE-2021-2226, CVE-2021-2170, CVE-2021-2180, CVE-2021-2298, CVE-2021-2305, CVE-2012-6708
- The following vulnerabilities were addressed in the ExtremeControl engine image:
    - CVE-2020-10663, CVE-2020-10933, CVE-2020-25613, CVE-2021-28965, CVE-2021-32029, CVE-2021-32028, CVE-2021-32027, CVE-2021-21705, CVE-2020-7068, CVE-2020-7071, CVE-2021-21702, CVE-2021-21704
- The following vulnerability was addressed in the ExtremeAnalytics engine image:
    - CVE-2020-15778

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: https://documentation.extremenetworks.com/netsight/XIQ-SE/XIQSE_21.09.10_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 21.09.10 supports upgrades from ExtremeCloud IQ - Site Engine version 21.04.10, as well as Extreme Management Center versions 8.4.4, 8.5.5, or 8.5.6. If you are upgrading from an earlier version of NetSight or Extreme Management Center, you must perform intermediate upgrades before upgrading to ExtremeCloud IQ - Site Engine version 21.09.10.

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 21.09.10.

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 21.09.10
	8.1.7	8.3.3	8.4.4	8.5.6	
ExtremeCloud IQ - Site Engine version 21.04.10					X
Extreme Management Center version 8.5.5, 8.5.6					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

Current Version	Intermediate Upgrade Versions Needed				Upgrade to ExtremeCloud IQ - Site Engine version 21.09.10
	8.1.7	8.3.3	8.4.4	8.5.6	
*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	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 21.09.10.

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 21.09.10, ensure the DNS server IP address is correctly configured.
- When upgrading to ExtremeCloud IQ - Site Engine version 21.09.10, 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 ExtremeControl engines, Fabric Manager, or another add-on feature, you must first perform the ExtremeCloud IQ - Site Engine upgrade to version 21.09.10 and then add the feature.

4.2.1 License Renewal

Upgrading to ExtremeCloud IQ - Site Engine version 21.09.10 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.

4.2.2 Free Space Consideration

When upgrading to ExtremeCloud IQ - Site Engine version 21.09.10, 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 21.09.10 when upgrading to ExtremeCloud IQ - Site Engine 21.09.10. However, both ExtremeCloud IQ - Site Engine and ExtremeControl engine must be at version 21.09.10 in order to take advantage of the new ExtremeControl21.09.10 features. ExtremeCloud IQ - Site Engine 21.09.10 supports managing ExtremeControl engine versions 8.4, 8.5, 21.4.10, and 21.09.10.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, you should also upgrade your assessment agent adapter to version 21.09.10 if you upgrade to ExtremeControl version 21.09.10.

You can download the latest ExtremeControlengine 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 21.09.10 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 21.09.10:

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 21.09.10 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 21.09.10, the Default Gateway IP Address is configured as part of the VLAN. In 21.09.10, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 21.09.10, merge any **Default Gateway IP Addresses** from the device into the configuration of ExtremeCloud IQ - Site Engine to prevent incorrect configuration of the device.

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

VSP SNMP performance is adversely affected as the number of VRF configurations increases. This issue can be resolved by upgrading to VSP release 8.1.1 or later or VSP8600 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 VSP Device Configuration

Topology links from VSP devices to other VSP or ERS devices might not display in a topology map (or might display inconsistently). To ensure topology map links display correctly, verify that the VSP device is configured to publish its management IP address in the autotopology (SONMP) data.

Ensure that the output of `show sys setting` command shows:

```
autotopology : on
ForceTopologyIpFlag : true
clipId-topology-ip : 0
```

If the output values displayed are different, configure the VSP device to publish management IP address in SONMP data by executing the following CLI commands:

```
(config)# autotopology
(config)# sys force-topology-ip-flag enable
(config)# default sys clipId-topology-ip
```

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.

Following a Wireless Manager upgrade, clear the Java Cache before starting the ExtremeCloud IQ - Site Engine client.

5. System Requirements

IMPORTANT: Wireless event collection is disabled by default in version 21.09.10 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 21.09.10.

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

Manufacturer	Operating System
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)™
Hyper-V (ExtremeCloud IQ - Site Engine Virtual Engine)	Hyper-V Server 2012 R2 Hyper-V 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
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	10,000

Specifications	Small	Medium	Enterprise	Large Enterprise
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
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 and Analytics 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

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

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

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

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

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

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

5.6 ExtremeControl Engine Version Requirements

For complete information on ExtremeControl engine version requirements, see the ExtremeCloud IQ - Site Engine Version 21.09.10 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	1 Physical NIC	3 Physical NICs

5.12.4 Guest and IoT Manager Supported Browsers

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

Medium	Browser	Version
Desktop	Microsoft Internet Explorer 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.

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