Extreme Management Center Customer Release Notes

Version 8.0.5.18
November, 2017

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. Its Control interface 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 8.0.5, 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 can be found on the Extreme Management Center (NetSight) (NMS) Documentation web page: https://extranet.extremenetworks.com/downloads. After entering your email

address and password, follow this path to the document: Software & Security > Extreme Management Center (NetSight) (NMS) > Documentation > Manuals & Release Notes > Extreme Management Center (NetSight) 8.0.5 > Extreme Management Center (NetSight) Suite.

Software Enhancements

Enhancements in Extreme Management Center 8.0.5

The new features and enhancements included in Extreme Management Center 8.0.5 are now located in the What's New in Extreme Management Center Version 8.0.5 topic.

Deprecated Features

The following legacy java applications are deprecated in version 8.0.5:

- ACL Manager
- Automated Security Manager
- Basic Policy (Console)
- Policy Control Console
- RMON (Device Manager)
- RoamAbout Wireless

The following Extreme Management Center features are deprecated in version 8.0.5:

- Isaac
- Monk
- Security Advisor

Known Issues Addressed

This section presents the known issues addressed in Extreme Management Center 8.0.5.18:

Extreme Management Center Issues Addressed	ID

Scheduled tasks that failed to complete were preventing tasks that followed from running.	-------
CLI rules you manually add to the `CLIRules.xml` file were removed from the database after upgrading Extreme Management Center.	-------
Some third-party devices were displayed as **Unknown** when selecting **Device Types** in the **Device Tree**.	-------
The Extreme Management Center device restart wizard was restarting devices immediately if the scheduled time was set to PM.	1360674
Wireless Controllers were not receiving license keys needed for a Subscription licensed model.	01329902 01385762
Changes made to scripts were not being saved on an Extreme Management Center server on which a Windows operating system is installed.	-------
Changing the **Polling Type** for a ZTP+ device to a value other than **ZTP+** may not save in Extreme Management Center.	-------
VLANs configured in the **Edit Device** window could not support lag ports.	1391086
After deleting a site, the site was still displayed on the **Site Summary** tab.	-------
Changing the name of an Extreme Management Center map was preventing its sub-maps from opening.	-------
When importing a map into Extreme Management Center, the percentage displayed in the Operations panel was misleading.	-------
Extreme Management Center was occasionally not upgrading successfully if the server license was not applied prior to starting the upgrade.	-------
ExtremeAnalytics™ Issues Addressed	**ID**
Running the `ethports.pl` script on a PV-A-300 Application Analytics engine (either manually or via an upgrade) was causing the fiber ports to display incorrectly in Extreme Management Center.	-------
Deploying an Application Analytics or Access Control engine or an Extreme Management Center server on multiple virtual machines using the same .OVA file was generating identical SSH server keys.	-------
The response times reported from wireless controllers were greater than the actual response times.	-------
ExtremeControl™ Issues Addressed	**ID**

Java exception errors were incorrectly displayed in the TAG.LOG file.	1398801
Restarting the Access Control server process was causing disconnected end-systems to be reported as connected.	01327126
Users with a subscription-based Extreme Management Center license were incorrectly receiving an end-system license error from their Access Control virtual engine after 3,000 users.	01390267

Policy Manager Issues Addressed	**ID**
PVI VLANs were converted to normal VLANs when the domain was opened in Extreme Management Center.	1387278
The parent folders in the device tree on the Policy tab may indicate devices are down when none of the devices in the domain are actually down.	-------
Automated services could not be configured from Extreme Management Center.	1388966

This section presents the known issues addressed in Extreme Management Center 8.0.4.54:

Extreme Management Center Issues Addressed	**ID**
Upgrading Management Center to version 8.0.2.42 generated unnecessary RADIUS log messages in the server.log file.	1334780
Upgrading Extreme Management Center to version 8.0.5 in a proxy environment was causing issues, the process now gathers the necessary configuration so the upgrade completes successfully.	-------
Sub levels of the device tree were being sorted by IP rather than the current sort setting.	01358222
A pool of database connections were slowly depleted until it became empty, which caused database errors and prevented users from logging in.	1360892 01364607
Custom reports created via the Reports > Custom Report tab in Extreme Management Center were not saved correctly on the Reports > Report Designer tab.	1318190
The IP Address column in the Network > Discovered tab was incorrectly displaying N/A for the DHCP address used by discovered ZTP+ devices. The column now displays dynamic IP addresses with an asterisk (*) to distinguish them from permanent static addresses (no asterisk).	-------

Updating the Serial Number of a device and then refreshing the device was not updating the Serial Number.	1229164
Deleting firmware was causing a data access exception in the server log.	-------
Extreme Management Center was incorrectly displaying unsupported legacy firmware versions as valid.	0283021
The Bridge Spanning Tree Information FlexView was displaying incorrect information.	1304851
FlexViews with names that contain a dash (-) were not loading properly.	1213960
Running a script that includes a period (.) was causing the script to fail.	1223350
EAPS and VLAN scripts for ExtremeXOS devices were incorrectly removed from earlier 8.0 Extreme Management Center versions.	-------
ZTP+ devices added to a site with a Starting IP address configured were not assigning IP addresses to the newly added devices.	-------
Users with administrative capabilities were unable to modify profiles via the Console legacy java application.	-------
Upgrading from Extreme Management Center version 7.x to 8.0 was causing the "World Map" to become a Site rather than a Map.	1367347
Previously, you were able to delete a profile associated with a site. You can now no longer delete profiles which are in use in Extreme Management Center until all references to the profile are removed.	1379165
Expanding a device tree with a large number of maps was loading slowly or not loading.	1351621
Large floorplan and topology map images were being scaled down to 890 x 670 pixels, which was causing map quality issues. Map images now have a maximum 3,000 x 2,000 pixels and can be larger by editing the `oneView.maxImageSize=3000x2000` line of the `NSJBoss.properties` file, however, increasing this value can cause stability and heatmap performance issues.	-------
Extreme Management Center security system was incorrectly processing authorization requests from backend systems.	01377737
ExtremeAnalytics™ Issues Addressed	**ID**

Packets routed through GRE tunnels on an Extreme Application Analytics virtual engine are incorrectly reported as dropped in the ifconfig output on the GRE interface. This scenario was tested and while these packets are reported as dropped, they are being inspected by the Application Analytics engine.	1305070

ExtremeControl™ Issues Addressed	**ID**
Enforcing RADIUS User Groups to an Extreme Access Control engine no longer displays a warning if a RADIUS server has not been configured.	1336689
Authenticating via 802.1X, changing the username, and then authenticating again via 802.1X, the Extreme Access Control engine was incorrectly using the old authentication request with the old username.	1337625

Policy Manager Issues Addressed	**ID**
Starting the Extreme Management Center server after importing a Policy Domain ZIP file was causing errors in the server log.	-------

Wireless Issues Addressed	**ID**
Immediately after enabling Wireless Collection, the Status column was incorrectly displaying Disabled.	01149093

Legacy Java Application Issues Addressed	**ID**
The Allow legacy credentials for messaging connection option in the Console legacy java application was displayed as enabled, but the functionality was not active in Extreme Management Center, so the option was removed.	1352882

This section presents the known issues addressed in Extreme Management Center 8.0.3.53:

Extreme Management Center Issues Addressed	**ID**
Restoring a configuration was failing for devices without a 'public' community string.	1357858
Running a script using the '$port' variable was overriding the Telnet/SSH port number.	-------
A security issue was fixed for the Extreme Management Center legacy java applications.	1357835
Sorting the Device Tree was not persisting locally in the client browser.	1274649

The **Save** button on the **Site** tab was not available when invalid data was included in one of the fields on the tab.	-------
A memory-access exception was infrequently seen from the SNMP library.	1319492
Devices not in new Vendor profile definitions were incorrectly showing empty family, device type and images from the company default values.	-------
Map paths were not working properly.	1293450
Deploying Extreme Management Center using a subscription license was not allowing access to all map features.	01328069
The Extreme Management Center, Extreme Application Analytics, and Extreme Access Control engines were vulnerable to CVE-2017-7494.	01333108
Replacing or updating a device via the **Replacement Serial Number** functionality in the **Edit Device** window with another device using the same IP address, the serial number was not updating.	1332525
The **Precedence** value of a User Authorization Group was not able to be modified via the web client.	1336469
Script tasks added to the **Scheduler** tab created prior to 8.0.2 were not running.	1337760
Motorola Wireless - TFTP Script was not running correctly.	1335472
800-Series devices were not correctly labeled in the DeviceView Port Tree.	01202446
ExtremeAnalytics Issues Addressed	**ID**
Web application rule fingerprints based on the flow hostname were not able to be created.	-------
The Network Service Dashboard, Response Time Dashboard, and Tracked Application Dashboard were incorrectly available as "Component" options in the Report Designer.	01304023
ExtremeControl Issues Addressed	**ID**
The RADIUS Shared Secret could not include a backslash (\).	01318586
User-defined SNMP credentials were removed from Extreme Access Control engines when upgrading to version 8.0.1.33.	1327535
Inverted LDAP User Rules were not matching because part of the check indicated the User did not exist.	1307052 1330783 1341531
Devices using Redpine Signals chipsets were being incorrectly identified as Nintendo DS devices via DHCP fingerprinting.	01318202

Some HP Printers were being incorrectly identified via DHCP fingerprinting.	01317925
Google Chromecast devices were being incorrectly identified as generic Android devices via DHCP fingerprinting.	01276067
Mitel IP phones were being incorrectly identified via DHCP fingerprinting.	1324217
After upgrading an Extreme Access Control engine configured to manage SNMP, a NullPointer exception similar to the following may have been logged: "Exception in thread "main", java.lang.NullPointerException at java.util.ArrayList.addAll (ArrayList.java:577)".	01339903
JMS traffic between Extreme Access Control and the Extreme Management Center server was not secure.	01335977
Selecting **Listen Only** for **eth1** in the **Interfaces** window for an Extreme Access Control engine was not removing any configured IPv6 address.	1317293

This section presents the known issues addressed in Extreme Management Center 8.0.2.42:

Extreme Management Center Issues Addressed	**ID**
Legacy java applications could not be opened from within Management Center if the default web server port was changed.	1245279
Extreme Management Center installation was not completing successfully on any system on which a non-Ubuntu Linux operating system was installed.	-------
ExtremeAnalytics Issues Addressed	**ID**
The Extreme Application Analytics engine could not be successfully upgraded if the `rsyslog.conf` file was modified.	-------
ExtremeControl Issues Addressed	**ID**
User-defined SNMP credentials were removed from Extreme Access Control engines when upgrading to version 8.0.1.33.	1327535

This section presents the known issues addressed in Extreme Management Center 8.0.1.33:

Extreme Management Center Issues Addressed	**ID**

Selecting All Devices in the left-panel drop-down menu in the Network > Devices tab caused performance issues. As a result, the All Devices selection was removed from the menu.	01243030

ExtremeControl Issues Addressed	**ID**
When both LDAP User Group and LDAP Host Group were included in an Access Control Configuration Rule, only LDAP User Group attributes were being searched.	-------

This section presents the known issues addressed in Extreme Management Center 8.0.0.130:

Extreme Management Center Issues Addressed	**ID**
Adding a new device to a device group via a right-click on the device group was incorrectly adding the device to the All Devices group.	01243030
User Names could not include a period (.).	1258335 01262468
Syslog messages were displaying with a Severity of Info for installations on the Windows operating system.	1144968
Automatically refreshing the syslog status was causing an excessively high number of events to be logged.	01241784 01256479
Licenses with old part numbers were incorrectly not recognized as valid when applied through Extreme Management Center (Administration > Diagnostics > Server > Server Licenses).	1280440
Some email servers that used a non-standard UTF character set were unable to deliver email from Extreme Management Center.	1279665
ExtremeControl Issues Addressed	**ID**
The Assessment Agent was causing excessive battery consumption on systems on which a MAC operating system was installed.	------
Users were unable to access self-registration page in captive portal if supplemental locales were configured.	01278866 01279112
Wireless Issues Addressed	**ID**
The Wireless > Threats tab was incorrectly displaying an RSS of 0 for all threats.	1254694

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 8.0.5:

- The following vulnerabilities were addressed in the Extreme Management Center, Extreme Access Control, and Extreme Application Analytics engine images:
    - CVE-2017-9233, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2015-8994, CVE-2016-10397, CVE-2017-11143, CVE-2017-11144, CVE-2017-11145, CVE-2017-11147, CVE-2017-11362, CVE-2017-11628, CVE-2017-9224, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-0663, CVE-2017-7375, CVE-2017-7376, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050, CVE-2017-9461, CVE-2017-11103, CVE-2017-10110, CVE-2017-10089, CVE-2017-10086, CVE-2017-10096, CVE-2017-10101, CVE-2017-10087, CVE-2017-10090, CVE-2017-10111, CVE-2017-10107, CVE-2017-10102, CVE-2017-10114, CVE-2017-10074, CVE-2017-10116, CVE-2017-10078, CVE-2017-10067, CVE-2017-10115, CVE-2017-10118, CVE-2017-10176, CVE-2017-10104, CVE-2017-10145, CVE-2017-10125, CVE-2017-10198, CVE-2017-10243, CVE-2017-10121, CVE-2017-10135, CVE-2017-10117, CVE-2017-10053, CVE-2017-10108, CVE-2017-10109, CVE-2017-10105, CVE-2017-10081, CVE-2017-10193, CVE-2013-7459, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-2123, CVE-2016-2125, CVE-2016-2126, CVE-2016-6210, CVE-2016-6515, CVE-2016-1252, CVE-2015-7973, CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8158, CVE-2016-0727, CVE-2016-1547, CVE-2016-1548, CVE-

2016-1550, CVE-2016-2516, CVE-2016-2518, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, CVE-2016-9427, CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5, CVE-2015-2059, CVE-2015-8948, CVE-2016-6261, CVE-2016-6262, CVE-2016-6263, CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633, CVE-2016-7444, CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-1248, CVE-2016-6313, CVE-2015-0245, CVE-2016-2119, CVE-2017-7494, CVE-2004-2761

- The following vulnerabilities were addressed in the Extreme Management Center and Extreme Access Control images:
    - CVE-2016-5423, CVE-2016-5424
- The following vulnerability was addressed in the Extreme Management Center image:
    - CVE-2017-1000117
- The following vulnerabilities were addressed in the Extreme Access Control and Extreme Application Analytics images:
    - CVE-2014-0209, CVE-2014-0210, CVE-2014-0211
- The following vulnerability was addressed in the Extreme Access Control image:
    - CVE-2016-6489

System Requirements

IMPORTANT: Extreme Management Center version 8.0.5 only runs on a 64-bit engine image. Any Extreme Management Center or Extreme Access Control engine currently running a 32-bit OS image must be upgraded to the newer 64-bit image prior to upgrading to 8.0.5. Please contact Extreme Networks Support with any questions.

Wireless event collection is disabled by default in version 8.0.5 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™ 5.5 server VMware ESXi™ 6.0 server VMware ESXi™ 6.5 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.

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	4 GB
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)

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
MU Events	No	Yes	Yes

Extreme Access Control 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:			
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:			
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.

Extreme Access Control 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 version 34 and later	34 and later
	Google Chrome version 33.0 and later	33.0 and later
	Safari	All versions
Mobile	Internet Explorer Mobile	11 and later (Windows Phone)
	Microsoft Edge	All versions
	Microsoft Windows 10 Touch Screen Native (Surface Tablet)	N/A
	Safari	7 and later
	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 Safari (iOS) or 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 Engine Version Requirements

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

Extreme Access Control 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.

Extreme Access Control SMS Gateway Requirements

The following SMS Gateways have been tested for interoperability with Extreme Access Control:

- Clickatell
- Mobile Pronto

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

Extreme Access Control SMS Text Messaging Requirements

The following mobile service providers are supported by default for SMS text messaging in an Extreme Access Control 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	

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 Extreme Management Center (NetSight) (NMS) Documentation web page: http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx.

IMPORTANT: The NetSight Server service may not start after installing Extreme Management Center version 8.0.5 on a system on which a Windows Server operating system is installed. Restarting Windows corrects this issue.

When starting the Extreme Management Center server after installing version 8.0.5 on a non-Extreme Management Center engine, the following error may display in the server.log: "Cannot run program "usr/local/Extreme_ Networks/NetSight/GovernanceEngine/governance-engine.py".

Important Installation Considerations

Important Requirement for Extreme Application Analytics Engines Version 8.0.5

When installing the 8.0.5 .ISO image on a PV-A-300 Application Analytics engine with add-on interface cards, the ordering of the interfaces may change unexpectedly. Run the `ethports.pl` script in the `/root/scripts` directory by entering `ethports.pl -F` in the command line to correct the ordering.

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 a 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 8.0.5 supports upgrades from Extreme Management Center version 7.1.3 only. If you are upgrading from a NetSight/Extreme Management Center version prior to 7.1.3, 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, and then upgrade to Extreme Management Center 8.0.5.

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 8.0.5 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 8.0.5 after upgrading from version 6.1 to 7.1.3, the upgrade does not complete successfully. To successfully upgrade the engine to version 8.0.5 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 8.0.5.

Important Upgrade Considerations

- When upgrading the Extreme Management Center server, Application Analytics engine, or Extreme Access Control engine to version 8.0.5, ensure the DNS server IP address is correctly configured. Additionally, upgrading requires an internet connection and may take additional time due to the upgrade of the Linux Ubuntu operating system from version 12 to version 14. During this time, the engine may not be accessible via SSH. 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.

- If your network is using Extreme Application Analytics engines, you must first perform the Extreme Management Center upgrade to version 8.0.5 and then add the Extreme Application Analytics engines.
- If you are running Data Center Manager (DCM), a Mobile Device Management (MDM) integration, or other OneFabric Connect or Fusion integration with Extreme Management Center:
  - You must install a Extreme Management Center Advanced (NMS-ADV) license with 8.0.5 when you upgrade. Contact your account team for information on obtaining this license.
- If you are accessing Web Services directly or through OneFabric Connect, you need to install a Extreme Management Center Advanced (NMS-ADV) license. Contact your account team for information on obtaining this license.
- 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.
- When upgrading to Extreme Management Center version 8.0.5, 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.

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

Custom FlexViews

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.

Upgrade Considerations for NAC Manager 8.0.5

General Upgrade Information

When upgrading to Extreme Management Center NAC Manager 8.0.5, you are required to upgrade your Extreme Access Control engine version to 7.1.3 or 8.0.5. Additionally, both Extreme Management Center NAC Manager and the Extreme Access Control engine must be at version 8.0.5 in order to take advantage of the new Extreme Access Control 8.0.5 features.

NOTE: Extreme Access Control 8.0.5 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 Management Center (NetSight) (NMS) Download web page http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx. Be sure to read through the *Upgrading to Extreme Access Control 8.0.5* document (available on the Extreme Management Center (NetSight) Documentation web page > Manuals & Release Notes > NetSight 8.0.5 > Network Access Control [NAC]) for important information.

In addition, if your ExtremeControl solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 8.0.5 if you upgrade to the

Extreme Access Control engine 8.0.5. Version 8.0.5 of the assessment agent adapter requires an operating system with a 64-bit architecture.

Upgrade Considerations for Wireless Manager 8.0.5

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

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 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.

Important URLs

The following URLs provide access to Extreme Management Center software products and product information:

- For information on product licensing, visit https://extranet.extremenetworks.com/Pages/default.aspx.
- To download the latest Extreme Management Center software products, visit the Extreme Management Center (NetSight) (NMS) web page: http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx.
- To download previously released Extreme Management Center products, visit the Extreme Management Center (NetSight) (NMS) web page: http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx.
- To register any Extreme Management Center products that are covered under a service contract, use the Service Contracts Management System at https://extranet.extremenetworks.com/Pages/default.aspx.

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

What's New in Extreme Management Center Version 8.0.5

This document provides an overview of the new features in Extreme Management Center version 8.0.5. 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.

IMPORTANT: Due to the infrastructure and functionality improvements in version 8.0.5 of Extreme Management Center, the hardware and operating system requirements are also changed. Refer to the below table and list for the recommended Extreme Management Center server hardware and operating systems.

Hardware Requirements

	Small	Medium	Large	Extra Large
Total CPUs	1	2	2	2
Total CPU Cores	8	16	16	16
Memory	16 GB	32 GB	64 GB	64 GB
Disk Size	240 GB	480 GB	960 GB	1.92 TB
IOPS	200	200	10,000	10,000

Recommended scale based on server configuration:				
Maximum APs	250	2,500	25,000	25,000
Maximum Wireless MUs	2,500	25,000	100,000	100,000
Maximum Managed Devices	100	1,000	10,000	10,000
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

Operating System Requirements

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.

	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 vSphere (client only)™
Hyper-V (Extreme Management Center Virtual Engine)	Hyper-V Server 2012 R2 Hyper-V Server 2016

New Features included in Extreme Management Center 8.0.5

Some of the features included in this version of Extreme Management Center include:

Installation/Upgrade

- Installation Improvement

Installation Improvement

When upgrading the Extreme Management Center engine, the upgrade log (`netsight_appliance_upgrade.log` in the `<install directory>/upgrade/logs directory`) is appended with the upgrade date in YYYYMMDD format, allowing you to retain a log for all engine upgrades.

Engines

- Ability to Configure Password Requirements for Engines
- Syslog Enhancement
- Ability to Audit CLI Commands

Ability to Configure Password Requirements for Engines

You can now configure a minimum password complexity requirement for the Extreme Access Control engine, the Extreme Application Analytics engine, and the Extreme Management Center server.

Syslog Enhancement

Commands entered via TCP are now saved in the syslog.

Systems on which the Ubuntu operating system are installed also record commands entered via UDP.

Ability to Audit CLI Commands

You can now save the commands entered via the CLI on the server, the Extreme Access Control engine, and the Extreme Application Analytics engine to the syslog for auditing purposes.

Extreme Management Center

- Enhancements to Extreme Management Center Maps
- Ability to Configure Login Message
- Improvement to Device Management
- Enhancements to Extreme Management Center Scripts
- Added Support for Additional Device Types
- DeviceView Enhancements
- Enhancements to Inventory Dashboard
- Database Backup Enhancements
- Enhancement to **Devices** Tab Navigation
- Ability to Export Device Details
- Ability to Automatically Disable Alarms

- ZTP+ Enhancements
- Ability to Update Certificates via Extreme Management Center
- Additional VLAN Configuration Available in the Network Tab
- Automatic Scripting Now Available for Devices Added to Sites
- Ability to Open Device Terminal Session via Extreme Management Center
- Enhancement to Map Links
- Enhancements to FlexViews
- Enhancement to Device Status
- Improvement to Device Statistics Collection
- Venue Report URL Change

Enhancements to Extreme Management Center Maps

You can now import Ekahau map files with a file type of .ESX as an Extreme Management Center map.

Additionally, when importing a map in Extreme Management Center, you can now overwrite an existing map.

Ability to Configure Login Message

Extreme Management Center now allows you to configure a message that displays to all users upon login.

Improvement to Device Management

The Asset Tag custom field is now available in Extreme Management Center, which allows you to search, filter, sort, and report based on the field value.

Enhancements to Extreme Management Center Scripts

The Scripts tab in Extreme Management Center now supports multi-vendor CLI prompt detection and includes a script to allow for configuring NFS mounts on the Extreme Management Center server.

Additionally, in Extreme Management Center, you can now run Machine to Machine Interface (MMI) scripts.

Added Support for Additional Device Types

Extreme Management Center now supports the following device types:

- X690-48T
- X690-48X
- C5215
- AP3915e-FCC
- AP3915i-FCC
- AP3915e-ROW
- AP3915i-ROW
- AP3917e-FCC
- AP3917i-FCC
- AP3917e-ROW
- AP3917i-ROW
- BOSS and VOSS devices
- Virtual wireless controller
- WiNG controllers and APs

DeviceView Enhancements

You can now open a DeviceView for devices on which the VOSS operating system is installed.

Additionally, you can now view syslog and trap events for a device in the on the **Device Logs** tab of a DeviceView and the temperature (in degrees Fahrenheit) on the **Device and Module Information** tab.

Enhancements to Inventory Dashboard

Firmware and Archive pie charts are now available in the Inventory Dashboard in the **Network** > Dashboard tab, which display the percentage devices with a firmware image and the percentage of archived devices, archived devices with changed configurations, and devices not archived, respectively.

Database Backup Enhancements

By default, version 8.0.5 of Extreme Management Center creates a binary database backup, which provides a more efficient method of backing up the database and uses less resources. The backup and restore processes function identically to previous versions of Extreme Management Center (via the **Administration** > **Backup/Restore** tab).

Enhancements to Devices Tab Navigation

The **Network** > Devices tab now contains a left-panel drop-down menu that allows you to filter for devices by specific criteria or select your sites.

Selecting an item in the drop-down menu filters the left-panel to display the devices or sites that apply to your selection.

Ability to Export Device Details

You can now export device details on the **Network** > **Device** tab as a CSV file on an ad hoc or scheduled basis.

Ability to Automatically Disable Alarms

You can now create a scheduled task that automatically disables alarms in Extreme Management Center for an amount of time you define.

ZTP+ Enhancements

In Extreme Management Center version 8.0.5, ZTP+ can automatically configure your Extreme Access Control engines. ZTP+ also now allows you to update your devices on an ongoing basis.

Additionally, ZTP+ now allows you to configure the following on your devices:

- LACP (Link Aggregation Control Protocol)
- PoE (Power over Ethernet)
- dot1x port authentication

- MAC address authentication
- Device and port statistics collection

For information about how to configure a ZTP+ enabled device, see ZTP+ Device Configuration in Extreme Management Center.

Ability to Update Certificates via Extreme Management Center

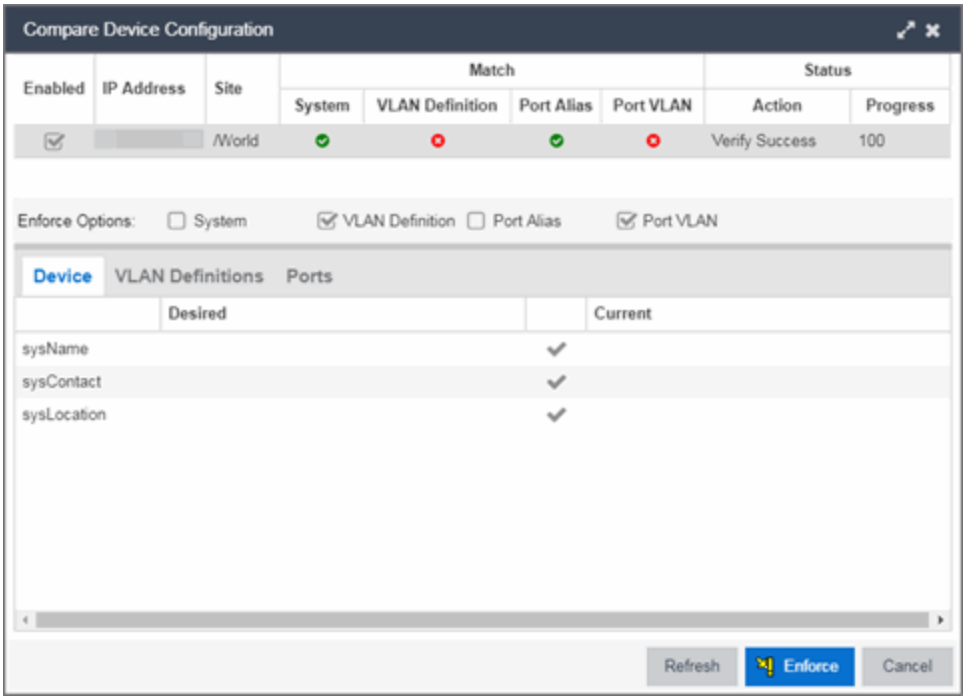
Via the **Administration** > Certificates tab, you can update the Extreme Management Center server certificate and your Extreme Access Control engine certificate.

Additional VLAN Configuration Available in the Network Tab

You can now view and compare device configurations using the **Compare Device Configuration** window. From this window you can edit basic information about the device, the device annotation, configure actions for the device, add or remove ports for the device, and configure VLANs for the device.

NOTE: This functionality is still in development and improvements are ongoing.

To access this window, click **Enforce Preview** in the Edit Device window.



The top of the window displays a list of the devices you selected to verify. Select a device in the table at the top of the window to display the configuration for that device in the bottom of the window. Devices on which the current configuration matches the desired configuration display a check icon (), while devices on which differences are detected display a red x (). The System column indicates the whether the information in the Device section matches, the Port Alias column indicates whether the information in the Ports section matches, and the VLAN Definition indicates whether the information in the VLAN Definitions section matches.

In each section, the configurations are separated into two columns:

- The Current column shows the configuration currently on the device.
- The Desired column shows the configuration you are saving to the device on the next enforce.

A check mark between the columns () indicates the Current configuration matches the Desired configuration.

A left arrow icon () indicates the configurations do not match. Clicking it copies the Current configuration to the Desired configuration so no configuration change is made when enforcing the device.

The Device section of the window displays any changes to basic information about the device.

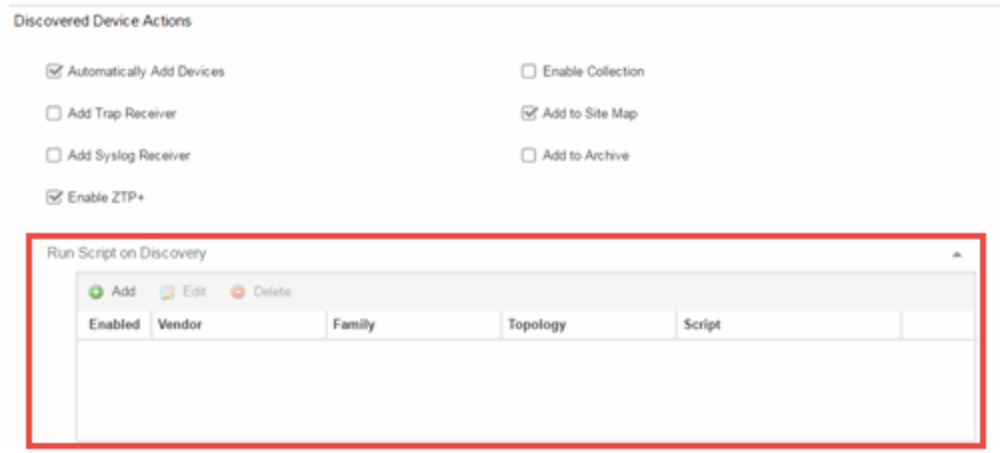
The Ports section of the displays any changes to the configuration of ports on the device.

The VLAN Definitions table displays the VLANs defined for the device selected at the top of the window.

Automatic Scripting Now Available for Devices Added to Sites

You can now automatically run a script you configure on devices you add to a site. Via the **Network** > **Devices** > **Site** tab, you can select a script created on the **Administration** > **Scripting** tab to run when a device is added to a site.

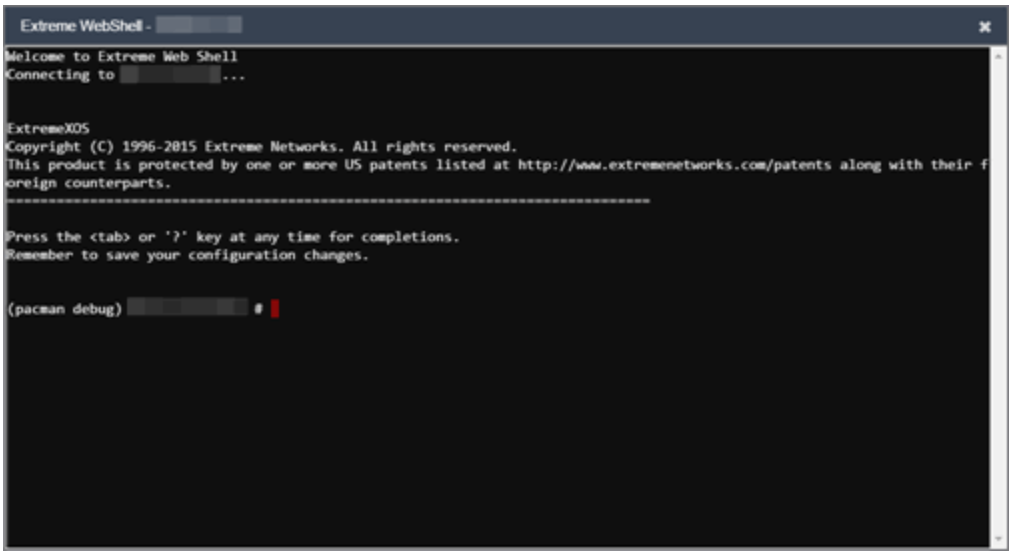
On the **Site** tab, use the **Run Script on Discovery** field in the Discovered Device Actions section of the window to select the script you want to run on devices added to the site.



Ability to Open Device Terminal Session via Extreme Management Center

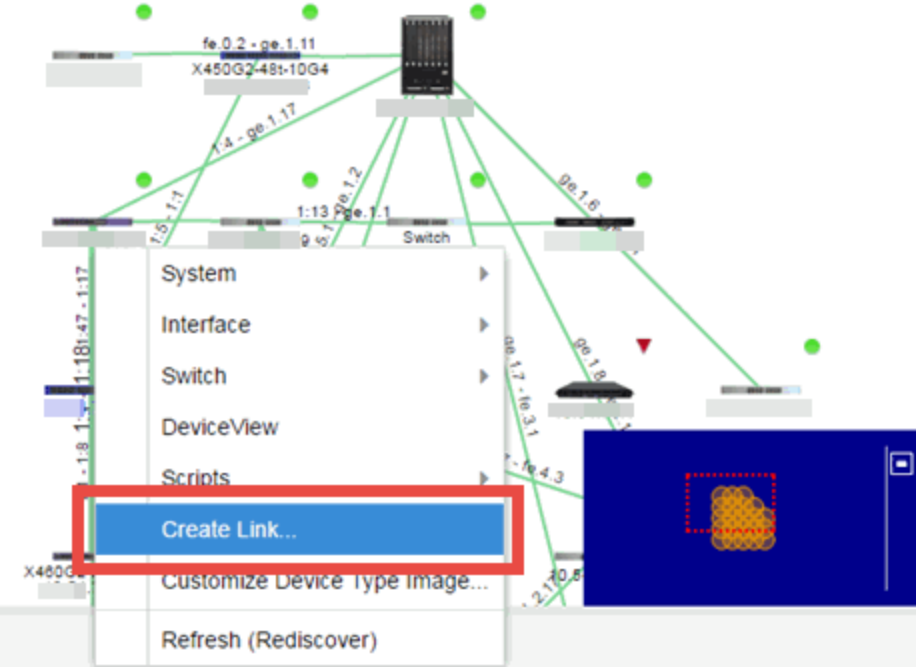
In Extreme Management Center version 8.0.5, you can open a device terminal session on the **Network** > **Devices** tab by right-clicking the device and selecting **Device** > **Open Device Terminal**.

The Extreme WebShell window opens, providing terminal console access to the device.

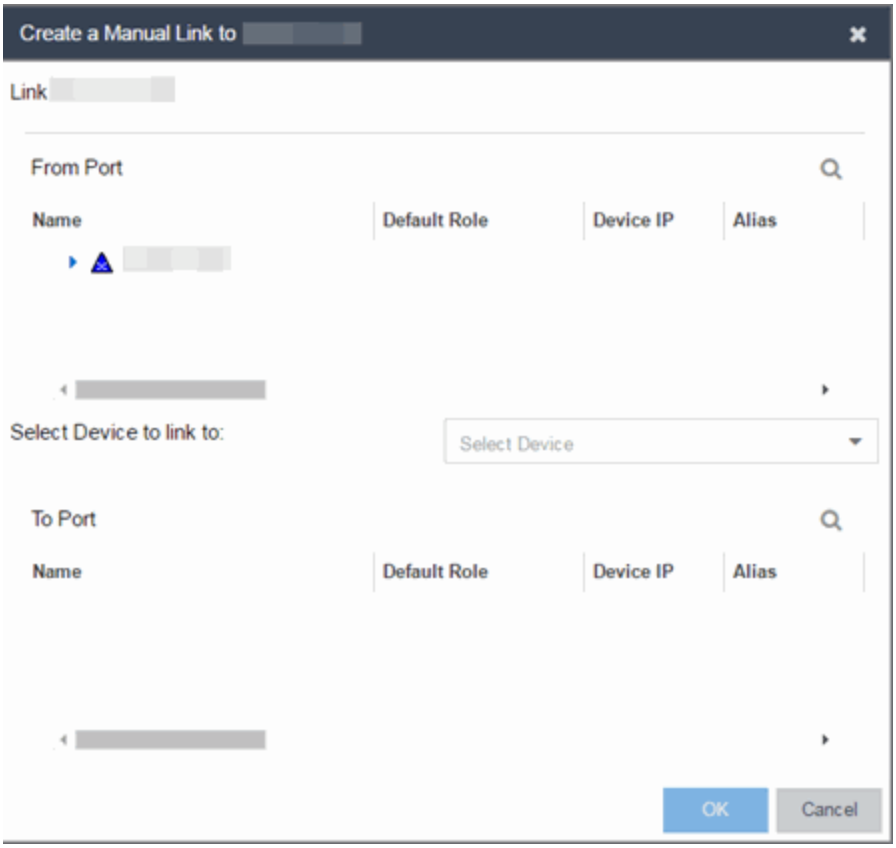


Enhancement to Map Links

You can now create manual links between devices in maps. To manually add a link between devices in a map, right click one of the devices and select **Create Link** from the menu.



The **Create a Manual Link** window displays, from which you can configure the link.



Enhancements to FlexViews

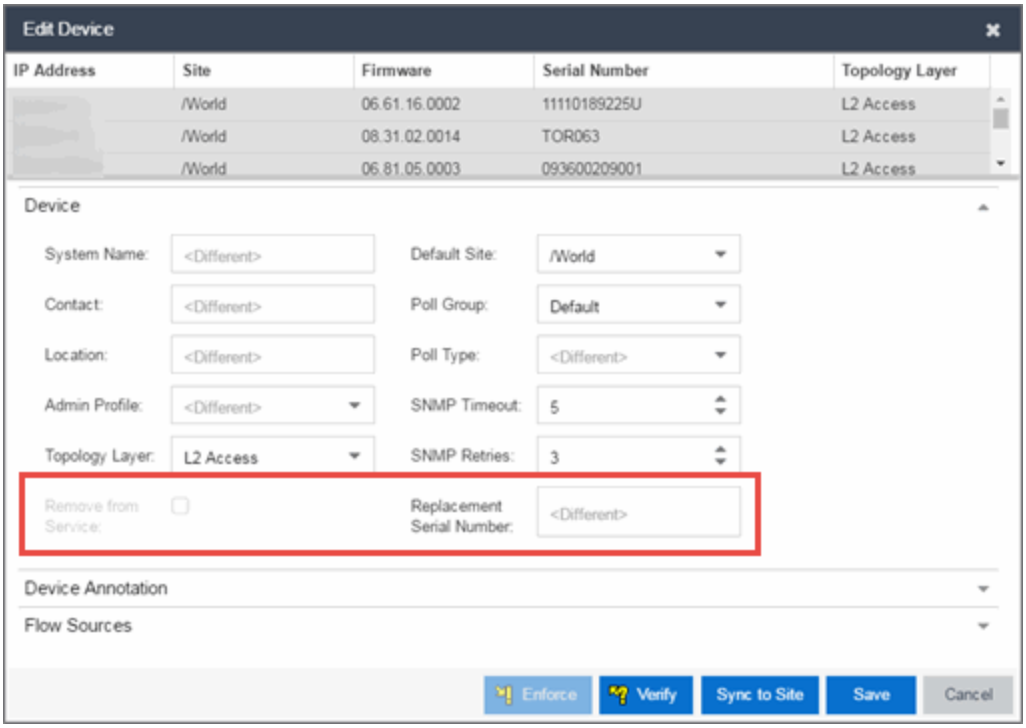
In previous versions of Extreme Management Center, you were limited to opening 10 FlexViews at one time. In version 8.0.5, there is no limit to the number of FlexViews you can open. Additionally, Extreme Management Center now displays FlexViews as they are loading, instead of requiring all information is available before presenting the data.

You can now also schedule FlexViews and FlexReports to run on a scheduled basis.

Enhancement to Device Status

In Extreme Management Center 8.0.5, you can indicate when a device is no longer in service via the Edit Device window (**Network** > Devices tab). When **Remove from Service** is selected, the device is not polled and alarms are not triggered for the device.

Additionally, you can indicate the serial number of a replacement device. When entered, Extreme Management Center restores the most recent archive of the device removed from service.



Improvement to Device Statistics Collection

Extreme Management Center now allows you to simultaneously enable or disable device statistic collection for devices in multiple device families.

Venue Report URL Change

Due to the infrastructure improvements included in version 8.0.5 of Extreme Management Center, the web site to access the Venue Report is changed to `https://<Extreme Management CenterServerIP>:<port>/connect/VenueReport`.

ExtremeControl

- Ability to Configure End-System Threshold Alarm
- Enhancements to Guest Registration
- Ability to Configure RADIUS Attributes
- RADIUS Response Attribute Enhancement
- Added RADIUS Support for WiNG Controllers
- Improvement to Alarms
- Added DHCP Fingerprint for VoIP phone

Ability to Configure End-System Threshold Alarm

You can now configure a threshold alarm in Extreme Management Center to alert you when the number of end-systems accessing your network is above a specified percentage of your license capacity.

Enhancements to Guest Registration

The Guest Registration portal now allows users to log into their Google or Microsoft account to complete the guest registration process.

Ability to Configure RADIUS Attributes

You can now configure individual switches to send RADIUS Attributes via the Access Control tab.

RADIUS Response Attribute Enhancement

Policy mappings now support three additional RADIUS response attributes. These attributes allow you to provide a complete ACL for a different third-party vendor.

Added RADIUS Support for WiNG Controllers

WiNG controller RADIUS attributes are now supported by ExtremeControl.

Improvement to Alarms

The Extreme Access Control engine now alerts you via an alarm when the JMS service between the Extreme Access Control engine and the Extreme Management Center server is unable to connect.

Added DHCP Fingerprint for VoIP Phone

Added an additional DHCP Fingerprint in Extreme Management Center version 8.0.5 to identify Unify OpenStage WL VoIP phones.

ExtremeAnalytics

- Response Time Dashboard Enhancement
- Ability to Assign a Role to a Location
- Enhancements to Application Analytics Fingerprints
- Dynamic Thresholds Available in Application Analytics Dashboards

Response Time Dashboard Enhancement

The Flow Grid of the Response Time Dashboard now filters out flows with a response time of zero.

Ability to Assign a Role to a Location

You can now configure Application Analytics locations with a role, which allow you to assign a function to the location.

Enhancements to Application Analytics Fingerprints

Application Analytics can now use fingerprints created via the **Policy** tab.

Additionally, you can now enforce Application Analytics fingerprints on Extreme wireless controllers.

Dynamic Thresholds Available in Application Analytics Dashboards

You can now configure the Expected Response Time bar graph in the Network Service and Tracked Application dashboards to monitor historical response times for network services and tracked applications to dynamically establish an "expected response time" threshold. When this functionality is enabled, Extreme Management Center alerts you when a response time occurs above the expected range.

ExtremeConnect

- ExtremeConnect Enhancements

ExtremeConnect Enhancements

ExtremeConnect, available via the Connect tab in Extreme Management Center, now includes a Services API tab, which allows you to perform a client/server application, known as a web service.

The available web services are organized based on the type of function they perform:

- Inventory Web Services — Perform Inventory Manager functions (e.g. backups or retrieving device properties).
- NAC Configuration Web Services — Perform ExtremeControl configuration functions.
- NAC End-System Web Services — Retrieve and modify ExtremeControl services, with a focus on accessing end-systems.
- NAC Web Services — Retrieve and modify general ExtremeControl services.
- NetSight Device Web Services — Retrieve and modify the devices in the Extreme Management Center database.
- Policy Web Services — Perform Policy Manager functions.
- Purview Web Services — Retrieve and modify ExtremeAnalytics data and configuration.
- Reporting Web Services — Retrieve and modify the Extreme Management Center reporting engine data configuration.

Information Governance Engine

- Ability to Configure Audit Test Chains
- Ability to Evaluate Device Configurations via the Governance Tab

Ability to Configure Audit Test Chains

Audit tests you create via the Governance tab can now be configured as test chains, where one test must complete successfully before a second test runs.

Ability to Evaluate Device Configurations via the Governance Tab

Extreme Management Center now includes the Governance tab, which provides oversight into the configuration of your devices. The tab, available with an additional license from Extreme Networks, allows you to test whether your devices are compliant with industry standards, including PCI and HIPAA. Each industry standard, known as a regime, includes a number of individual audit tests, focused on evaluating a specific device configuration. After a governance audit is performed, the results give your network an overall score and include a score for each device tested. The results also include information to help improve your score in the future.

Policy

- Improvements to Policy Tab Functionality

Improvements to Policy Tab Functionality

You can now copy and paste most elements included in a domain (e.g. Roles, Services, Rules) on the **Policy** tab. Additionally, the **Devices/Port Groups** > **Devices** tab contains a drop-down menu allowing you to filter the devices displayed by specific criteria.

Wireless

- New Wireless Reports

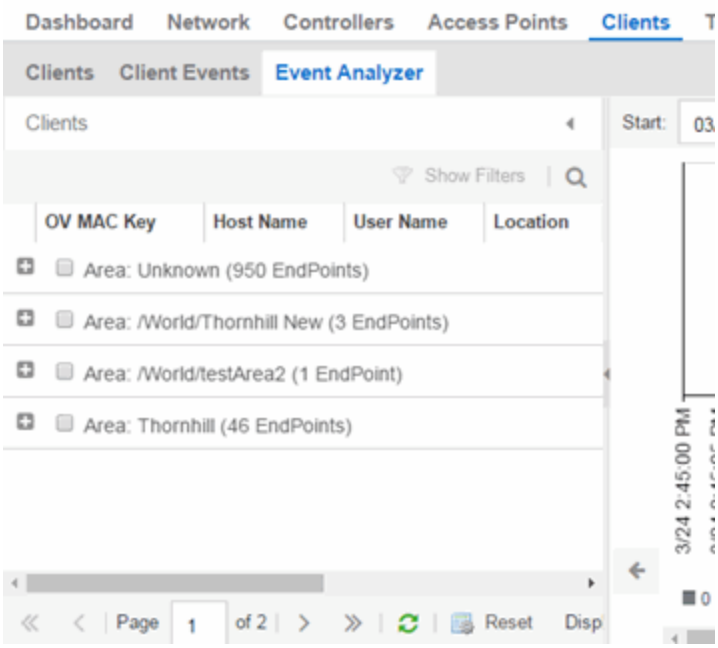
New Wireless Reports

In version 8.0.5, the **Wireless** > **Clients** > **Event Analyzer** tab provides information about events caused by wireless end-points connecting to your network.

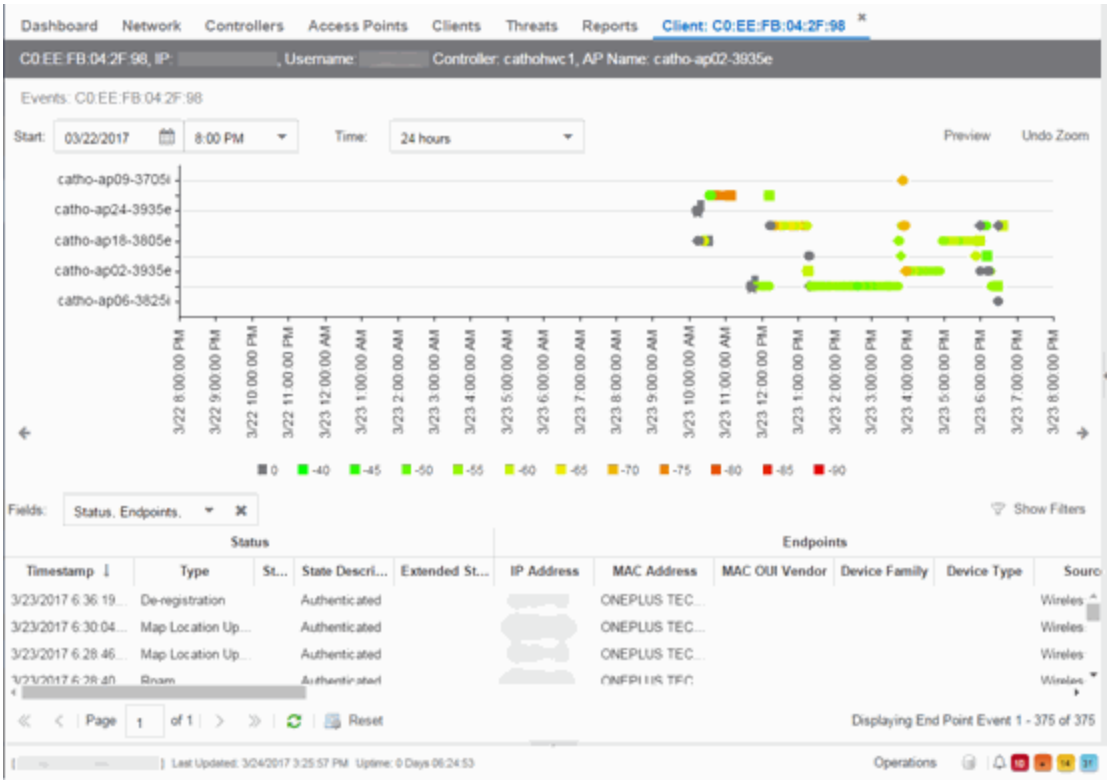
You can access the tab in a number of ways and the information presented changes depending on the method you use:

- Navigating via **Wireless** > **Clients** > **Event Analyzer** shows all end-points.
- Clicking a Location on the **Wireless** > **Clients** tab opens the Event Analyzer for the end-points that occurred for all APs in that Location.
- Clicking a MAC address on the **Wireless** > **Clients** tab opens the Event Analyzer for only that end-point.

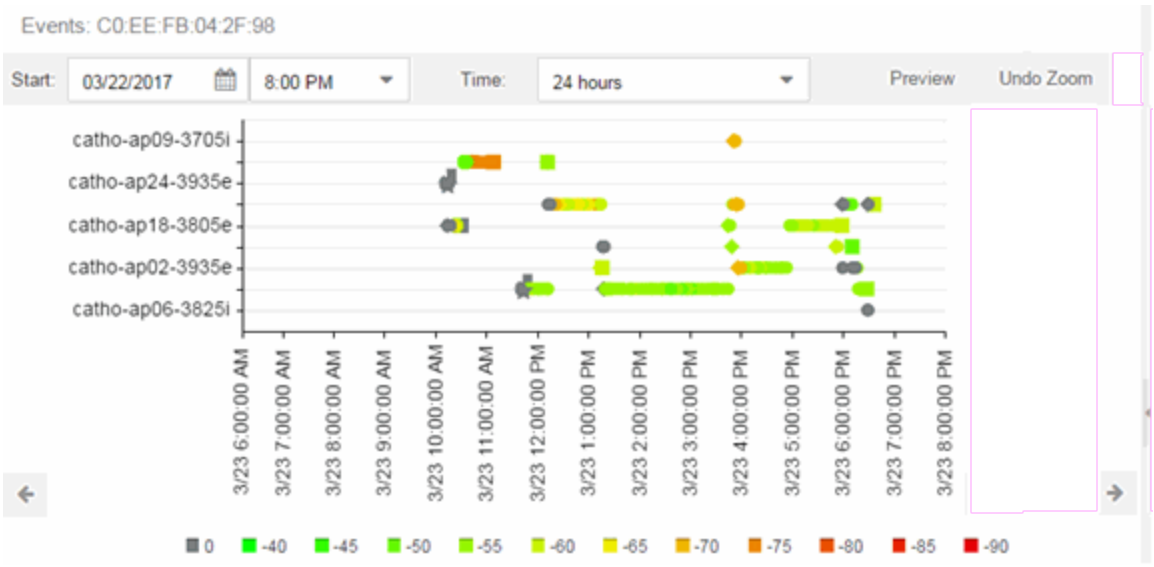
When accessing the tab using the top two methods, a Clients section is available in the left-panel. This section provides you with the ability to display end-point events for specific AP locations.



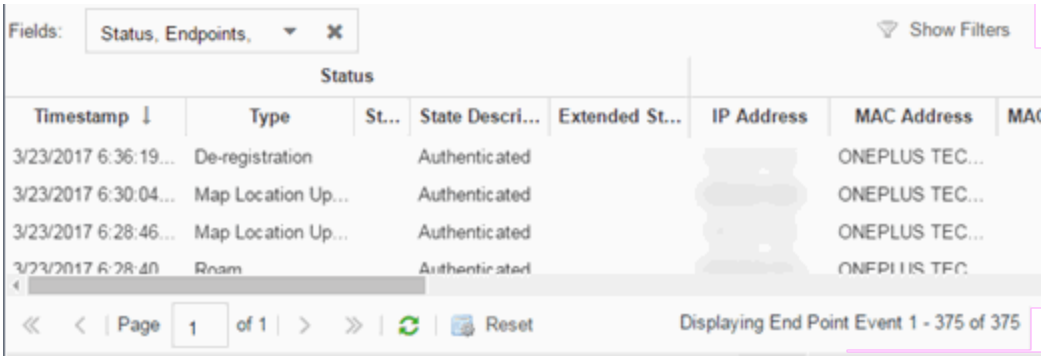
Once you select the appropriate end-points or areas, this section can be collapsed by clicking the left arrow.



The RSS graph at the top of the tab shows the signal strength (in dBm) between the end-point and each of the APs to which it connected. The shape of the end-point event indicators in the graph indicate the type of event.



The Events table at the bottom of the tab contains details about the end-point events for your network, or for the wireless location or MAC address you selected.



Use the **Fields** drop-down menu to select groups of columns to display in the table:

- Select **Status** to display the following columns in the table:
  - Timestamp
  - Type
  - State
  - State Description
  - Extended State
- Select **Endpoints** to display the following columns in the table:
  - IP Address
  - OV MAC Key
  - MAC Address
  - MAC OUI Vendor
  - Host Name
  - Device Family
  - Device Type
  - Source
- Select **User Access** to display the following columns in the table:
  - User Name
  - Policy
  - Authorization

    - Profile
    - Reason
    - Auth Type
    - Registration Type
    - RADIUS Server IP
- Select **Location** to display the following columns in the table:
    - Switch Port
    - Switch Port Index
    - Switch Location
    - AP Name
    - AP Serial #
    - BSSID
    - SSID
    - Protocol
    - Location Type
    - Location
    - Location Details
    - Area Type
    - Area
    - Access Control Engine/Source IP
- Select **Metrics** to display the following columns in the table:
    - RSS
    - SNR
- Select **Threat/Risk** to display the following columns in the table:
    - Categories
    - Start Time
- Select **Network Service** to display the following columns in the table:
    - Switch IP
    - Controller IP

11/2017
P/N: 9035078-09
Subject to Change Without Notice

Extreme Management Center® Feature Migration

This document provides a preliminary time frame for the migration of legacy java application functionality into Extreme Management Center. The information in this table is subject to change.

Functionality	Removed	8.0.4	8.1
ACL Manager	X		
Automated Security Manager	X		
Basic Policy (Console)	X		
Inventory Manager	X		
Policy Control Console	X		
RMON (Device Manager)	X		
RoamAbout Wireless	X		
EAPS provisioning (beta feature)	X		
Asset tag display and editing local to EMC server		X	
On demand capacity planning reports by site		X	
Workflow improvements for device inventory manager			X
Asset tag setting on devices that support it			X
Firmware management support in sites			X
Archive configuration templates creation			X
Historical collection of capacity planning support for port usage			X
FlexReports for port usage historical capacity planning			X