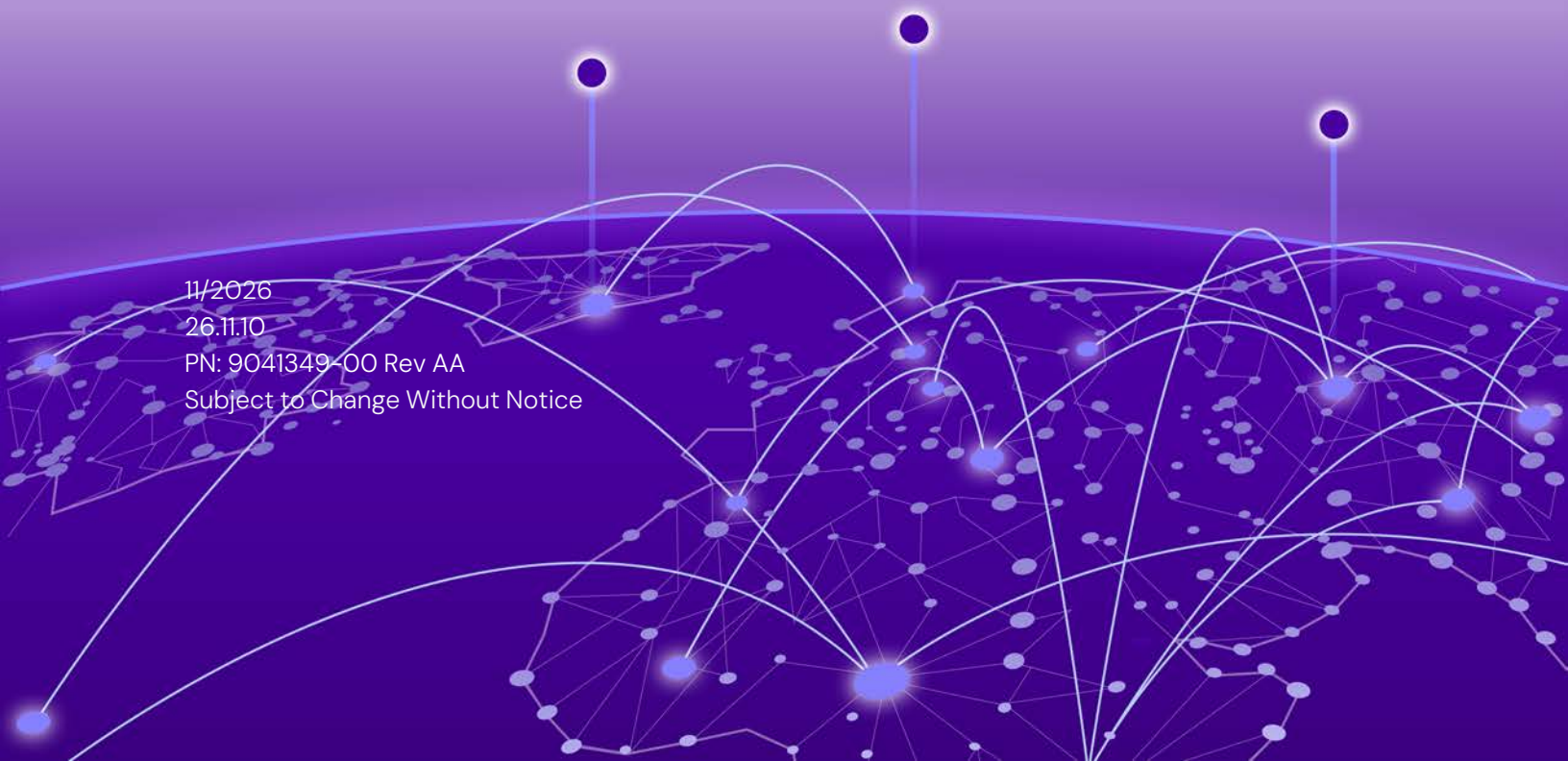
ExtremeCloud™ IQ Site Engine v26.11.10 Known Restrictions and Limitations Reference Guide:

Installation, Firmware Compatibility, and Troubleshooting Solutions

11/2026
26.11.10
PN: 9041349-00 Rev AA
Subject to Change Without Notice



Abstract

The known restrictions and limitations for ExtremeCloud IQ Site Engine version 26.11.10 outlines critical software, platform, and configuration constraints affecting deployment, operation, and integration across the suite of components. Over 100 categorized issues are documented across installation, upgrades, web applications, SNMP behavior, firmware compatibility, Java dependencies, and platform-specific anomalies (Linux, macOS, Windows). Version 26.11.10 removes EAP-TEAP primary and secondary authentication requirements for ExtremeControl. Key technical findings include Java Web Start failures, SNMPv3 credential mismatches, VLAN enforcement inconsistencies, and ZTP+ provisioning delays on high-port-count devices. This document highlights limitations in ExtremeAnalytics GRE tunnel reporting, ExtremeControl EAP-TEAP fall-through, and agent-based assessment on macOS and Windows platforms. This document also details legacy device constraints, such as unsupported MIB operations, firmware rollback risks, and policy enforcement failures on older hardware. Workarounds, configuration scripts, and CLI-based solutions are provided where applicable. This document is intended for experienced IT administrators and network engineers managing hybrid environments with ExtremeCloud IQ Site Engine.

Copyright © 2026 Extreme Networks, Inc. All Rights Reserved.

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

ExtremeCloud™ IQ Site Engine v26.11.10Known Restrictions and Limitations Reference Guide: 1

Installation, Firmware Compatibility, and Troubleshooting Solutions 1

Abstract 2

Extreme Networks® Software License Agreement 4

Table of Contents 10

Known Restrictions and Limitations 12

Install/Uninstall/Upgrades 13

ExtremeCloud IQ Site Engine Applications 15

General 15

Web Applications 19

ExtremeCloud IQ Site Engine Clients Running Mac OS 20

Alarm and Event Manager 21

Device Firmware 21

FlexViews 22

VLAN 22

RoamAbout Wireless Manager 23

FlexView Editor/MIB Tools 23

Inventory Manager 24

General 24

Device Firmware 26

ExtremeCloud IQ Site Engine 27

ExtremeAnalytics 32

ExtremeControl 33

General 33

Agent-Based Assessment 36

Access Control Engines 39

Policy Manager 41

General 41
Policy Manager and ExtremeWireless Controller (EWC) 43
Legacy Devices 45
Console 45
Inventory Manager 48
NAC Manager 49
Policy Manager 50
Connect Modules 52

Known Restrictions and Limitations

The known restrictions and limitations for the ExtremeCloud IQ Site Engine 26.11.10 release are listed below. Solutions for these restrictions and limitations are noted, if available.

To report an issue not listed in this document, contact Extreme Networks Support.

- Install/Uninstall/Upgrades
- ExtremeCloud IQ Site Engine Applications
    - General
    - Web Applications
    - ExtremeCloud IQ Site Engine Clients Running Mac OS
    - Alarm and Event Manager
    - Device Firmware
    - FlexViews
    - VLAN
    - RoamAbout Wireless Manager
- FlexView Editor/MIB Tools
- Inventory Manager
    - General
    - Firmware
- ExtremeCloud IQ Site Engine
- ExtremeAnalytics
- ExtremeControl
    - General
    - Agent-Based Assessment
    - Access Control Engines
- Policy Manager
    - Policy Manager and ExtremeWireless Controller (EWC)
- Legacy Devices
    - Console
    - Inventory Manager
    - NAC Manager
    - Policy Manager

- Connect Modules

Install/Uninstall/Upgrades

This table displays the Known Restrictions and Limitations for the ExtremeCloud IQ Site Engine Suite install, uninstall, and upgrade functionality.

Problem 1 :	Linux platforms. The ExtremeCloud IQ Site Engine installation fails and displays this error meesage `java: /xcb_xlib.c:52: xcb_xlib_unlock: Assertion 'c->xlib.lock' failed`
Solution:	This problem stems from a Java compatibility issue with XCB. The following workaround was posted on the OpenSuse 10.3 website at http://en.opensuse.org/Xlib.lock Set the following environment variable in the shell where the java process will be executed: export LIBXCB_ALLOW_SLOPPY_LOCK=true Since this issue affects ExtremeCloud IQ Site Engine both during installation and application execution, you should add the environment setting to the .profile file for the root user as indicated in the SUSE workaround under the section Making the Change Permanent.
Problem 2:	ExtremeCloud IQ Site Engine Engine Upgrade. Following an upgrade to the ExtremeCloud IQ Site Engine engine, the engine's system description is incorrect when viewed in a management application such as ExtremeCloud IQ Site Engine web-based application or MIB Tools. This happens because the upgrade scripts update the sysDescr for the engine but do not restart snmpd. This prevents the SNMP agent from returning the correct version of the engine when this OID is requested.
Solution:	Manually restart the snmpd process by executing the "/etc/rc.d/rc.net-snmp restart" command from a command shell at the engine CLI.
Problem 3:	An ExtremeCloud IQ Site Engine client application launched via Java Web Start following an upgrade experiences null pointer exceptions or classes not loading.
Solution:	This problem is documented as a bug in Java versions 1.6_18 through 1.7_04. Typically, subsequent client launches do not have the issue. An alternative solution is to update to the latest Java JRE (1.7_04 or later).
Problem 4	Cent OS 7 no longer installs all of the required PERL modules to support installing NetSight.
Solution:	To resolve this issue, execute the following command: "yum install -y perl-Data-Dumper".

Problem 5:	User passwords for engines on which the Linux operating system is installed do not expire.
Solution:	Follow the instructions found in the How to Configure Your Password to Expire.
Problem 6	Syntax for CIFS/NFS mounts used for off-box backups occasionally does not work after the upgrade due to syntax changes.
Solution:	Follow the instructions found in the How to Mount A Remote CIFS or NFS File Share On Extreme Management Center.
Problem 7:	The Site Engine installation script aborts if spaces are used in the password.
Solution:	Create a password without spaces prior to the installation. The password can be changed after the product is installed. Spaces are also not supported in the username.
Problem 8:	The installation of purview 23.7.10 ISO image on PV-A-300 appliances hangs and freezes with a blank screen.
Solution:	Install version 23.4.12 from the ISO image and then upgrade to 23.7.10.
Problem 9:	The offline upgrade to version 23.7.10 might fail for Application Analytics Engine and Access Control Engines. The `/root/dist_upgrade.log` contains messages of "`Failed to fetch https://127.0.0.1/ubuntu/universe/libp/libprelude/xxxx.deb 404 Not Found [IP: 127.0.0.1 80]`"
Solution:	Use the online upgrade, or deploy the new engine, or uninstall custom packages.
Problem 10:	Online installation fails when Internet access terminates during the OS upgrade or if upgrade servers are too busy.
Solution:	Fix the Internet connectivity issue and rerun the upgrade.
Problem 11:	PVA-300 appliance local upgrade to 23.7.10 fails to boot.
Solution:	Use the online upgrade.
Problem 12:	There is no serial number duplicity, there is no MAC duplicity, ExtremeCloud IQ reports "License not required", and ExtremeCloud IQ Site Engine reports "Onboard Pending".

Solution:	Delete ExtremeCloud IQ Site Engine from ExtremeCloud IQ and onboard ExtremeCloud IQ Site Engine again. You can use the following procedure: 1. Login to ExtremeCloud IQ and navigate to **Manage > Devices**. 2. Delete ExtremeCloud IQ Site Engine fromExtremeCloud IQ. 3. Refresh the table, wait until the count of devices stops decreasing when you refresh the table. This can take several minutes to delete all the records in the database. 4. When ExtremeCloud IQ Site Engine and all ExtremeCloud IQ Site Engine managed devices are no longer displayed in ExtremeCloud IQ, then login to ExtremeCloud IQ Site Engine. 5. Navigate to **Administration > Diagnostics > level: Advanced > System > ExtremeCloud IQ Device Message Details > Auto Onboard ExtremeCloud IQ Site Engine**. 6. Provide credentials to ExtremeCloud IQ and select **Submit**. 7. When successful, select **Force Onboard to ExtremeCloud IQ**. 8. Login to ExtremeCloud IQ and navigate to **Global Settings > License Management,** then check and configure the **NAC Entitlements Allocations.**
Problem 13:	Installation from ISO image fails on VMware ESXi version 6,x.
Solution:	Deploy the virtual machine from OVA.

ExtremeCloud IQ Site Engine Applications

This section includes the Known Restrictions and Limitations that apply to all the ExtremeCloud IQ Site Engine Suite applications.

General

Problem 1 :	Linux. You cannot specify a range of pages when printing from tables on Linux systems. If you select Print from the Table Tools popup menu, the resulting print settings window does not open to a sufficient size (and cannot be resized) to enable access to the page range fields.
Solution:	The only option is to print the entire table.
Problem 2:	When you launch an application from the **Administration > Diagnostics > Server > Server > Utilities** you see "Unable to launch the application."

Solution:	The following steps provide a workaround for this problem: 1. From the Start menu, open the Control Panel. 2. Select Java to open the Java Control Panel. 3. In the General tab, select the Temporary Internet Files > View button. 4. In the Java Cache Viewer window, select all the listed applications and delete them. 5. Close the window. Select OK in the Java Control Panel. You are now able to launch the application.
Problem 3:	Inconsistencies in user preferences can occur when the user authenticated to the operating system is different from the ExtremeCloud IQ Site Engine authenticated user.
Problem 4:	If your v1 and v2 community names are identical, then changing one of the community names using the Manage SNMP Passwords tab (in the Authorization/Device Access tool) will delete the other community name. For example, if you have a v1 "public" community name and a v2 "public" community name, then changing the v1 name will delete the v2 name. In addition, the opposite is also true: changing a public v2 community name will delete the public v1 community name, if they are identical.
Solution:	Configure the SNMP community manually.
Problem 5:	If the Client/Server SNMP Redirection option is enabled from an ExtremeCloud IQ Site Engine client, and the ExtremeCloud IQ Site Engine Server is stopped and restarted, when the client re-establishes contact to the server, the SNMP redirection no longer operates even though the option is still enabled.
Solution:	On the client system, disable then re-enable the Redirect Client/Server SNMP Communications option in the Client/Server SNMP Redirection panel in the Suite Options (Tools > Options).
Problem 6:	ExtremeCloud IQ Site Engine does not support restoring a database that was saved on a Linux system to a Windows system.

Problem 7:	Linux platforms. Launching an ExtremeCloud IQ Site Engine application from a local client results in the following Java error: java.lang.UnsatisfiedLinkError: /export/JDK/jdk1.6.0_02/jre/lib/i386/libdeploy.so: libstdc++.so.5: cannot open shared customer file: No such file or directory at java.lang.ClassLoader$NativeLibrary.load(Native Method) at java.lang.ClassLoader.loadLibrary0(ClassLoader.java:1751) at java.lang.ClassLoader.loadLibrary(ClassLoader.java:1647) at java.lang.Runtime.load0(Runtime.java:770) at java.lang.System.load(System.java:1005) at com.sun.deploy.config.UnixConfig.loadLibDeploy(UnixConfig.java:38) at com.sun.deploy.config.UnixConfig.<clinit>(UnixConfig.java:26) at com.sun.deploy.config.ConfigFactory.newInstance(ConfigFactory.java:11) at com.sun.deploy.config.Config.getInstance(Config.java:662) at com.sun.deploy.config.Config.<clinit>(Config.java:678)
Solution:	The libstdc++.so.5 library must be installed for ExtremeCloud IQ Site Engine applications to launch via Java Web Start on Linux platform systems. For example, the following methods have been used to add this library to RHEL 5. Other versions of Linux can provide alternate methods for updating system libraries; refer to your platform's documentation for the appropriate procedure. To install the library: 1. Go to https://rhn.redhat.com/network/software/packages/details.pxt?pid=291176. (A Red Hat Network account is required for access) 2. Download the compat-libstdc++-33-3.2.3-47.3.i386.rpm 3. Run the command: rpm -i compat-libstdc++-33-3.2.3-47.3.i386.rpm 4. Verify that libstdc++.so.5 displays in the /usr/lib directory. The following steps can be used to install the library if there is no Red Hat Network account: If RHEL 5 is already installed: Run the command: yum install compat-libstdc++-33.i386 (This requires that the yum repositories have been previously configured). If you are installing RHEL 5: 1. During the RHEL 5 installation, at the software selection screen, select Customize now. 2. On the next screen, in the left-hand panel, select Base System. In the right-hand panel, select Legacy Software Support. These selections will install the compat-libstdc++ packages.

Problem 8:	Unable to launch an ExtremeCloud IQ Site Engine application from **Administration > Diagnostics > Server > Server Utilities** and an "Unable to download" error message is displayed. This problem only occurs when using Internet Explorer with HTTPS (rather than HTTP) to access the Launch page. The problem occurs in ExtremeCloud IQ Site Engine version 4.0.1 or later. This problem does not occur with Mozilla Firefox.
Solution:	This is an issue with Internet Explorer, and is described in the Microsoft Knowledge Base article https://support.microsoft.com/kb/323308. Use the registry-based workaround described in the KB article to resolve the problem. This is no longer an issue when using Internet Explorer 10 or later.
Problem 9:	The ExtremeCloud IQ Site Engine Help's Search and Quick Search does not jump to the first instance of a search term in the search results when using Chrome as the browser. In addition, for all browsers, when the search term is located inside a table within the topic, the search highlights all instances it finds of the term, but does not jump to the first instance of that term.
Solution:	The workaround is to scroll through the topic to find the highlighted terms. This will be fixed in a future release.
Problem 10:	ExtremeCloud IQ Site Engine applications fail to load or stop responding while starting up when launched on an OpenSuSe platform.
Solution:	OpenSuSe installs OpenJDK by default, which utilizes IcedTea to launch web start applications. IcedTea is not officially supported. Install Java from Oracle and launch the ExtremeCloud IQ Site Engine applications using javaws.
Problem 11:	**SPBM Nickname** fields do not get updated correctly in **Configure Device > Topology** tab after XIQ-SE upgrade.
Solution:	You must **Configure > Read Device** after the ExtremeCloud IQ Site Engine upgrade.
Problem 12:	The license revocation at the Extreme Portal may fail.
Solution:	Contact GTAC and provide the VRK file. The GTAC will revoke the file manually.
Problem 13:	You cannot use scripting (including CLI scripts and workflows), configuration backup & restore, and firmware upgrade when the 4120 or 4220 switch is added to multiple ExtremeCloud IQ Site Engines. Authentication failure is reported.
Solution:	A maximum of one ExtremeCloud IQ Site Engine can fully manage the 4120 and 4220 series. Remove the switch from all Site Engines and add it to one Site Engine.
Problem 14:	Links from devices running multiple areas are not displayed on the map (**Map > View > Show Fabric Connect**). Devices running Fabric Engine firmware 8.10 and 9.0. have a known defect when SNMPv1 or SNMPv2 is used.

Solution:	Use SNMPv3 and allow access to the isisRemote context.
	
	Configuration example:
	
	`snmp-server view ALL 1`
	`snmp-server group RW "" auth-priv read-view ALL write-view ALL notify-view ALL`
	`snmp-server user snmpuser group RW md5 snmpauthcred des snmpprivcred`
	`snmp-server group "RW" "isisRemote" auth-priv read-view ALL write-view ALL notify-view ALL`
	
	if the SNMPv3 is already used then you can use script "Enable reading multi-area fabric links" to configure the context isisRemote on devices running Fabric Engine firmware prior to 9.0.3.

Web Applications

Problem 1:	When authenticating to an ExtremeCloud IQ Site Engine web application, if you fail to submit your login credentials within the server's configured session timeout, an HTTP 400 error is returned and you are directed to an error page.
Solution:	Resubmit the original URL to access the login page. This is typically done by pressing the browser's back button. When you have the login page you can submit your login credentials and authenticate to the web application.
Problem 2:	Windows OS only. There is a known issue when using certain versions of Java 1.7 on Windows to launch an ExtremeCloud IQ Site Engine client application. If you are using Java 1.7u6 or Java 1.7u7, under certain conditions Java Web Start will fail to start the client application. The conditions are if you have enabled ExtremeControl engine administration client diagnostics or changed the client trust mode in the **Server Information Certificates** tab to something other than the default. These two conditions cause the client application URL to contain a question mark. When this happens, Windows displays a message indicating that the Java Web Start Launcher has stopped working. The problem details indicate "Problem Event Name: BEX" and "Application Name: javaws.exe".

Solution:	This is a known issue with Java 1.7, and is described in the following Java bug report: http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7192904 At this time, there is no indication of when Sun will fix this issue. Java 1.7u7 is the latest version of Java at the time this issue was discovered, and it can continue to be present in subsequent versions. The best workaround for this issue is to not use any version of Java 1.7 later than update 5, which is available in the Java Archive section of the Java web site. However, this issue will not be present with any version of Java if you don't enable client diagnostics, and if you use the default client trust mode, which prompts the end user to accept or reject any untrusted server certificate.
Problem 3:	When attempting to access ExtremeCloud IQ Site Engine using Firefox Quantum 62.0.3, ExtremeCloud IQ Site Engine occasionally does not load.
Solution:	Ensure **Cached Web Content** is selected in the Firefox options and clear the cache.

ExtremeCloud IQ Site Engine Clients Running Mac OS

Problem 1:	Installing the Agent-Based Assessment Agent on the MAC OS version 10.8 occasionally displays an "Unidentified Developer" warning if you have installed the Security Update 2014-005. This issue occurs because the security update invalidates the previous install/code signing certificate that is used to identify the Agent-Based Assessment Agent.
Solution:	There are two work-around methods to install the agent: you can either right-click on the NacAgentInstall.mpkg file and select open, which displays the warning, but enables you to proceed with the installation, or you can change the System Preferences > Security & Privacy setting to enable applications downloaded from *** Anywhere ***.
Problem 2:	The Java Web Start icon is displayed on the system Dock instead of the ExtremeCloud IQ Site Engine application icons.
Solution:	In order for each ExtremeCloud IQ Site Engine application to display the correct icon, you need to access the Java Web Start settings and have Web Start generate the application shortcuts to the local file system. To do this, go to /Applications/Utilities/Java Preferences, access the "Network" tab, and select the "View Cached Files..." button. Select the application you want to display an icon for, and select "Install Shortcut." The correct icon for each application is then displayed on the Dock.

Problem 3:	Attempting to use Facebook to register an end-system on the network (selecting the **Register with Facebook** button in the Captive Portal window) via the Mac Captive Network Assistant browser can fail, displaying an error stating that cookies are required and to enable them in the browser.
Solution:	Connect to the network via the system browser (i.e. Safari).

Alarm and Event Manager

Problem 1 :	On Red Hat Linux: Scripts that launch GUI based executables (e.g. xterm, xpdf) that have been configured as an Alarm Action do not launch correctly. On SuSE Linux: Scripts that launch GUI based executables (e.g. xterm, xpdf) that have been configured as an Alarm Action do not launch correctly. Testing a script that has been configured as an Alarm Action works, but the script doesn't launch when triggered by Alarm Criteria (e.g. By Device Status Change). Executing scripts that launch non-GUI based programs works correctly on Red Hat and SuSE Linux. These problems do not appear on Red Hat Enterprise WS, ES.

Device Firmware

Problem 1:	The E5 device always reports TFTP firmware download as successful, even when the TFTP firmware download fails because of a problem with the firmware filename. A TFTP firmware download or TFTP configuration upload will fail if the length of the entry for the Last Filename is longer than the Full Image Path entry for the firmware being downloaded. The corruption is caused by remnants of the longer (earlier) filename. For example, attempting to download firmware with a Full Image Path of firmware/03.00.07 when the Last Filename is images/E5/Lowrider/03.00.06 results in a corrupted filename of firmware/03.00.07r/03.00.06. The r/03.00.06 portion of the corrupted filename is a remnant of the Last Filename.
Solution:	This problem will be corrected by firmware version 03.00.11.
Problem 2:	C2 Devices only. Starting in firmware version 03.03.14, some of the pre-defined FlexViews like Port Spanning Tree Information, will not return properly.
Solution:	Telnet to the device and, using Local Management, navigate to the Network Configuration View and Save the configuration.

FlexViews

Problem 1:	Some MIB tables do not work in FlexViews. Any column in a FlexTable that is instanced by TimeFilter is empty for devices whose firmware improperly implement TimeFilter.
Solution:	The MIB tables can have time filters in them. MIB tables with time filters do not work in FlexViews.
Problem 2:	Attempting to Enforce values for MIB objects that are not supported in a device will report a Set Failure. In particular, this will occur when attempting to map a transmission priority to a traffic class in E5 or Vertical Horizon devices using FlexView Table Editor to map priority using the dot1dTrafficClass MIB. This also poses a problem for E1 devices. While the device does recognize the dot1dTrafficClass MIB, attempting to SET a value fails. This occurs because although these devices do support mapping of Priorities 0-7 to four separate Traffic Classes, the mapping is global to each Priority as opposed to each instance of that Priority. FlexView attempts to perform the mapping per instance (dot1dTrafficClass) and the SET fails.
Problem 3:	The order of bits for writable, enumerated MIB objects is occasionally displayed incorrectly for FlexViews . When a device returns bits for an enumerated object in the incorrect (reverse) order, the value will be displayed incorrectly in the FlexView. When the value displays incorrectly in a FlexView, it cannot be reliably used to edit and enforce values for enumerated OIDs on devices. You can verify whether the bits are returned in the correct order by examining the raw bit value, either through MIB Tools or by creating an expression column that displays the raw value for the column containing the Bits values.
Solution:	Verify the correct order of bits, as suggested, or use MIB Tools to edit and set writable enumerated OIDs.

VLAN

Problem 1:	The Advanced Port view of the **Console VLAN** tab is not supported on the 800-Series.
Problem 2:	ExtremeXOS/Switch Engine devices do not enable you to configure multiple VLANs on the same port.
Solution:	To configure VLANs on an ExtremeXOS/Switch Engine device, enter '`configure vlan untagged-ports auto-move on`' in the ExtremeXOS/Switch Engine device command line. This command is only available in the ExtremeXOS/Switch Engine device version that supports dot1q VLAN MIBs.

RoamAbout Wireless Manager

Problem 1:	WPA Clients settings do not apply for WPA2 specific authentication types. To see the problem, open the Element Configuration window, select a Wireless Interface in the left-panel tree, and select the right-panel **Security** tab. The WPA Clients settings (Supported, Required, Not Supported) are available, and apply only to the following authentication types: Open System, Shared Key, WPA, WPA-PSK, WPA-WPA2-Mixed, and WPA-WPA2-PSK-Mixed. WPA2 Clients settings are not currently supported via SNMP and are not available for selection. The WPA2 Client settings apply to the WPA2 and WPA2-PSK authentication types and must be set via WebView or CLI. If you select the WPA2 or WPA2-PSK authentication type, the WPA Client settings are still available for selection but they do not apply. However, be aware that if you change the WPA Client setting to Required and then hit Apply or OK, the authentication type will change to WPA-WPA2-Mixed or WPA-WPA2-PSK-Mixed, respectively.

FlexView Editor/MIB Tools

This section includes the Known Restrictions and Limitations for FlexView Editor/MIB Tools.

Problem 1:	MIB Tools will report a Set Failure with a "No Such Name" error when attempting to set a value for a MIB object that is not supported in the device. In particular, this will occur when attempting to map a transmission priority to a traffic class in E5 or Vertical Horizon devices using MIB Tools to map priority using the dot1dTrafficClass MIB. This also poses a problem for E1 devices. While the device does recognize the dot1dTrafficClass MIB, attempting to SET a value fails. This occurs because although these devices do support mapping of Priorities 0-7 to four separate Traffic Classes, the mapping is global to each Priority as opposed to each instance of that Priority.
Problem 2:	Cabletron trap OIDs (1.3.6.1.4.1.52.0*) cannot be displayed in the MIB tree in MIB Tools. This branch in the MIB tree has been disabled to avoid naming conflicts.
Solution:	To see the trap description for a particular trap, type the OID for the trap into the Current Object field and press Enter. The description will be displayed in the Details panel.

Problem 3:	A query on the dot3adAggPortDebugRxState MIB returns <Not Defined> as the Formatted Value in the Results table. This happens because the keyword "current(1)" displays all in lowercase in the MIB enumeration and cannot be imported correctly. The same problem can happen in other MIBs with the following keywords: mandatory(x) optional(y) obsolete(z)
Solution:	A workaround to display the correct Formatted Value in MIB Tools is to use a text editor to edit the MIBs in the ExtremeCloud IQ Site Engine client "mibs" directory and change the keyword so that it is not all lowercase. For example: Current(1) Mandatory(x) Optional(y) Obsolete(z)
Problem 4:	Starting the MibTools/FlexView editor causes a "Microsoft Visual C++ Runtime Library Debug Assertion Failed!" error.
Solution:	Select the **Ignore** button**.**

Inventory Manager

This section includes the Known Restrictions and Limitations that apply to the ExtremeCloud IQ Site Engine Inventory Manager feature.

General

Problem 1:	Downgrading firmware/boot PROM to a previous revision.

Solution:	Downgrading firmware/boot PROM is inherently risky due to possible feature differences between revisions. Restoring configurations from different firmware revisions carries the same risk. Should you need to downgrade your firmware/boot PROM to an earlier version, it is recommended that you use one of the following two procedures: 1. Downgrade the firmware/boot PROM on a network device using the Firmware Upgrade Wizard or Boot PROM Upgrade Wizard. Do not proceed to the Restart portion of the wizard, instead select [Finish]. Restore an archived configuration that was previously created with the firmware image being downloaded. This will reset the device. **or** 2. Downgrade the firmware on a network device using the Firmware Upgrade Wizard or Boot PROM Upgrade Wizard. Complete the downgrade using the wizard Restart screen. Clear NVRAM on the device and reconfigure the network configuration parameters of the device using the local console.
Problem 2:	Creating multiple devices for a single router (based on the router's different IP addresses for its different interfaces), could result in SNMP errors or TFTP server performance problems.
Solution:	Create only one device for a router using the IP address of the router's main interface.
Problem 3:	Aborting a Timed Restart occasionally does not stop all resets. The Timed Restart section of the Firmware Upgrade Wizard and Restart Wizard has the option to abort the operation after it has been started. In some circumstances, it is possible that the Abort message will get overwritten by the process that sets the reset timers. This can cause some devices to reset as scheduled.
Solution:	To abort a Timed Restart operation that you have already started, select the Abort button after all devices have a "Restart Request Status" of "Success". Note: The Abort button is not a guarantee that you can back out of a Timed Restart operation, since it is possible that reset timers expire before you decide to abort the operation.
Problem 4:	A firmware or boot PROM upgrade fails with an "Operation Failed" or "Access Violation" message.
Solution:	If the firmware image being transferred is not stored in the firmware directory specified for the file transfer protocol being used, the upgrade operation will fail. Verify that the firmware image is accessible to the file transfer method (FTP, TFTP, or SCP) configured for the device. For information, see File Transfer Settings Options and How to Set a File Transfer Method in the Inventory Manager online Help.

Problem 5:	If you change a firmware image in your firmware directory but the filename stays the same, performing a firmware Refresh will not update the image information. For example, if you replace a firmware image with an image of the same name but a newer version number, and then perform a firmware Refresh, Inventory Manager will continue to display the older firmware version number.
Solution:	Delete the firmware image from Inventory Manager and then perform a firmware Refresh. You can also update a firmware's version number on the firmware image's **General** tab.
Problem 6:	When using a remote file transfer server to perform a firmware or boot PROM upgrade, the operation fails with an "SNMP Timeout" error.
Solution:	Verify that Inventory Manager has SNMP contact to the device, that the device has TFTP, FTP, or SCP access to the remote server, and that the path and file name are correct.
Problem 7:	Archive save operations performed on Cisco devices using scripts will not work when using an SCP server on Linux.
Solution:	Use an FTP or TFTP server on Linux

Device Firmware

Problem 1:	The E5 serial number is occasionally not displayed in Inventory Manager.
Solution:	Upgrade the E5 firmware to version 3.00.06 and clear NVRAM. The serial number should now display correctly.
Problem 2:	Archive operations on E1 devices fail following a failed firmware upgrade operation.
Solution:	Restart the E1 device. Following a reset, the archive operation should be successful.
Problem 3:	E1 Devices only. Archive and Restore Archive operations occasionally do not work properly if the device is modeled using a Routing IP address.
Solution:	Create (add) E1 devices using a Switch IP address.
Problem 4:	E1 and N-Series devices utilizing SNMPv3. When restoring a configuration or performing a configuration template download, you are not able to regain contact with the device. In addition, the error message "SNMP Error - Unknown User Name" displays in the Message column of the Restore Configurations window (Restore Wizard) or the Download Template Configurations window (Template Download Wizard).
Solution:	To regain contact with the device, you must reenter the SNMP user information via CLI. In addition, N-Series devices require that you restart the Inventory Manager Server, however E1 devices do not.
Problem 5:	E5 Devices only. An archive operation fails with a "Config file is empty" message.

Solution:	Restart the E5 device. Following a reset, the archive operation should be successful.
Problem 6:	A2, B2, C2, and N3 Devices with SNMPv3 credentials only. Following an archive restore operation, Inventory Manager loses contact with the device because the device is returning a wrong SNMP value.
Solution:	You must restart the ExtremeCloud IQ Site Engine Server to contact the device.
Problem 7:	E1 Devices only. A Restore Configuration or Download Configuration Template operation fails with a General Error.
Solution:	It is possible that the operation was actually successful even though Inventory Manager reported that it failed. Perform an archive of the device's configuration file and use the View Configuration File window to determine if the configuration was actually restored or downloaded to the device.
Problem 8:	X430 Devices only. After upgrading the device firmware, devices are occasionally slow to validate a new firmware image. This can result in the device timing out.
Solution:	Write a new script to increase the amount of idle time before the device times out. For example, changing the Firmware Upgrade section from `@COMMANDDONE 30` to `@COMMANDDONE 120` increases the amount of time the device is idle before it times out from thirty seconds to two minutes.

ExtremeCloud IQ Site Engine

This section includes the Known Restrictions and Limitations that apply to ExtremeCloud IQ Site Engine.

Problem 1:	An error occurs if a report is not to completely load before selecting a new report.
Solution:	Reloading the report should correct the problem.
Problem 2:	Some report data is inaccurate when there is a large Time Zone difference between the ExtremeCloud IQ Site Engine server and a remote ExtremeCloud IQ Site Engine client. This happens with the Wireless Summary, Controllers Down, and APs Down reports.
Solution:	Remote desktop to the ExtremeCloud IQ Site Engine server and run ExtremeCloud IQ Site Engine locally or run ExtremeCloud IQ Site Engine on a machine that has the same settings for Time Zone and Current Time as the ExtremeCloud IQ Site Engine server machine.
Problem 3:	When the Device Availability report is launched from the **Network** tab (via the right-click menu option "View Device Availability"), a popup warning message is displayed in the web browser. When you accept the message, the report is displayed in either a new window or a new tab.

Problem 4:	ExtremeCloud IQ Site Engine charts do not display when viewed with Internet Explorer 9.
Solution:	From the browser toolbar, go to **Tools** > **Internet Options** > **Advanced** tab. In the Settings list, deselect the "Do not save encrypted files to disk" option. If security is a concern, you can go to **Tools** > **Internet Options** > **General** tab, and under Browsing history, check the "Delete browsing history on exit" option.
Problem 5:	In rare instances when a large number of very complex reports are loaded in ExtremeCloud IQ Site Engine at the same time, an error is reported in the server log and an "Error Encountered" message is displayed in the browser.
Solution:	This error can be ignored. This will be fixed in a future release.
Problem 6:	Some combinations of ExtremeCloud IQ Site Engine capabilities do not work as expected. There can be links or menu items that do not work and result in an access-denied message when used. Some page elements do not display properly and other page elements show data that should be disabled.
Solution:	ExtremeCloud IQ Site Engine supports five categories of users, as described in ExtremeCloud IQ Site Engine Access Requirements of the top-level ExtremeCloud IQ Site Engine Help topic: • Full Read/Write Access: full read/write access to all ExtremeCloud IQ Site Engine features. • Read-Only Access: read-only access to all ExtremeCloud IQ Site Engine features. • Limited Read-Only Access: limited read-only access to only ExtremeCloud IQ Site Engine reporting and wireless data. • End-System Information, Read-Only Access: read-only access to ExtremeCloud IQ Site Engine end-system information. • End-System Information, Read/Write Access: read/write access to ExtremeCloud IQ Site Engine end-system information. For each category, there are a specific set of ExtremeCloud IQ Site Engine capabilities which are configured to enable the appropriate access. Other combinations of ExtremeCloud IQ Site Engine capabilities are possible. However, the result occasionally does not work as expected. Always test any set of ExtremeCloud IQ Site Engine capabilities before putting them into use. Be sure that the different features of ExtremeCloud IQ Site Engine work as expected, and familiarize yourself with what information is provided and what information is not provided.

Problem 7:	When performing a Search in a web FlexView, the Search query overrides any Filters currently configured for the view. This results in additional data being displayed.
Solution:	Filter multiple columns in the FlexView to reduce the amount of data displayed.
Problem 8:	If you disable and then re-enable one or more data sets in the legend for the Authentication Types graph in the ExtremeControl Dashboard, the graph lines are redrawn in the wrong position.
Solution:	Resizing the browser window corrects the graph, however the y-axis occasionally shows duplicated values. In this case, resize the browser again.
Problem 9:	**Maps** tab. When using Internet Explorer 8 to view an OSGeo map, an IE Security Warning message is displayed. Selecting Yes in the Security Message results in an ExtremeCloud IQ Site Engine "Could not load report" error message.
Solution:	If the security issue is a concern, change the map to a different map type, such as Image.
Problem 1 0:	**Maps** tab. When viewing a map using Internet Explorer 8, map device icons disappear following the launch of device information from the right-click menu.
Solution:	Refresh the web page to correct the problem.
Problem 1 1:	When expanding and collapsing ExtremeCloud IQ Site Engine navigation panels using the >> and << arrow buttons, odd behavior can result. For example, the navigation panel can disappear or be grayed out. This is caused by not selecting squarely on the arrow button.
Solution:	Restore the navigation panel by selecting squarely on the arrow buttons to expand/collapse the panel.
Problem 1 2:	The PDF file attached to an ExtremeCloud IQ Site Engine Scheduled Report email is empty when the ExtremeCloud IQ Site Engine Server is installed on a 64-bit openSUSE 12 server or a 64-bit Red Hat 5.9 server.

Solution:	There are five packages of libraries that must be installed on the 64-bit openSUSE 12 server in addition to the default libraries: libopenssl-devel-1.0.1e-1.4.1.x86_64.rpm linux-glibc-devel-3.7.1-2.1.3.noarch.rpm glibc-devel-2.17-4.4.1.x86_64.rpm zlib-devel-1.2.7-7.1.1.x86_64.rpm libpng12-0-1.2.50-6.4.1x86_64.rpm* *This is for the NetSight 6.3 release going forward. There is one package of libraries that must be installed on the 64-bit Red Hat 5.9 server in addition to the default libraries: openssl-devel-0.9.8e-26.el5_9.1.x86_64.rpm
Problem 1 3:	When adding a Cisco device to a map, the map does not show connections between the Cisco device and the neighboring devices.
Solution:	Manually run "Refresh (Rediscover)" on the devices to which the Cisco device is connected.
Problem 1 4:	When a Wireless Controller is deleted from ExtremeCloud IQ Site Engine and then re-added, any maps with APs associated with that controller need to be resaved. This causes the APs to be reassociated with that controller and the map data to be uploaded.
Problem 1 5:	Ports/interfaces with a type of propVirtual (typically VLAN ports with a "vm" prefix in the Name) cannot be used by scripts in ExtremeCloud IQ Site Engine. As a result, the scripting engine removes the port/interface before being passed to the script.
Problem 1 6:	When accessing ExtremeCloud IQ Site Engine using the Mozilla Firefox web browser on a system using the Microsoft Windows operating system, the bottom line of dialog boxes is occasionally not fully visible.
Solution:	Change the text size setting in Windows operating systems to match the following criteria: • **Smaller** in Windows 2012. • **Smaller - 100%** in Windows 7 and Windows 8. • **100%** in all other versions of Windows.
Problem 1 7:	Legacy E6/E7 devices do not support a VLAN ID (VID) of 0 (which denies traffic), or 4095 (which permits traffic without tagging it) in ExtremeCloud IQ Site Engine. A Policy Manager enforce in ExtremeCloud IQ Site Engine fails if the domain contains a role or rule using either of these VIDs.
Solution:	Set policy for the E6/E7 device using the Policy Manager java application or change the domain configuration to use a VID other than 0 or 4095.

Problem 1 8:	Legacy E6/E7 devices do not support domains containing roles or rules using the deny access control in ExtremeCloud IQ Site Engine.
Solution:	Set policy for the E6/E7 device using the Policy Manager java application or change the domain configuration to use a VID that does not forward traffic.
Problem 19:	ExtremeCloud IQ Site Engine does not support SNMP traps configured prior to the device being added to ExtremeCloud IQ Site Engine.
Solution:	Remove the trap and reconfigure the trap via ExtremeCloud IQ Site Engine.
Problem 20:	When ExtremeCloud IQ Site Engine configures the SysLog server on an ExtremeXOS/Switch Engine device, the **ServerIP** is not included.
Solution:	Delete the **Config_Syslog** file in the `<install directory>/appdata/scripting/override$` folder.
Problem 21:	Running a command via the **Execute CLI Commands** option on the **Devices** tab that does not complete (**Results** are a failure), going back to the **Commands** tab, changing the commands, and selecting **Execute** to run the new command can display the following error: `Error executing command Busy executing commands`
Solution:	Select **Cancel** to close the **Execute CLI Commands** window and reopen the window with the new command.
Problem 22:	When running a command via the **Execute CLI Commands** option on the **Devices** tab and the command output pauses for more than one second, the **Results** tab occasionally does not display the entire output of the CLI command execution. This does not affect the command execution.
Problem 23:	Vertical scroll bars do not work when accessing ExtremeCloud IQ Site Engine using Mozilla Firefox version 59.0.1.
Solution:	Upgrade to Firefox version 61.0.1.
Problem 24:	Creating an archive of a device on which the ERS operating system is installed and with **cmd-interface** set to **menu** results in removal of management IP and can result in loss of connectivity between ExtremeCloud IQ Site Engine devices.

Solution:	Enter the following in the device CLI:
	
	`config t`
	`cmd-interface cli`
	`exit`
	`save config`

Problem 25:	Configuring ZTP+-enabled ExtremeXOS/Switch Engine devices with more than 50 ports can take more time than other devices. The time to configure increases with the number of ports.

Problem 26:	When ExtremeCloud IQ Site Engine sends a configuration change to a ZTP+-enabled device on which the **Local Changes Alarm** option is enabled, the local changes detected alarm occurs, regardless of whether local changes were made to the device.
Problem 27:	Firmware on SLX 9140 and SLX 9240 devices can not be upgraded via TFTP in ExtremeCloud IQ Site Engine version 26.11.10. To upgrade firmware on these devices, use SCP or SFTP.
Problem 28:	Enforcing a static VLAN via ExtremeCloud IQ Site Engine on an ExtremeXOS/Switch Engine device that will override a dynamic VLAN with the same VID completes successfully, but HTTP ERROR:409 CONFLICT errors are displayed in the server.log file.
P**roblem 29:**	Renaming Port Templates for a Site does not update the Port Role in the **Configure Device** window.
Solution:	Update the Port Role manually.
Problem 30:	If an "AutoSense" Port Template exists prior to upgrading to ExtremeCloud IQ Site Engine version 21.9, delete the Port Template. Beginning in ExtremeCloud IQ Site Engine version 21.9, AutoSense is a predefined port template.
Problem 31:	Do not rename the system Port Templates that are pre-installed in ExtremeCloud IQ Site Engine version 21.9. The Port Templates are used by ZTP+ to map LLDP to Port Roles.
Problem 32:	ZTP+ process for devices running VOSS 8.5 and Fabric Engine does not disable auto-sense on the port even if configured to do so. If a non-auto-sense port template or configuration is assigned to the port during ZTP+ process, then this setting is ignored.
Solution:	Enforce the settings after the ZTP+ is finished.
Problem 33:	If the VSP8608 has over 150 VRFs/VLANs, the VRF ID value in **Configure Device > VLAN Definitions** could be reported incorrectly as -1.
Solutions:	The root cause of this behavior is the timeout of the SNMP communication. Increase the timeout value at **Administration > Options > SBI > Configuration > SBI Engine Transaction Timeout**.

Problem 34:	VOSS/Fabric Engine devices running version 9.4 and older require the following two switch configurations, otherwise secondary IPs are not listed for non-default VRFs.
	`snmp-server view "vrf" 1.3.6.1.4.1.2272.1.8.32`
	`snmp-server view "vrf" 1.3.6.1.4.1.2272.1.8.33`

ExtremeAnalytics

This section includes the Known Restrictions and Limitations that apply to ExtremeAnalytics.

Problem 1:	Packets routed through GRE tunnels on an ExtremeAnalytics virtual engine are reported as dropped in the ifconfig output on the GRE interface.
Solution:	Ignore the packets reported as dropped, as they are being inspected by the ExtremeAnalytics engine.
Problem 2:	SLX collector IP is not removed from the device after a telemetry source is deleted when a Single ERSPAN is assigned to eth1.
Solution:	Use CLI to remove the telemetry configuration from the SLX device.

ExtremeControl

This section includes the Known Restrictions and Limitations that apply to the ExtremeControl.

General

Problem 1:	When the Send VLAN Only feature is configured, the Active/ Default Role port mode on network devices requires a particular DHCP configuration. The DHCP lease time for the pool of IP addresses that corresponds to the default role's VLAN must be short (e.g. less than 1 minute) because the Active/Default Role port mode enables end-systems to obtain IP addresses via the DHCP protocol before they are authenticated to a VLAN.
Problem 2:	The EAP-TLS is rejected if the RADIUS certificate is signed by an intermediate CA.
Solution	To validate the full chain of certificates, add all intermediate certificates and the root CA certificate. For example, in a scenario where **Root > Inter1 > Inter2 > Inter3** (and Inter3 signed the client certs) you need to add all of the Inter and the Root to trust the full chain.
Problem 3:	For Enterasys devices only. Switch management via TELNET/WebView will fail with the following configuration in the Add/Edit Switches to ExtremeControl Appliance Group window: Auth Access Type = "Management Access" or "Any Access" RADIUS Attributes to Send = "RFC 3580 options" This is because switches check the "mgmt" attribute in the Filter-ID for Telnet management.
Solution:	To avoid this problem, set the Auth Access Type to "Network Access."
Problem 4:	The Last Scanned column in the **End-Systems** tab (which displays the last time a scan was performed on an end-system) is updated even if the scan failed. Therefore, it looks like the end-system was successfully scanned on the date that is listed, when in fact it was not.

Solution:	In the **End-Systems** tab, if the Last Scanned time is roughly the same as the Last Seen time (a few seconds earlier or so), and the end-system's State is "Error," then the end-system most likely was not scanned. Disregard the end-system's Extended State as it will stay in whatever state it was prior to the scan failing.
Problem 5:	E7 Devices. The RFC 3580 options (configured as RADIUS Attributes to Send in the Add/Edit Switches to Appliance Group window) are not supported on E7 devices.
Problem 6:	Assisted Remediation and Registration web pages take a long time (at least a minute) to display on the web browser.
Solution:	Add the ExtremeControl Engine name to your DNS server.
Problem 7:	In a network where Registration is deployed, the end-system cannot get to the Registration web page. The end-system's web browser gets stuck in the captive portal and provides the message "Please wait while your request is processed."
Solution:	This problem happens when the "Resolve IP Address" option is set to "Only for Assessment" in the **Appliance Settings IP Resolution** subtab. The "Resolve IP Address" option must be set to "Always" when Registration is deployed.
Problem 8:	In an ExtremeControl deployment utilizing RFC3580 and Agent-Based Assessment, if the end user exits out of the agent, ExtremeControl does not immediately detect the disconnect and put the end-system into quarantine. The disconnect will be detected after three failed agent heartbeats, which, by default, takes six minutes (3 * 2-minute default accept heartbeat interval).
Problem 9:	Enterasys A2 and A4 devices. If you have configured a primary and backup RADIUS server in your AAA configuration, all authentication requests go to the backup RADIUS server first. This can also happen if you have defined just a primary RADIUS server and also checked the "Use Primary RADIUS Server for Redundancy in Single ExtremeControl Appliance Config" checkbox in the Appliance Settings > **Credentials** tab.
Solution:	This will be fixed in a future firmware release for the A2 and A4 devices.
Problem 10:	The Registration System Administration web page does not update the group entry from Pending to Registered after the pending end-system has been approved.
Solution:	Manually refreshing the page after a few seconds will update the group.
Problem 11:	Refreshing the ExtremeControl Dashboard while the web page is loading causes an error in the server.log file.
Problem 12:	The Registration web page does not display on iPad devices using the Dolphin browser.
Solution:	Use a different browser such as Safari, Mercury, or Chrome.

Problem 13:	Custom field information in the Add/Edit End-System Group window does not dynamically update until you close and reopen the window.
Problem 14:	In certain circumstances where a firewall is enabled on an end-system or when a credentials scan cannot be performed, agent-less assessment can provide a less accurate OS detection for an end-system than DHCP fingerprinting.
Problem 15 :	If ExtremeControl Facebook Registration is configured with the Display AUP option selected, and the end user has reset the Safari browser to its factory settings, the end user can need to go through the registration process twice.
Problem 16:	Enforcing a Network Access RADIUS configuration to a switch with an existing RADIUS Management Server configuration that points to a non-ExtremeControl RADIUS server will re-write the existing management server configuration with the RADIUS Shared Secret defined in the ExtremeControl Configuration.
Solution:	Under Global and Appliance Settings->Appliance Settings->Default (or appropriate configuration)->Credentials configure the Share Secret to be the same as the shared secret used for the existing management access configuration.
Problem 17:	End-System Events exported to HTML can lose proper rendering after a certain point if the file is too large.
Solution:	Use a different browser to view the file, increase allocated browser memory, export a shorter list of events or export to a different format (such as csv).
Problem 18:	When using EAP-TEAP the fall-through option in AAA rules requires the computer authentication as EAP-TLS and the user authentication as MsCHAP to function.
Problem 19:	The Access Control Rule to reject 802.1X (PEAP-INNER-TUNNEL) also affects EAP-TEAP authentication using PEAP.
Solution:	If the 802.1X with PEAP-INNER-TUNNEL is not allowed and EAP-TEAP is allowed, then instead of assigning the "reject NAC profile" you can assign a "deny all NAC profile".
Problem 20:	The Access Control Rule to reject 802.1X (TTLS-INNER-TUNNEL) also affects EAP-TEAP authentications using either EAP-TLS or PEAP.
Solution:	If the 802.1X with TTLS-INNER-TUNNEL is not allowed and EAP-TEAP is allowed, then instead of assigning the "reject NAC profile" you can assign a "deny all NAC profile".
Problem 21:	The EAP-TLS Certificates with SHA1 are rejected. The radius server fails to start with the SHA1 certificate in use. Error in the log: "ca md too weak"
Solution:	Use certificates with more secure protocols, such as SHA256. The alternative option is to modify the SECLEVEL of the operating system, see: https://extreme-networks.my.site.com/ExtrArticleDetail?an=000113343.

Problem 22:	Change of the property "USE_FREERADIUS_V3OLD" could cause the radius service not to start for the first time.
Solution:	Enforce the setting to Access Control Engine again.

Agent-Based Assessment

Problem 1:	When the Agent-Based Assessment Agent is installed on a system on which the Windows 8.1 operating system is installed with the Windows Defender anti-virus program, the Security Center can incorrectly indicate that Windows Defender is Running when Windows Defender is disabled.
Solution:	Include the RTP Enabled setting in the Antivirus test to properly display the anti-virus status of Windows Defender.
Problem 2:	When installing the Agent-Based Assessment Agent on a Macintosh system on which a previous version of the Agent-Based Assessment Agent is currently installed, an error message can display that the installation has failed and to contact the manufacturer/vendor. This issue occurs because of a cache corruption when installing the new agent files.
Solution:	Exit the installation, delete the Applications/Utilities/NacAgent.app file, empty the recycle bin, and then install the Agent-Based Assessment Agent.
Problem 3:	When installing the Agent-Based Assessment Agent on a system on which MAC OS version 10.8 is installed, an "Unidentified Developer" warning can display if you have installed the Security Update 2014-005. This issue occurs because the security update invalidates the previous install/code signing certificate that is used to identify the Agent-Based Assessment Agent.
Solution:	There are two work-around methods to install the agent: 1. Right-click on the NacAgentInstall.mpkg file and select open, which displays the warning, but enables you to proceed with the installation. 2. Change the System Preferences > Security & Privacy setting to enable applications downloaded from *** Anywhere ***.
Problem 4:	During an agent-based assessment, auto-remediation fails for the P2P Software test and causes the end-system to remain quarantined. This happens when the agent is installed as a service, and the test set is configured to run a mandatory P2P software check with auto-remediate selected. Remediation fails (the software is not removed) and the end-system remains in quarantine.
Problem 5:	On Windows 2000 and Windows 7, the registry occasionally does not reflect the current state of the screen saver settings. This can cause the Screen Saver test for "Enabled" to pass or fail in error.

Problem 6:	The agent-based assessment test for EMULE P2P software is not supported on Mac end-systems.
Problem 7:	Some versions of Mac OS X will show an agent icon on the Dock. Newer updates of the OS do not seem to exhibit this issue.
Problem 8:	Firewall remediation is not supported on Mac OS X v10.4 Tiger.
Problem 9:	If the agent-based test set includes a File Check test and the agent version is ExtremeControl 3.1.3 (or older), the scan will not complete.
Problem 1 0:	The agent on Mac OS X can unexpectedly exit.
Solution:	Running the uninstall script in the /Application/Utilities/NacAgent.app/Contents/Resources/ directory and then reinstalling the agent resolves the problem.
Problem 1 1:	If you install a Persistent agent over a Service agent of the same version, the Service agent will not be uninstalled. The Control Panel Add/Remove programs will show that both agents are installed, and the agent will continue to run in Service mode after the next restart of the machine. However, if you upgrade to a new version of the Persistent agent, this problem will not happen because all older/existing versions of the agent will be uninstalled first.
Solution:	Use the Control Panel Add/Remove programs to remove the Service agent prior to installing the Persistent agent.
Problem 1 2:	Auto-remediation will not work when running the Patch Auto Update test for agent-based assessment on Mac OS X v10.7 Lion.
Solution:	You must manually enable or disable Software Update under System Preferences on the end-system.
Problem 1 3:	On some Windows XP systems, when Auto Update is enabled but never installed any updates successfully, ExtremeControl will incorrectly report that updates had been recently performed.
Problem 1 4:	The Patch Auto Update test for agent-based assessment is not supported on Mac OS X v10.8 Mountain Lion, v10.9 Mavericks, v10.10 Yosemite, and v10.11 El Capitan.
Problem 1 5:	Launching the dissolvable ExtremeControl agent (Agent.jnlp) on end-systems running Mac OS X results in the following message: "Agent.jnlp can't be opened because it is from an unidentified developer." This message results on OS X systems with Security settings set to only enable applications from identified developers.

Solution:	There are three work-around methods for this scenario that will force the agent to run. They are listed below in the preferred solution order. 1. Find the downloaded jnlp file and choose the Open or Open With (Java Webstart) option. You will see a dialog with an "Open" button. 2. Open the Preferences > **Security & Privacy** tab after a failed jnlp launch and you will see the jnlp file listed with an "Open Anyway" button. Select this button to run the jnlp file. 3. Open the Preferences > **Security & Privacy** tab and change the "Allow apps downloaded from" option to "Anywhere" and then select the jnlp file again.
Problem 1 6:	On Mac OS X systems, if you run the dissolvable agent and then install the persistent agent, you can have two agent processes running.
Solution:	You can either exit the old process for the dissolvable agent, or restart your Mac. After the restart, the dissolvable agent will no longer be running.
Problem 1 7:	Using Auto-Remediate functionality that results in the Agent attempting to Auto-Remediate can cause your system to present a UAC (User Account Control) prompt, depending on your UAC settings. If you select **Yes** to enable the Network Command Shell to make changes, the Auto-Remediate completes successfully, while selecting **No** can result in being quarantined.
Problem 1 8:	Mac OS X end-systems on which Agent-Based assessment is configured accessing the network via the Mac Captive Network Assistant browser can be placed into a quarantine state after connecting to the network. Additionally, the ExtremeControl Agent can go into a "disconnected" state, causing the ExtremeControl Remediation page to display. Attempting to download the Agent from this page fails.
Solution:	Connect to the network via the system browser (i.e. Safari).
Problem 1 9:	Results for the "Up to Date" anti-virus test can incorrectly state that your anti-virus software is not up to date when running Sophos EndPoint Protection.
Problem 20:	Assessment agents can no longer establish a TLS1.0/TLS1.1 session; rejected due to Protocol Failure.

Solution:	On each Access Control Engine perform the following: `cd /opt/nac/server/config` `cp config.properties config.properties.original` `nano / nano config.properties` * Add the following cipher override. The last two strings are TLS1-compatible ciphers. `enterasys.tomcat.ciphers=ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-ECDSA-CHACHA20-POLY1305,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-SHA256,ECDHE-RSA-AES128-SHA256,ECDHE-ECDSA-AES256-SHA384,ECDHE-RSA-AES256-SHA384,ECDHE-ECDSA-AES128-SHA,ECDHE-RSA-AES128-SHA` * Save the file. Restart the Control appliance using: `nacctl restart`

Access Control Engines

Problem 1:	This problem applies to Access Control engines configured for redundancy that are running agent-based assessment with remediation enabled. If the primary Access Control engine goes down, new end-systems are not able to download the agent from the Remediation Web Page. When the end user selects the link to download the agent, the user is again brought to the Remediation Web Page and is unable to download the agent. This is because the policy-based routing (PBR) configured on the router continues to redirect the web traffic sourced from quarantined end-systems to the remediation web server instead of sending it to the secondary Access Control engine (where the agent could be downloaded).

Solution:	The remediation policy-based routing ACL needs to be modified to enable traffic to pass to the secondary Access Control engine. In the following example, the line in red denotes the line added to address the problem. In this line, xx.xx.xx.xx is the IP address of the secondary Access Control engine. By denying this traffic in the ACL, it will not be redirected to the primary engine.
	`access-list 100 deny tcp any host xx.xx.xx.xx eq 8080`
	`access-list 100 permit tcp any any eq 8080 dscp 32`
	`access-list 100 permit tcp any any eq 80 dscp 32`
	`route-map 100 permit 100`
	`match ip address 100`
	`set next-hop 10.20.30.40`

Problem 2:	When installing Access Control engine software on an SNS-TAG-ITA engine using the USB flash drive, the drive is not recognized properly and the "boot:" prompt never displays. After choosing the boot device from the BIOS Boot Manager menu, the cursor blinks and the install does not proceed.

Solution:	When the engine is booting, press F2 for the BIOS setup menu. Select "USB Flash Drive Emulation Type" and hit Enter. Press the spacebar to change the Front USB from Auto to Hard Disk, and hit Enter. After the setting is changed, the engine boots from the USB flash drive normally.
Problem 3:	If the engine system time is set back a significant amount (e.g. minutes), the timing support in critical engine processes are adversely affected. A likely indication of this problem would be that the engine icon in the NAC Manager left-panel tree turns orange.
Solution:	Reboot the engine.
Problem 4:	Changing the internal communication certificate on the ExtremeCloud IQ Site Engine server or reverting an Access Control engine to a previous release, can cause a communication issue between ExtremeCloud IQ Site Engine and the Access Control engine(s). The following errors can be reported in the server.log, but resolve automatically after the next polling: ERROR [com.enterasys.netsight.tam.server.ApplianceEnforcer] error communicating with Access Control engine web service: org.apache.axis2.AxisFault: server certificate change is restrictedduring renegotiation ERROR [com.enterasys.netsight.tam.server.NacStatusPoller] Error polling appliance at IP: 1.2.3.4 with error: server certificate change is restrictedduring renegotiation
Problem 5:	User passwords for engines on which the Linux operating system is installed do not expire.
Solution:	Follow the instructions found in the How to Configure Your Password to Expire.
Problem 6:	The Agent-less Assessment server does not start on the initial startup of the IA-A-25 and IA-A-305 Access Control engines.
Solution:	Open the `/etc/init.d/nacservices` file and add a close bracket (]) to lines 77 and 189 after `[ $TAG_TYPE = "ia305"` (e.g. change `[ $TAG_TYPE = "ia305" || [ $TAG_TYPE = "ia25" ]` to `[ $TAG_TYPE = "ia305" ] || [ $TAG_TYPE = "ia25" ]`.
Problem 7:	When the Access Control Engine interface mode is configured to Management Only, the End-System Registration service is also available.
Solution:	You can use a firewall or access control lists to limit unwanted access to the Management interface, or you can use the Advanced Mode to uncheck both Portal Management and End-System services to disable the portal access to the interface.

Problem 8:	RadSec configuration on a switch fails if the switch runs software earlier than Switch Engine 33.6.1 or Fabric Engine 9.3, or if OpenAPI is not running on the switch.
Solution:	Upgrade the switch to a supported software version and enable OpenAPI on the switch. For Fabric Engine, a switch license might also be required. For more information, see the switch documentation.
Problem 9:	RadSec configuration for ExtremeCloud IQ Controller is not supported.
Problem 10:	You cannot use self-signed certificates, including the default RADIUS server certificate, to secure RadSec communication. A switch does not trust the default RADIUS server certificate, and the RadSec connection fails with an unknown CA error.
Solution:	Replace the default RADIUS server certificate with a certificate that your CA issues. Add the certificate of the CA that issued the replacement certificate to the RADSec Client CA Certificate table and assign it to the switches. Add the CA that issued the certificate of each switch to the Trusted Authorities of the AAA configuration.

Policy Manager

This section includes the Known Restrictions and Limitations that apply to the ExtremeCloud IQ Site Engine Policy Manager feature.

General

Problem 1:	(Windows XP only.) A Web-based Authentication user fails to connect to the switch for the Web Authentication web page, and an error message states that the Microsoft Java VM (Virtual Machine) must be downloaded before the page will be displayed. This occurs because, while most XP systems are set up with the Java VM, this particular machine was not.
Solution:	Download the Microsoft Java VM from www.microsoft.com and install it.
Problem 2:	Even though Layer 3 Priority rules are not supported on N-Series Gold devices, if you have created a TCI rule through local management on a Gold device, you will be able to import that rule using the Import From Device wizard. However, when you perform an Enforce, the rule will be Excluded, and will be deleted from the device.
Solution:	This issue will be addressed in a future release.
Problem 3:	Renaming a role causes the role to not be assigned properly during authentication.
Solution:	When you rename a role in Policy Manager, the role name in the filter-id also needs to be updated in the RADIUS configuration.

Problem 4:	Enterasys C2 and B2 devices do not implement the attribute required for Policy Manager to detect or display a Role Override in the Type column of the **Port Usage** tab.
Problem 5:	(Enterasys C2 and B2 devices only.) Rate limits only work for Priority 0.
Problem 6:	(Enterasys B2 devices only.) Terminating an 802.1X session results in the Duration field being reset to "497+2:27:51" on the **Port Usage** tab.
Problem 7:	The N-Series Platinum devices and X devices enable users to create LLC (DSAP/SSAP) rules with a mask less than 17 bits (i.e. 0xFFFF000000) via CLI. If these rules are imported from devices (File > Import Policy Configuration From Device), either the rules are not imported successfully or the masks of the rules are imported correctly but the masks are not displayed correctly in the Edit Rule window.
Problem 8:	(Devices with Class of Service mode set to either "Rate Limits Disabled" or "Priority Based Rate Limits" in the **Device General** tab.) A rule with an associated user-defined Class of Service (CoS) that does not include an 802.1p priority, will not be written to the devices during an enforce, even though the Enforce Preview window lists the rule as "Included" for the next enforce. This happens whether the CoS has a ToS value defined or not. As long as the CoS does not include an 802.1p priority, the rule will not be enforced.
Solution:	This will be fixed in a future release.
Problem 9:	(All Enterasys fixed switching devices running 1.01, 4.01, or 5.01 firmware.) When the device has multiple authenticated 802.1X RFC3580 sessions on a port, the **Port Usage** tab End User Session entry for one user will have complete data, but the remaining entries will be missing the following data: Terminate Cause, User Name, Received/Transmitted Bytes, and Received/Transmitted Frames.
Problem 10:	(All Enterasys fixed switching devices.) Setting the Authenticated User Counts (Port Properties Window > **Authentication Configuration** tab) results in an error message even though the new values are set correctly on the device.
Solution:	Performing a Refresh will display the correct values on the tab.
Problem 1 1:	(G3 devices and C3/B3 devices running 1.01 firmware.) You are unable to create any Ethertype traffic classification rules after having created seven Ethertype rules with a "Contain to VLAN" action. This is due to a firmware issue that restricts the G3/C3/B3 to a maximum of seven VLAN Ethertype rules. When this maximum is achieved, you are unable to create Ethertype rules of any type (VLAN/Permit/Deny).
Solution:	If you create only six VLAN Ethertype rules (instead of the maximum of seven) you will be able to continue to create as many Permit/Deny Ethertype rules as desired (up to the 100 rules per role limit).

Problem 12:	(ExtremeControl Controllers) Because rule precedence is preconfigured on the ExtremeControl Controller, the default rule precedence reported in the **Policy Manager Role Device Support** tab occasionally does not match the actual rule precedence configured on the ExtremeControl Controller.
Problem 13:	Policy Rule Hit Reporting does not report rule hits for certain Layer 2 and Layer 3 rules (VLAN ID, IP Protocol Type, and IPX Packet Type), and the Server Log displays an "Incoming syslog message has error. Could not find rule." error.
Solution:	This happens when Policy Rule Hit Reporting cannot resolve a generated rule hit to a rule in Policy Manager because the machine-readable attribute is enabled. When Policy Rule Hit Reporting is enabled for a N-Series device, the etsysPolicyRuleSyslogMachineReadableFormat attribute should be set to disabled. You can verify this using MIB Tools, or using the CLI command "show policy syslog."
Problem 14:	It is possible to delete a role that is in use by an end-system connected to an ExtremeWireless Controller. If this happens, the end-system will be disconnected from the network.
Solution:	The end-system will need to reauthenticate for network access.
Problem 15:	Enterasys A2 and A4 devices. If you have configured a primary and secondary RADIUS server for these devices, all authentication requests go to the secondary RADIUS server first.
Solution:	This will be fixed in a future firmware release for the A2 and A4 devices.
Problem 16:	When managing Enterasys stackable devices running firmware images before 06.71.01, the Flood Control feature must be disabled in the Domain Managed CoS Components menu (in the Class of Service Configuration window). Otherwise, errors will occur during enforce and verify operations.
Problem 17:	First-generation ExtremeXOS/Switch Engine devices (e.g. Summit 450) in a stacked configuration do not support policy functionality, but can be added to a Policy Manager domain.
Solution:	Remove the unsupported devices from the Policy Manager domain.
Problem 18:	The policy enforcement takes time based on the size of the stack. The higher the stack is, the higher the latency is, the longer it takes to enforce policy.
Solution:	Do not use stack higher than 4 units or expect longer time to accomplish the enforce policy

Policy Manager and ExtremeWireless Controller (EWC)

Problem 1 :	Policy Manager only supports wireless controller version 8.01.03 and higher.

Problem 2:	Menu options to create Inbound and Outbound User Based Rate Limit port groups in the Class of Service Configuration (CoS) windows are grayed out. This is because user-defined CoS rate limit port groups are not supported on the EWC. Default port group membership cannot be modified, and only the Default port group is enforced to the wireless controller.
Problem 3:	When the non-authenticated policy is configured to have a "no change" topology on the wireless controller, wireless end-systems that are authenticated successfully to an authenticated policy (obtained dynamically) will either be unable to get a DHCP IP address, or will end up getting an incorrect DHCP IP address.
Solution:	To solve the problem, use the ExtremeWireless Wireless Assistant to set the non-authenticated policy to a topology other than "no change," or a topology with the Mode set to something other than "Bridge Traffic Locally at AP."
Problem 4:	For networks with wireless controllers with firmware version 8.01.xx. The wireless controller uses an *internal VLAN* for processing traffic. (See the Policy Manager Configuration Concepts Help topic's section on ExtremeWireless Wireless Controller Configuration > Internal VLAN.) This internal VLAN is set by default to use VID 1 and the static name of "DEFAULT VLAN." If you are using a Default VLAN with a VID 1 on wired devices in your domain configuration, you must change the internal VLAN to another value to avoid problems with Policy Manager enforce and/or forwarding traffic on the controller.

Solution:	There are two options: 1. Leave the controller's internal VLAN as VID=1 and don't use any VLAN with a VID=1 in your domain configuration (for example, don't use contain to VLAN 1). 2. Change the controller's internal VLAN to a different VID. Note that in both options, the controller's internal VLAN is still named DEFAULT VLAN*. With option 2, changing the internal VLAN to some other VID avoids problems forwarding traffic on the controller. For ExtremeCloud IQ Site Engine 4.2.0 and earlier, the new internal VLAN VID must not already be modeled in Policy Manager when it is modified on the controller, so that when VLANs are read from the device, it maintains the name DEFAULT VLAN. Do not rename this VID or use it in a domain configuration, or Policy Manager enforce fails. Be aware that if you rename the controller's internal DEFAULT VLAN (in Policy Manager), you cannot change it back to DEFAULT VLAN, as duplicate names can not be used in the domain. *Wireless Controller firmware version 8.11 will change this behavior so the internal VLAN will be named "INTERNAL VLAN" to be more easily identified, and default to VID 4094. Again, do not use this in a domain configuration.
Problem 5:	When managing wireless controllers in a high availability (HA) synchronized pair using Policy Manager, policies are not properly written to the controllers.
Solution:	Disable synchronization on the controllers.

Legacy Devices

This section includes the Known Restrictions and Limitations that apply to Enterasys legacy devices.

Console

Problem 1 :	When the EngineID is changed for a device using an SNMPv3 credential, Console will lose contact with the device and will not re-negotiate with the device to learn the new EngineID to re-establish contact with the device. This condition can be verified by attempting to contact the device using MIB tools.
Solution:	If querying the device with MIB tools is successful, shut down and restart Console to re-establish contact with the device.

Problem 2:	When an X-Pedition is configured to run the OSPF routing protocol, it is possible during TFTP transfer that the device will send TFTP packets from different source ports. This will cause the transfer to fail with a "TFTP Error: Undefined error". For security reasons this is not supported by the ExtremeCloud IQ Site Engine TFTP Server.
Solution:	When OSPF routing protocol is being used on your network, you must configure your X-Pedition devices to use a single port for TFTP traffic. Refer to the ***X-Pedition User Reference Manual*** for information about using the system set tftpsource command.
Problem 3:	When different generations of SmartSwitch 6000/ E7 family switches are mixed within a single chassis, Console will create multiple **Grouped by Chassis** groups for the chassis. In this example, note that the serial number is the same for both groups. Grouped By |_ Chassis |_ SmartSwitch 6000 [00001D837733] (2) |_ 172.16.34.5 |_ 172.16.34.7 E7 [00001D837733] (1) |_ 172.16.34.6
Solution:	Examine the serial number associated with each chassis to determine when multiple groups represent the same chassis.
Problem 4:	(Linux) An initial Discover, performed immediately after install, stops prematurely. Console stops sending discover packets. Subsequent Discovers work properly.
Solution:	Wait 3-5 minutes following installation or system reboot before starting a Discover on Linux systems.
Problem 5:	The V2 does not support sets to the MAU MIB. Therefore you cannot use the Console's Properties - Port View to configure ifMauEntry or ifMauAutoNegEntry MIB objects.
Problem 6:	If Discover finds a device that already exists in the database, but the existing device is configured with a different profile, the device displays in the Discovered Devices table, noted as *Exists* with the current profile for the existing device within angle brackets. The same information should appear in a tooltip, however that profile information is blank in the tooltip. Saving the device changes the existing profile to the one listed in the Profile column.

Problem 7:	VLAN. On an X-Pedition router, a VLAN definition cannot be overwritten to an existing VID that is used by the System Static VLAN (e.g., SYS_L3_ InterfaceName). When such VLAN Definition is compared in the VLAN Details window, the following information is displayed: Setting Name | VLAN Config | | Device Config ==========+==========+==+========== VLAN Name | Not Defined | | SYS_L3_InterfaceName VID | 3 | | 3 Write To Device | N/A | != | Undefined VLAN will be removed on enforce The message is misleading because: • You cannot overwrite the System Static VLAN on a router. • Since the VLAN Definition with VID=3 is not defined in a VLAN Model, the Enforce operation does not make sense.
Solution:	MERGE the VLAN from the router into the VLAN Model.
Problem 8:	VLAN. On an X-Pedition (SSR) router, you cannot directly change the PVID for a Basic Port from one non-Default VLAN to another non-Default VLAN. For example, changing PVID 7 to PVID 8 will not work.
Solution:	Change the PVID to the Default VLAN and then change the PVID to the new non-Default VLAN. For example, change PVID 7 to PVID 1 then to PVID 8.
Problem 9:	VLAN. On the X-Pedition Router, assigning a PVID (that exists on the device) in the Basic Port view and enforcing can incorrectly report an error, placing a red X in the PVID table cell.
Solution:	Refresh the table by performing a Retrieve to remove the X.
Problem 1 0:	VLAN management on the RoamAbout AP4102 is not supported in ExtremeCloud IQ Site Engine Console.

Problem 11:	Device Manager. Console Device Manager will report a Set Fail when attempting to set a value for a MIB object that is not supported in the device. In particular, this will occur when attempting to map a transmission priority to a traffic class in E5 or Vertical Horizon devices using Bridge Extension Port Traffic Class window in Device Manager. With the exception of the VH-2402S-L3 and the VH-8G-L3 which only support one traffic class, these switches support only two Traffic Classes: 0 (Low) which maps to Priority 0-3 and 1 (High) which maps to Priority 4-7. Device Manager attempts to perform the mapping even though these switches cannot map transmission priorities to traffic classes. This also poses a problem for E1 devices. Although these devices do support mapping of Priorities 0-7 to four separate Traffic Classes, the mapping is global to each Priority as opposed to each instance of that Priority. Device Manager attempts to perform the mapping per instance (dot1dTrafficClass) and the SET fails.
Problem 12:	Device Manager. Continuous (packet) capture is not supported for E1 devices. Continuous capture packet download on the E1 does not wrap when buffer is full. Selecting continuous capture on an E1 behaves the same as "stop when full".
Problem 13:	HP OpenView Integration. The enterasys-link-flap-mib.txt fails to load when the loadmibs script is executed.
Problem 14:	SmartSwitch 6000 with firmware version, 04.05.06 inserts hex Fs into the chassis serial number. This causes an extra Grouped By/Chassis group to be created in the Console left panel.
Problem 15:	X-Pedition Routers running firmware revision E9.1.7 do not provide information about port auto-negotiation capabilities. As a result, the capabilities columns in the Port Properties view displays N/A for all of the capabilities columns for these devices.
Problem 16:	Using ExtremeCloud IQ Site Engine Console or MIB Tools to set values for sysName, sysLocation, and sysContact on a Roamabout R2 is successful. However, those values are not persisted after resetting the device.
Problem 17:	False failure message when enforcing VLANs to a device (e.g., RoamAbout2) that does not support CreateAndWait and NotInService. The VLAN is created successfully.
Solution:	Select the device in the left panel, access the **VLAN** tab and Retrieve the Device VLAN information to verify that the VLAN was successfully created.

Inventory Manager

Problem 1:	When an X-Pedition router is configured to run the OSPF routing protocol, it is possible during TFTP transfer that the device will send TFTP packets from different source ports. This will cause the transfer to fail with a "TFTP Error: Undefined error." For security reasons, this is not supported by the ExtremeCloud IQ Site Engine TFTP Server.

Solution:	When OSPF routing protocol is being used on your network, you must configure your X-Pedition devices to use a single port for TFTP traffic. Refer to the X-Pedition Router User Reference Manual for information about using the `system set tftpsource` command.
Problem 2:	If you have an AppleTalk Routing Engine (ARE) in an SSR, the AppleTalk configuration is not captured during an Archive operation.
Problem 3:	The firmware upgrade operation fails on an ER16 and displays the message "SNMP Error-Timeout". This problem is due to a limitation on the ER16, and happens when: the ER16 is configured with a primary and backup CM, the primary CM has more than 1 image loaded on its flash card, and both the primary and backup CM have the same image chosen for next boot.
Solution:	When performing a firmware upgrade on an ER16 configured with a primary and backup CM, verify that there is only one image loaded on the primary CM's flash card.
Problem 4:	Second generation devices (e.g. 2H252-25R) incorrectly display a value in the Bytes Trans. column of the Active Status Panel (Details view) for an Archive Save operation that fails because the TFTP server is not running.
Problem 5:	For X-Pedition routers, changing the Asset Tag in the **Device General** Tab fails with the following message: SNMP Error = General Error writing value [NetworkAdmin] to oid [sysContact.0]. This is because current versions of X-Pedition firmware do not support asset tags. However, despite the failure status, the System attributes do get set properly on the device and the asset tag is stored in the Inventory Manager database.
Problem 6:	XSR devices running firmware version 5.0 only. Inventory Manager is not able to perform firmware upgrades or archive save/restore operations on these devices.
Solution:	You can perform these operations via CLI. This problem is fixed in the 5.0.0.1 version of the XSR firmware.

NAC Manager

Problem 1 :	The Extreme Networks NAC Manager Solution does not support MAC Authentication on the RoamAbout AP4102.

Policy Manager

Problem 1:	On the RoamAbout R2, ICMP (Ping) and Telnet deny rules still permit ICMP and Telnet to the R2's IP address itself.
Solution:	This is a known issue that has been identified with regard to the RoamAbout R2.
Problem 2:	On the RoamAbout R2, configuring port-based 802.1X through Policy Manager does not configure tumbling keys. 802.1X under XPSPI will not support 802.1X without tumbling keys enabled. Therefore, the default port state will not permit the client to "associate" with the R2.
Solution:	Use ExtremeCloud IQ Site Engine Console, AP Manager, CLI, or Telnet to set up tumbling keys when configuring 802.1X on the RoamAbout R2.
Problem 3:	If the RoamAbout R2 acquires an IP address via BOOTP, and the user then adds an IP address statically and saves the configuration, RADIUS client requests will continue to use the original IP address.
Solution:	Reboot the device and the new IP address will be used by the RADIUS client portion of the firmware.
Problem 4:	(RoamAbout AP3000 devices only.) When setting the Number of Retry Attempts and the Retry Timeout Duration in the device **RADIUS** tab, the values are only applied to the primary RADIUS server.
Solution:	Use the CLI to set these values for each RADIUS server.
Problem 5:	(RoamAbout R2 devices only.) If the R2's community names are set to the factory default settings, the device cannot be created in Policy Manager using SNMPv1. In addition, if an existing R2 is reset to factory defaults, it will be removed from Policy Manager (if it is set to the factory default SNMPv1 community names) when it is recontacted.

Solution:	If you are creating the device with SNMPv1 (SNMPv3 is recommended), the default community names on the device must be updated. There are four SNMPv1 community names on the R2: • Community #1 -- enables limited read-only access (MIB II system group) • Community #2 -- enables creation of new views • Community #3 -- enables read-only access to all MIBs • Community #4 -- enables read/write access to all MIBs Policy Manager creates the device based on community names #3 and #4. For read-only access, set community name #3 on the device (using CLI or AP Manager) and then use that community name for the Read Only community name in your device list or the Create Device window. For read/write access, set community name #4 on the device, and then use that community name for the Read Write and Super User community names in your device list, or the Read Write community name in the Create Device window.
Problem 6:	(RoamAbout AP3000 devices only.) Due to recent firmware changes, the port-level RFC3580 VLAN Authorization enable/disable option is not supported.
Solution:	Use the Web or CLI to set this option at the port level.
Problem 7:	The following issues have been identified with regard to the RoamAbout R2: • Authenticated R2 users cannot be terminated through Policy Manager. • The status of an 802.1X client on the R2 is not updated if reauthentication is disabled, and the supplicant either moves out of range of the wireless network while authenticated, or terminates the wireless session without logging off or shutting down the client gracefully. The R2 will only remove these entries after a timeout period has expired having not heard from the supplicant. • Both the primary and secondary RADIUS servers must have the same password.
Problem 8:	E7 Rate Limiting: The E7 with 5.00.xx-5.04.09 firmware uses the incorrect transmit rate for Rate Limiting. The rate is in kilobits instead of kilobytes. For example, if you set a rate limit of 5 MB (megabytes) using Policy Manager, it only transmits 5 megabits, or approximately 625 kilobytes.
Solution:	Upgrade your firmware version.
Problem 9:	E1 devices do not support rate limits in excess of 125 MB/S, and any rate limits over 125 MB/S should fail on E1 devices when enforced. However, if you create a rate limit of 537 MB/S or more, when you enforce the rate limit, it succeeds on E1 devices. In addition, the rate limit actually set on the device is incorrect and does not match the rate limit that was enforced, causing a verify to fail.

Solution:	To avoid a false success on enforce of rate limits exceeding 536MB/S, add your E1 devices to the Exclusion list in the rate limit's **General** tab, and re-enforce the rate limit. To avoid enforce failing on E1 devices for rate limits exceeding 125 MB/S, add your E1 devices to the exclusion list prior to enforce. This will be fixed in a future E1 firmware release.
Problem 1 0:	(E1 and E6/E7 devices configured for web-based authentication only.) Ports configured for Active/Discard mode display the temporary IP address assigned to the user prior to authentication (instead of the permanent IP address assigned after authentication) in the IP Address column of the right-panel **Port Usage** tabs.
Problem 1 1 :	(V2 devices only.) When setting the Number of Retry Attempts and the Retry Timeout Duration in the device **RADIUS** tab, the values are not applied to the RADIUS server(s).
Solution:	Use the CLI to set these values for each RADIUS server.
Problem 1 2:	(E1 devices only.) RADIUS accounting configuration is enabled on the device **RADIUS** tab when you change an E1 device using SNMPv3 credentials to use SNMPv1. (Only SNMPv3 devices support RADIUS accounting, so if the E1 is using SNMPv1, RADIUS accounting should not be configurable.)
Solution:	Refresh (View > Refresh) will fix the problem -- RADIUS accounting will be non-configurable for the E1 (using SNMPv1) device.
Problem 1 3:	(E1 devices using SNMPv1.) Configuring RADIUS Accounting Server(s) using the Device Configuration Wizard fails and errors occur in the Event Log.
Solution:	Only E1 devices using SNMPv3 support RADIUS Accounting. Therefore, you cannot configure accounting servers for E1 devices that are using SNMPv1.

Connect Modules

Problem 1:	During the JAMF/Casper solution upgrade, the connect module gets HTTP error 504/502. The previously learned devices managed by JAMF/Casper go to a decommissioned state.
Solution:	Disable the Casper module in the Connect menu before upgrading the JAMF/Casper solution. Enable the module after the upgrade of JAMF/Casper is finished.