Extreme Management Center Customer Release Notes

Version 8.0.0.130
April, 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.

Older licensing keys (starting with INCREMENT) are no longer supported as of NetSight 5.0 and later. If you have one of these keys, please contact Extreme Networks Support for license upgrade information.

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 Center8.0

The new features and enhancements included in Extreme Management Center8.0 is now located in the What's New in Extreme Management Center Version 8.0 topic.

Known Issues Addressed

This section presents the known issues that were addressed in Extreme Management Center8.0.0.130:

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.

Instructions on determining your engine OS and upgrade procedures can be found in the *Migrating or Upgrading to a 64-bit Extreme Management Center Engine* document or the *Upgrading to a 64-bit Extreme Access Control Engine* document available on the Management Center (NetSight) (NMS) Documentation web page: http://extranet.extremenetworks.com/downloads. After entering your email address and password, follow this path to the document: Software & Security > Management Center (NetSight) (NMS) > Documentation > Manuals & Release notes > NetSight 8.0 > Network Access Control (NAC) and NetSight Appliances. 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.

- Windows (qualified on the English version of the operating systems)
  - Windows Server® 2012 and 2012 R2
  - Windows Server® 2016
  - Windows® 7
  - Windows® 10
- 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
- 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**	**Large**	**Extra Large**
Operating System	64-bit Desktop • Windows • Ubuntu • Red Hat	64-bit Server • Ubuntu • Red Hat	64-bit Server • Ubuntu • Red Hat	64-bit Ubuntu Server
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

	Small	Medium	Large	Extra Large
IOPS	200	200	1,000	1,000
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
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

- Recommended — Dual-Core 2.4 GHz Processor, 2 GB RAM
- Free Disk Space - 100 MB
  (User's home directory requires 50 MB for file storage)
- Java Runtime Environment (JRE) (Oracle Java only):
  - version 6
  - version 7, update 40 or later
  - version 8
- Supported Web Browsers:
  - Microsoft Edge and Internet Explorer version 11
  - Mozilla Firefox 34 and later
  - Google Chrome 33.0 and later

NOTES: Browsers must have JavaScript enabled in order for the web-based views to function.

While it is not required that cookies be enabled, impaired functionality results if they are not. This includes (but is not limited to) the ability to generate PDFs and persist table configurations such as filters, sorting, and column selections.

Virtual Engine Requirements

VMWare:

The Management Center, Access Control, and Application Analytics virtual engine is packaged in the .OVA file format defined by VMware and must be deployed on either a VMware ESX™ server, or a VMware ESXi™ server with a vSphere™ client.

IMPORTANT: The ESXi free license supports a maximum of 8 CPU cores, while the Application Analytics virtual engine installation requires 12 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.

The following versions of VMware ESX or VMware ESXi servers and vSphere clients are supported: 5.1, 5.5, and 6.0.

Hyper-V:

Hyper-V virtual engines are supported on Windows Server 2012 R2 running Hyper-V Server 2012.

The Management Center, Access Control, and Application Analytics virtual engines support a disk format of VHDX.

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.

The Access Control, Application Analytics, and Management Center virtual engines use the following resources from the server on which they are installed:

- Access Control virtual engine — configured with 12 GB of memory, four CPUs, two network adapters, and 40 GB of thick-provisioned hard drive space.
- Application Analytics virtual engine — configured with 12 GB of memory, 12 CPUs, two network adapters, and 40 GB of thick-provisioned hard drive space. This configuration provides a flow rate capacity of 200K flows per minute (FPM), and can be increased for additional capacity. An additional

1GB RAM is required for every 8 interfaces or GRE tunnels configured on the virtual engine.

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

- Management Center virtual engine:
  - Standard — configured with 8 GB of memory, four CPUs, one network adapter, and 200 GB of thick-provisioned hard drive space.
  - Enterprise — configured with 12 GB of memory, 12 CPUs, one network adapter, and 1 TB of thick-provisioned hard drive space.

Extreme Access Control Agent OS Requirements

These are the supported operating systems for end-systems connecting to the network through an Extreme Networks Access Control deployment that is implementing agent-based assessment.

- Windows Vista
- Windows XP
- Windows 2008
- Windows 2003
- Windows 2000
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Mac OS X — Tiger, Leopard, Snow Leopard, Lion, Mountain Lion, Mavericks, Yosemite, El Capitan, Sierra

The end-system must support the following operating system disk space and memory requirements as provided by Microsoft® and Apple®:

- Windows Install — 80 MB of physical disk space for installation files; 40 MB of available memory (80 MB with Service Agent)
- Mac Install — 10 MB of physical disk space for installation files; 120 MB of real memory

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

Extreme Access Control Supported End-System Browsers

Supported Desktop Browsers

The following browsers are supported for desktop end-systems connecting to the network through Extreme Networks Access Control:

- Microsoft Edge and Internet Explorer version 11
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later
- Safari

Supported Mobile Browsers

The following browsers are supported for mobile end-systems connecting to the network through the Mobile Captive Portal of Extreme Networks Access Control:

- IE11+ (Windows Phone)
- Microsoft Edge
- Microsoft Windows 10 Touch Screen Native (Surface Tablet)
- Safari 7+
- iOS 9+ Native
- Android 4.0+ Chrome
- Android 4.4+ Native
- Dolphin
- Opera

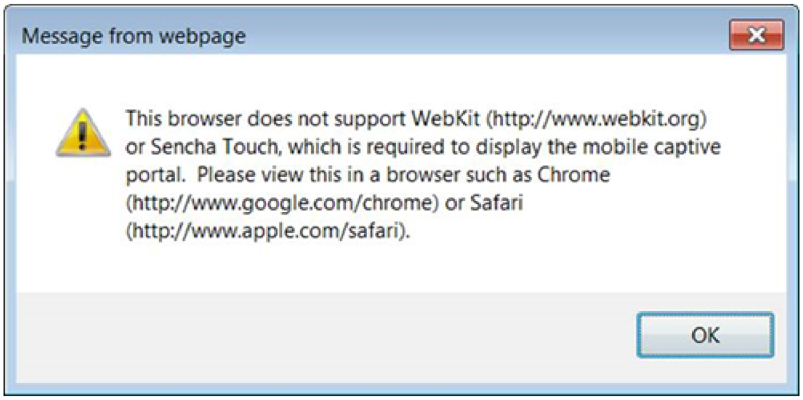
NOTES: A native browser indicates the default, system-installed browser. Although this may be Safari (iOS) or Chrome (Android), this also includes the default, system-controlled browser used for a device’s Captive Network Detection. Typically, this is a non-configurable option for Wi-Fi Captive Network 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://*<ip_of_engine>*/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:



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).

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

Extreme Management Center and Wireless Manager Requirements

Use Management Center and Wireless Manager to monitor and configure ExtremeWireless Controllers running firmware version 8.32 or later.

IMPORTANT: Management Center version 8.0 supports up to 7,500 APs and 50,000 clients across all managed wireless controllers. For sites with more than the supported number of APs and clients, contact your sales representative to acquire an additional Management Center license.

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 the Windows Server 2008 operating system is installed. Restarting Windows corrects this issue.

Important Installation Considerations

Important Requirement for Inventory Manager 8.0

Following a new installation of Management Center 8.0 (not an upgrade), if you restore a database from Management Center version 5.1 or earlier, you need to go to the Inventory Manager menu bar and select **Tools > Options > Data Storage**. Go to the **Directory Path** option and modify the path to point to the new Management Center 8.0 installation directory. If you don't do this, your Inventory Manager data including capacity reports, configuration templates, and property files are stored in the wrong directory.

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 backup 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.

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 Upgrading a Hardware 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 (NetSight) 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 (NetSight) 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.
- Older Management Center licensing keys (starting with INCREMENT) are no longer supported as of Management Center 5.0 and later. If you have one of these keys, please contact Extreme Networks Support for license upgrade information.
- The 4.xx version of the NAC Request Tool is not compatible with the 8.0 Management Center server. If you are using the NAC Request Tool you need to upgrade the version of NAC Request Tool to version 8.0.

Upgrade Considerations for NAC Manager 8.0

Important Captive Portal Changes

In Management Center 6.1, the Access Control captive portal was enhanced to provide a more modern look and feel. If you used the custom style sheet, you need to review pages, as there are most likely changes required to allow the custom styles to display correctly with the new page layout. After upgrading, log on as an Access Control administrators to the screen preview page (https://<Access Control engine IP>/screen_preview) of the Access Control captive portal to verify that the portal looks acceptable for display to end users. If your portal configuration is limited to setting colors and images, the new portal look and feel functions properly, although you may want to set some of the new color options.

General Upgrade Information

When upgrading to Management Center NAC Manager 8.0, you are not required to upgrade your Access Control engine version to 8.0. However, 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. Management Center NAC Manager 8.0 supports managing Access Control engine versions 7.0, 6.3, and 6.2.

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 Control8.0* 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.

Agent Version for Extreme Access Control Agent-Based Assessment

If you are using onboard agent-based assessment, be aware that the agent version is upgraded during the Access Control engine software upgrade. If you would like end-systems to update their agent to the new version, you must configure your assessment test set to test for the new agent version.

The agent version included in the Access Control engine version 8.0 is 1.15.0.0. This version includes internationalization and supports the following languages: Catalan, Czech, Dutch, English, Finnish, French, German, Italian, Korean, Norwegian, Polish, Portuguese, Spanish, and Swedish.

Upgrading NAC Request Tool

The 4.xx version of the NAC Request Tool is not compatible with the 8.0 Management Center server. If you are using the NAC Request Tool, you need to upgrade your version of the NAC Request Tool to version 8.0.

Upgrade Considerations for Management Center 8.0

- Beginning in 5.1, all Management Center maps intended to utilize the advanced map features of wireless coverage and client location triangulation should be created with a Base Map type of Floor Plan. Management Center maps created in NetSight version 4.4 or 5.0 that include both APs and walls are automatically converted to the Floor Plan Base Map type when the upgrade is performed. This allows Floor Plan map features to be available for those maps.
- Beginning in 5.1, managed wireless controllers (8.32 or later) are automatically synchronized to match OneView map floor plan data. If the floor plan data defined in Management Center maps is not consistent with data on the controller, the controller updates accordingly.

Upgrade Considerations for Policy Manager 8.0

- Policy Manager 8.0 only supports ExtremeWireless Controller version 8.01.03 and later. If you upgrade to Management Center 8.0 prior to upgrading your controllers, then Policy Manager does not allow you to open a domain where the controllers already exist or add them to a domain. A dialog indicating that your controllers do not meet minimum version requirements displays and explains they must be upgraded before they can be in a domain.

- Policy Manager 5.0 changed how it handles rule containment VLANs and Role VLAN Egress VLANs. This may cause Verify to fail following an upgrade to 8.0 when upgrading from versions prior to 5.0. If this happens, enforce the domain configuration to update the static VLAN table.
- Following an upgrade to ExtremeWireless Controller version 8.31 and higher, a Policy Manager enforce fails if it includes changes to the default access control or any rules that are set to contain. To allow Policy Manager to modify the default access control or set rules to contain, you must disable the "Allow" action in policy rules contains to the VLAN assigned by the role checkbox accessed from the Wireless Controller's web interface on the Roles > Policy Rules tab. This allows the enforce operation to succeed.

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

04/2017
P/N: 9035078
Subject to Change Without Notice

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
Operating System	64-bit Desktop • Windows • Ubuntu • Red Hat	64-bit Server • Ubuntu • Red Hat	64-bit Server • Ubuntu • Red Hat	64-bit Ubuntu Server
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	1,000	1,000
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
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.

- Windows (qualified on the English version of the operating systems)
    - Windows Server® 2012 and 2012 R2
    - Windows Server® 2016
    - Windows® 7
    - Windows® 10
- 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
- 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:

- 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

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 process functions identically to previous versions of Management Center (via the **Administration** > **Backup/Restore** tab), but the restore process must now be performed using the command line of the Management Center server.

The restore runs using the `mysqlbackup_restore` script in the *`<install directory>`*`\scripts` directory.

To restore the Management Center database backup:

1. Ensure you are running the **same version** of Management Center used when creating the database backup on the Management Center server.
2. Access a console terminal to the Management Center server to which you are restoring the database.
3. Navigate to the scripts directory:
   - On a Windows server, enter *`cd <install directory>`*`\scripts`.
   - On a Linux server, enter `cd` *`<install directory>`*`/scripts`.
4. Run the mysqlback_restore script:
   - On a Windows server, enter `mysqlbackup_restore.bat` *`"<full backup directory structure configured on`* ***`Backup/Restore`*** *`tab, including path>"`*

     (e.g. `mysqlbackup_restore.cmd "Program Files\Extreme Networks\NetSight\backup\netsight_03272017.sql"`).

   - On a Linux server, enter `./mysqlbackup_restore.sh` *`<full backup directory structure configured on`* ***`Backup/Restore`*** *`tab, including path>`*

     (e.g. `./mysqlbackup_restore.sh /usr/local/Extreme_Networks/NetSight/backup/netsight_03272017.sql/`).

The database backup is restored.

ZTP+ Enhancements

In Management Center version 8.0, ZTP+ can automatically configure your Access Controlengines. ZTP+ also now allows you to update your devices on an ongoing basis.

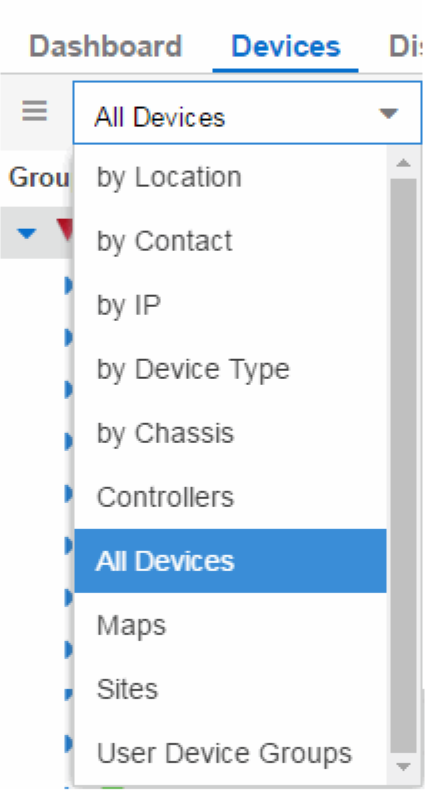
Additionally, ZTP+ now allows you to configure the following on your devices:

- 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, view all devices on your network, or select maps or sites.



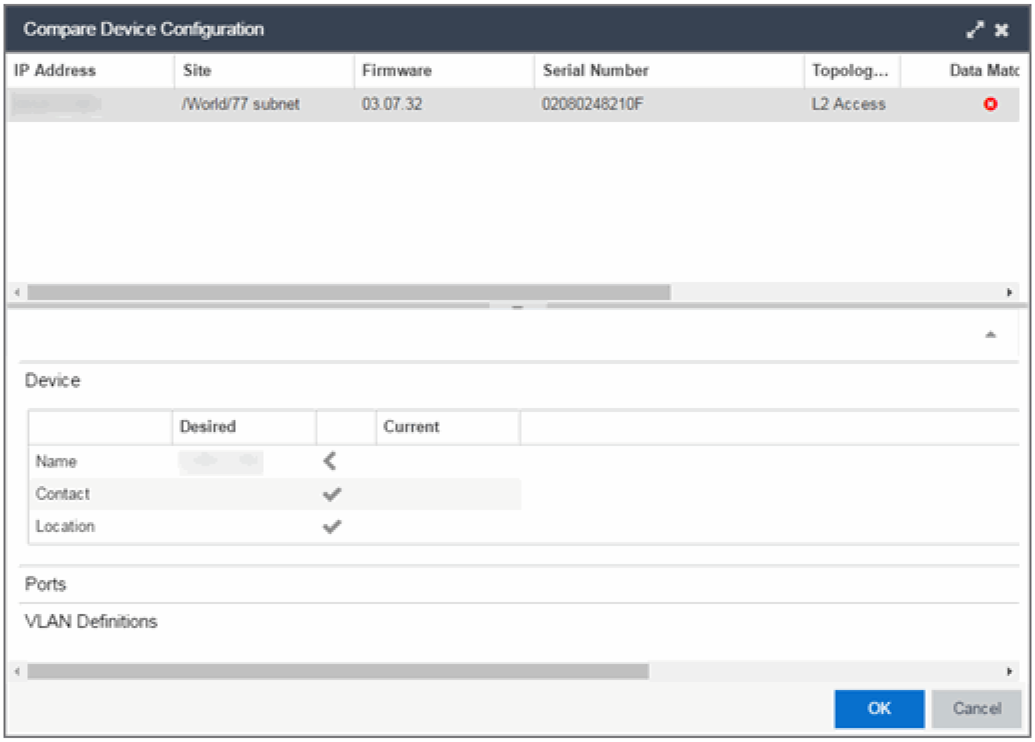
Selecting an item in the drop-down menu filters the Groups/Maps left-panel to display the devices, maps, or sites that apply to your selection.

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.

To access this window click **Verify** in the Edit Device window.

This window is also accessible by clicking **Verify** on Site tab.



IP Address	Site	Firmware	Serial Number	Topolog...	Data Matc
[redacted]	/World/77 subnet	03.07.32	02080248210F	L2 Access	✗

Device

	Desired		Current
Name	[redacted]	‹	
Contact		✓	
Location		✓	

Ports

VLAN Definitions

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 Data Match column indicates the whether the information in the Device section matches, the Ports Match column indicates whether the information in the Ports section matches, and the VLANs Match 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.

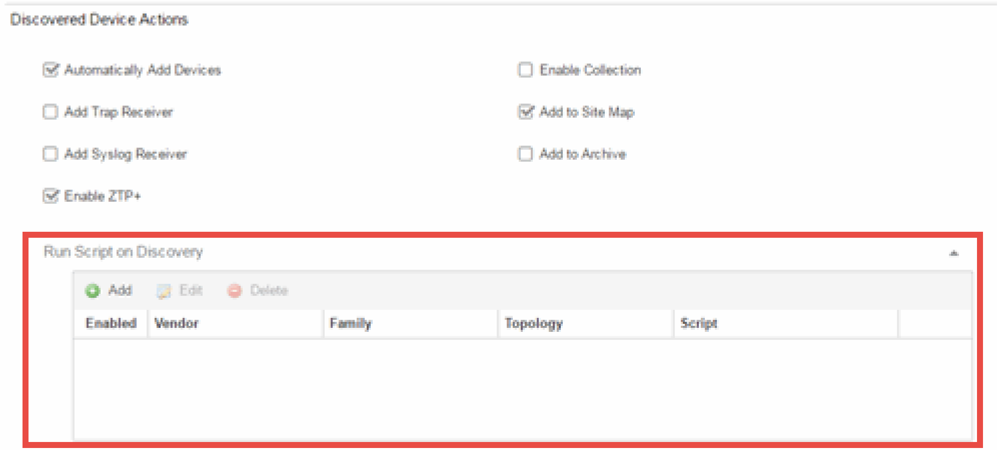
The Ports section of the displays any changes to the configuration of ports on the device.

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.



Discovered Device Actions

☑ Automatically Add Devices

☐ Add Trap Receiver

☐ Add Syslog Receiver

☑ Enable ZTP+

☐ Enable Collection

☑ Add to Site Map

☐ Add to Archive

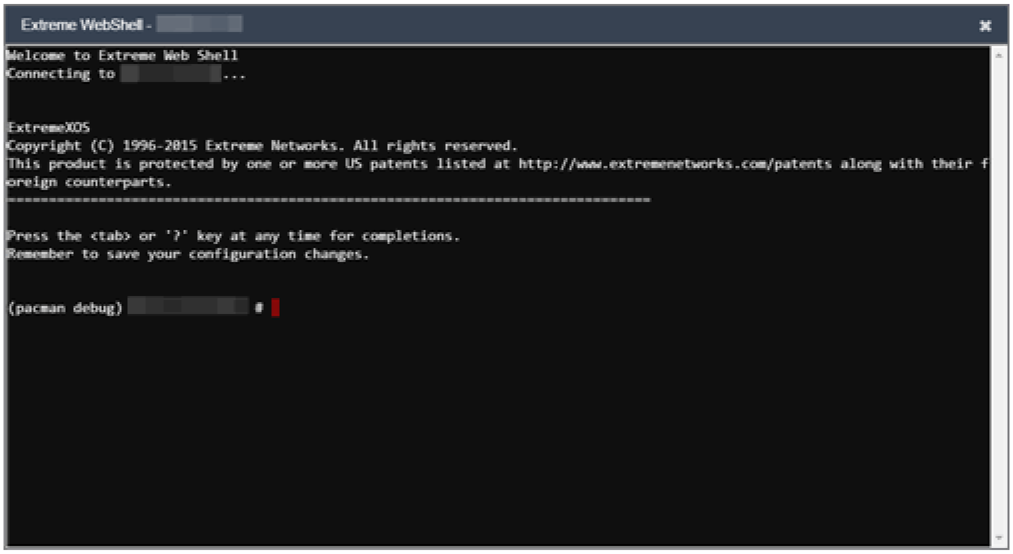
Run Script on Discovery

Enabled	Vendor	Family	Topology	Script

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.

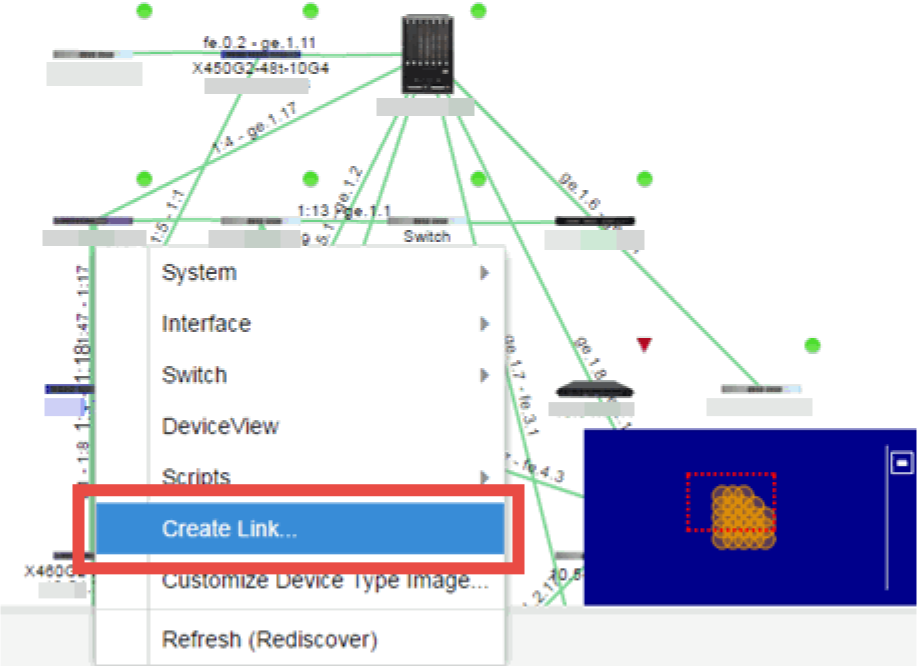


Extreme WebShell - [redacted]

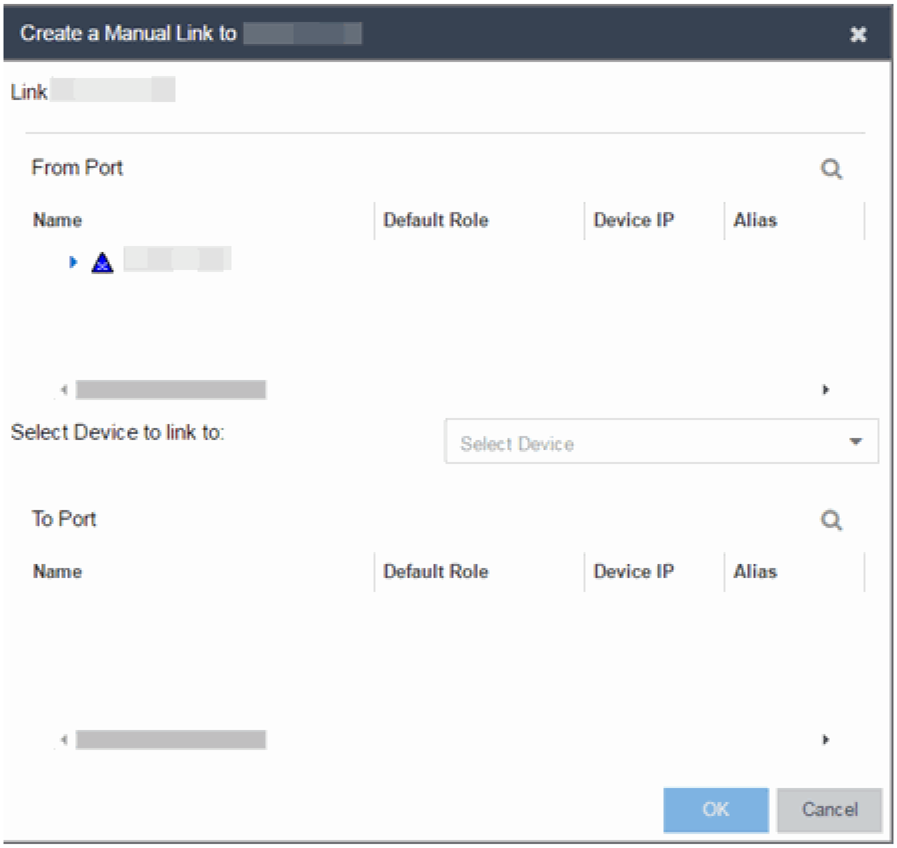
```
Welcome to Extreme Web Shell
Connecting to [redacted]...


ExtremeXOS
Copyright (C) 1996-2015 Extreme Networks. All rights reserved.
This product is protected by one or more US patents listed at http://www.extremenetworks.com/patents along with their f
oreign counterparts.
==============================================================================

Press the <tab> or '?' key at any time for completions.
Remember to save your configuration changes.


(pacman debug) [redacted] #
```

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.



Create a Manual Link to [redacted]

Link [redacted]

From Port

Name	Default Role	Device IP	Alias
[redacted]			

Select Device to link to: Select Device

To Port

Name	Default Role	Device IP	Alias

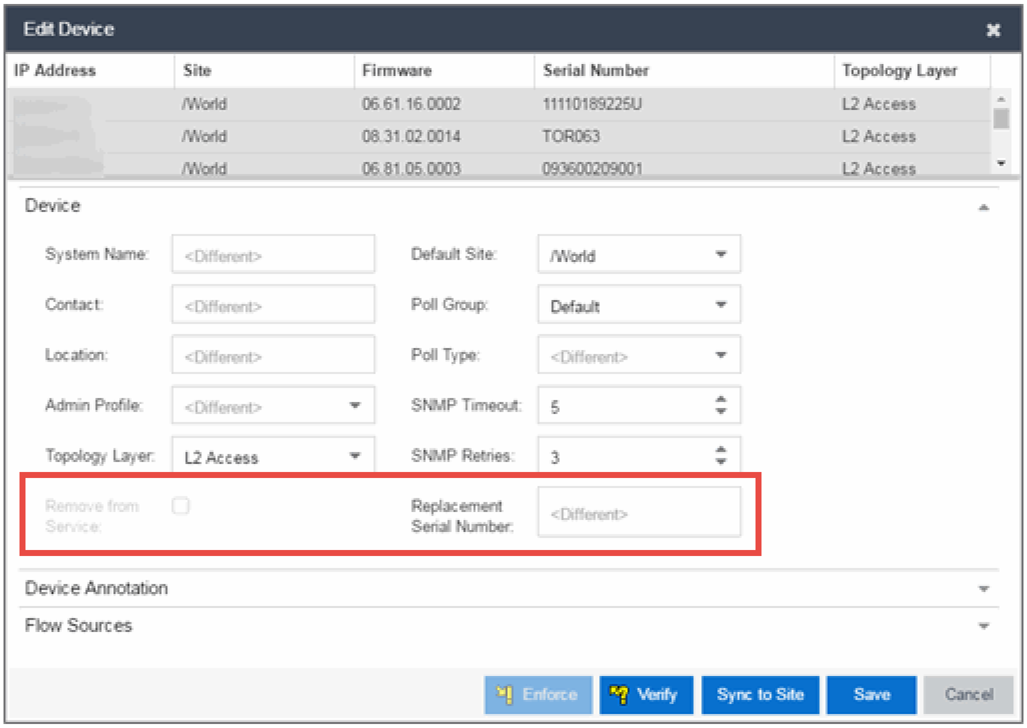
Added DHCP Fingerprint for VoIP Phone

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.



Edit Device

IP Address	Site	Firmware	Serial Number	Topology Layer
[redacted]	/World	06.61.16.0002	11110189225U	L2 Access
[redacted]	/World	08.31.02.0014	TOR063	L2 Access
[redacted]	/World	06.81.05.0003	093600209001	L2 Access

Device

System Name:	<Different>	Default Site:	/World
Contact:	<Different>	Poll Group:	Default
Location:	<Different>	Poll Type:	<Different>
Admin Profile:	<Different>	SNMP Timeout:	5
Topology Layer:	L2 Access	SNMP Retries:	3
Remove from Service:	□	Replacement Serial Number:	<Different>

Device Annotation

Flow Sources

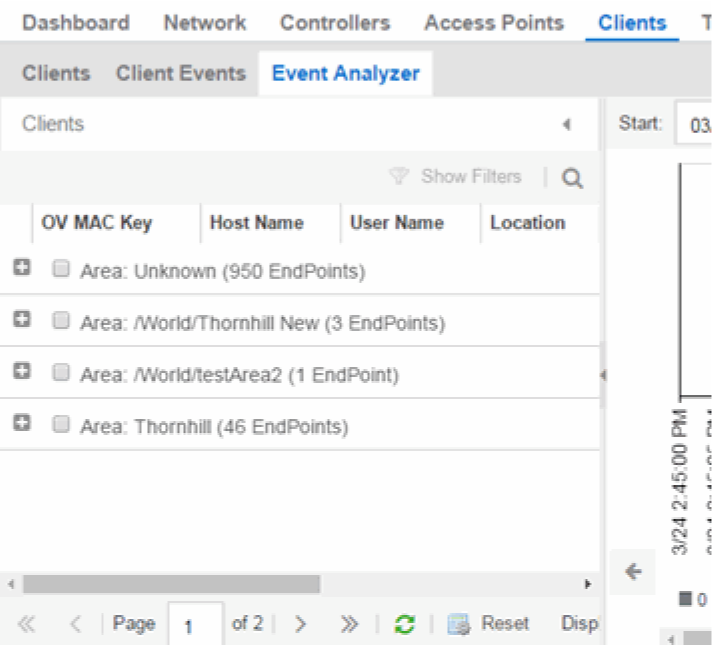
New Wireless Reports

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.



Dashboard Network Controllers Access Points Clients T

Clients Client Events Event Analyzer

Clients

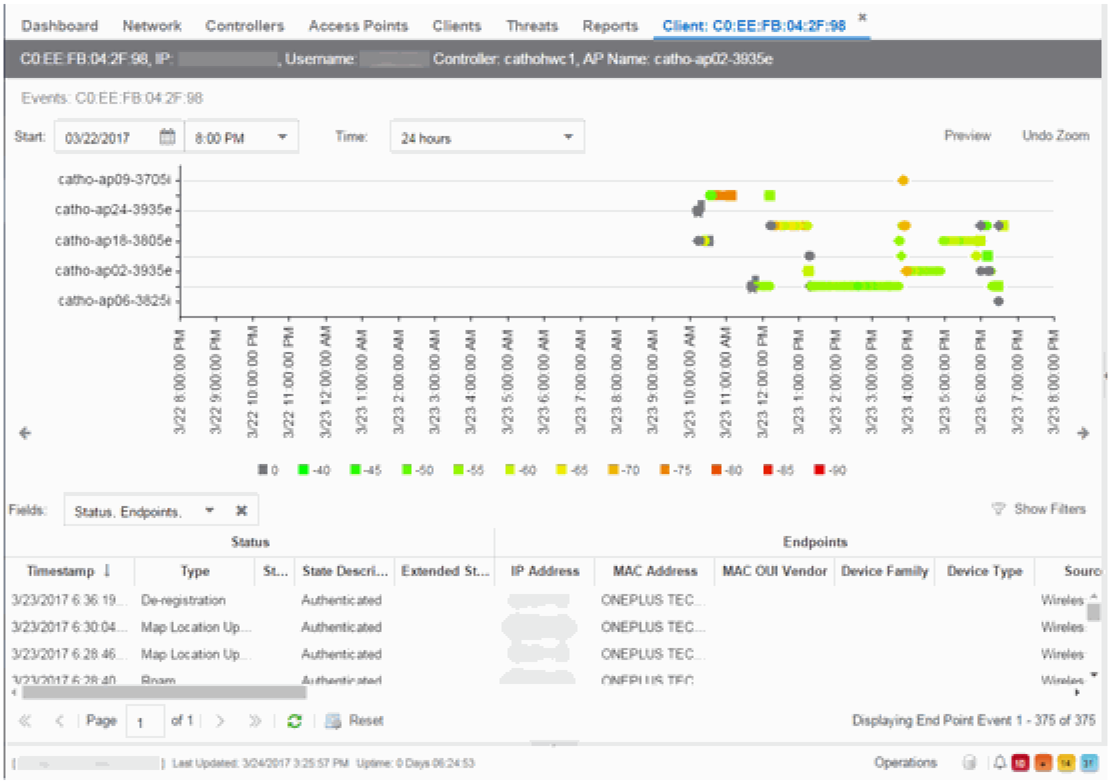
Show Filters

	OV MAC Key	Host Name	User Name	Location
⊞ □	Area: Unknown (950 EndPoints)			
⊞ □	Area: /World/Thornhill New (3 EndPoints)			
⊞ □	Area: /World/testArea2 (1 EndPoint)			
⊞ □	Area: Thornhill (46 EndPoints)			

Page 1 of 2 Reset Disp

Start: 03

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



Dashboard Network Controllers Access Points Clients Threats Reports Client: C0:EE:FB:04:2F:98 ×

C0:EE:FB:04:2F:98, IP: [redacted], Username: [redacted] Controller: cathohwc1, AP Name: catho-ap02-3935e

Events: C0:EE:FB:04:2F:98

Start: 03/22/2017 8:00 PM Time: 24 hours

Preview Undo Zoom

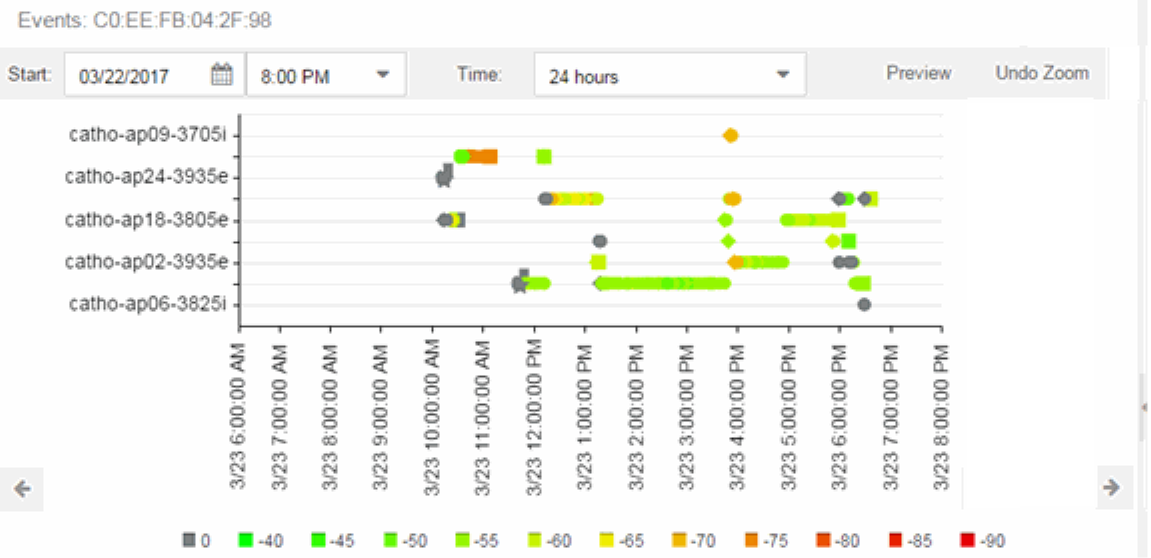
Fields: Status, Endpoints, Show Filters

Status					Endpoints					
Timestamp	Type	St...	State Descri...	Extended St...	IP Address	MAC Address	MAC OUI Vendor	Device Family	Device Type	Sourc
3/23/2017 6:36:19...	De-registration		Authenticated		[redacted]	ONEPLUS TEC...				Wireles
3/23/2017 6:30:04...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...				Wireles
3/23/2017 6:28:46...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...				Wireles
3/23/2017 6:28:40	Roam		Authenticated		[redacted]	ONEPLUS TEC				Wireles

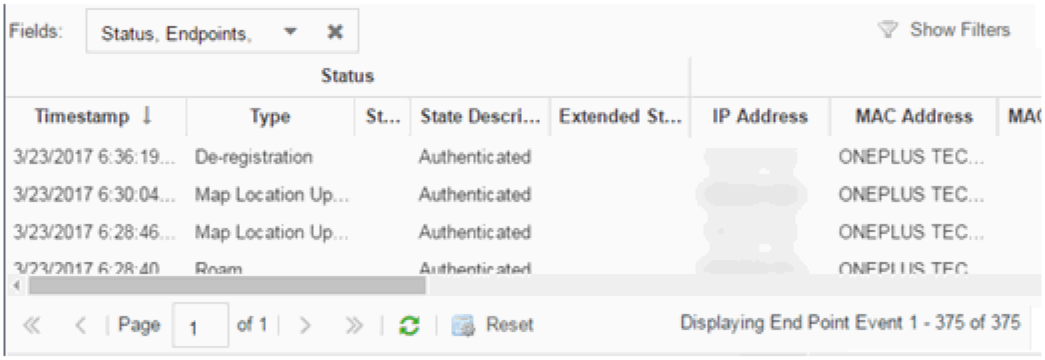
Page 1 of 1 Reset Displaying End Point Event 1 - 375 of 375

Last Updated: 3/24/2017 3:25:57 PM Uptime: 0 Days 06:24:53 Operations

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.



Status							
Timestamp ↓	Type	St...	State Descri...	Extended St...	IP Address	MAC Address	MA(
3/23/2017 6:36:19...	De-registration		Authenticated		[redacted]	ONEPLUS TEC...	
3/23/2017 6:30:04...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...	
3/23/2017 6:28:46...	Map Location Up...		Authenticated		[redacted]	ONEPLUS TEC...	
3/23/2017 6:28:40	Roam		Authenticated		[redacted]	ONEPLUS TEC	

Displaying End Point Event 1 - 375 of 375

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`.