ExtremeCloud™ IQ Site Engine Release Notes

10/2024
24.10.10
PN: 9039110-00 Rev AA

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks/

Contact

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

- Global Technical Assistance Center (GTAC) for Immediate Support
    - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
    - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.
3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4. LICENSE TYPES.

   - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
   - *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.

5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

   The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part,

or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

   a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

   b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

   You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.

10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

    a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.

    b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.

12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.
    NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN

NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS. Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.

    a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

    b. This Agreement may not be changed or amended except in writing signed by both parties hereto.

    c. You represent that You have full right and/or authorization to enter into this Agreement.

    d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.

    e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

    f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

    g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

    h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

       Extreme Networks, Inc.
       145 Rio Robles
       San Jose, CA 95134 United States
       ATTN: General Counsel

Table of Contents

24.10.10 Release Notes

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

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

IMPORTANT:

- For upgrade and installation requirements, as well as configuration considerations, see ExtremeCloud IQ Site Engine Configuration and Requirements.
- ExtremeCloud IQ Site Engine version 24.10.10 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 an ExtremeCloud IQ Connect level account. You must use a commercial or trial subscription.
- ExtremeCloud IQ Site Engine is not compatible with ExtremeCloud IQ HIQ. You must use a standard VIQ or MSP account.
- For the information shared between ExtremeCloud IQ Site Engine and ExtremeCloud IQ , see ExtremeCloud IQ Connection.

For information regarding the features supported by specific devices, see the Firmware Support Matrix. Version 24.10.10 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

Starting in ExtremeCloud IQ Site Engine version 23.2.10 each stack member consumes a license in connected mode. In connected mode, ExtremeCloud IQ Site Engine now reports stack members to ExtremeCloud IQ. If you use stacks in connected mode, ensure that enough

ExtremeCloud IQ Pilot licenses are in the license pool before upgrading to ExtremeCloud IQ Site Engine 23.2.10 or later.

Beginning with ExtremeCloud IQ Site Engine version 21.4.10, your ExtremeAnalytics license is included as part of your ExtremeCloud IQ Pilot license. Separate licenses are no longer required.

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

End of Software Maintenance

In ExtremeCloud IQ Site Engine version 24.7.10 and after, the following components and features are deprecated and removed:

- ExtremeCompliance, also known as Information Governance Engine
- Public Cloud Dashboard

The following components and features reached end-of-software-maintenance on 30th September 2023:

- Guest and IoT Manager - last version is 23.7.11.6
- Fabric Manager - last version is 22.9.13.5
- Posture Assessment (both the agent-based and agent-less)

The mobile application "ExtremeManagement ZTP+" will be removed from the Google Play store by August 27, 2024.

Onboarding ExtremeCloud IQ Site Engine to ExtremeCloud IQ in Connected Deployment Mode

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

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

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

Enhancements

The following enhancements were made to ExtremeCloud IQ Site Engine in this release. For additional information about each of the enhancements listed in the release notes, see ExtremeCloud IQ Site Engine Documentation.

ExtremeCloud IQ Site Engine

ExtremeCloud IQ Site Engine Enhancements
Addressed CVE-2024-3596 when RADIUS Authentication is enabled for the SSH access to appliances.
Added support for OVA deployment on Nutanix AHV hypervisor with Prism Central.

ExtremeAnalytics

ExtremeAnalytics Enhancements
Adjusted installer of Application Analytics Engine to remind the user about option to change web credentials.

ExtremeManagement

ExtremeManagement Enhancements
Added option to cycle PoE on the port or selection of ports for EXOS/Switch Engine and VOSS/Fabric Engine devices through Tasks > Macro > Cycle Port POE.
Enhanced functionality of Search Network, Search with Compass > Device Group dropdown to allow search as you type.
Added the following info to the Restore Saved Backup Configuration window if ExtremeCloud IQ Site Engine is in connected mode: "Devices onboarded to ExtremeCloud IQ after this backup was created will become orphaned. Manual deletion in ExtremeCloud IQ may be needed.".
Enhanced support for Compass search with VOSS/Fabric Engine devices to include Node Alias.
Updated Apache CXF to 3.5.9 to fix CVE-2024-28752. Updated Wildfly /usr/local/Extreme_ Networks/NetSight/wildfly/modules/system/layers/base/org/apache/cxf/main/cxf-core-3.1.6.jar to 3.5.9
Addressed Blast RADIUS Attack (CVE-2024-3596) vulnerability when GUI access is using RADIUS backend.
A change of state from Managed to Unmanaged, and Unmanaged to Managed is now logged to the event log for support purposes.

ExtremeControl

ExtremeControl Enhancements
Implemented new NBI API calls to configure NAC rules: • mutation > accessControl > deleteNacRule • mutation > accessControl > createNacRule Implemented new NBI API calls to read NAC configuration: • query > accessControl > allNacZones • query > accessControl > allNacPortals • query > accessControl > allNacProfiles • query > accessControl > nacRules
Updated Extreme RADIUS dictionary file to reflect the latest available attributes.
Implemented new NBI API calls updateAAARadiusAuthenticationRule to modify RADIUS servers used by AAA rules.
Implemented new Captive portal option "Portal Redirect To Engine's FQDN" to help with HA deployment with Entra ID backend.
Adjusted installer of Access Control Engine to remind the user about option to change web credentials.
Addressed Blast RADIUS Attack (CVE-2024-3596) vulnerability when Captive Portal is using RADIUS backend.

Customer Found Defects and Known Issues

Customer Found Defects Addressed 24.10.10

ExtremeAnalytics CFDs Addressed	ID
Addressed an issue with analytics fingerprints that referenced Rhapsody. Removed Rhapsody name and replaced with Napster. Deleted APP:RHAPSODY fingerprint.	03008506

ExtremeControl CFDs Addressed	ID
Addressed an issue when a CRL error occurs, an empty list returned and persisted with the partial CRL in the pem file. Now when the loading CRL store error occurs, the system will not store the CRL list that's downloaded. A new warning message appears in the tag.log.	02635631 02994980
An internet upgrade on a nac appliance, from either version 8.5 or 23.4.12 to 24.2.13 should now work regardless of the version of php installed.	02862076
Addressed an issue when multiple users are interacting with the Policy Domain settings in different browser windows, it was possible for the Policy Domain cache to be made invalid and cause all the switches in that Domain to be removed.	02864298

ExtremeControl CFDs Addressed	ID
Addressed an issue where the NBI could not specify Policy Attributes to Send as "None", which is allowed in the Policy UI.	02931050
Addressed the policy mapping dropdown. Now lists the names correctly when 'Access Point' does not exist.	02945449
Addressed an issue where Entra ID authentication wasn't working when 802.1X_PEAP_ INNER_TUNNEL was set at the top (or higher than Entra ID) of AAA rule.	02957555
Addressed an issue with EAP-TEAP authentication fails after 50 round trips. Increased the EAP round trip limit from 50 to 100.	02957695
Addressed an issue where multiple postgres versions could be installed after a NAC upgrade. Now after upgrading a NAC appliance from ubuntu20.04 to ubuntu22.04 the only version of postgres that will be installed is postgres 10.	02982817
Addressed an issue with a NAC database error when receiving a large number of framed IPv6 addresses in a RADIUS accounting packet.	02972738
Addressed an issue with DHCP IP rediscover triggers on disconnected end-systems. Now for disconnected end-systems, even after a DHCP IP request is received, it will not trigger the IP update for those end-systems.	02986199
Addressed an issue where Access Control was not closing the resources after use and causing the file descriptor leak. This has been resolved.	03005223
Addressed filtering issues on the AP Mac, AP Name, AP Serial Number, and SSID columns of the End-System table.	03015891 03020595
Addressed an issue where an end-system export would fail with zero records returned.	03020595

ExtremeManagement CFDs Addressed	ID
Addressed an issue where NBI queries for a Site VLAN configuration would not provide VLANs inherited from Service Definitions, only those inherited from parent Sites.	02888806
Addressed an issue where TLS 1.0 and 1.1 still in use on SMTP TCP port 25. Fixed by disabling TLS 1.0 and 1.1 for postfix Nessus scan rules 104743 and 157288.	02916753 02923682 02936014
Addressed an issue where ZTP+ was providing three sets of SNMP notification configuration (one for each version of SNMP), which was causing incorrect SNMP configuration on the device.	02927535
Addressed an issue with ZTP+ not applying all of the user's desired Access Control settings when configuring a device.	02928057
Addressed an issue with a failure to assign VLAN PVID to Fabric Engine ports that have Auto-Sense disabled during enforcement.	02928599
Addressed an issue when an EXOS/Switch Engine device does not have HTTP or HTTPS web server enabled, ExtremeCloud IQ Site Engine will receive a connection denied error. We were previously showing an exception with stack trace, which could be alarming to customers. Instead, we now display a line of debug output indicating the communication error to the device, avoiding the stack dump.	02929479

ExtremeManagement CFDs Addressed	ID
Addressed an issue where the NBI was not validating that the input data contained a valid group name. If an invalid group name was provided, the intended changes would not be carried out.	02931010
Addressed an issue with VLANs that were associated with L2VSNs being pruned inappropriately.	02932137
Addressed an issue where a device could get stuck in a Pending state after changing from the wrong SNMP profile to the correct SNMP profile.	02950353
Addressed an issue where ZTP+ was automatically configuring Insight ports on VOSS/Fabric Engine devices.	02951715
Addressed an issue where the VLAN configuration panel was hidden for S-Series and K-Series devices, for which VLAN configuration is supported.	02955977
NBI modification of the Endpoint Locations data will now allow the user to identify the Site to be changed by either Site ID or Site Location.	02958069
Addressed an issue where configuring multiple devices at once would lose some changes to the devices annotations.	02959925
Addressed an issue where Memory Utilization on BOSS devices was not updating as expected. The collected OIDs have been updated to show the expected memory changes.	02966290
Addressed an issue where XOS Port Utilization was not showing as a percent value.	02972267
Addressed an issue where Export Serial number menu action was not exporting non-managed devices.	02992071
Addressed an issue if the timestamp new version failed then consecutive View Last Configuration followed by Save a Copy fails with "Missing or empty config file".	02998649
Addressed an issue where Automated Port Templates were not being applied to devices onboarded with ZTP+.	03001139
Addressed an issue with some end-system filters malfunctioning. Corrected the filtering behavior of the Last Seen and Site columns.	03002205
Addressed an issue where the statistics collection for MS Workstations was not working. Resolved by restored Device collection of HOST-RESOURCE-MIB for family "MS Workstation" and "PC Workstation" .	03003601
Addressed in issue where migrating a large number of workflows in a large database could stop the migration script from processing.	03008603
Addressed an issue where all stack members did not report to ExtremeCloud IQ.	03009199
Addressed an issue where the Compare Configuration feature was not functioning as expected.	03011450
Addressed an issue with backup logging errors if the nsserver was running under non-root account	03021837

Known Issues Addressed in 24.10.10

ExtremeCloud IQ Site Engine Issues Addressed
Addressed an issue of after an IP address change through the dnetconfig, in some situations, the NSJboss.properties was not updated and the server did not start properly.

Updated help for migrateFromVersion24_2.sh script. If the timeout attribute is provided then the timeout value is now mandatory.
Custom DHCP fingerprints are now included in backup and restore.
Custom autogroups are now included in backup and restore.
NAC enforce backups are now included in backup and restore.
Restore Initial Database now works properly again.
Addressed an issue where TACACS+ could not find platform independent libraries <prefix>. ExtremeCloud IQ Site Engine login with TACACS+ is now successful.
Addressed an issue with restoring a backup through backup_restore.sh the "Disable the Connection to ExtremeCloud IQ" was not working in some scenarios.

ExtremeControl Issues Addressed

Change of the Custom End-System Information Labels attribute name is now also reflected in the End-System Groups.
Value in Entra ID Realm field is now automatically converted to lowercase. Value in Entra ID Realm field now does not allow @ and other unsupported special characters.
Addressed an issue when the deletion of many records in the policy mappings table skipped some records.
Addressed an issue with a negative ISID ID for Dynamic ACLs and Policy Vlan Islands. When Policy Vlan Islands are used together with VOSS/Fabric Engine and Dynamic ACLs then the FA-VLAN-ISID is now excluded from the PER_USER_ACL_VOSS.
Fixed corrupted packages netplan.io and tcpd in the Access Control Engine.

ExtremeManagement Issues Addressed

Addressed an issue where = was invalid but seen on real devices. Now allowing = to be used as a target Display Name.
Addressed an issue when some Fabric Extend links were missing or displayed twice.

Addressed Vulnerabilities

This section presents the vulnerabilities reported by vulnerability scanners in previous versions. The following components received updates in 24.10 regardless of whether the vulnerability could have been exploited or not. If you need more information on vulnerability testing, see Security and Vulnerability Testing.

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

CVE-2016-1585, CVE-2022-48772, CVE-2023-26112, CVE-2023-27043, CVE-2023-52884, CVE-2023-52887, CVE-2023-7207, CVE-2024-23848, CVE-2024-25741, CVE-2024-26677, CVE-2024-27012, CVE-2024-31076, CVE-2024-33621, CVE-2024-33847, CVE-2024-34027, CVE-

2024-34777, CVE-2024-35247, CVE-2024-35927, CVE-2024-36014, CVE-2024-36015, CVE-2024-36032, CVE-2024-36270, CVE-2024-36286, CVE-2024-36489, CVE-2024-36894, CVE-2024-36971, CVE-2024-36972, CVE-2024-36974, CVE-2024-36978, CVE-2024-37078, CVE-2024-37356, CVE-2024-38381, CVE-2024-38546, CVE-2024-38547, CVE-2024-38548, CVE-2024-38549, CVE-2024-38550, CVE-2024-38552, CVE-2024-38555, CVE-2024-38558, CVE-2024-38559, CVE-2024-38560, CVE-2024-38565, CVE-2024-38567, CVE-2024-38570, CVE-2024-38571, CVE-2024-38573, CVE-2024-38578, CVE-2024-38579, CVE-2024-38580, CVE-2024-38582, CVE-2024-38583, CVE-2024-38586, CVE-2024-38587, CVE-2024-38588, CVE-2024-38589, CVE-2024-38590, CVE-2024-38591, CVE-2024-38596, CVE-2024-38597, CVE-2024-38598, CVE-2024-38599, CVE-2024-38601, CVE-2024-38605, CVE-2024-38607, CVE-2024-38610, CVE-2024-38612, CVE-2024-38613, CVE-2024-38615, CVE-2024-38618, CVE-2024-38619, CVE-2024-38621, CVE-2024-38623, CVE-2024-38624, CVE-2024-38627, CVE-2024-38633, CVE-2024-38634, CVE-2024-38635, CVE-2024-38637, CVE-2024-38659, CVE-2024-38661, CVE-2024-38662, CVE-2024-38780, CVE-2024-39276, CVE-2024-39277, CVE-2024-39301, CVE-2024-39466, CVE-2024-39467, CVE-2024-39468, CVE-2024-39469, CVE-2024-39471, CVE-2024-39475, CVE-2024-39480, CVE-2024-39482, CVE-2024-39487, CVE-2024-39488, CVE-2024-39489, CVE-2024-39490, CVE-2024-39493, CVE-2024-39494, CVE-2024-39495, CVE-2024-39496, CVE-2024-39499, CVE-2024-39500, CVE-2024-39501, CVE-2024-39502, CVE-2024-39503, CVE-2024-39505, CVE-2024-39506, CVE-2024-39507, CVE-2024-39509, CVE-2024-40901, CVE-2024-40902, CVE-2024-40904, CVE-2024-40905, CVE-2024-40908, CVE-2024-40911, CVE-2024-40912, CVE-2024-40914, CVE-2024-40916, CVE-2024-40927, CVE-2024-40929, CVE-2024-40931, CVE-2024-40932, CVE-2024-40934, CVE-2024-40937, CVE-2024-40941, CVE-2024-40942, CVE-2024-40943, CVE-2024-40945, CVE-2024-40954, CVE-2024-40956, CVE-2024-40957, CVE-2024-40958, CVE-2024-40959, CVE-2024-40960, CVE-2024-40961, CVE-2024-40963, CVE-2024-40967, CVE-2024-40968, CVE-2024-40970, CVE-2024-40971, CVE-2024-40974, CVE-2024-40976, CVE-2024-40978, CVE-2024-40980, CVE-2024-40981, CVE-2024-40983, CVE-2024-40984, CVE-2024-40987, CVE-2024-40988, CVE-2024-40990, CVE-2024-40994, CVE-2024-40995, CVE-2024-41000, CVE-2024-41002, CVE-2024-41004, CVE-2024-41005, CVE-2024-41006, CVE-2024-41007, CVE-2024-41009, CVE-2024-41027, CVE-2024-41034, CVE-2024-41035, CVE-2024-41040, CVE-2024-41041, CVE-2024-41044, CVE-2024-41046, CVE-2024-41047, CVE-2024-41048, CVE-2024-41049, CVE-2024-41055, CVE-2024-41087, CVE-2024-41089, CVE-2024-41092, CVE-2024-41093, CVE-2024-41095, CVE-2024-41097, CVE-2024-41671, CVE-2024-41810, CVE-2024-41957, CVE-2024-42068, CVE-2024-42070, CVE-2024-42076, CVE-2024-42077, CVE-2024-42080, CVE-2024-42082, CVE-2024-42084, CVE-2024-42085, CVE-2024-42086, CVE-2024-42087, CVE-2024-42089, CVE-2024-42090, CVE-2024-42092, CVE-2024-42093, CVE-2024-42094, CVE-2024-42095, CVE-2024-42096, CVE-2024-42097, CVE-2024-42098, CVE-2024-42101, CVE-2024-42102, CVE-2024-42104, CVE-2024-42105, CVE-2024-42106, CVE-2024-42109, CVE-2024-42115, CVE-2024-42119, CVE-2024-42120, CVE-2024-42121, CVE-2024-42124, CVE-2024-42127, CVE-2024-42130, CVE-2024-42131, CVE-2024-42137, CVE-2024-42140, CVE-2024-42145, CVE-2024-42148, CVE-2024-42152, CVE-2024-42153, CVE-2024-42154, CVE-2024-42157, CVE-2024-42160, CVE-2024-42161, CVE-2024-42223, CVE-2024-42224, CVE-2024-42225, CVE-2024-42228, CVE-2024-42229, CVE-2024-42232, CVE-2024-42236, CVE-2024-42240, CVE-2024-42244, CVE-2024-42247, CVE-2024-43374, CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-47175, CVE-2024-6119, CVE-2024-6232, CVE-2024-6923, CVE-2024-7006, CVE-2024-7592, CVE-2024-8088, CVE-2024-8096

Installation, Upgrade, and Configuration Changes

Installation Information

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, see ExtremeCloud IQ Site Engine Suite Installation.

Upgrading Without an Internet Connection

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

```
!!! ATTENTION !!!

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

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

Custom FlexViews

When reinstalling ExtremeCloud IQ Site Engine Console, the installation program saves copies of any FlexViews you created or modified in the `<install directory>\.installer\backup\current\appdata\System\FlexViews` folder.

If you are deploying FlexViews via the ExtremeCloud IQ Site Engine server, save them in the `appdata\VendorProfiles\Stage\MyVendorProfile\FlexViews\My FlexViews` folder.

Custom MIBs and Images

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

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

Important Upgrade Information

A special Data Migration Procedure is required to upgrade ExtremeCloud IQ Site Engine from versions older than 24.7. The minimum version to upgrade Analytics Engines and Access Control Engines is 24.2.13.

NOTE:

ExtremeCloud IQ Site Engine Version 24.10.10 contains an OS upgrade. Internet connectivity is required to download custom packages.

The installer prompts "Do you want to use the Internet to perform the OS upgrade?". The offline upgrade path is supported when no custom packages are installed (answer N). The online upgrade is required when custom packages are manually installed (answer Y). An online upgrade is recommended when an online upgrade was used previously, however there is a risk of session timeout due to 15 minutes of screen inactivity.

To upgrade Access Control Engines and Application Analytics Engines you can use the directive --keepalive to decrease the chance of a session expiry timeout from 15 minutes of no screen activity.

From Version (currently running)	To Version (next step in upgrade path)
ExtremeCloud IQ Site Engine **24.7.x**	ExtremeCloud IQ Site Engine **24.10**
ExtremeCloud IQ Site Engine **24.2.x**	Fresh installation of ExtremeCloud IQ Site Engine **24.10** and follow the Data Migration Procedure
Application Analytics Engine, Access Control Engine **24.2.15**	Application Analytics Engine, Access Control Engine **24.10**
ExtremeCloud IQ Site Engine **23.4.12, 23.7.x, 23.11.x, 24.2.x**	ExtremeCloud IQ Site Engine **24.2.15**
ExtremeCloud IQ Site Engine **21.x, 22.x, 23.2.x 23.4.10, 23.4.11**	ExtremeCloud IQ Site Engine **23.4.12**

From Version (currently running)	To Version (next step in upgrade path)
Extreme Management Center version **8.5.7**	ExtremeCloud IQ Site Engine **24.2.15**
Extreme Management Center version **8.2.x to 8.5.6**	Extreme Management Center **8.5.7**
Extreme Management Center version **8.0.x to 8.1.x**	Extreme Management Center **8.3.3.11**
NetSight version **7.1.4.1**	Extreme Management Center **8.3.3.11**
NetSight version **7.x**	NetSight **7.1.4.1**
NetSight version **6.3.0.186**	NetSight **7.1.4.1**
NetSight version **6.x**	NetSight **6.3.0.186**

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

If you use LDAPS with a Fully Qualified Domain Name (FQDN) in the URL to authorize a user to the OneView, then ExtremeCloud IQ Site Engine presents the Server Certificate (located in Administration > Certificates > Server Certificate Information) to the LDAPS server. If the LDAPS server presents a certificate that does not match the LDAPS URL, then the certificate is rejected with the error "Certificate Unknown".

The best practice is to use a trusted certificate if the LDAPS URL is defined with FQDN, otherwise the LDAPS server might not accept the LDAPs connection. The alternative option is to use an IP address in the LDAPS URL instead of FQDN.

Important Upgrade Considerations

- If your network is using ExtremeAnalytics or ExtremeControl engines, or another add-on feature, you must first perform the ExtremeCloud IQ Site Engine upgrade to version 24.10.10 and then upgrade the feature.
- To upgrade Traffic Sensor from version 21.x, a fresh installation is recommended. If the fresh installation cannot be used, then please check Knowledge Base for a special procedure.
- If the online upgrade fails due to an Internet connectivity issue, fix the connectivity issue and rerun the upgrade.

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

- When upgrading the ExtremeCloud IQ Site Engine server, ExtremeAnalyticsengine, or ExtremeControlengine to version 24.10.10, ensure the DNS server IP address is correctly configured.
- When upgrading to ExtremeCloud IQ Site Engine version 24.10.10, 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
  ```

License Renewal

Upgrading to ExtremeCloud IQ Site Engine version 24.10.10 requires you to transition from perpetual to subscription-based license model. Existing NMS licenses do not provide access to ExtremeCloud IQ Site Engine. If your perpetual licenses were not transitioned to subscription-based licenses, contact your Extreme Networks Representative for assistance.

Free Space Consideration

When upgrading to ExtremeCloud IQ Site Engine version 24.10.10, 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.

Site Discover Consideration

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

ExtremeAnalytics Upgrade Information

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

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

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

ExtremeControl Version 8.0 and later

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

To allow this functionality, add the following permissions:

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

Other Upgrade Information

Immediately after you install version 24.10.10 on the ExtremeControlengine, the date and time does not properly synchronize and the following error message displays:

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

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

Additionally, the following message might display during the ExtremeControl upgrade to version 24.10.10:

No domain specified

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

Upgrading ExtremeControl Engine to Version 24.10.10

General Upgrade Information

The EAP-TLS Certificates with SHA1 are considered weak and are not accepted anymore. The radius server fails to start with the SHA1 certificate. You can use a more secure certificate, such as SHA256.

You are not required to upgrade your ExtremeControl engine version to 24.10.10 when upgrading to ExtremeCloud IQ Site Engine version 24.10.10. However, both ExtremeCloud IQ Site Engine and ExtremeControl engine must be at version 24.10.10 in order to take advantage of the new ExtremeControl version 24.10.10 features. ExtremeCloud IQ Site Engine version 24.10.10 supports managing ExtremeControl engine versions 23.x and up to 24.10.10.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, you should also upgrade your assessment agent adapter to version 24.10.10 if you upgrade to ExtremeControl version 24.10.10.

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

Agent Version for NAC Agent-Based Assessment - Legacy

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

LDAPS servers with FQDN

If the LDAPS server URL uses a Fully Qualified Domain Name (FQDN), then the LDAPS client of Access Control Engine presents the internal Communication Certificate to the LDAPS server. If the LDAPS server URL uses a FQDN then the LDAPS client of ExtremeCloud IQ Site Engine presents the Server Certificate (located in Administration > Certificates > Server Certificate Information) to the LDAPS server. If the LDAPS server presents a certificate that does not match the LDAPS URL, then the certificate is rejected with the error “Certificate Unknown”

The best practice is to use trusted certificates if the LDAPS URL is defined with FQDN, otherwise the LDAPS server might not accept the LDAPS connection. If the LDAPS server URL uses an IP address then the LDAPS client (of both Access Control Engine and ExtremeCloud IQ Site Engine) does not present the Certificate to the LDAPS server.

Upgrading to Policy Manager 24.10.10

- Policy Manager 24.10.10 only supports ExtremeWireless Controller version 10.51. If you upgrade to ExtremeCloud IQ Site Engine 24.10.10 prior to upgrading your controllers, then Policy Manager does not allow you to open a domain where the controllers already exist or add them to a domain. A dialog is

displayed indicating your controllers do not meet minimum version requirements and that they must be upgraded before they can be in a domain.

- Following an upgrade to Wireless Controller version 8.31 and higher, a Policy Manager enforce fails if it includes changes to the default access control or any rules that are set to contain. To allow Policy Manager to modify the default access control or set rules to contain, you must disable the **"Allow" action in policy rules contains to the VLAN assigned by the role** checkbox accessed from the Wireless Controller's web interface on the Roles > **Policy Rules** tab. This will allow the enforce operation to succeed.

Fabric Configuration Information

Certificate

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

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

Authentication Key

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

Service Configuration Change

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

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

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

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

CLIP Addresses

Using the CLIP Addresses table in the Configure Device window, you can enter addresses in both IPv4 and IPv6 formats. However, ExtremeCloud IQ Site Engine version 24.10.10 only supports applying a single address (either IPv4 or IPv6) to a Loopback Interface.

Gateway Address Configuration Change

In versions of ExtremeCloud IQ Site Engine prior to 24.10.10, the Default Gateway IP Address is configured as part of the VLAN. In 24.10.10, the Default Gateway IP Address is configured as part of the VRF.

When enforcing VRFs to a device after upgrading to version 24.10.10, merge any **Default Gateway IP Addresses** from the device into the configuration of ExtremeCloud IQ Site Engine to prevent incorrect configuration of the device.

Upgrading VSP-8600

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

Removing Fabric Connect Configuration

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

Password Configuration

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

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

VRF Configuration

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

Device Configuration Information

VDX Device Configuration

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

NOTE:

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

1. Access the **Network** > **Devices** tab.
2. Right-click on the device in the Devices table.
3. Select **Tasks** > **Config** > **VDX Config Basic Support**.

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

Rediscover VDX devices after upgrading to ExtremeCloud IQ Site Engine.

VOSS/Fabric Engine Device Configuration

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

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

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

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

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

The **Status** of LAG links in maps will start working after the next polling following an upgrade to ExtremeCloud IQ Site Engine. You can initiate the polling of a device by performing a refresh/rediscovery of the device.

ERS Device Configuration

ERS devices might automatically change VLAN configurations you define in ExtremeCloud IQ Site Engine. To disable this, change the `vlan configcontrol` setting for ERS devices you add to ExtremeCloud IQ Site Engine by entering the following in the device command line:

```
CLI commands
enable
config term
vlan configcontrol flexible
```

Additionally, configure all VLANs on the port for an ERS device with the same tag status (tagged or untagged). If enforcing to an ERS device on which a port has at least one VLAN as tagged, ExtremeCloud IQ Site Engine adds all untagged VLANs to the tagged VLAN list and clears the untagged VLAN list.

Creating an archive for ERS devices using the **Network** > **Archives** tab does not complete successfully if Menu mode (cmd-interface menu) is used instead of CLI mode (cmd-interface cli). See How To Set Default Management Interface To Either Menu or CLI Mode to create the archive.

SLX Device Configuration

When creating a ZTP+ Configuration for an SLX 9240 on which firmware version 18s.01.01 or 18s.01.02 is installed, the ZTP+ process fails if the **Administration Profile** value uses SSH or Telnet CLI credentials. ExtremeCloud IQ Site Engine indicates that the SSH or CLI profile is not supported by the device.

To create a ZTP+ configuration for an SLX 9240:

1. Create a new Device Profile with the **CLI Credential** set to **< No Access >**.

   NOTE: The SLX ZTP+ Connector does NOT support configuring CLI credentials on the device.

2. Create the ZTP+ Configuration and select the new **Device Profile** you created in Step 1 as the **Administration Profile**.
3. After the ZTP+ process successfully completes and the device is added to ExtremeCloud IQ Site Engine, select a **Device Profile** that uses the correct CLI credentials for the SLX device in the **Administration Profile**.

ExtremeXOS Device Configuration

ExtremeXOS/Switch Engine devices on which firmware version 30.3.1.6 is installed do not download and install new firmware versions successfully via the ZTP+ process. To correct the issue, access the **Network** > **Firmware** tab in ExtremeCloud IQ Site Engine, select the ExtremeXOS device you are updating via ZTP+, and change the **Version** field in the Details right-panel from **builds/xos_30.3/30.3.1.6** to **30.3.1.6**.

Firmware Upgrade Configuration Information

ExtremeCloud IQ Site Engine supports firmware downloads and uploads to devices using TFTP, FTP, SCP, and SFTP. However, before firmware images can be downloaded or uploaded from the server, ExtremeCloud IQ Site Engine needs the root path or directory for each of the protocols. The following default root paths for each protocol are configurable from the **Administration** > **Options** > **Inventory Manager** tab:

Protocol Root Path:

- TFTP: /tftpboot/firmware/images/
- FTP: /tftpboot/firmware/images/
- SCP: /root/firmware/images/
- SFTP: /root/firmware/images/

To upload firmware images that are 2 GB or less to the server, use the ExtremeCloud IQ Site Engine**Network** > **Firmware** tab. For files larger than 2 GB, use a third-party client (such as SCP, WinSCP, or FTP).

For example, to use SCP to upload a firmware image to the SCP root path on the server, enter the following:

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

Wireless Manager Upgrade Information

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

Server and Client System Requirements

IMPORTANT:

Wireless event collection is disabled by default in version 24.10.10 due to the increase in disk space usage required. To enable event collection, select Enable Event CollectionEvent Analyze. Then select Administration > Options > Event Analyzer.

Internet Explorer is not supported in ExtremeCloud IQ Site Engine version 24.10.10.

ExtremeCloud IQ Site Engine Server Requirements

Manufacturer	Operating System
Linux	Red Hat Enterprise Linux 9.4
VMware® (ExtremeCloud IQ Site Engine Virtual Engine)	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server VMware ESXi™ 6.7 server VMware ESXi™ 7.0 server VMware ESXi™ 8.0 server vSphere (client only)™
Microsoft® Hyper-V (ExtremeCloud IQ Site Engine Virtual Engine)	Windows® Server 2016 Windows® Server 2019
Nutanix (ExtremeCloud IQ Site Engine Virtual Engine)	AHV: 20230302.101026 AOS: 6.8.1 Prism Central: 2024.2

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

ExtremeCloud IQ Site Engine Client Requirements

These are the operating system requirements for remote ExtremeCloud IQ Site Engine client machines.

Manufacturer	Operating System
Windows (qualified on the English version of the operating systems)	Windows® 10 and 11
Linux	Red Hat Enterprise Linux 9.4
Mac OS X®	Monterey

ExtremeCloud IQ Site Engine Server and Client Hardware Requirements

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

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

ExtremeCloud IQ Site Engine Server Requirements

	Small	Medium	Enterprise	Large Enterprise
Total CPUs	1	2	2	2
Total CPU Cores	8	16	24	24
Memory	16 GB	32 GB	64 GB	64 GB
Disk Size	240 GB	480 GB	960 GB	1.92 TB
IOPS	200	200	10,000	10,000
Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000 air gap 8,000 connected	10,000 air gap 8,000 connected
ExtremeControl End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
ExtremeAnalytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

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

ExtremeCloud IQ Site Engine Client Requirements

	Requirements
CPU Speed	3.0 GHz Dual Core Processor
Memory	8 GB (4 GB for 32-bit OS)

	Requirements
Disk Size	300 MB (User's home directory requires 50 MB for file storage)
Java Runtime Environment (JRE) (Oracle Java only)	Version 8
Browser[1] (Enable JavaScript and Cookies)	Microsoft Edge Mozilla Firefox Google Chrome

[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.

Virtual Engine Requirements

The ExtremeCloud IQ Site Engine, ExtremeControl, and ExtremeAnalytics virtual engines must be deployed on a VMware, Hyper-V server, or Nutanix.

- ExtremeCloud IQ Site Engine virtual engines are packaged in the .OVA file format for VMware deployment.
- ExtremeCloud IQ Site Engine virtual engines are packaged in the .ZIP file format for Hyper-V deployment.
- ExtremeCloud IQ Site Engine virtual engines are packaged in the .OVA file format for Nutanix deployment through Prism Central.

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

ExtremeCloud IQ Site Engine Virtual Engine Requirements

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

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

ExtremeControl Virtual Engine Requirements

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

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

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

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

- Up to 12,000 end-systems if your network uses Captive Portal functionality.
- Up to 24,000 end-systems if your network does not use Captive Portal functionality.

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

ExtremeAnalytics Virtual Engine Requirements

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

IMPORTANT:

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

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

Fabric Manager Requirements

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

ExtremeControl Agent OS Requirements

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

Manufacturer	Operating System	Operating System Disk Space	Available/Real Memory
Windows[1]	Windows Vista Windows XP Windows 2008 Windows 2003 Windows 7 Windows 8 Windows 8.1 Windows 10	80 MB	40 MB (80 MB with Service Agent)
Mac OS X	Catalina Tiger Snow Leopard Lion Mountain Lion Mavericks Yosemite El Capitan Sierra	10 MB	120 MB

[1]Certain assessment tests require the Windows Action Center (previously known as Windows Security Center), which is supported on Windows XP SP2+, Windows Vista, and Windows 7, Windows 8, and Windows 8.1 operating systems.

ExtremeControl Agent support for Antivirus or Firewall products includes, but is not limited to, the following families of products:

- McAfee
- Norton
- Kaspersky
- Trend Micro
- Sophos

ExtremeControl Agent operating system support for the above products includes the latest Windows or Mac OS X versions currently available at the time of product release. The ExtremeControl Agent running on MAC Operating Systems requires Java Runtime Environment (JRE) support. Some features of various products might not be supported. For additional information on specific issues, see Known Restrictions and Limitations.

ExtremeControl Supported End-System Browsers

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

Medium	Browser
Desktop	Microsoft Edge Microsoft Internet Explorer Mozilla Firefox Google Chrome
Mobile	Internet Explorer Mobile Microsoft Edge Microsoft Windows 10 Touch Screen Native (Surface Tablet) iOS Native Android Chrome Android Native Dolphin Opera

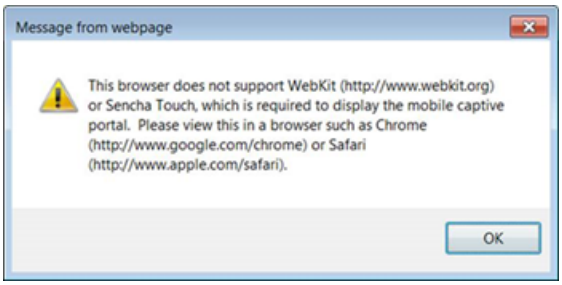
NOTES: A native browser indicates the default, system-installed browser. Although this might be Chrome (Android), this also includes the default, system-controlled browser used for a device's Captive Network Detection for a device. Typically, this is a non-configurable option for Wi-Fi Captive Network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

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

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

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

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



ExtremeControl Engine Version Requirements

For complete information on ExtremeControl engine version requirements, see Important Upgrade Information.

ExtremeControl VPN Integration Requirements

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

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

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

ExtremeControl SMS Gateway Requirements

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

- Clickatell
- Mobile Pronto

ExtremeControl SMS Text Messaging Requirements

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

AT&T	Sprint PCS
Alltel	SunCom

Bell Mobility (Canada)	T-Mobile
Cingular	US Cellular
Metro PCS	Verizon
Rogers (Canada)	Virgin Mobile (US and Canada)

ExtremeAnalytics Requirements

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

Ekahau Maps Requirements

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

Guest and IoT Manager Requirements

Guest and IoT Manager Server OS Requirements

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

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

Guest and IoT Manager Outlook Add-in Client Requirements

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

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

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

Guest and IoT Manager Virtual Engine Requirements

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

Specifications	Minimum	Recommended
Total CPU Cores	2	4
Memory	2 GB	4 GB

Specifications	Minimum	Recommended
Disk Size	80 GB	80 GB
Interfaces	1 Physical NIC	3 Physical NICs

Guest and IoT Manager Supported Browsers

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

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

[1]Mobile Browsers are supported only for the Guest Self-Service Provisioning flow.

NOTES:

- A mobile device can access the Guest and IoT Manager Application by using any desktop-supported browsers available on a mobile device. Before login, make sure to select the Desktop site option in the browser options.
- Browsers set to a zoom ratio of less than 100% might not display Guest and IoT Manager Application properly (for example, missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.
- Guest and IoT Manager Application is best viewed in 1920 x 1080 resolution or higher. Lower resolutions might result in improper layouts in some cases.
- If you are using self-signed certificates, they must be added in the Trusted Root Certificate store on the client machine or you might observe issues in the “print” use cases. This is only applicable for Microsoft Edge and Microsoft Internet Explorer browsers.