Extreme Management Center Customer Release Notes

Version 8.0.2.42
June, 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.

Management Center is distinguished by its web-based, unified control interface. Graphical and exceptionally easy-to-use, 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.

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

The Management Center Release Notes provide information on the new features and enhancements included in version 8.0, 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 > Extreme Management Center (NetSight) Suite.

Software Enhancements

Enhancements in Extreme Management Center 8.0

The new features and enhancements included in Extreme Management Center 8.0 are now located in the [What's New in Extreme Management Center Version 8.0](#) topic.

Deprecated Features

The following legacy java applications are deprecated in version 8.0:

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

The following Management Center features are deprecated in version 8.0:

- Isaac
- Monk
- Security Advisor

Known Issues Addressed

This section presents the known issues that were 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.	-------

Application Analytics Issues Addressed	**ID**
The Application Analytics engine could not be successfully upgraded if the `rsyslog.conf` file was modified.	-------

Extreme Access Control Issues Addressed	**ID**
User-defined SNMP credentials were removed from Access Control engines when upgrading to version 8.0.1.33.	1327535

This section presents the known issues that were 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

Extreme Access Control 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 that were 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 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 Management Center.	1279665
Extreme Access Control 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, and 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 – 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:

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

- The following vulnerabilities were addressed in the Extreme Access Control and 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 only runs on a 64-bit engine image. Any [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. Please contact Extreme Networks Support with any questions.

Extreme Management Center Server and Client OS Requirements

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

IMPORTANT: Only 64-bit operating systems are officially supported on the Management Center server. Any 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 Management Center client only)	El Capitan Sierra
VMware® (Management Center Virtual Engine	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server vSphere (client only)™
Hyper-V (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 Management Center server and Management Center client machines.

Extreme Management Center Server

	Small	Medium	Enterprise	Large Enterprise
Total CPUs	1	2	2	2

	Small	Medium	Enterprise	Large Enterprise
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:

	Small	Medium	Enterprise	Large Enterprise
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
Access Control End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
Application Analytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

Extreme Management Center Client

	Requirements
CPU Speed	2.4 GHz Processor
Memory	2 GB
Disk Size	100 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 Management Center, Access Control, and Application Analytics virtual engines must be deployed on a VMWare or Hyper-V server with a disk format of VHDX.

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

- The Hyper-V Management Center virtual engines are packaged in the .ZIP file format.

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

Management Center Virtual Engine Requirements

	Small	Medium	Enterprise	Large Enterprise
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:

	Small	Medium	Enterprise	Large Enterprise
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
Access Control End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
Application Analytics	No	Yes	Yes	Yes
MU Events	No	Yes	Yes	Yes

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:

	Small	Medium	Enterprise
Access Control 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 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.

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

	Small	Medium	Enterprise
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 Application Analytics virtual engine installation require 16 CPU cores. This is only available by purchasing a permanent license. To use the 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 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 Access Control 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.

For the Mac operating system, NAC Manager supports the testing of the following antivirus software:

ClamX AV 2.2.2	Sophos 4.9
ClamXAV 2.7.5	Sophos 7.1.10
McAfee 8.6	Sophos 7.2
McAfee 9.0	Symantec AV 10
McAfee 9.5	Symantec Endpoint 11
McAfee Internet Security for MAC	Symantec Endpoint 12 and 12.1
Norton 11	Titanium Internet Security for MAC
Norton Antivirus for MAC	

Extreme Access Control 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 Access Control.

	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:

Message from webpage

This browser does not support WebKit (http://www.webkit.org) or Sencha Touch, which is required to display the mobile captive portal. Please view this in a browser such as Chrome (http://www.google.com/chrome) or Safari (http://www.apple.com/safari).

OK

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 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 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 Access Control:

- Clickatell
- Mobile Pronto

Other SMS Gateways that support the SMTP API should be able to interoperate with 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 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

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 Management Center, redeem your Entitlement ID for a license key. Refer to the instructions included with the Entitlement sent to you.

For complete installation instructions, refer to the installation documentation located on the 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 Management Center version 8.0 on a system on which a Windows Server operating system is installed. Restarting Windows corrects this issue.

When starting the Management Center server after installing version 8.0.2 on a non-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 Application Analytics Engines Version 8.0.2

After installing a version 8.0.2 .ISO image on a physical Application Analytics engine, open the `/etc/sysctl.conf` file and locate the `vm.nr_hugepages` row. Remove any number following a decimal point to change the value to a whole number.

For example, if the `sysctl.conf` file displays `vm.nr_hugepages = 2667.67`, change the value to `vm.nr_hugepages = 2667`.

Save the file and enter `sysctl -p` in the command line to update the engine with the new configuration.

Running the engine without editing this value results in performance issues.

Custom FlexViews

When re-installing 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.

Evaluation License

If you have requested a Management Center evaluation license, you receive 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 supports upgrades from Management Center version 7.1 only. If you are upgrading from a NetSight/Management Center version prior to 7.1, you must perform an intermediate upgrade. For example, if you are upgrading from Management Center 7.0, you must first upgrade to Management Center 7.1, and then upgrade to Management Center 8.0.

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 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 8.0.2 after upgrading from version 6.1 to 7.1.2, the upgrade does not complete successfully. To successfully upgrade the engine to version 8.0.2 after upgrading from version 6.1 to 7.1.2, enter `dpkg --purge postgresql*` in the command line, then upgrade the Application Analytics engine to version 8.0.2.

Important Upgrade Considerations

- When upgrading the Management Center server, Application Analytics engine, or Access Control engine to version 8.0, 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.

- If your network is using Application Analytics engines, you must first perform the Management Center upgrade to version 8.0 and then add the 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 Management Center:

  - The OneFabric connect module is disabled after upgrading and requires a new version in order to operate with Management Center 8.0. You must install an updated module that supports Management Center 8.0. Contact your account team for information on obtaining this update.

  - You must install a Management Center Advanced (NMS-ADV) license with 8.0 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 Management Center Advanced (NMS-ADV) license. Contact your account team for information on obtaining this license.

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

Upgrade Considerations for NAC Manager 8.0

General Upgrade Information

When upgrading to Management Center NAC Manager 8.0, you are required to upgrade your Access Control engine version to 7.1.2 or 8.0. Additionally, both Management Center NAC Manager and the Access Control engine must be at version 8.0 in order to take advantage of the new Access Control 8.0 features.

NOTE: Access Control 8.0 is not supported on the 2S Series and 7S Series Access Control Controllers.

You can download the latest Access Control engine version at the 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* document (available on the Management Center (NetSight) Documentation web page > Manuals & Release Notes > NetSight 8.0 > Network Access Control [NAC]) for important information.

In addition, if your Access Control solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 8.0 if you upgrade to the Access Control engine 8.0. Version 8.0 of the assessment agent adapter requires an operating system with a 64-bit architecture.

Upgrade Considerations for Wireless Manager 8.0

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

Configuration Considerations

Firewall Considerations

- The Extreme Management Center Server runs on a set of non-standard ports. These TCP ports (4530-4533) must be accessible through firewalls for clients to connect to the server.
  4530/4531: JNP (JNDI)
  4532: JRMP (RMI)
  4533: UIL (JMS)

- Port 8080 (Default HTTP traffic) must be accessible through firewalls for users to install and launch Management Center client applications.

- Port 8443 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Management Center Server Administration web pages, Management Center, and Extreme Access Control Dashboard.

- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the Access Control Engine Administration web pages.

- The following ports must be accessible through firewalls for the Management Center Server and an Access Control engine to communicate:
  Required Ports (all bi-directionally)
  TCP: 4530-4533, 4589, 8080, 8443, 8444
  UDP: 161, 162

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

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

- The following ports must be accessible through firewalls for the Management Center Server and Wireless Controllers to communicate:
  SSH: 22

SNMP: 161, 162
Langley: 20506

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

- The following ports must be accessible (bi-directionally) through firewalls for the Management Center Server and an Application Analytics engine to communicate:
TCP: Ports 4530-4533, 4589, 8080, 8443
UDP: Ports 161, 162
To Application Analytics engine:
UDP: Port 2055 (NetFlow)
TCP: 22, 8443

  For GRE Tunnels to the Application Analytics engine IP Protocol 47

- Port 2055 must be accessible through firewalls for the 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

This document provides an overview of the new features in Management Center version 8.0. 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 of Management Center, the hardware and operating system requirements are also changed. Refer to the below table and list for the recommended 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:

	Small	Medium	Large	Extra Large
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
Access Control End-Systems	N/A	50,000	200,000	200,000
Statistics Retention (Days)	90	180	180	360
Application Analytics	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 Management Center server and remote 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 Management Center client only)	El Capitan Sierra
VMware® (Management Center Virtual Engine	VMware ESXi™ 6.0 server VMware ESXi™ 6.5 server vSphere (client only)™
Hyper-V (Management Center Virtual Engine)	Hyper-V Server 2012 R2 Hyper-V Server 2016

New Features included in Management Center 8.0

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

- Ability to Evaluate Device Configurations via the **Governance** Tab
- Dynamic Thresholds Available in Application Analytics Dashboards
- Extreme Connect Enhancements
- Database Backup Enhancements
- ZTP+ Enhancements
- Enhancement to **Devices** Tab Navigation
- Additional VLAN Configuration Available in the **Network** Tab
- Automatic Scripting Now Available for Devices Added to Sites
- Ability to Open Device Terminal Session via Management Center
- Enhancement to Map Links
- Added DHCP Fingerprint for VoIP phone
- Enhancement to Device Status
- New Wireless Reports

- Improvement to Device Statistics Collection
- Enhancements to FlexViews
- Venue Report URL Change

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.

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, Management Center alerts you when a response time occurs above the expected range.

Extreme Connect Enhancements

Extreme Connect, available via the Connect tab in 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 Access Control configuration functions.

- [NAC End-System Web Services](#) — Retrieve and modify Access Control services, with a focus on accessing end-systems.
- [NAC Web Services](#) — Retrieve and modify general Access Control services.
- [NetSight Device Web Services](#) — Retrieve and modify the devices in the Management Center database.
- [Policy Web Services](#) — Perform Policy Manager functions.
- [Purview Web Services](#) — Retrieve and modify Application Analytics data and configuration.
- [Reporting Web Services](#) — Retrieve and modify the Management Center reporting engine data configuration.

Database Backup Enhancements

By default, version 8.0 of 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 Management Center (via the **Administration** > **Backup/Restore** tab).

ZTP+ Enhancements

In Management Center version 8.0, ZTP+ can automatically configure your 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](#).

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.

by IP ▼
by Chassis
by Contact
by Device Type
by IP
by Location
Sites
User Device Groups
Wireless Controllers
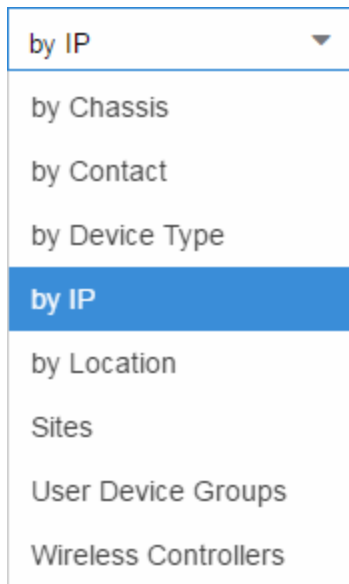
Selecting an item in the drop-down menu filters the left-panel to display the devices or sites that apply to your selection.

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.
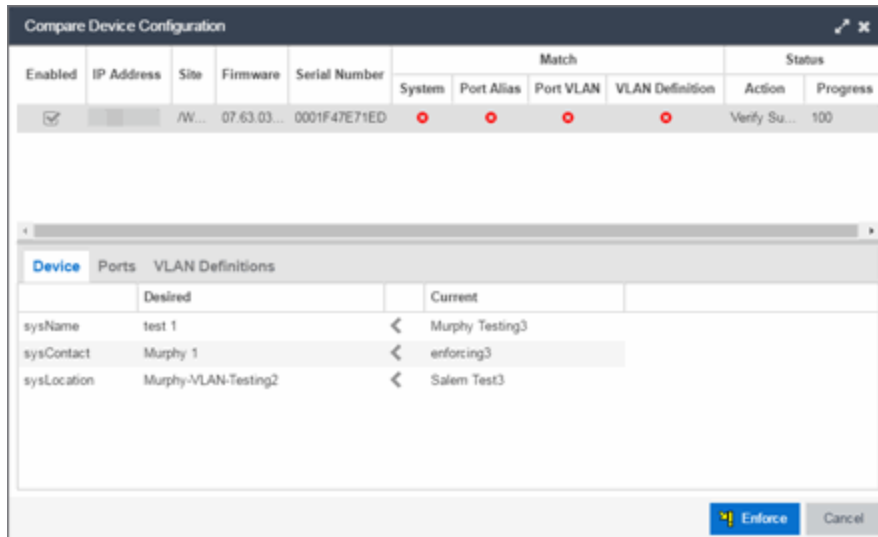
The top of the window displays a list of the devices you selected to verify. Select a device in the table at the top of the window to display the configuration for that device in the bottom of the window. Devices on which the current configuration matches the desired configuration display a check icon (●), 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.
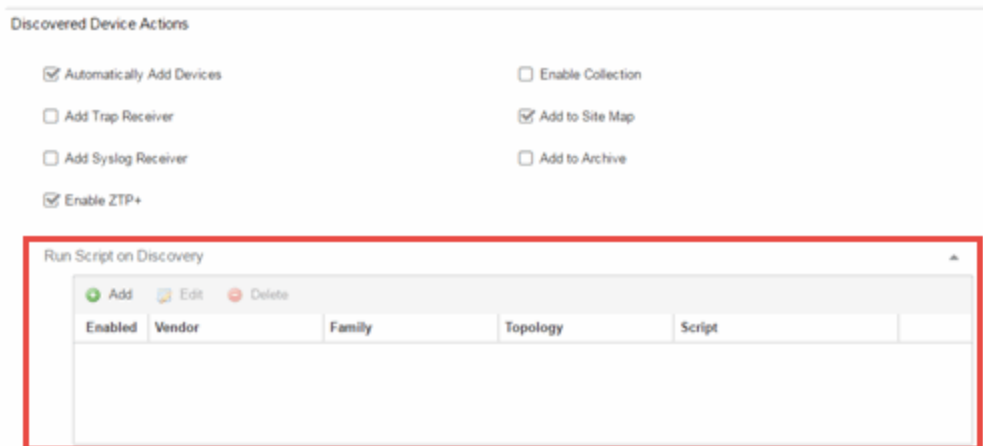
Ability to Open Device Terminal Session via Management Center

In Management Center version 8.0, 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.
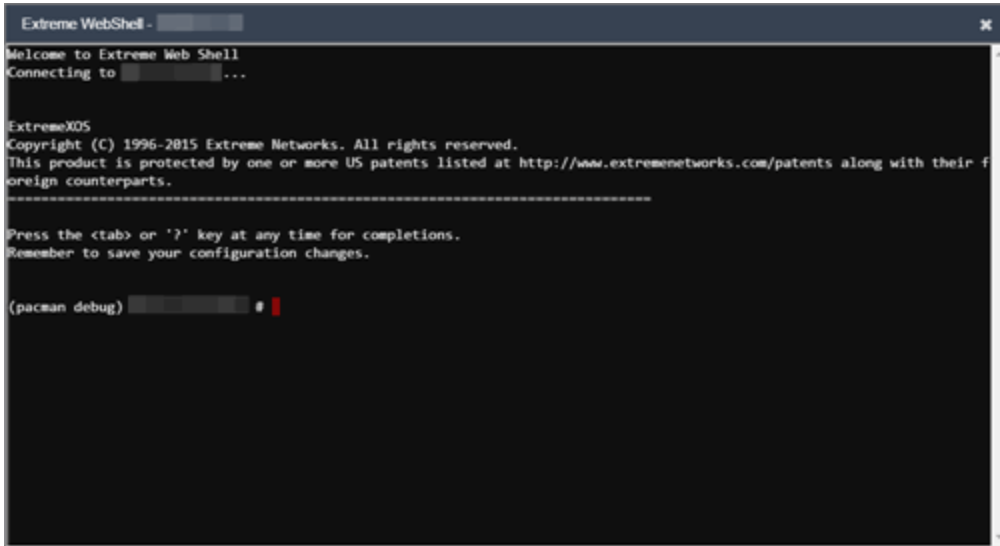
Enhancement to Map Links

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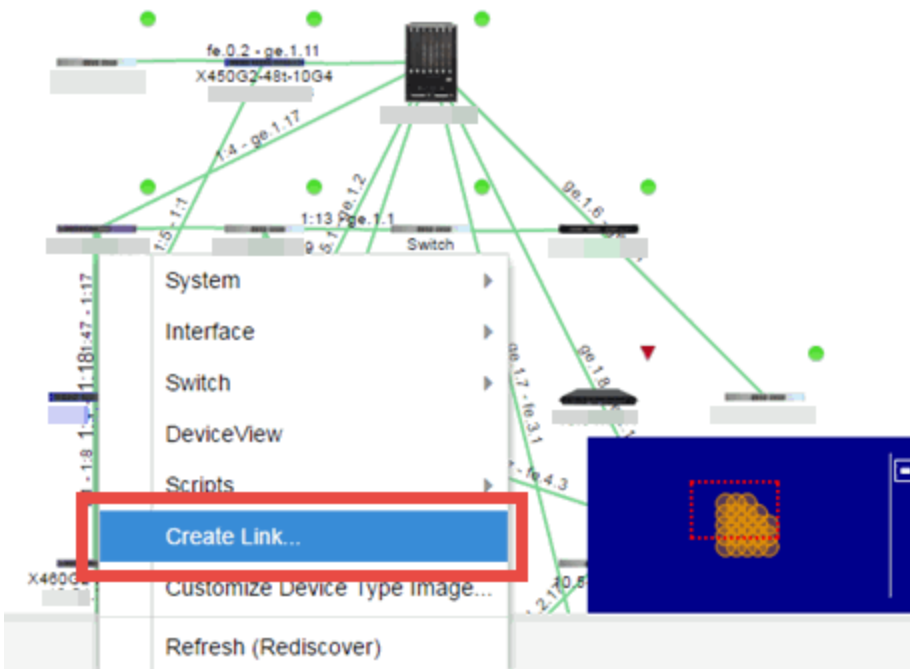
The **Create a Manual Link** window displays, from which you can configure the link.

Added DHCP Fingerprint for VoIP Phone

Added an additional DHCP Fingerprint in Management Center version 8.0 to identify Unify OpenStage WL VoIP phones.

Enhancement to Device Status

In Management Center 8.0, 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, Management Center restores the most recent archive of the device removed from service.

New Wireless Reports

In version 8.0, 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.
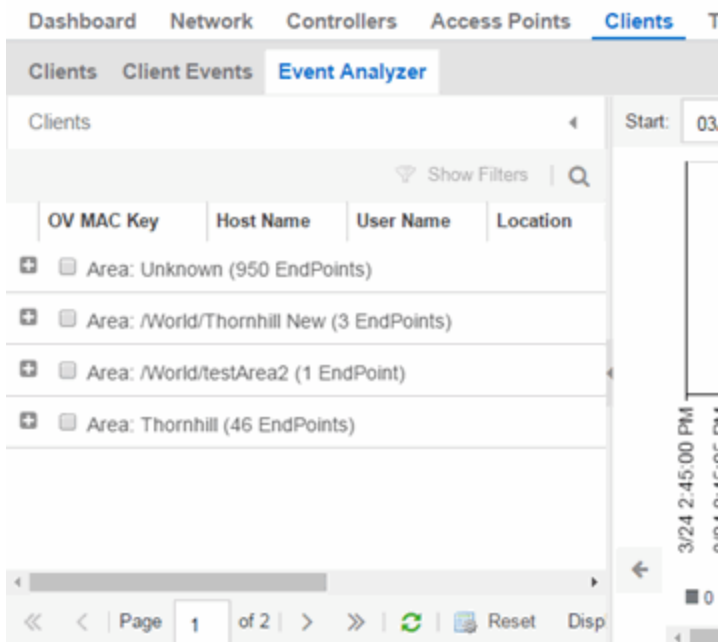
Once you select the appropriate end-points or areas, this section can be collapsed by clicking the left arrow.
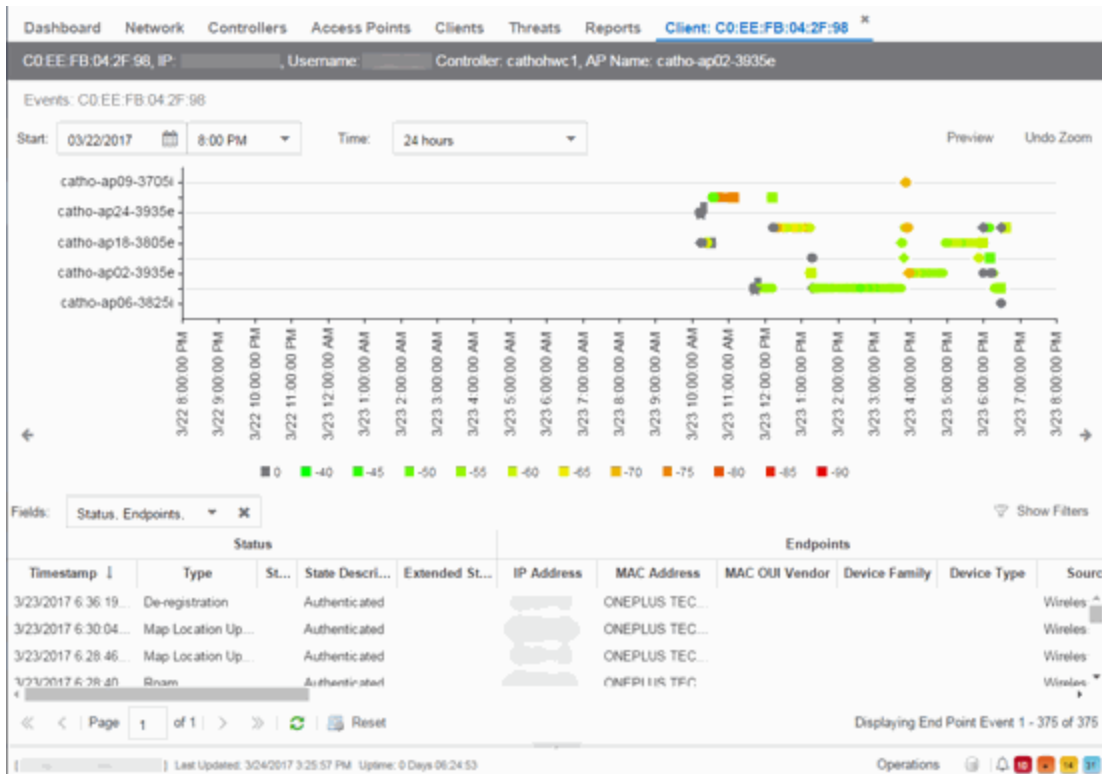
The RSS graph at the top of the tab shows the signal strength (in dBm) between the end-point and each of the APs to which it connected. The shape of the end-point event indicators in the graph indicate the type of event.
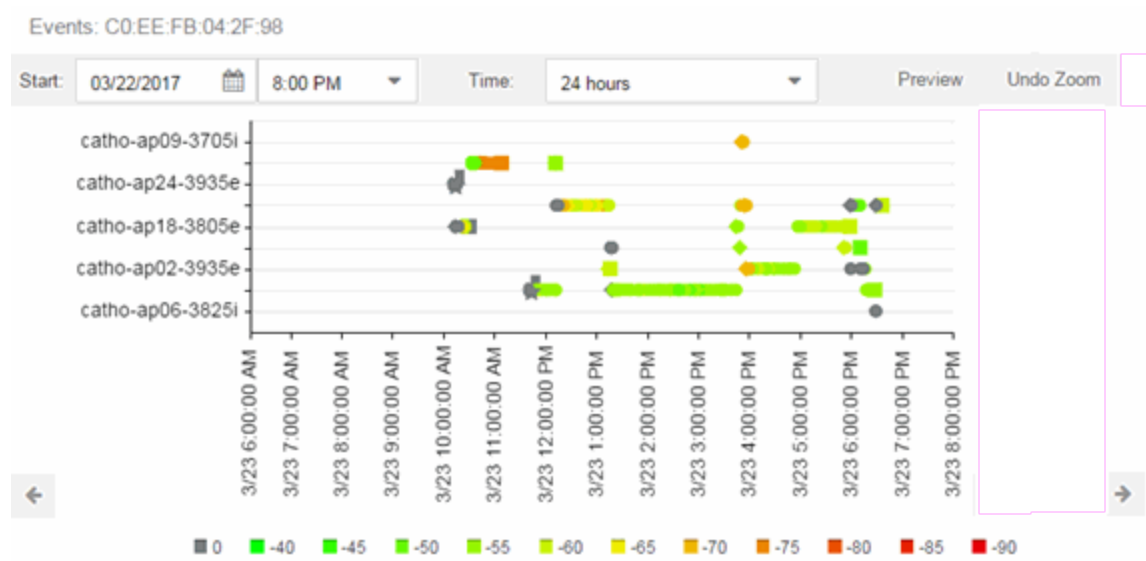
The Events table at the bottom of the tab contains details about the end-point events for your network, or for the wireless location or MAC address you selected.

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 ControlEngine/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

Improvement to Device Statistics Collection

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

Enhancements to FlexViews

In previous versions of Management Center, you were limited to opening 10 FlexViews at one time. In version 8.0, there is no limit to the number of FlexViews you can open. Additionally, Management Center now displays FlexViews as they are loading, instead of requiring all information is available before presenting the data.

Venue Report URL Change

Due to the infrastructure improvements included in version 8.0 of Management Center, the web site to access the Venue Report is changed to
`https://<Management CenterServerIP>:<port>/connect/VenueReport.`

06/2017
P/N: 9035078-03
Subject to Change Without Notice