Extreme Management Center Known Restrictions and Limitations

The known restrictions and limitations for the Extreme Management Center 8.0 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

This table displays the Known Restrictions and Limitations for the Extreme Management Center Suite install, uninstall, and upgrade functionality.

Problem 1:	Linux platforms. The Extreme Management Center installation fails and the following error is seen: 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 Extreme Management Center 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:	Extreme Management Center Engine Upgrade. Following an upgrade to the Extreme Management Center engine, the engine's system description is incorrect when viewed in a management application such as Extreme Management Center 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 Extreme Management Center 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:	If you are upgrading a 64-bit Extreme Management Center engine from 4.4 to 5.0 or higher, and you have defined remote mount points using CIFS, you will need to update the fstab file by adding the additional option unc=\\\\<Windows ip>\\<Windows share>. Failure to do so could cause the remote mount to be mounted improperly, which could cause files to be stored on the local hard drive that were intended for the remote drive.
Problem 5:	VMware Tools does not start after upgrading to Extreme Management Center version 6.0. VMware tools were built into Extreme Management Center\Extreme Access Control\Application Analytics virtual engines starting in Extreme Management Center 5.1. Affected systems: Virtual engines upgraded from version 5.0.0.180 directly to version 6.0. Virtual engines upgraded from version 4.4 directly to version 6.0.
Solution:	To resolve this issue, execute the following command: "/usr/bin/vmware-config-tools –d". For version 4.4 customers, perform an interim upgrade to a GA version of Extreme Management Center 5.0 and then upgrade to Extreme Management Center version 6.0.
Problem 6:	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 7:	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 help topic.

Extreme Management Center Applications

This section includes the Known Restrictions and Limitations that apply to all the Extreme Management Center Suite applications.

General

This table displays the Known Restrictions and Limitations for the Extreme Management Center Suite applications in 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 allow 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 Extreme Management Center Launch page or from the Applications menu (in any of the Extreme Management Center applications) you see the error message "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. Double-click on 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. Click OK in the Java Control Panel. You should now be able to launch the application.
Problem 3:	Inconsistencies in user preferences may occur when the user authenticated to the operating system is different from the Extreme Management Center 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:	Use the "set snmp community public" command in CLI to change the community names.
Problem 5:	If the Client/Server SNMP Redirection option is enabled from an Extreme Management Center client, and the Extreme Management Center 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:	Extreme Management Center does not support restoring a database that was saved on a Linux system to a Windows system.

Problem 7:	Linux platforms. Launching an Extreme Management Center application from a local client results in the following Java error: java.lang.UnsatisfiedLinkError: /export/JDK/jdk1.6.0_ 02/jre/lib/i386/libdeploy.s o: 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 Extreme Management Center 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 may provide alternate methods for updating system libraries; please 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 appears 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:	When connecting to the Extreme Management Center Server from a remote client station, the user gets a login prompt, but then receives a "No Services Found" error. This problem exists because all user accounts are mapped to a network drive, so when the Extreme Management Center java client app gets installed, it gets installed on the network mount. When the user launches the remote client, java is not passing the correct mounted specified path.
Solution:	The following steps must be performed for each user on each client PC: 1. Create an app.properties file in the <user.home>\Application Data\NetSight 2. Add these lines to the app.properties file. ns.path=H:\\Application Data\\NetSight user.home=H: This assumes that H: is always mapped the user.home directory.
Problem 9:	A remote Extreme Management Center client connecting to an Extreme Management Center Server experiences slow performance.
Solution:	To resolve this problem, perform one of the following steps: • Add an entry for the Extreme Management Center Server to the hosts file on the client machine. or • Clear the Java Cache (javaws -viewer and delete all Extreme Management Center Clients) and download the client using the IP address and not the host name of the server: http://<server_ip>:8080/Clients/.
Problem 10:	Unable to launch an Extreme Management Center application from the Extreme Management Center Launch page, 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 Extreme Management Center 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 no longer appears to be an issue when using Internet Explorer 10 or later.
Problem 11:	The Extreme Management Center 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 12:	Extreme Management Center 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 Extreme Management Center applications using javaws.

Web Applications

This table displays the Known Restrictions and Limitations for the Extreme Management Center Suite web applications.

Problem 1:	The following problems occur when Extreme Management Center web applications (such as the Management Center web-based application and Extreme Access Control Dashboard) are launched in Internet Explorer version 7: • All tables revert to their default state when the web page is refreshed: column order, sort and filter parameters, and hidden/shown column selections will not be remembered. • On the **Network** tab, the Show FlexView window does not remember the last selected FlexView. • In the Extreme Access Control Dashboard End-Systems web page, the Page Size setting reverts back to 50 when the page is refreshed instead of remembering the last value.
Solution:	This is due to a limitation in Internet Explorer version 7. Update to a newer browser version.
Problem 2:	When authenticating to an Extreme Management Center 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. Once you have the login page you can submit your login credentials and authenticate to the web application.
Problem 3:	Windows OS only. There is a known issue when using certain versions of Java 1.7 on Windows to launch an Extreme Management Center 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 Extreme Access Control 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 may 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.

Extreme Management Center Clients Running Mac OS

This table displays the Known Restrictions and Limitations for Extreme Management Center Clients running a Mac operating system.

Problem 1:	Installing the Agent-Based Assessment Agent on the MAC OS version 10.8 you may receive 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 allows you to proceed with the installation, or you can change the System Preferences > Security & Privacy setting to allow applications downloaded from *** Anywhere ***.
Problem 2:	The Java Web Start icon is displayed on the system Dock instead of the Extreme Management Center application icons.
Solution:	In order for each Extreme Management Center 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:	Launching Extreme Management Center applications on Extreme Management Center clients running Mac OS X results in a message similar to the following: "NACMgr.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 allow applications from identified developers.
Solution:	There are three work-around methods for this scenario that will force the application 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 see a dialog with an "Open" button. 2. Open the Preferences > Security & Privacy tab after a failed jnlp launch and you see the jnlp file listed with an "Open Anyway" button. Click 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 click on the jnlp file again.
Problem 4:	Attempting to use Facebook to register an end-system on the network (clicking the **Register with Facebook** button in the Captive Portal window) via the Mac Captive Network Assistant browser may 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).

Console

This section includes the Known Restrictions and Limitations that apply to the Extreme Management Center Console application.

General

This table displays the Known Restrictions and Limitations for Console in general.

Problem 1:	Launching SSH from the right-click menu when a device is selected in the left panel does not work if there are multiple copies of the cygwin1.dll file on your system.
Solution:	Search for cygwin1.dll using the Windows Start > Find/Search facility and delete all but the most recent version. The most recent version should reside in *x*:`\cygwin\bin`, where *x* is the drive on which you have installed the cygwin distribution.

Problem 2:	Ping does not work when running Console as a user without Administrative privileges on a Windows platform. Ping-related features will not work on the Console Client when running as a user without Administrative privileges: • Discovery using Ping • Ping-related Compass functions • Ping options from the right-click menu
Solution:	Run Console as a user with Administrative privileges.
Problem 3:	An Extreme Management Center Database Restore reports errors if you attempt to restore a database containing information from more Extreme Management Center applications than are currently installed. This can occur if you save the database, uninstall an application, then attempt to restore the database.
Solution:	Save your database after uninstalling applications and use this saved database as your backup copy.
Problem 4:	The SNMPTrap Service synchronizes its timestamp with your system's clock when the service is launched, but does not recognize changing to or from Daylight Savings Time while running. This causes a one hour discrepancy in the timestamps for Traps and Informs that appear in Console after making the change.
Solution:	Stop and Restart the SNMPTrap Service when changing to or from Daylight Savings Time.
Problem 5:	Performing IP Range Discover for a large range of devices (greater than 200 devices) using only an SNMPv3 profile fails. The Status Bar reports "Timed Out." For example: 254 IPs Queried, 1 Completed, 224 Timed Out, 0 Discovered Devices.
Solution:	Increase the SNMP Timeout for Discover to be 5 seconds. Refer to How to Set Options - Discover for more information.
Problem 6:	In the Trap Receiver Configuration window, attempting to apply an SNMPv1 Trap Credential and an SNMPv2 Trap Credential that both use the same community name fails.
Solution:	Use MIB Tools or device CLI to apply the trap credentials.
Problem 7:	In the Trap Receiver Configuration window, selecting "Both" in the Type field of the Trap Receiver Configuration table only creates a single trap receiver for Traps. It does not create a receiver with an identical credential for Informs. In addition, if you create a single receiver for Traps and then attempt to add a receiver with the same credential for Informs, the **Apply** button is not enabled, and you cannot apply the receiver to your devices.
Solution:	Create and/or use a different credential to create the receiver for Informs.

Problem 8:	The Refresh (Rediscover) feature shows a *Completed* status message before the refresh is actually finished. Any requests that you make before the refresh is done will either be blocked (indicated by a *Tree is busy* message) or could produce unpredictable results.
Solution:	If you are refreshing a large number of devices, check the CPU utilization and wait until it has settled down to 0% before requesting the next action.
Problem 9:	Console may hang when attempting to *Retrieve* Properties that cause the table to expand into thousands of rows. For example, Port Properties on several devices with a large number of ports in a single operation. It is not possible to define a finite limitation. The table size is related to your system's memory resources.
Solution:	Retrieve Properties for fewer devices at a time and/or increase the available memory.
Problem 11:	(Linux) The Extreme Management Center Server Statistics window (Server Information - Server Stats button) fails to show the percentage of CPU usage consumed by the Extreme Management Center Server. The percentage is always zero (0.0%).
Problem 12:	Device List > Import Devices operations fail if the device list includes values with <space> characters (e.g., "authpwd=pass word" vs. "authpwd=password").
Solution:	Device lists do not support <space> characters in their parameter values. Remove any <space> characters from your values and then re-import the device list. Alternately, you can delete the device (that has <space> characters in its values) from the device list and use the Add Device window (which accepts values with <space> characters) to create the device.
Problem 13:	The Authorization Group that appears in the title bar in the title of Console's main view is not updated when the group membership of the current user is changed in the Groups and Users tab of the Authorization and Device Access window.
Solution:	The title shows the correct Authorization Group when a new Console Client session is started.
Problem 14:	Occasionally, the Extreme Management Center Server reports errors during shutdown. For example, you may see error messages like these: 2005-09-28 08:36:49,375 INFO [org.jboss.system.server.Server] JBoss SHUTDOWN: Undeploying all packages <more error messages here> 2005-09-28 08:36:52,125 INFO [org.jboss.system.server.Server] Shutdown complete
Solution:	These errors do not affect the operation of Console.

Problem 15:	The "Use System Name" and "Use User Defined Nickname" settings for displaying devices in the device tree are not used to populate the tree when starting Console. For example, if you have selected the "Use User Defined Nickname" setting, the nicknames will not be used in the device tree if you restart Console.
Solution:	Go to the Data Display Format options view (Tools > Options > Data Display Format) and change the setting to a different setting, click Apply, and then change it back to the desired setting, and click OK. The display format is used in the device tree until the next time you restart Console.
Problem 16:	TFTP Download and Reset is not supported by Extreme Management Center Console for devices running in High Availability Upgrade (HAU) mode. The download will complete but manual reset will be required to complete the upgrade.
Problem 17:	An Extreme Management Center Database Restore fails due to insufficient memory for maps. The following error is displayed in the server.log: <Date and Time>,901 WARN [com.enterasys.netsight.tools.database.RestoreHook$ErrorThread] ERROR 2006 (HY000) at line 1391: MySQL server has gone away
Solution:	Edit the my.ini file located at <install directory>/mysql/my.ini. Change the following line from: max_packet_length=32 to max_packet_length=64 Restart the Extreme Management Center Server and Database and reattempt the restore operation.

Alarm and Event Manager

This table displays the Known Restrictions and Limitations for Console's 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

This table displays the Known Restrictions and Limitations for firmware for devices managed by Console.

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

This table displays the Known Restrictions and Limitations for Console FlexViews.

Problem 1:	Some MIB tables may not work in FlexViews. Any column in a FlexTable that is instanced by TimeFilter may be left empty for devices whose firmware improperly implement TimeFilter.
Solution:	The MIB tables may 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:	FlexViews may not present the correct order of bits for writeable, enumerated MIB objects. 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 appears 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 writeable enumerated OIDs.

VLAN

This table displays the Known Restrictions and Limitations for using VLANs in Console.

Problem 1:	VLAN management on the ExtremeWireless Controller is not supported in Extreme Management Center Console.
Problem 2:	The Advanced Port view of the **Console VLAN** tab is not supported on the 800-Series.

RoamAbout Wireless Manager

This table displays the Known Restrictions and Limitations for 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 click on 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.

Device Manager

This table displays the Known Restrictions and Limitations for Console's Device Manager.

Problem 1:	Device Manager fails to launch when launched as a standalone tool from the Tools section of the Extreme Management Center Launch Page.
Solution:	This problem happens when Device Manager is launched as a standalone tool before any Extreme Management Center application has been launched. Device Manager uses files that are put into place when a client is downloaded during the launch of an Extreme Management Center application. Once you have launched an Extreme Management Center application, Device Manager can be launched as standalone tool.
Problem 2:	When using the Configuration Upload/Download feature to receive configuration information from a device, a filename for an existing file must be specified; if a File Name is specified for a file that does not exist in the TFTP root directory, the upload fails reporting, tftpServerError(8). This occurs when the nstftpd process has been started automatically with Extreme Management Center Console (the normal case) or if it is started from the Services Manager menu from the Windows Task Bar, or via /etc/rc2.d/S99NsTftp start on Linux.

Solution:	You must specify an existing file, as the File Name in the Configuration Upload/Download window. If a particular file does not exist, create an empty text file with that filename in the TFTP root directory that can be used with the Configuration Upload/Download. As an alternative, you can start the nstftpd process from the command line with a -c option. When started with the -c option, nstftpd is allowed to create files if they do not already exist. nstftpd is located in the <install directory>/services/ directory in the Extreme Management Center. For example: 1. Stop TFTP from the Services Manager (Windows). 2. Navigate to the <install directory>/services directory. Linux: cd <install directory>/services Windows: cd <install directory>\services 3. Restart nstftpd using the -c option. nstftpd -c
Problem 3:	Packets using Cabletron Interswitch Message Protocol traffic are not decoded.
Problem 4:	N-Series devices allow a maximum number of two historyControlEntries per port. The default configuration includes two entries for each port and attempting to create another will appear to be successful however, the index status cannot be set to valid.

MIB Tools

This table displays the Known Restrictions and Limitations for Console's MIB Tools.

Problem 1:	MIB Tools fails to launch when launched as a standalone tool from the Tools section of the Extreme Management Center Launch Page.
Solution:	This problem happens when MIB Tools is launched as a standalone tool before any Extreme Management Center application has been launched. MIB Tools uses files that are put into place when a client is downloaded during the launch of an Extreme Management Center application. Once you have launched an Extreme Management Center application, MIB Tools can be launched as standalone tool.

Problem 2:	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 3:	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 4:	A query on the dot3adAggPortDebugRxState MIB returns <Not Defined> as the Formatted Value in the Results table. This happens because the keyword "current(1)" appears 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 Extreme Management Center client "mibs" directory and change the keyword so that it is not all lowercase. For example: Current(1) Mandatory(x) Optional(y) Obsolete(z)

Inventory Manager

This section includes the Known Restrictions and Limitations that apply to the Extreme Management Center Inventory Manager application.

General

This table displays the Known Restrictions and Limitations for Inventory Manager in 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 Reset 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 Reset 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 Reset may not stop all resets. The Timed Reset section of the Firmware Upgrade Wizard and Reset 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 Reset operation that you have already started, click the Abort button after all devices have a "Reset Request Status" of "Success". Note: The Abort button is not a guarantee that you can back out of a Timed Reset operation, since it is possible that reset timers may 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

Firmware

This table displays the Known Restrictions and Limitations for Inventory Manager that relate to device firmware.

Problem 1:	The E5 serial number may not be 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:	Reset the E1 device. Following a reset, the archive operation should be successful.
Problem 3:	E1 Devices only. Archive and Restore Archive operations may 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" appears 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:	Reset 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 Extreme Management Center 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 may be slow to validate a new firmware image. This may 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.

Management Center

This section includes the Known Restrictions and Limitations that apply to Extreme Management Center.

Problem 1:	An error may occur if a report is not allowed to completely load before clicking on a new report.
Solution:	Reloading the report should correct the problem.
Problem 2:	Some report data may be inaccurate when there is a large Time Zone difference between the Management Center server and a remote Management Center client. This happens with the Wireless Summary, Controllers Down, and APs Down reports.

Solution:	Remote desktop to the Management Center server and run Management Center locally or run Management Center on a machine that has the same settings for Time Zone and Current Time as the Management Center 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:	Management Center 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 Management Center 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 Management Center capabilities do not work as expected. There may be links or menu items that do not work and result in an access-denied message when used. Some page elements may not display properly and other page elements may show data that should be disabled.

Solution:	Management Center supports five categories of users, as described in the Management Center Access Requirements section of the top-level Management Center Help topic: • Full Read/Write Access: full read/write access to all Management Center features. • Read-Only Access: read-only access to all Management Center features. • Limited Read-Only Access: limited read-only access to only Management Center reporting and wireless data. • End-System Information, Read-Only Access: read-only access to Management Center end-system information. • End-System Information, Read/Write Access: read/write access to Management Center end-system information. For each category, there are a specific set of Management Center capabilities which are configured to enable the appropriate access. Other combinations of Management Center capabilities are possible. However, the result may not work as expected. Always test any set of Management Center capabilities before putting them into use. Be sure that the different features of Management Center 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 Extreme Access Control Dashboard, the graph lines are redrawn in the wrong position.
Solution:	Resizing the browser window corrects the graph, however the y-axis may show 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. Clicking Yes in the Security Message results in a Management Center "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 10:	**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 11:	When expanding and collapsing Management Center navigation panels using the >> and << arrow buttons, odd behavior may result. For example, the navigation panel may disappear or be grayed out. This is caused by not clicking squarely on the arrow button.
Solution:	Restore the navigation panel by clicking squarely on the arrow buttons to expand/collapse the panel.
Problem 12:	The PDF file attached to a Management Center Scheduled Report email is empty when the Management Center 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 13:	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 14:	When a Wireless Controller is deleted from Management Center 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 15:	Ports/interfaces with a type of propVirtual (typically VLAN ports with a "vm" prefix in the Name) cannot be used by scripts in Management Center. As a result, the scripting engine removes the port/interface before being passed to the script.
Problem 16:	When accessing Management Center using the Mozilla Firefox web browser on a system using the Microsoft Windows operating system, the bottom line of dialog boxes may not be 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 17:	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 Management Center. A Policy Manager enforce in Management Center 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 18:	Legacy E6/E7 devices do not support domains containing roles or rules using the deny access control in Management Center.
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:	Configuring custom images for Portal Configurations via the Extreme Management Center web interface may cause Portal images not to display correctly or at all.
Solution:	Configure images using the legacy NAC Manager java client.
Problem 20:	Management Center does not support SNMP traps configured prior to the device being added to Management Center.
Solution:	Remove the trap and reconfigure the trap via Management Center.

NAC Manager

This section includes the Known Restrictions and Limitations that apply to the Extreme Management Center NAC Manager application.

General

This table displays the Known Restrictions and Limitations for NAC Manager in 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 allows end-systems to obtain IP addresses via the DHCP protocol before they are authenticated to a VLAN.

Problem 2:	For Enterasys devices only. Switch management via TELNET/WebView will fail with the following configuration in the Add/Edit Switches to Extreme Access Control Appliance Group window: Auth Access Type = "Management Access" or "Any Access" Gateway 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 3:	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, you may think that 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 4:	E7 Devices. The RFC 3580 options (configured as Gateway RADIUS Attributes to Send in the Add/Edit Switches to Appliance Group window) are not supported on E7 devices.
Problem 5:	Assisted Remediation and Registration web pages take a long time (at least a minute) to display on the web browser.
Solution:	Add the Extreme Access Control Gateway name to your DNS server.
Problem 6:	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 7:	When using NAC Manager from a remote client in which the hostname of the Extreme Management Center Server cannot be resolved to its IP address, certain actions (such as selecting an end-system in a table or selecting an item in the left-panel tree) causes the application to freeze briefly (approximately six seconds). This is caused by a delay that happens when NAC Manager sends or requests information to or from the Extreme Management Center database on the server.

Solution:	A workaround is to add the IP address of the Extreme Management Center Server to which the client is connecting, to the client's "hosts" file. On Windows, the hosts file is found at C:\WINDOWS\system32\drivers\etc\hosts. For example, if the Extreme Management Center Server has a hostname of netsight145 and an IP address of 10.20.30.40, you would add the following line to the hosts file: 10.20.30.40 netsight145
Problem 8:	The following agent-based assessment tests fail on end-systems running the Windows Server 2008 operating system: Antivirus and Firewall. If the test status is set to Mandatory, the end-system will be quarantined.
Solution:	Add a scoring override for the Antivirus and Firewall test with a search string that specifies a regular expression for the Windows Server 2008 operating system.
Problem 9:	The following message appears in the NAC Manager Events log: "Web Service calls to Extreme Access Control Engine <IP address> appear to be slow. This may be caused by there being no hostname for the engine in DNS. If this is the case, adding a host name to the hosts file on the Management Center Server will resolve the issue." This message is only seen when the Extreme Management Center server is running on a Windows platform system.
Solution:	Add an entry for the Extreme Access Control engine to the hosts file on the Extreme Management Centerserver.
Problem 10:	In an Extreme Access Control deployment utilizing RFC3580 and Agent-Based Assessment, if the end user exits out of the agent, Extreme Access Control 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 11:	Enterasys A2/B2/C2/D2/I3, and E1/E7 devices. Due to lack of MIB support in the firmware, performing a Force Reauth action or deleting a stale end-system causes the currently authenticated end-system to be reauthenticated. For example, consider the scenario where user A is authenticated and unplugged, and user B is authenticated on the same port where user A was authenticated. If you perform a Force Reauth or delete user A, then user B will be reauthenticated.
Solution:	This will be fixed in a future firmware release.
Problem 12:	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 Extreme Access Control 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 13:	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 14:	Refreshing the Extreme Access Control Dashboard while the web page is loading causes an error in the server.log file.
Problem 15:	If you use NAC Manager to update the RADIUS server certificate (using the Manage Appliance Certificates window), you must leave the Server Private Key Passphrase field blank, otherwise certificate-based RADIUS authentication (for example, EAP-TLS, PEAP, and EAP-TTLS) will not operate successfully. This field is located on the **Appliance Settings Credentials** tab (**Tools** > **Manage Advanced Configurations** > **Appliance Settings** > **Credentials** tab > **EAP-TLS Configuration**).
Solution:	This will be fixed in a future release.
Problem 16:	The Mobile Screen Preview (accessed from the Edit Portal Configuration window > Launch Portal Web Page > Preview Web Page) does not display in Internet Explorer or Firefox browsers.
Solution:	The preview page will display properly on the following mobile devices: IPod Touch, IPad, IPhone, Android Phone/Tablet/NetBook, and Blackberry devices running version 6 or greater. It will also display properly on browsers that support the WebKit web browser engine, such as Chrome and Safari. This will be fixed in a future release.
Problem 17:	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 18:	Custom field information in the Add/Edit End-System Group window does not dynamically update until you close and reopen the window.
Problem 19:	Agent-less assessment update files downloaded by an Extreme Management Center 4.4 server are not compatible with 5.0 Extreme Access Control engines running the Ubuntu 64-bit OS.
Solution:	Update the Extreme Management Center server to 5.0. The 64-bit compatible files are downloaded the next time an update is available and the download is either run manually using the Help > Check for Assessment Updates menu option in NAC Manager or via the scheduled updates configured in the Extreme Management Center Suite options. To download the 64-bit compatible files immediately to an Extreme Management Center 5.0 server, delete the update directory under the <install directory>/appdata/NACMgr directory, then run the Check for Assessment Updates option in NAC Manager.

Problem 20:	In Advanced Configuration > Appliance Settings > **Network** Tab > Manage SSH Configuration, configuring a RADIUS user with Administrative privileges is not supported on a 32-bit Extreme Access Control engine. You can only grant Administrative privileges to Local users on the 32-bit engine.
Solution:	You must upgrade to a 64-bit Extreme Access Control engine for this functionality.
Problem 21:	In certain circumstances where a firewall is enabled on an end-system or when a credentials scan cannot be performed, agent-less assessment may provide a less accurate OS detection for an end-system than DHCP fingerprinting.
Problem 22:	If Extreme Access Control 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 may have to go through the registration process twice.
Problem 23:	Enforcing a Network Access RADIUS configuration to a switch with an existing RADIUS Management Server configuration that points to a non-Extreme Access Control RADIUS server will re-write the existing management server configuration with the RADIUS Shared Secret defined in the Extreme Access Control 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.

Agent-Based Assessment

This table displays the Known Restrictions and Limitations for NAC Manager's agent-based assessment functionality.

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 may 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, you may receive an error message 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, you may receive 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: 1. Right-click on the NacAgentInstall.mpkg file and select open, which displays the warning, but allows you to proceed with the installation. 2. Change the System Preferences > Security & Privacy setting to allow 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 may not reflect the current state of the screen saver settings. This may 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 Extreme Access Control 3.1.3 (or older), the scan will not complete.
Problem 10:	The agent on Mac OS X may unexpectedly exit.
Solution:	Running the uninstall script in the /Application/Utilities/NacAgent.app/Contents/Resources/ directory and then reinstalling the agent may resolve the problem.
Problem 11:	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 12:	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 13:	On some Windows XP systems, when Auto Update is enabled but never installed any updates successfully, Extreme Access Control will incorrectly report that updates had been recently performed.
Problem 14:	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 15:	Launching the dissolvable Extreme Access Control 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 allow 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. Click 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 click on the jnlp file again.
Problem 16:	On Mac OS X systems, if you run the dissolvable agent and then install the persistent agent, you may 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 17:	Using Auto-Remediate functionality that results in the Agent attempting to Auto-Remediate may cause your system to present a UAC (User Account Control) prompt, depending on your UAC settings. If you click **Yes** to allow the Network Command Shell to make changes, the Auto-Remediate completes successfully, while clicking **No** may result in being quarantined.

Problem 18:	Mac OS X end-systems on which Agent-Based assessment is configured accessing the network via the Mac Captive Network Assistant browser may be placed into a quarantine state after connecting to the network. Additionally, the Extreme Access Control Agent may go into a "disconnected" state, causing the Extreme Access Control 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).

Access Control Engines

This table displays the Known Restrictions and Limitations for 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 clicks on 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 allow 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 gateway.
	
	`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 appears. 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:	Access Control engine is red (down) in NAC Manager after reverting to a pre-4.0.x Access Control version.
Solution:	When a 4.0.x (or higher) engine present in the Management Center database is reverted to a pre-4.0.1 Access Control version (for example, using the engine backup and recovery function), a restart of the Management Center server is required to re-establish communication to the engine.
Problem 5:	Changing the internal communication certificate on the Management Center server or reverting an Access Control engine to a previous release, may cause a communication issue between Management Center and the Access Control engine(s). The following errors may 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 6:	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 help topic.

Policy Manager

This section includes the Known Restrictions and Limitations that apply to the Extreme Management Center Policy Manager application.

Problem 1:	In the Print window, the Print Range area has a Pages option with the default values of "from 1 to 9999".
Solution:	Enter the desired values.

Problem 2:	When no printer is configured, clicking the Print button on the toolbar or selecting File > Print results in a Printing Error message; closing the error message results in repeated error messages.
Solution:	Close the error message box three times.
Problem 3:	Periodically, when you try to access local management or when a user tries to log in via a browser, access is denied although the RADIUS Server log shows that access has been granted.
Solution:	Log in again and access will be successful.
Problem 4:	Selecting a SmartTrunk port in the **Network Elements** tab produces error messages in the Event Log.
Solution:	Policies cannot be configured on logical ports such as SmartTrunk ports. You can prevent logical ports from being displayed in the **Network Elements** tab by opening the Options window (Tools > Options), selecting the Ports view, and checking the Hide Logical Ports checkbox.
Problem 5:	Selecting a SmartTrunk port in Policy Manager produces error messages in the Policy Manager Event Log similar to these: ERR - Failed getting port authentication data. ERR - Contacting device [172.20.3.58]. ERROR : Pdu NoSuchName In MIB Tools, the SmartTrunk port is not shown in the etsysPwaAuthPwaState attribute. This only occurs if the SmartTrunk port has been activated/configured.
Solution:	Web-based authentication operates only on physical (bridge) ports; it is not supported on trunking ports. This is consistent with how 802.1X handles port aggregation; it requires authentication of the individual ports rather than the aggregated port.
Problem 6:	(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 7:	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 8:	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 9:	(Linux and UNIX only.) You cannot specify a range of pages when printing on UNIX or Linux systems. If you right-click and select Print or use File > Print, the resulting print settings window does not open to a sufficient size (and cannot be resized) to allow access to the page range fields.
Solution:	For these systems, the only option is to print the entire table.
Problem 10:	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 11:	(Enterasys C2 and B2 devices only.) Rate limits only work for Priority 0.
Solution:	This will be fixed in a future firmware release.
Problem 12:	(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.
Solution:	This will be fixed in a future firmware release.
Problem 13:	The Authorization Group that appears in the title bar of Policy Manager's main view is not updated when the group membership of the current user is changed in the **Groups and Users** tab of the Authorization and Device Access window.
Solution:	The title shows the correct Authorization Group when a new Policy Manager Client session is started. This problem will be fixed in a future release.
Problem 14:	The N-Series Platinum devices and X devices allow 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.
Solution:	This will be fixed in a future release.
Problem 15:	(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 16:	When you attempt to assign an SNMPv3 device to a Policy Domain, a warning window states the device is identified as unsupported. However, the device is in the Console database and you can do SNMP writes to it.

Solution:	Policy Manager does not support write-only profiles. Any write profile should also have the read ability set. A read-only profile can exist and be set as the read profile for the device, but Policy Manager uses the write profile for reading as well as writing.
Problem 17:	(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 18:	(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 19:	(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. Once 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 20:	(Extreme Access Control Controllers) Because rule precedence is preconfigured on the Extreme Access Control Controller, the default rule precedence reported in the **Policy Manager Role Device Support** tab may not match the actual rule precedence configured on the Extreme Access Control Controller.
Problem 21:	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 22:	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 23:	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 24:	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 25:	First-generation ExtremeXOS 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.

Policy Manager and ExtremeWireless Controller (EWC)

This section includes the Known Restrictions and Limitations that apply to networks running Policy Manager with ExtremeWireless Controllers.

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 Extreme Management Center 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 are not allowed 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, this may not be used 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.

Wireless Manager

This section includes the Known Restrictions and Limitations that apply to the Extreme Management Center Wireless Manager application.

Problem 1:	Extreme Management Center Wireless Manager will not launch if the old HiPath Wireless Manager product is also installed on the system.
Solution:	Before installing Extreme Management Center Wireless Manager, uninstall HiPath Wireless Manager and clear the java cache.
Problem 2:	Multiple devices in Extreme Management Center Console may be mapped to a single wireless controller in Wireless Manager. Multiple entries can be created in Extreme Management Center Console for a wireless controller by discovering the controller using different SNMP contexts, or by managing it through different interfaces.
Problem 3:	The wireless controller and Wireless Manager display different lists of APs serving a WLAN service.
Solution:	The wireless controller's configuration shows APs assigned to the WLAN services, even if the AP is not active on the controller. APs that were manually defined on the controller and which have not yet discovered the controller can be assigned to WLAN Services and appear in the controller's list of APs serving the WLAN. Wireless Manager only shows APs that are either currently actively offering the WLAN service or that were previously reported as serving that WLAN service. When a WLAN service is disabled in the wireless controller configuration, then Wireless Manager would show the SSID but the number of APs would be 0.
Problem 4:	Extreme Management Center Wireless Manager does not support assigning the same AP to a different set of VNSs depending on whether it is active on its home controller or on its foreign controller.
Problem 5:	Cleaning up the Wireless Manager database does not reset Extreme Management Center Console Options > Console > Wireless Manager settings.
Solution:	Functions as designed.
Problem 6:	When cloning a task, Wireless Manager also clones the task's deployment targets. You cannot add or remove targets from the task, however, per controller settings can be changed.
Solution:	Functions as designed.
Problem 7:	The Deploy VNS task wizard does not include foreign APs in the list of targets that can be assigned to the VNS (WLAN Service).
Solution:	Assign the APs to the VNS on their home controller instead.
Problem 8:	Extreme Management Center Wireless Manager is not supported on Mac OS X.
Problem 9:	Wireless Manager can only configure controllers running version 8.01 or later.
Problem 10:	You cannot configure mesh and WDS WLAN services from Wireless Manager.
Solution:	Use the ExtremeWireless Wireless Assistant to configure mesh and WDS WLAN services.

Problem 11:	After a controller has been upgraded, Wireless Manager may not be able to retrieve data from it, if the controller was using a custom shared secret for securing its communication with Wireless Manager.
Solution:	From the Wireless Controller GUI, go to Wireless Controller > Secure Connections and delete and re-add the entry for Wireless Manager.
Problem 12:	Wireless Manager capacity upgrade licenses cannot be applied if an active Extreme Management Center Evaluation license is in effect.
Solution:	The Wireless Manager capacity upgrade license can be applied once the Evaluation license expires or is removed, so long as the base Extreme Management Center Console license is active.
Problem 13:	Unable to deploy a template to a pre-8.01.02 ExtremeWireless Wireless Controller whose 7 day grace period for a license violation had passed, but whose license violation was later corrected.
Solution:	Manually re-sync the controller in Wireless Manager, or wait for Wireless Manager's daily scheduled poll of the controller to retrieve any configuration changes.
Problem 14:	When using the Conflict Resolution Wizard, if a user selects "Use changed settings" and a template is deployed to multiple controllers, the Task Deployment Wizard is displayed to allow the user to redeploy the template to those controllers.
Solution:	The Task Deployment Wizard is automatically displayed to assist you in redeploying the updated template to its deployment targets. If you would rather do this at a later time, just dismiss the dialog and redeploy it at your convenience.
Problem 15:	The Adaptive Management feature has the following limitations on pre-8.01.02 EWCs: 1) The number of logged in users (displayed on the controller) increases with every click of a menu item. 2) If your default browser is IE 9, all menu items display the controller's default login page.
Solution:	Upgrade your controller software to version 8.01.02 or later.
Problem 16:	Browser certificate related warnings may appear when clicking links in the adaptive management menu for a controller.
Solution:	See the Wireless Manager User Guide for instructions on how to handle these warnings for the different kinds of browsers.
Problem 17:	When you have multiple controllers and you open an Adaptive Management UI session for each one in quick succession, after accepting the security exception and logging in for both controllers, the first will work as intended, however the second will produce this error message: The requested resource (/wm/jsp/j_security_check) is not available.
Solution:	Wait a few seconds before opening another Adaptive Management UI session for another controller.

Problem 18:	Wireless Manager does not support Policy VLAN Islands (PVIs). When synchronizing with Policy Manager, Wireless Manager will exclude all island VLANs (or topologies) and any roles or policy rules reported by Policy Manager to be using island VLANs.
Solution:	If you plan to use Wireless Manager for EWC configuration, don't use island VLANs in a policy domain containing EWCs.
Problem 19:	For a role in a Policy Manager domain with assigned controllers, WM will automatically associate the topology corresponding to the VLAN assigned by the role's "Wireless Default Access Control" action setting. However, if this property is not set in the role, but instead its 'Default Access Control' action is set to 'Contain to VLAN' then that topology / VLAN will be referenced by the role.
Problem 20:	When using Firefox version 24 or 25 as your default browser, the browser window that launches from Adaptive Management UI links fails to display popup windows.
Solution:	Use Chrome or Internet Explorer as your default browser for better integration with the Adaptive Management UI feature.
Problem 21:	Changing an AP's Ethernet port settings (i.e., Speed or Mode) on EWCs prior to V9.01 does not trigger any change notifications.
Solution:	Click Verify to force WM to update the synchronization status of its templates.
Problem 22:	During a VNS/WLAN template deployment, if you select "Use PM to enforce" it may fail with the error "The Policy Manager enforcement failed".
Solution:	Close any Policy Manager clients that are working in the domain and retry the deployment.
Problem 23:	Since version 5.1, Wireless Manager has not supported the configuration of roles and Classes of Service (CoS). Instead, Extreme Management Center Policy Manager should be used for configuring Roles and CoS. See the section "Migrating Legacy Role and CoS Templates" in the Wireless Manager User Guide for more details. Note: Legacy templates will be automatically deleted on upgrade to Extreme Management Center 6.3.
Problem 24:	When importing templates from Wireless Controllers and automatically from Policy Manager (for those domains with assigned controllers), duplicate templates may result. To avoid duplicate templates, use the following steps: 1. Add your controllers to Policy Manager policy domains. 2. Import the domain configuration from your controllers into Policy Manager. 3. Save your changes to the domain configuration. 4. Import templates from all controllers. This will also correct the topology type of any topologies created in WM on behalf of PM, to match that 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 Extreme Management Center 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 appears 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 may 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 10:	VLAN management on the RoamAbout AP4102 is not supported in Extreme Management Center 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 Extreme Management Center 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 Extreme Management Center 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 Extreme Access Control 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 allow 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 allow 802.1X without tumbling keys enabled. Therefore, the default port state will not allow the client to "associate" with the R2.
Solution:	Use Extreme Management Center 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 -- allows limited read-only access (MIB II system group) • Community #2 -- allows creation of new views • Community #3 -- allows read-only access to all MIBs • Community #4 -- allows read/write access to all MIBs Policy Manager will create 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 10:	(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 11:	(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 12:	(E1 devices only.) RADIUS accounting configuration is allowed 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 13:	(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.

04/2017
8.0 Revision -00
PN: 9035079