Extreme Networks ®

Extreme Management Center Release Notes

8/2018
P/N: 9035219-06
Subject to Change Without Notice

Table of Contents

Extreme Management Center Customer Release Notes

Version 8.1.4.40
August, 2018

Extreme Networks Extreme Management Center® provides a rich set of integrated management capabilities for centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources.

Extreme Management Center is distinguished by its web-based, unified control interface. Graphical and exceptionally easy-to-use, Extreme Management Center simplifies troubleshooting, help desk support tasks, problem-solving and reporting. ExtremeControl provides specialized visibility and control for managed and unmanaged devices connecting to the network.

Extreme Management Center's granularity reaches beyond ports, VLANs, and SSIDs down to individual users, applications, and protocols. Extreme Management Center increases efficiency, enabling IT staff to avoid time-consuming manual device-by-device configuration tasks. Extreme Management Center fills the functionality gap between traditional element managers that offer limited vendor-specific device control, and expensive, complex enterprise management applications.

The Extreme Management Center Release Notes provide information on the new features and enhancements included in version 8.1, as well as system requirements, and installation and upgrade information.

> **IMPORTANT:** There are important upgrade and installation requirements for this release. Please review this information in the Important Installation Considerations and Important Upgrade Considerations sections.

The most recent version of these release notes as well as the most recent firmware compatibility matrix can be found on the Extreme Networks

Documentation site: https://www.extremenetworks.com/support/release-notes. Follow this path to the document: Management and Orchestration > Extreme Management Center > Release 8.1.

Software Enhancements

Enhancements in Extreme Management Center 8.1

The new features and enhancements included in Extreme Management Center 8.1 are located in the What's New in Extreme Management Center Version 8.1 topic.

Known Issues Addressed

This section presents the known issues addressed in Extreme Management Center 8.1.4.40:

Extreme Management Center Issues Addressed	ID
The **Auto Group Delimiter** option was not available in Extreme Management Center, which only allowed groups to be separated by a slash (/).	1406779
The Extreme Management Center Webserver was not closing client connections effectively, which led to the server becoming unresponsive.	1392392
Attempting to replace a device that is not managed by Extreme Management Center via ZTP+ functionality by selecting the **Remove from Service** checkbox and entering a value in the **Replacement Serial Number** field in the **Configure Device** window was not completing successfully.	------
The values displayed in the **Peak Received Bandwidth** column of the **XOS Port Utilization** FlexView for ExtremeXOS devices was not formatted properly.	1547468
Selecting an Extreme Management Center legacy java application (e.g. Console) using the default memory configuration on the Extreme Management Center server resulted in a memory error and the application did not open successfully.	------

Opening the **Interface History** report for a port occasionally failed to load.	01714720
An error message was incorrectly displayed in the `server.log` file for devices on which Historical Collection is not enabled.	1714720
Extreme Management Center was slow to initialize or timed out when restarting the Extreme Management Center server.	
Attempting to add a device to a site via a device discover occasionally did not complete properly.	01638773
ERS 45xx and 48xx firmware images were not mapping to the correct device family.	------
ERS devices were not using the binary configuration file for configuration restore.	------
Restoring the configuration of an ExtremeXOS device was not restoring SSH keys.	------
Attempting to open a device terminal to VSP products was failing and displaying the following error message: "Error: failed to connect".	------
ERS devices were not logging in correctly through scripts and the device terminal.	------
ZTP+ was not allowing mappings to templates other than access and interswitch.	------
Extreme Management Center incorrectly identified a phone as an interswitch device when displayed in a map as the neighbor of a ZTP+ enabled device.	------
Creating an archive for an ERS device in Extreme Management Center was resulting in the removal of the device's management IP address.	01710930
If Extreme Management Center saved a large number of files in the appdata directory, server performance was affected.	------
Attempting to upgrade from SLX version 17r.1.00 or earlier to version 17r.2.00 was not completing properly. For the upgrade to complete, first perform an intermediate upgrade to version 17r.1.01.	------
Attempting to upgrade the firmware on a SLX-9850 device was failing due to insufficient wait time in factory scripts.	------
Some ports on switches running VOSS were not appearing in the Device View.	------

Sending the `radius server host` command using Python or Tcl scripting was timing out on an ERS device.	------
Running CLI commands via the **Execute CLI Commands** or running a script over SSH sessions to ERS devices occasionally were not completing successfully.	1556975
The IP Address column in the Discovered tab was not sorting when selected for ZTP+ enabled devices. This was due to an asterisk (*) character as field value for ZTP+ devices. The information in the column is now presented in two columns, **Configured IP** and **Discovered IP**.	------
Adding a device via a subnet discovery was occasionally resulting in a "java.lang.NullPointerException" error.	------
Adding multiple ZTP+ enabled devices simultaneously was occasionally resulting in a "java.lang.NullPointerException" error.	------
Verifying or configuring the state of syslog registration was resulting in a "java.lang.NullPointerException" error.	------
ExtremeAnalytics Issues Addressed	**ID**
Application response times were not being calculated for all DHCP flows.	01685720
Enforcing a new configuration to an Application Analytics engine that was commissioned using **Manual** mode was overwriting the interfaces section of the configuration.	------
ExtremeControl Issues Addressed	**ID**
ExtremeControl occasionally incorrectly displayed end-systems connected wirelessly as moving to a new AP after initially authenticating on the network.	01224358
Apple systems on which the Mac OS X "Mojave" (10.14 beta 4) is installed was displaying as 'unknown' when using agent-based assessment.	------
Attempting to clear an existing RFC3580 VLAN to policy role mapping occasionally fails and leaves dialog box open.	------
When an end-system contained in an HTTP session was in a disconnected state, it was occasionally resolving to the incorrect end-system.	01558760

Event logs created when a user requested Administrative access to Extreme Management Center was incomplete.	------
Creating a Basic AAA Configuration with the **Authenticate Requests Locally** checkbox not selected in the NAC Manager legacy java application was causing a **RADIUS Server """ cannot be found** error when the configuration was enforced to an Access Control engine.	------
Creating policy rules for the Summit x590 in the legacy Policy Manager java application was not completing successfully.	------
The legacy Policy Manager java application became unresponsive when opening Enforce Preview for an IPv6 rule.	------
When navigating the left-panel tree in the **Policy** tab, Extreme Management Center occasionally became unresponsive and displayed "Please wait...".	------
ExtremeControl was not recognizing DHCP fingerprints for Microsoft Surface Tablet on which the Windows 10 operating system is installed.	01725333

This section presents the known issues addressed in Extreme Management Center 8.1.3.65:

Extreme Management Center Issues Addressed	ID
Charts and graphs in reports and dashboards could not be zoomed using the Microsoft Internet Explorer browser.	------
Upgrading to Extreme Management Center version 8 from a version earlier than 7.1.4 was causing scripts to not execute properly.	01519067
Extreme Management Center was sending the incorrect Authentication configuration to ZTP+ enabled ExtremeXOS devices when the **Authentication** option was set to **All** on the **Port Templates** tab for a site.	01509821
The automatic refresh of data in tables in Extreme Management Center was removing user-defined filters.	1520032
Attempting to open the Operation Log in Extreme Management Center was occasionally not successful.	01526700
Running CLI commands via the **Execute CLI Commands** menu option for which the results are a failure, changing the commands, and then running again was resulting in the following error: "Error executing command, Busy executing command".	------

Attempting to execute a CLI command on a Cisco device was not successful.	------
When there were a large number of devices with a **Poll Type** of **Ping** and many of those devices do not respond to ARP requests, it was occasionally impacting the ability to reliably ping other devices that are operational. The result was devices may incorrectly appear to be down.	1529599
After starting the Extreme Management Center server, Extreme Management Center occasionally did not start successfully or started very slowly.	------
Traffic between the Extreme Management Center server and clients was vulnerable to the information disclosure vulnerability.	1406831
Extreme Management Center was not properly displaying results when enforcing to a device as a user with no write access.	1538252
The first two ports on the **Ports** tab in the DeviceView were incorrectly displayed in the Container group for Extreme Networks Matrix E1 devices.	1510623
Devices for which **Remove from Service** is selected in the **Configure Device** window were still generating alarms and traps.	1408751
The **Created Date** column of the **Archives by Device** tab in the Device Archives report was empty.	1404379
Changing the **Poll Group Interval** was not changing the frequency for devices with a **Poll Type** of **Ping** until after restarting the Extreme Management Center server.	------
Creating an archive for a device was incorrectly changing the **Asset Tag**.	1392468
If purging for the ctAlias table was set to off and multiple addresses existed for the same MAC address in the ctAlias table, then IP address resolution would fail.	1385539
An exception causing a stack trace was occurring sporadically.	1255515
Extreme Management Center was always discovering the chassis ID for a device via LLDP, which occasionally caused errors when searching for a neighbor device by MAC address.	1250253
Creating a VLAN on two or more devices and adding the VLAN to a port on only one of the devices was causing the script to incorrectly display a pause icon on the devices on which the VLAN was not being added to a port to indicate the script was still running.	1269132

After creating an archive of a Cisco device, the process became unresponsive and an SNMP error displayed.	1316235
The **# Devices** field in the **Archive** tab was not correctly displaying the actual number of devices archived.	01358223

ExtremeControl Issues Addressed	**ID**
ExtremeControl was not updating an end-station's location IP address when a RADIUS accounting packet is received after the end-system moves (roams) to a different wireless access point or controller.	1240042
Wireless Display (WiDi) devices were incorrectly identified in Extreme Management Center as Amazon Kindle devices.	01401031
Users authenticating via 802.1x were occasionally incorrectly identified as moving to a new location.	01224358
The default hostname for ExtremeControl engines was causing errors.	------

This section presents the known issues addressed in Extreme Management Center 8.1.2.59:

Extreme Management Center Issues Addressed	**ID**
The link status of links in partially configured MLAG configurations was occasionally incorrect, depending on the order in which the devices were evaluated.	1159285
Changing the TFTP **Root Directory Path** in the **Inventory Manager** Options tab did not update the local TFTP server configuration file.	1388438
Upgrading to Extreme Management Center version 8.0 or later was causing a slow Extreme Management Center server restart on systems with a large event cache.	1347771 1387738 1404758
Users with read-only capabilities were incorrectly able to remove a RADIUS authentication server from a device.	1400627

ExtremeAnalytics Issues Addressed	**ID**
Deleting a PV-FC-180 flow source from an Application Analytics engine using the **Analytics** tab in Extreme Management Center was causing network outages in environments that were not configured as STP.	01411331

ExtremeControl Issues Addressed	**ID**
The error messages displayed when configuring a AAA Trusted Certificate Authorities were not distinguishing between different CRL URLs errors.	1405759

ExtremeControl was incorrectly handling unresolveable usernames when looking up a plain text password via the Novell E-directory.	01410626
Configuring an SMS Gateway in Extreme Management Center, then navigating away from the screen, the configured SMS Gateway value was not displayed.	01419015

Policy Issues Addressed	ID
Port MAC authentication was failing if multiple ports were specified on an ExtremeXOS device in Policy Manager.	1392473
Attempting to change the authentication type preference in Extreme Management Center **Authentication Configuration** was returning an error and not completing successfully.	01416486

This section presents the known issues addressed in Extreme Management Center 8.1.1.41:

Extreme Management Center Issues Addressed	ID
Using the carat (^) character in an Extreme Management Center Access Control script caused CLI commands to fail.	1409461
Opening the **Advanced Settings** window (**Control** > **Access Control** > **Engine** > **Switches**), the **Override Shared Secret** option was automatically enabling.	01404416
No data was displayed in the **Used** column in the Port Usage Details report (**Reports** > **Reports** > **Device** window).	01408284
Adding a device into a device group that shares a name with an existing device group was causing devices to be moved to an incorrect device group.	1410232
Some historical device and port data was not fully migrated in the 8.1.0 EA release.	------
Virtual engines deployed on Hyper-V were configured with an incorrect amount of memory.	01389976

ExtremeAnalytics Issues Addressed	ID
Installing or initially deploying a version of Application Analytics prior to version 8.1.1.41 on an Analytics engine was allowing users to enter an incorrect ethernet port, which prevented the Application Analytics sensor from starting.	1349973
Flow Collector Diagnostics were occasionally not displaying correctly.	------

ExtremeControl Issues Addressed	ID
Applying a filter to an Extreme Management Center Access Control group was incorrectly applying the filter to all groups of the same type.	1364312
Searching for attributes in the **LDAP Test** window was returning accurate search results, but the **Attribute Name** on the **User Search** and **Host Search** tabs on the **Access Control** tab was incorrect.	01408240
Juniper EX ports and port-ranges could not be added to Access Control Location Groups.	01404485

This section presents the known issues addressed in Extreme Management Center 8.1.0.52:

Extreme Management Center Issues Addressed	ID
Editing and saving an existing Port Usage Details report was removing the list of report targets from the report.	------
Selecting a FlexView for a device via the right-click menu in a Topology map was not opening the FlexView.	1398215
Scheduled tasks that failed to complete were preventing tasks that followed from running.	------

ExtremeControl Issues Addressed	ID
Attempting to remove an entry that did not exist as a member of an end-system group was not producing an error message.	1212731

Policy Issues Addressed	ID
Enforcing a change to a device via the **Enforce Preview** window on the **Policy** tab was not indicating whether the change was supported on the device.	1223404

Security and Vulnerability Testing

Security is something that is taken seriously by Extreme Networks. Our commitment to achieving and maintaining a strong security stance for our products enables our customers to have confidence in networking, software, and management infrastructure provided by the company.

The Software Quality Assurance team at Extreme Networks scans every Extreme Management Center release using the current versions of multiple anti-virus solutions, updated to include the latest virus signatures.

Additionally, all Extreme Networks products undergo rigorous security testing with best-of-breed industry standard scanners. Further, all product binary images are scanned with sophisticated anti-virus solutions for evidence of viruses and malware before the images are uploaded to customer-facing portals. Whenever issues are discovered by these scanners and anti-virus solutions, a well-defined triage process is engaged for remediation or mitigation of such findings. This enables Extreme Networks to engineer solutions that heighten the security of our products, and new releases are made available as necessary in order to address any discovered security vulnerabilities. This has several additional benefits in terms of helping customers maintain networks that are compliant under various regulatory or industry standards such as HIPAA, SoX, and PCI.

Extreme Networks also monitors industry security information data sources, such as CERT, the full-disclosure mailing list, and various authoritative CVE announcements for vulnerabilities that could potentially apply to our products. When such a vulnerability is found, we follow a process by which high severity vulnerabilities (such as the ShellShock bug in the bash shell from late 2014) are prioritized over lower severity vulnerabilities. The severity itself is derived from the Common Vulnerability Scoring System (CVSS) score which provides the most widely accepted measure for vulnerability severity. For applicable vulnerabilities, we provide feedback to CERT to keep them updated on the status of our findings.

Further, for many of our products that are based on a Linux engine image – Extreme Management Center and Extreme Access Control, for example – we harden the engines by ensuring that we do not start unnecessary services and we do not install unnecessary software. In addition, we apply security updates from the upstream Linux distribution.

Taken together, the security of Extreme Networks products is maintained and verified. For all inquiries about our security processes, contact Global Technical Assistance Center (GTAC).

Vulnerabilities Addressed

This section presents the Vulnerabilities addressed in Extreme Management Center 8.1:

- The following vulnerabilities were addressed in the Extreme Management Center, Extreme Access Control, and Extreme Application Analytics engine images:

- CVE-2017-14062, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-7407, CVE-2017-8816, CVE-2017-8817, CVE-2016-7098, CVE-2017-13089, CVE-2017-13090, CVE-2017-6508, CVE-2017-1000376, CVE-2016-6515, CVE-2016-6210, CVE-2017-14867, CVE-2016-4476, CVE-2016-4477, CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088, CVE-2017-1000408, CVE-2017-1000409, CVE-2017-15670, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426, CVE-2018-1000001, CVE-2017-16611, CVE-2018-10545, CVE-2018-10546, CVE-2018-10547, CVE-2018-10548, CVE-2018-10549, CVE-2018-0494, CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303, CVE-2016-1000111, CVE-2016-3186, CVE-2016-5102, CVE-2016-5318, CVE-2017-11613, CVE-2017-12944, CVE-2017-17095, CVE-2017-18013, CVE-2017-5563, CVE-2017-9117, CVE-2017-9147, CVE-2017-9935, CVE-2018-5784, CVE-2017-2862, CVE-2017-2870, CVE-2017-6311, CVE-2017-16612, CVE-2016-10713, CVE-2018-1000156, CVE-2018-6951, CVE-2018-6594, CVE-2015-8853, CVE-2016-6185, CVE-2017-6512, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913, CVE-2018-0737, CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2017-10790, CVE-2018-6003, CVE-2017-15412, CVE-2017-17433, CVE-2017-17434, CVE-2018-2825, CVE-2018-2826, CVE-2018-2814, CVE-2018-2811, CVE-2018-2794, CVE-2018-2783, CVE-2018-2798, CVE-2018-2796, CVE-2018-2799, CVE-2018-2797, CVE-2018-2795, CVE-2018-2815, CVE-2018-2800, CVE-2018-2790, CVE-2015-4000, CVE-2003-1491, CVE-2004-1473

System Requirements

IMPORTANT: Extreme Management Center version 8.1 only runs on a 64-bit engine image. Any Extreme Management Center or Extreme Access Control (ExtremeControl) engine currently running a 32-bit OS image must be upgraded to the newer 64-bit image prior to upgrading to 8.1. Please contact Global Technical Assistance Center (GTAC) with any questions.

Wireless event collection is disabled by default in version 8.1 due to the increase in disk space usage required. To enable event collection, select **Enable Event Collection** on the **Administration** > **Options** > **Event Analyzer** tab.

Extreme Management Center Server and Client OS Requirements

These are the operating system requirements for both the Extreme Management Center server and remote Extreme Management Center client machines.

IMPORTANT: Only 64-bit operating systems are officially supported on the Extreme Management Center server. Any Extreme Management Center server currently running a 32-bit OS must be upgraded to a 64-bit OS.

	Operating System
Windows (qualified on the English version of the operating systems)	Windows Server® 2012 and 2012 R2 Windows Server® 2016 Windows® 7
Linux	Red Hat Enterprise Linux WS and ES v6 and v7 Ubuntu 14
Mac OS X® (remote Extreme Management Center client only)	El Capitan Sierra
VMware® (Extreme Management Center Virtual Engine	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server VMware ESXi™ 6.7 server vSphere (client only)™
Hyper-V (Extreme Management Center Virtual Engine)	Hyper-V Server 2012 R2 Hyper-V Server 2016

Extreme Management Center Server and Client Hardware Requirements

These are the hardware requirements for the Extreme Management Center server and Extreme Management Center client machines.

NOTES: ExtremeControl and ExtremeAnalytics are not supported on Small Extreme Management Center servers.

Extreme Management Center Server

	Small	Medium	Enterprise	Large Enterprise
Total CPUs	1	2	2	2
Total CPU Cores	8	16	16	16
Memory	16 GB	32 GB	64 GB	64 GB
Memory allocated to Java:				
-Xms	8 GB	12 GB	24 GB	24 GB
-Xmx	12 GB	18 GB	36 GB	36 GB
Disk Size	240 GB	480 GB	960 GB	1.92 TB
IOPS	200	200	10,000	10,000

Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000	10,000
ExtremeControl End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
ExtremeAnalytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

Extreme Management Center Client

	Requirements
CPU Speed	3.0 GHz Dual Core Processor
Memory	8 GB (4 GB for 32-bit OS)
Disk Size	300 MB (User's home directory requires 50 MB for file storage)
Java Runtime Environment (JRE) (Oracle Java only)	Version 8
Browser* (Enable JavaScript and Cookies)	Microsoft Edge (version 41.16.199.10000.0 in compatibility mode) Internet Explorer (version 11 in compatibility mode) Mozilla Firefox (version 34 or later*) Google Chrome (version 33.0 or later)

*Browsers set to a zoom ratio of less than 100% may not display Extreme Management Center properly (e.g. missing borders around windows). Setting your browser to a zoom ratio of 100% corrects this issue.

**When accessing Extreme Management Center using Firefox version 59.0.1 on a non-touchscreen system on which a Windows operating system is installed, the vertical scroll arrows do not display.

Virtual Engine Requirements

The Extreme Management Center, Extreme Access Control, and Extreme Application Analytics virtual engines must be deployed on a VMWare or Hyper-V server with a disk format of VHDX.

- The VMWare Extreme Management Center virtual engines are packaged in the .OVA file format (defined by VMware).
- The Hyper-V Extreme Management Center virtual engines are packaged in the .ZIP file format.

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

Extreme Management Center Virtual Engine Requirements

	Small	Medium	Large
Total CPU Cores	8	16	16
Memory	16 GB	32 GB	64 GB
Memory allocated to Java:			
-Xms	8 GB	12 GB	24 GB
-Xmx	12 GB	18 GB	36 GB
Disk Size	240 GB	480 GB	960 GB
IOPS	200	200	10,000

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

	Small	Medium	Large
MU Events	No	Yes	Yes

Extreme Access Control (ExtremeControl) Virtual Engine Requirements

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

Recommended scale based on server configuration:

	Small	Medium	Enterprise
ExtremeControl End-Systems	3,000	6,000	9,000/12,000[1]
Authentication	Yes	Yes	Yes
Captive Portal	No	Yes	Yes/No[1]
Assessment	No	Yes	No

[1]The Enterprise Extreme Access Control engine configuration supports two different scale options:

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

Extreme Application Analytics Virtual Engine Requirements

	Small	Medium	Enterprise
Total CPU Cores	8	16	16
Memory	12 GB	32 GB	64 GB
Disk Size	40 GB	480 GB	960 GB
IOPS	200	10,000	10,000

Recommended scale based on server configuration:

	Small	Medium	Enterprise
Flows Per Minute	250,000	500,000	750,000

IMPORTANT: The ESXi free license supports a maximum of 8 CPU cores, while the medium and enterprise Extreme Application Analytics virtual engine installation require 16 CPU cores. This is only available by purchasing a permanent license. To use the Extreme Application Analytics virtual engine with an ESXi free license, adjust the number of CPU cores to 8.

Ensure at least 4 GB of swap space is available for flow storage on the Extreme Application Analytics virtual engine or impaired functionality may occur. Use the `free` command to verify the amount of available RAM on your Linux system.

ExtremeControl Agent OS Requirements

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

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

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

Extreme Access Control Agent support for Antivirus/Firewall products includes, but is not limited to, the following families of products:

- McAfee
- Norton

- Kaspersky

- Trend Micro

- Sophos

Extreme Access Control Agent operating system support for the above products includes the latest Windows/Mac OS X versions currently available at the time of product release. Not all features of all products may be supported. For additional information on specific issues, see Known Issues and Limitations.

ExtremeControl Supported End-System Browsers

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

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

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

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

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

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

- If the browser is compatible, the page displays properly.

- If the browser is not compatible with the Mobile Captive Portal, the following error appears:
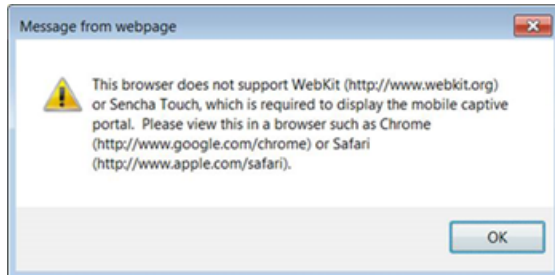
Extreme Access Control (ExtremeControl) Engine Version Requirements

For complete information on Access Control engine version requirements, see the Upgrade Information section of these Release Notes.

ExtremeControl VPN Integration Requirements

This section lists the VPN concentrators supported for use in Extreme Access Control VPN deployment scenarios.

Supported Functionality: Authentication and Authorization (policy enforcement)
Cisco ASA
Enterasys XSR

Supported Functionality: Authentication
Juniper SA (requires an S-Series Stand Alone (SSA) system in order to provide access control)

NOTE: For all Extreme Access Control VPN Deployment scenarios, an S-Series Stand Alone (SSA) system is required to change authorization levels beyond the initial authorization, for example, when using assessment.

ExtremeControl SMS Gateway Requirements

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

- Clickatell
- Mobile Pronto

Other SMS Gateways that support the SMTP API should be able to interoperate with ExtremeControl, but have not been officially tested.

ExtremeControl SMS Text Messaging Requirements

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

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

ExtremeAnalytics Requirements

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

Ekahau Maps Requirements

Extreme Management Center supports importing Ekahau version 8.x maps in .ZIP format.

Installation Information

When you purchased Extreme Management Center, you received a Licensed Product Entitlement ID that allows you to generate a product license key. Prior to installing Extreme Management Center, redeem your Entitlement ID for a license key. Refer to the instructions included with the Entitlement ID sent to you.

For complete installation instructions, refer to the installation documentation located on the Documentation web page: https://www.extremenetworks.com/support/documentation/.

IMPORTANT: The NetSight Server service may not start after installing Extreme Management Center version 8.0 on a system on which a Windows Server operating system is installed. Restarting Windows corrects this issue.

The **Governance** tab is available and supported by Extreme on an Extreme Management Center engine running the Linux operating system supplied by Extreme. Other Linux operating systems can support Governance functionality, but python version 2.7 or higher must be installed. Additionally Governance functionality requires the git, python2, python mysql module, python setuptools module, and python "pygtail" module packages be installed and related dependencies managed by the customer for their server's unique operating system and version.

Important Installation Considerations

Custom FlexViews

When re-installing Extreme Management Center Console, the installation program saves copies of any FlexViews you created or modified in the *<install directory>* `\.installer\backup\current\appdata\System\FlexViews` folder.

If you are deploying FlexViews via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\FlexViews\` folder.

Custom MIBs and Images

If you are deploying MIBs via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\MIBs\` folder.

If you are deploying device images (pictures) via the Extreme Management Center server, they are saved in the `appdata\VendorProfiles\Stage\MyVendorProfile\Images\` folder.

Evaluation License

If you have requested an Extreme Management Center evaluation license, you received an Entitlement ID. This Entitlement ID allows you to generate a product evaluation license key. Refer to the instructions included with the Entitlement ID to generate the license key. Use the key when you install the product.

Evaluation licenses are valid for 30 days. To upgrade from an evaluation license to a purchased copy, contact your Extreme Networks Representative to purchase the software. Refer to the Upgrading an Evaluation License section of the *Extreme Management Center Installation Guide* for instructions on upgrading your evaluation license.

Upgrade Information

Extreme Management Center 8.1 supports upgrades from Extreme Management Center version 8.0 only. If you are upgrading from a NetSight/Extreme Management Center version prior to 8.0, you must perform an intermediate upgrade. For example, if you are upgrading from Extreme Management Center 7.0, you must first upgrade to Extreme Management Center 7.1.3, then to version 8.0, and then upgrade to Extreme Management Center 8.1.

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

The NetSight Server service may not start after upgrading Extreme Management Center to version 8.0 on a system on which the Windows Server 2008 operating system is installed. Restarting Windows corrects this issue.

When upgrading the Application Analytics engines to version 8.1 after upgrading from version 6.1 to 7.1.3, the upgrade does not complete successfully. To successfully upgrade the engine to version 8.1 after upgrading from version 6.1 to 7.1.3, enter `dpkg --purge postgresql*` in the command line, then upgrade the Application Analytics engine to version 8.1.

Important Upgrade Considerations

- When upgrading the Extreme Management Center server, Application Analytics engine, or Extreme Access Control (ExtremeControl) engine to version 8.1, ensure the DNS server IP address is correctly configured. Additionally, upgrading requires an internet connection. If no internet connection is available, see Migrating or Upgrading to a 64-bit Extreme Management Center Engine.

    IMPORTANT: If a network proxy is required to access the internet, perform the following steps:

    1. Enter one of the following commands, depending on your configuration:
        - `export http_ proxy=http://`*`yourproxyaddress`*`:`*`proxyport`* if a username and password are not required.
        - `export http_ proxy=http://` *`username`* `:`*`password`*`@`*`yourproxyaddress`*`:`*`proxyport`* if a username and password are required.
    2. Run the binary upgrade for the engine.

- When upgrading to Extreme Management Center version 8.1, ensure the -Xms and -Xmx settings in the `nsserver.cfg` file are set to the values defined in the [Requirements table](#) and then restart the server:
    - On a server running a Linux operating system, enter `service nsserver restart` in the command line to restart the server.

- On a server running a Windows operating system, right-click the **NetSight Services Manager** icon in the notification area of the task bar and select **NetSight Server** > **Restart Server** to restart the server.

- When upgrading a 64-bit Extreme Management Center server or when upgrading from a 32-bit to a 64-bit Extreme Management Center server, if the -Xmx setting is set below 1536m, it increases to 1536m.

  > **NOTE:** The `nsserver.cfg` file is located in the *<install directory>*`\NetSight\services` folder.

- If your network is using Extreme Application Analytics engines, you must first perform the Extreme Management Center upgrade to version 8.1 and then add the Extreme Application Analytics engines.

- If you are running Data Center Manager (DCM), a Mobile Device Management (MDM) integration, or other ExtremeConnect or Fusion integration with Extreme Management Center, or are accessing Web Services directly or through ExtremeConnect, you need to install an Extreme Management Center Advanced (NMS-ADV) license. Contact your Extreme Networks Representative for information on obtaining this license.

Custom FlexViews, Custom MIBs, and Images

See the Custom FlexViews and Custom MIBs and Images sections in the [Important Installation Considerations](#) for additional information.

Upgrade Considerations for ExtremeControl 8.1

General Upgrade Information

When upgrading to Extreme Management Center 8.1, you are required to upgrade your Extreme Access Control (ExtremeControl) engine version to 8.0 or 8.1. Additionally, both Extreme Management Center and the Extreme Access Control engine must be at version 8.1 in order to take advantage of the new Extreme Access Control 8.1 features.

> **NOTE:** Extreme Access Control 8.1 is not supported on the 2S Series and 7S Series Extreme Access Control Controllers.

You can download the latest Extreme Access Control engine version at the Extreme Portal: https://extremeportal.force.com. Be sure to read through the

Upgrading to Extreme Access Control 8.1 document (available on the **Documentation** tab of the Portal) for important information.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 8.1 if you upgrade to the Extreme Access Control engine 8.1. Version 8.1 of the assessment agent adapter requires an operating system with a 64-bit architecture.

Access Control Version 8.0 and newer

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

To allow this functionality, add the following permissions:

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

Upgrade Considerations for ExtremeWireless 8.1

Wireless Manager Upgrade Information

Following a Wireless Manager upgrade, clear the Java Cache before starting the Extreme Management Center client.

ExtremeWireless Upgrade Information

As of version 8.1.4, Extreme Management Center now supports the ExtremeCloud Appliance. This version now includes support for high-level ciphers, which allow Extreme Management Center to communicate with both the ExtremeCloud Appliance and ExtremeWireless version 10.41.

IMPORTANT: For ExtremeWireless controllers on which version 10.41.01 or later is installed to synchronize with Extreme Management Center version 8.1.4 or later, you need to disable the use of weak ciphers. Enter the following commands to support higher ciphers:

```
secureconnection
weak-ciphers disable
message-bus-ciphers AES128-SHA256 3
```

A warning displays stating the following:

```
Warning: [AES128-SHA256] contains no NetSight client
ciphers....
```

Ignore the warning and enter `apply` in the command line.

Verify the setting is configured properly by entering the following:

```
EWC.extremenetworks.com:secureconnection# show
```

If properly configured, the following message displays:

```
Weak Ciphers: disable
Message Cipher: AES128-SHA256 3
```

Configuration Considerations

Firewall Considerations

- Port 8080 (Default HTTP traffic) must be accessible through firewalls for users to install and launch Extreme Management Center client applications.
- Port 8443 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Extreme Management Center Server Administration web pages, Extreme Management Center, and Extreme Access Control Dashboard.
- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Extreme Access Control (ExtremeControl) Engine Administration web pages.
- The following port must be accessible through firewalls for the Extreme Management Center Server and an Extreme Access Control Assessment Server to

communicate:
TCP: 8445

- The following ports must be accessible through firewalls for the Extreme Management Center Server and an Extreme Access Control engine to communicate:
Required Ports (all bi-directionally)
TCP: 4589, 8080, 8443, 8444
UDP: 161, 162

- The following port must be accessible through firewalls for Extreme Access Control engine to Extreme Access Control engine communication:
TCP: 8444

- The following ports must be accessible through firewalls for Extreme Access Control engine-to-Extreme Access Control engine communication in order for assessment agent mobility to function properly:
TCP: 8080, 8443

- The following ports must be accessible through firewalls from every end-system subnet subject to the Extreme Access Control assessment agent to every Extreme Access Control engine in order to support agent mobility:
TCP: 8080, 8443

- The following ports must be accessible through firewalls for the Extreme Management Center Server and Wireless Controllers to communicate:
SSH: 22
SNMP: 161, 162
Langley: 20506

- The following port must be accessible through firewalls for Assessment Agent updates:
TCP: 80 from Extreme Management Center to internet.

- The following ports must be accessible through firewalls for Extreme Management Center firmware updates:
TCP: 443 from Extreme Management Center to internet

- The following ports must be accessible through firewalls for the Extreme Management Center Server and WAS to communicate:
TCP: Port 8443 — Used by WAS to authenticate Extreme Management Center users. This port corresponds to Extreme Management Center's HTTPs Web Server port.
TCP: Port 443 — Import data from Extreme Management Center into WAS.
TCP: Port 8080 — Upgrade WAS from WAS UI.

- The following ports must be accessible (bi-directionally) through firewalls for the Extreme Management Center Server and an Extreme Application Analytics engine to communicate:
  TCP: Ports 4589, 8080, 8443
  UDP: Ports 161, 162
  To Extreme Application Analytics engine:
  UDP: Port 2055 (NetFlow)
  TCP: 22, 8443

  For GRE Tunnels to the Extreme Application Analytics engine IP Protocol 47
- Port 2055 must be accessible through firewalls for the Extreme Management Center Server to receive NetFlow data.

Supported MIBs

The following directory contains the IETF and Private Enterprise MIBs supported by Extreme Management Center applications:
  `<install directory>`\appdata\System\mibs directory
Navigate to the directory and open the .index file to view an index of the supported MIBs.

Additional MIB Support information is available at
www.extremenetworks.com/support/policies.

Getting Help

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

- Global Technical Assistance Center (GTAC) for Immediate Support
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.

- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

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

- A description of the failure

- A description of any action(s) already taken to resolve the problem

- A description of your network environment (such as layout, cable type, other relevant environmental information)

- Network load at the time of trouble (if known)

- The device history (for example, if you have returned the device before, or if this is a recurring problem)

- Any related Return Material Authorization (RMA) numbers

![Extreme Customer-Driven Networking logo]

What's New in Extreme Management Center
Version 8.1

This document provides an overview of the new features and enhancements included in the following areas of Extreme Management Center version 8.1:

- Engines
- Extreme Management Center
- ExtremeControl

- [ExtremeAnalytics](#)

- [ExtremeConnect](#)

- [Information Governance Engine](#)

- [Third-Party Integrations](#)

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

Engines

- [RAID Management Tools Now Included on Extreme Networks Engines](#)

- [Ability to Manage SSH Configuration on Extreme Management Center Engine](#)

- [New Default Device Terminal Session](#)

- [Improvement to Inventory Event](#)

RAID Management Tools Now Included on Extreme Networks Engines

RAID management tools are now installed on the Extreme Management Center, Access Control, and Application Analytics physical engines.

Ability to Manage SSH Configuration on Extreme Management Center Engine

You can now manage the SSH configuration on the Extreme Management Center engine.

New Default Device Terminal Session

The Linux user **Netsight**, created on the Extreme Management Center engine, now uses Bash as its default device terminal session.

Improvement to Inventory Event

The **Path Not Found** event generated when clicking **Refresh** on the **Firmware** tab now includes the path and file transfer directory in the **Operations** panel and the log on the **Event** tab.

Extreme Management Center

- ExtremeWireless Enhancements
- Introducing the Workflows Tab
- Improvements to Scripting Functionality
- Ability to Configure Variables for Use in Scripts and Workflows
- Ability to Use Device Configuration Templates
- Added Event Log Configuration
- Enhancements to Device Verification
- Ability to Assign NSI to Policy Role
- Ability to Create Port Groups
- Ability to Run Tasks via Interface Summary
- New Refresh Button for Event Log Data
- Introducing the Impact Analysis Dashboard
- Ability to Run CLI Commands on Multiple Devices
- Ability to Configure Low Disk Space Threshold
- Added URL Encoding Option
- Ability to Clear Alarms from Devices Tab
- Ability to Attempt to Contact Devices with Currently Configured Profile
- Added Most Rejected End-Systems Daily Report
- Added Support for Additional Device Types
- Enhancements to Maps Functionality
- Enhancements to Scheduled Tasks
- FlexViews for BOSS and VOSS Devices
- Enhancements to ZTP+
- Configure Device Window Enhancements
- Improvement to Device Polling
- Site Enhancements
- Port Usage Details Improvements
- Enhancement to SysLog

- [Additional Information Included in PortViews](#)

- [Enhancement to Report Dashboard Layout](#)

- [Events Enhancement](#)

ExtremeWireless Enhancements

As of version 8.1.4, Extreme Management Center now supports the ExtremeCloud Appliance.

> **NOTE:** There are [configuration considerations](#) when using the ExtremeCloud Appliance.

The ExtremeCloud Appliance and Extreme Management Center version 8.1.4 provide the same level of monitoring and configuration functionality as an Identifi Wireless Controller with improved security.

The following wireless enhancements are also included in version 8.1.4 of Extreme Management Center:

- Improved security by using TLSv1.2 and stronger ciphers between ExtremeCloud Appliance/Identifi controller and Extreme Management Center.

- WiNG AP families are now viewable in the Access Points table on the **Wireless** tab, including AP76xx, AP84xx, and AP85xx.

- Added Wireless Client Events and additions to Reports for WiNG APs.

  > **NOTE:** Heat maps in Extreme Management Center do not currently support WiNG APs. Additionally, policy configuration in Extreme Management Center is not currently supported on the Extreme Cloud Appliance. This functionality is expected to be added in the next Extreme Management Center major release.

Introducing the Workflows Tab

Workflows you create are modeled as diagrams, with each action linked in a path that a workflow execution can take. Once you create a workflow, Extreme Management Center performs a single action or a complex series of steps with a single click. You can also define a set of actions that take place if an action occurs successfully, and another set of actions that take place if that action does not occur successfully.
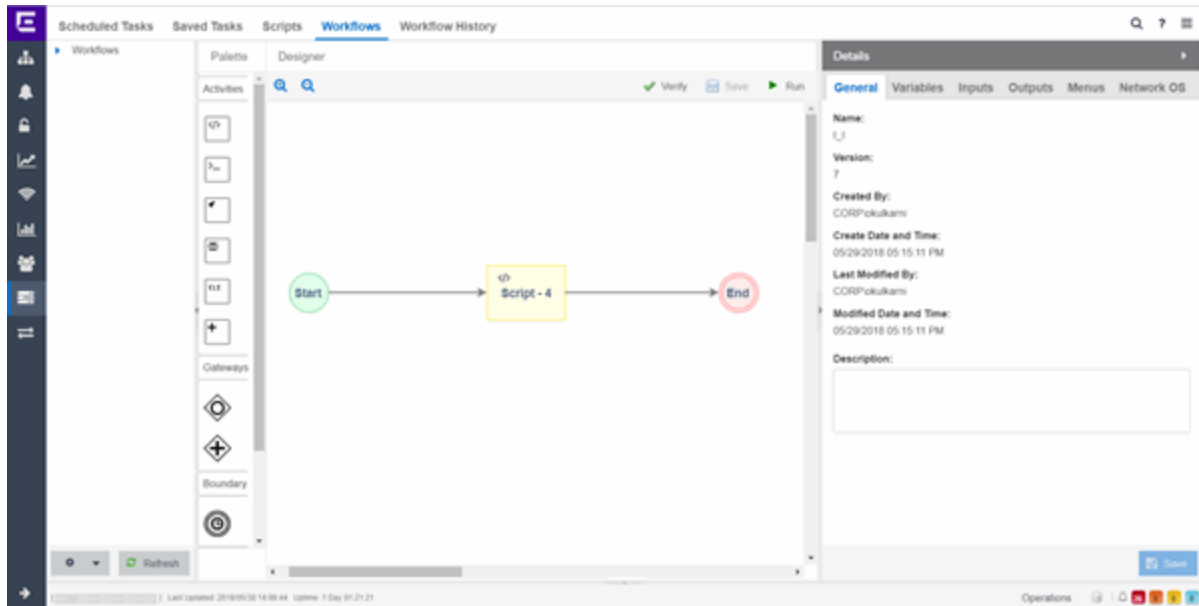
Improvements to Scripting Functionality

Creating a script via the **Scripts** tab, now included as part of the **Tasks** tab, is redesigned in version 8.1 to maximize ease of use. Additionally, scripts you create can now be included in workflows, which are designed to perform a complex series of steps.

Ability to Configure Variables for Use in Scripts and Workflows

Via the **Site** tab, Extreme Management Center now allows you to configure custom variables for use in scripts and workflows.

Ability to Use Device Configuration Templates

Extreme Management Center now provides you with device configurations you can use as a template for your device types.

Added Event Log Configuration

Via the **Event Configuration** tab, you can now configure the sources associated with an Event Type, associate event and trap sources with the log file location, and select the logging pattern used to create the log file.

Enhancements to Device Verification

Extreme Management Center now verifies the CLI credentials required to access an ExtremeXOS device are valid when a device is added to your network. If the

CLI credentials are not valid, an alarm occurs.

Via the **Devices** tab, you can now attempt to contact devices and device groups you select with the currently configured profile.

Ability to Assign NSI to Policy Role

You can now assign an NSI (Network Service Identifier) to a policy role when you select **Contain to VLAN** as a default action.

Ability to Create Port Groups

Via the **Devices** tab, you can now create port groups you can then use in reports you create.

Ability to Run Tasks via Interface Summary

You can now run tasks via the right-click menu of a device's Interface Summary.

New Refresh Button for Event Log Data

A new **Refresh** button allows you to update the Event log data displayed on the **Events** tab.

Introducing the Impact Analysis Dashboard

The Impact Analysis dashboard (available on the **Network** tab) displays a real-time summary of Availability, Performance, Capacity/Health, and Configuration data for your network. The criteria for each chart is configurable and clicking each chart opens a report displaying details about the impacted elements.

Only devices successfully discovered using SNMP are included in the Reference Firmware chart in the Impact Analysis Dashboard.

Ability to Run CLI Commands on Multiple Devices

You can now run CLI commands on multiple devices simultaneously via the **Execute CLI Commands** option on the **Devices** tab.

Ability to Configure Low Disk Space Threshold

In version 8.1, you can configure the amount of free space remaining on the Extreme Management Center server below which Extreme Management Center

stops writing non-critical data to the database. Additionally, crossing the threshold you define automatically generates an event in the log.

Added URL Encoding Option

Extreme Management Center now allows you to determine whether passwords are encoded or not in URLs when performing a file transfer.

Ability to Clear Alarms from Devices Tab

You can now clear an alarm associated with a device from the **Devices** tab.

Added Most Rejected End-Systems Daily Report

You can now view the top ten most rejected end-systems via the Most Rejected End-Systems Daily report, available on the **Reports** tab.

Added Support for Additional Device Types

Extreme Management Center now supports the following device types:

- BOSS
- VOSS
- SLX
- ICX
- WLAN-9100

Enhancements to Maps Functionality

The following enhancements to maps are included in this release:

- System-defined links in maps created via LLDP can now be overwritten manually.
- A FlexView showing link utilization in percent and bytes is now available via the right-click menu on a map link.
- You can now create multiple links between devices.
- The following devices types now fully support floorplan map functionality:
  - AP3916ic-FCC
  - AP3916ic-ROW

Enhancements to Scheduled Tasks

You can now schedule your FlexViews and FlexReports via the Scheduled Tasks tab and export them as .CSV files. Additionally, you can now use email lists in scheduled tasks.

FlexViews for BOSS and VOSS Devices

FlexViews for BOSS and VOSS devices are now available in Extreme Management Center.

Enhancements to ZTP+

The following enhancements to ZTP+ functionality are included in this release:

- Extreme Management Center now generates events when upgrading a device, when a device is upgraded to the latest version, and when a configuration is sent to a device via ZTP+.

- Devices added via ZTP+ now provide the **dot1dIndex** value in the **Ports** tab in the **DeviceView**.

- ZTP+ devices are now included in the **Port Usage** report.

- You can now create **ZTP+**, **ZTP+ Events**, and **ZTP+ Transactions** Custom Criteria Alarms via the **Category Criteria** window. Additionally, Extreme Management Center now creates an event when a configuration is enforced to a ZTP+ enabled device.

- Via the **Administration** > **Diagnostics** tab, you can enter the serial numbers of specific ZTP+-enabled devices, so that only those devices appear in the Enhanced Zero Touch Provisioning diagnostic debug.

- Extreme Management Center allows you to define a reference image for each device type using ZTP+ in the **Firmware** tab.

- You can now enable node alias, SpanGuard, Loop Protect, MVRP (multiple VLAN registration protocol), on a port via ZTP+ functionality.

- You can define a **Poll Type** using ZTP+ functionality.

- Extreme Management Center allows you to discover devices added to sites via ZTP+ using DHCP.

- Extreme Management Center allows you to schedule device firmware upgrades via ZTP+

- You can now use the discovered IP address for a device as the device IP address for devices discovered using ZTP+.

Configure Device Window Enhancements

The **Configure Device** (formerly **Edit Device**) window now includes the following enhancements:

- The top of the window now displays a list of selected devices to allow you to enable quickly changing multiple devices at once.
- The **Ports** tab now contains a **Collection** column, which indicates whether historical collection is enabled on the port.
- **VLAN Definition** and **Ports** tabs now show all selected devices.
- **VLAN Definition** and **Ports** tabs are now paged to help improve performance with many devices selected.
- All columns can be filtered and sorted.
- VLANs can be added to more than one device at a time.
- The **Vendor Profile** tab allows you to add, configure, and edit device vendor information via Extreme Management Center.

Improvement to Device Polling

Extreme Management Center now supports native ICMP polling for IPv4 and IPv6.

Site Enhancements

You can now import VLAN data from a device that supports 802.1Q into the VLAN definition of the site. Additionally, in version 8.1, you can enable port collection via the **Port Templates** tab.

Port Usage Details Improvements

The Port Usage Details report now includes site information, the number of ports being used, and the percentage of traffic utilization as compared to the total port traffic capacity.

Enhancement to SysLog

Extreme Management Center now supports the ability to specify a non-standard UDP port for syslog alarm actions.

Additional Information Included in PortViews
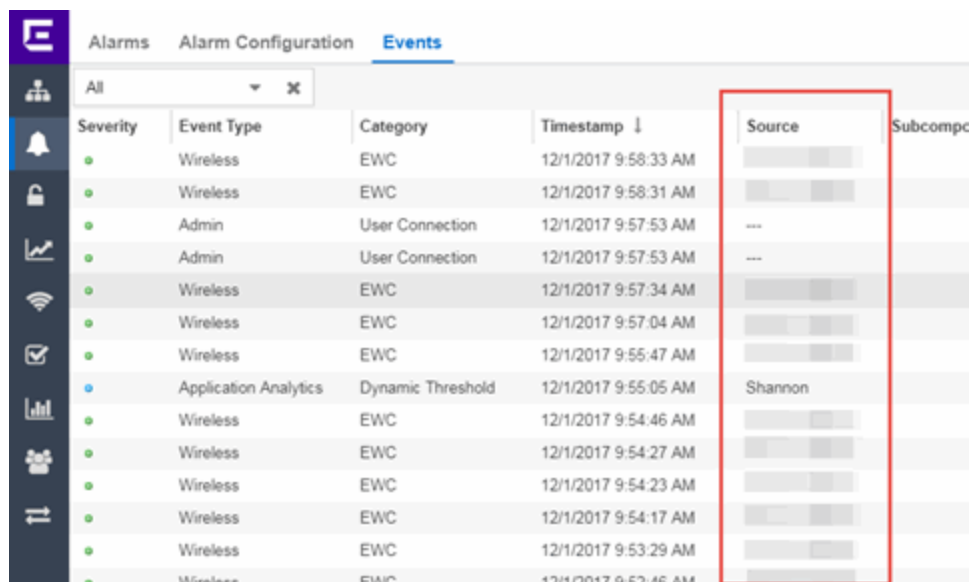
Extreme Management Center now displays the **Port by Name (Alias)** for all Extreme devices in Interface Details included in a PortView.

Enhancement to Reports Dashboard Layout

In Extreme Management Center 8.1, you can customize your Reports dashboard layout design by dragging and dropping components onto the report grid in Report Designer. Once in place, the components provide a live preview of the reports you chose.

Events Enhancement

A **Source** column is added to the **Events** tab in Extreme Management Center, where you can view the hostname of the device from which an event originated.

ExtremeControl

- [Ability to Disable Live Updating of End-System Tables](#)
- [Additional Configuration Support for Certificate Revocation Lists (CRLs)](#)
- [Active Directory/MSCHAPv2 Enhancement](#)
- [ExtremeControl Now Supports Identity Engines (IDE)](#)
- [Support for Fortinet Devices](#)

- [Support for Per-User ACLs](#)

- [Ability to View Ports Using a Policy Role](#)

- [Added DHCP Fingerprint for IGEL Device](#)

- [Additional Information Included in Events](#)

- [Enhancement to Group Editor](#)

- [Improvements to Captive Portal Usability](#)

- [Enhancements to Guest Registration](#)

- [Added DHCP Fingerprint for Medical Devices](#)

- [Enhancements to End-Systems](#)

- [Improvements to ExtremeControl Authentication](#)

- [Enhancements to ExtremeControl Rules](#)

- [ExtremeControl Usability Improvements](#)

- [Enhancement to Creating a Policy Rule Using an Application Flow](#)

- [Enhancement to Enforce Preview](#)

- [Enhancement to Port Authentication Wizard](#)

Ability to Disable Live Updating of End-System Tables

Via the [Access Control Options](#) on the **Administration** tab, ExtremeControl now allows you to disable the live updating of end-system tables in Extreme Management Center.

Additional Configuration Support for Certificate Revocation Lists (CRLs)

ExtremeControl supports configuring RADIUS to allow missing CRLs when conducting CRL checks, similar to existing support for allowing expired CRLs. Additionally, added alerts and alarms for authentications allowed with missing or expired CRLs, and alerts and alarms for rejects for same conditions.

Active Directory/MSCHAPv2 Enhancement

ExtremeControl now supports MSCHAPv2 when the Active Directory Server is set to the highest security level.

ExtremeControl Now Supports Identity Engines (IDE)

Identity Engines (IDE) formerly manufactured by Avaya, can now be used as Access Control engines in ExtremeControl. End-Systems authenticated by IDE are displayed in the **End-Systems** tab.

Support for Fortinet Devices

ExtremeControl now supports login RADIUS MGMT login attempts from Fortinet devices.

Support for Per-User ACLs

ExtremeControl policy now supports Per-User ACLs (PU-ACL) from third-party vendors passed via RADIUS authentication requests. During a policy enforce, the roles and associated rules are translated into ACLs and pushes them to the appropriate Access Control Engines.

Ability to View Ports Using a Policy Role

Selecting a role in the **Policy** tab now allows you to view the ports on which the role is set to the default.

Added DHCP Fingerprint for IGEL Devices

Added an additional DHCP Fingerprint in Extreme Management Center version 8.1 to identify IGEL Linux devices.

Additional Information Included in Events

Additional information is now included in Access Control engine events generated when an administrator or management login occurs.

Enhancement to Group Editor

You can now import group entries directly from .CSV files.

Improvements to Captive Portal Usability

The following usability improvements are included in this release:

- HTTP session connections are enhanced.
- You can now select multiple rows in tables included in the Captive Portals area of the **Control** tab.

- The Acceptable Use Policy is now hidden by default on the mobile captive portal and can be displayed by clicking the **AUP** button.

- The Dutch (Netherlands) language bundle is now included in the captive portal.

Enhancements to Guest Registration

The Guest Registration portal now allows users to log into their Yahoo or Salesforce account to complete the guest registration process. Additionally, you can also create a generic guest registration portal using OpenID Connect.

Additionally, the Google and Microsoft Guest Registration options, which formerly used the OAuth authorization framework, are improved in this release. These authentication methods now include an identity layer through the use of OpenID Connect.

Added DHCP Fingerprints for Medical Devices

Added additional DHCP fingerprints to identify medical devices based on the MAC OUI.

Enhancements to End-Systems

The following end-system enhancements are included in this release:

- The **End-Systems** tab now includes an End-System Events and Health Results section, which provides information about the end-system selected at the top of the tab.

- The End-System, End-System Events and Health Results windows all update automatically with new data.

- End-System data can now be exported to a .CSV file and you can filter the data in the file.

Improvements to ExtremeControl Authentication

The following ExtremeControl authentication improvements are included in this release:

- ExtremeControl now saves unsuccessful RADIUS authentication requests when Data Collection is enabled. This information can be exported as a report via the **Custom Report** tab.
- ExtremeControl now saves the client certificate fingerprint for EAP-TLS authenticated sessions.
- ExtremeControl now supports multiple Certificate Authorities and Certificate Revocation Lists from the same issuer in AAA Configuration when the Subject Key Identifier/Authority Key Identifier extensions are unique.

Enhancements to ExtremeControl Rules

The following enhancements to ExtremeControl rules are included in this release:

- New default rules
- Ability to copy existing rules to create new rules
- Added a description field for rules
- Ability to group rules

ExtremeControl Usability Improvements

The **Access Control** tab now includes the following usability improvements:

- Ability to disable default live end-system updates on the **Options** tab.
- Ability to configure Access Control engine settings at the engine group level, which configures all of the engines in the group
- Ability to reorder LDAP Configurations on the **Configuration** > **AAA** tab
- Ability to copy, create and modify RADIUS Attribute Configurations
- Ability to export a table on which a filter is applied to a .CSV file
- Ability to select a default policy domain for an Access Control engine group

Enhancement to Creating a Policy Rule Using an Application Flow

Creating a policy rule using a flow you select on the **Application Flows** tab, is enhanced to support application type rules in addition to IP UDP/TCP.

Enhancement to Enforce Preview

The **Enforce Preview** window now indicates devices that do not have the minimum firmware version required to support a new feature for that platform.

Enhancement to Port Authentication Wizard

Via the Authentication Configuration wizard, you can now create templates for loading and saving the authentication configuration settings.

ExtremeAnalytics

- Ability to Collect Flow Information on ExtremeXOS Devices
- Ability to Generate Application Telemetry Reports via **Devices** Tab
- New Insights Dashboard
- New ExtremeAnalytics Reports
- Ability to Configure Devices As Application Telemetry Sources
- Enhancements to Network Locations
- Application Flows Performance Improvement

Ability to Collect Flow Information on ExtremeXOS Devices

Via Application Telemetry, ExtremeAnalytics now allows you to use your ExtremeXOS devices as flow collectors.

Ability to Generate Application Telemetry Reports via Devices Tab

You can now generate application telemetry reports via the **Application Telemetry** menu on the **Devices tab**.

New Insights Dashboard

The **Analytics** tab includes a new Insights Dashboard, available from the **Dashboard** drop-down menu.

The Insights Dashboard features ring charts that display real-time network and application usage and service data:

- **Engines** — Indicates the number of Application Analytics engines configured in your network engines and the states of the engines.

- **Disk Usage** — Indicates the percentage of disk space Extreme Management Center is using.

- **Flow Rate** — Indicates the percentage of flows per minute analyzed by the Application Analytics engine to the total flow rate included in your license.

- **Network Response** — Indicates the response time for network services accessed at your network locations.

- **Application Response** — Indicates the response time for applications accessed at your network locations.
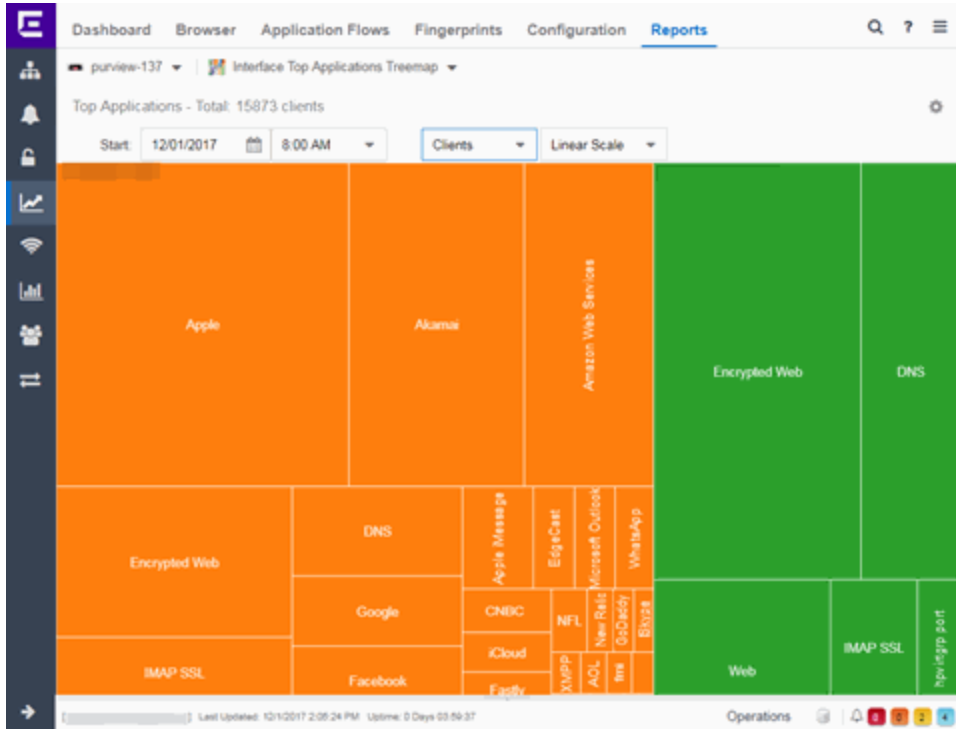
Additionally, a **Views** menu allows you to drag and drop graphs and charts into the Dashboard to provide more in-depth information about your network.
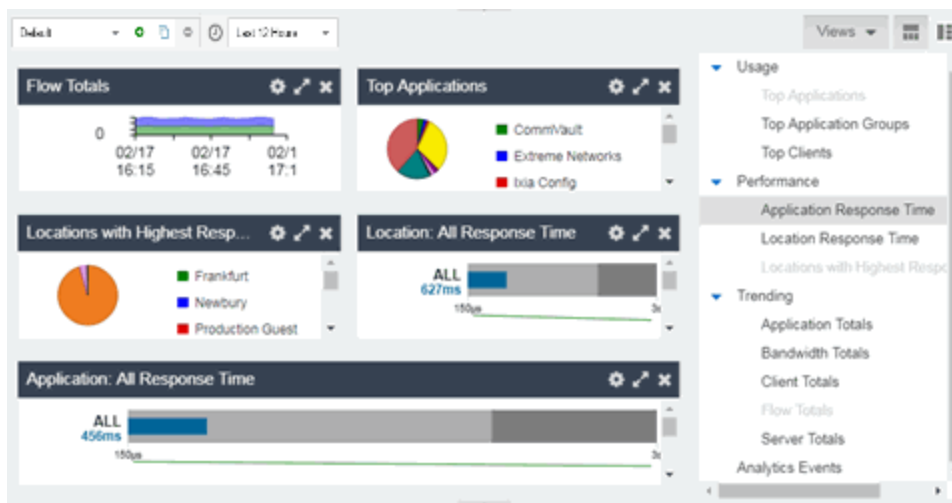
The graphs and charts allow you to view information available in other ExtremeAnalytics dashboards (e.g. the Tracked Applications dashboard) and reports in one centralized location. You can copy a dashboard and use it as a template to create a new one. Saved dashboards are available to all users.

New ExtremeAnalytics Reports

The Analytics Interface Top Applications Treemap, Top Clients by Interface, and Top Interfaces by Application ExtremeAnalytics reports are now available on the **Analytics** tab.

Ability to Configure Devices As Application Telemetry Sources

You can now configure ExtremeXOS devices as application telemetry flow sources.

Enhancements to Network Locations

You can now assign roles to network locations, which helps specify the purpose of a location as Access, Core, Data Center, or DMZ. Additionally, for network

configurations with multiple Application Analytics engines, you can now configure the primary location for each engine to improve the accuracy of flow traffic statistics.

Application Flows Performance Improvement

In version 8.1, the performance of the ExtremeAnalytics **Application Flows** tab is improved.

ExtremeConnect

New ExtremeConnect Modules

ExtremeConnect allows you to integrate with Amazon Web Services, Microsoft InTune MDM, Google GSuite, and Aruba Clearpass via new modules on the **Connect** tab.

Information Governance Engine

Your version of IGE is automatically upgraded when installing Extreme Management Center 8.1. The new version provides you with the GDPR (General Data Protection Regulation) regime, new audit tests, and support for ExtremeSwitching 200-Series (200-Series), BOSS, and VOSS devices. Regimes and audit tests you create in version 8.0 are retained following the upgrade.

- [Ability to Test Additional Device Types](#)
- [Added Additional Regime](#)
- [Ability to Export IGE Dashboard Data](#)

Ability to Test Additional Device Types

Version 8.1 adds support for WiNG wireless devices in IGE. You can now test your WiNG wireless devices using audit tests in the PCI, HIPPA and GDPR compliances, which evaluate your devices for a Wireless Intrusion Prevention System, firewall and management policy for security measures. These tests are designed to monitor the network for threats, penetrations, and intrusions.

Additionally, version 8.1 adds support for 200-Series devices. Audit Tests in the PCI, HIPAA, and GDPR regimes for 200-Series devices provide you with the ability to adopt a stronger security policy, helping you prevent a wide range of

attacks and provide protection from threats, penetrations, and intrusions. Version 8.1 also allows you to create audit tests for third-party (non-Extreme Networks) devices.

Added Additional Regime

Via the **Governance** tab, you can now test whether your devices are compliant with the GDPR (General Data Protection Regulation) industry standard. The regime includes new audit tests focused on evaluating the configuration of your devices against the standard.

Ability to Export IGE Data

You can now export audit test results as a .PDF. The report contains a summary of the regime test results as well as a breakdown of the results for each device tested.

Third-Party Integrations

StackStorm (ST2) Integration into Extreme Management Center

StackStorm (ST2) is an event-driven automation program that you can now use via Extreme Management Center for facilitated troubleshooting, auto-remediation, security responses, complex deployments, and more. ST2 allows you to process Trap, Alarm, or Syslog messages directly from the Extreme Management Center.