6480 Via Del Oro
San Jose, CA 95119
+1 408-579-2800

Customer Release Notes

Extreme Networks Extreme Management Center (formerly NetSight)®

Version 7.0.9.4
January, 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 7.0, 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) 7.0 > Extreme Management Center (NetSight) Suite.

Software Enhancements

Enhancements in Extreme Management Center 7.0

This section presents the new features and enhancements included in Extreme Management Center 7.0.

Extreme Management Center Suite

- Introduction of Extreme Management Center (formerly OneView):NetSight is now called Extreme Management Center to reflect the change to a web-based platform.
- Functionality from legacy java clients now available in web-based Management Center (formerly OneView): Moved administration tasks (e.g. device discovery, firmware upgrades, archiving firmware images, options, user capabilities, policy functionality, etc.) and the Extreme Access Control (formerly NAC) Captive Portal into Management Center. Accomplishing tasks involving multiple areas of Management Center (formerly NetSight) is now simplified using easily navigable tabs in Management Center.
- Improved interface look and feel: The look and feel of the interface is improved to reflect the change from NetSight to Management Center. Additionally, a more responsive and context-sensitive help system is now available as a frame within the Management Center interface.
- Streamlined workflows: Complex workflows are now easier to perform as tabs in Management Center are organized logically to allow you to quickly move from one step to another.
- Added new license option: Management Center licenses can now be purchased on a subscription basis with pricing based on the number of small, medium, and large switches and the number of APs. This provides a more flexible option allowing customers to purchase a license that fits the size of their deployment.

NOTE: In order to use subscription licensing, version 10.11.02.X or newer must be installed on wireless controllers.

- Support for 32-bit servers deprecated: Management Center no longer supports 32-bit operating systems. To install version 7.0, an upgrade to a 64-bit system is required.
- Extreme Connect integration with Extreme Management Center: You can now use Extreme Connect with Extreme Management Center (requires NMS-ADV license).
- Wireless MU history and End-System events now stored in the database: Wireless MU history and end-system events, previously stored in log files, are now available in the database to provide a more robust data set with which to create reports.

Device Support

- Added policy support for additional device type: Extreme 770 devices now allow policy management in Access Control.
- Added ZTP+ functionality: ZTP+ (Zero Touch Provisioning Plus) is now available on ExtremeXOS devices running version 21.1 and Application Analytics engines. ZTP+ allows users to add supported devices to Management Center with minimal configuration. To use this feature on an ExtremeXOS device, download the XOS XMOD from the ExtremeXOS Application Support Site. The feature comes included in the Application Analytics installation.
- Ability to schedule device discovery: Management Center now allows you to schedule a device discovery.
- Added support for additional device types: Management Center now supports the following device types:
  - ExtremeXOS version 21.1
  - X440G2
  - X620
  - Wireless controllers running version 10.21
  - AP3912i-FCC
  - AP3912i-ROW

Extreme Management Center (formerly OneView)

- Added Beta Module to Extreme Connect: Added the Beta module to the Connect tab, which contains a Location Based Services API (Real-Time).

    - Allows 3rd party solutions to register to wireless MU event stream
    - MU events are forwarded "as they occur" (real-time)
    - Supports HTTP protocol and XML or JSON data format
    - Event filters (list of MACs or IPs, areas, maps, event types) can be defined per listener
    - Aggregates and forwards MU events from all managed Extreme wireless controllers
- Enhancement to report locations: The VenueReport, which uses locations configured in Application Analytics, now supports the use of wildcard characters to include multiple locations in the report.
- Database backup and restore functionality available in Management Center: Added the ability to backup and restore the database from within the web-based Management Center (formerly OneView).
- Improvement to Management Center statistics collection:Management Center now collects additional wireless bandwidth protocol statistics for venue customers.
- Added the ability to select a default configuration to devices added to Management Center: Maps can now become sites in Management Center, allowing you to create a default configuration for devices added via a device discover or using ZTP+ functionality.
    - Additional Site Features: The following are additional site features:
        - Site discover can optionally add newly discovered devices to an archive named for the site.
        - You can archive all of the devices added to a site.
        - Enhancements to Sites on newly discovered devices: The following functionality is now available as a beta feature on sites for ExtremeXOS and EOS devices only:
            - Ability to add device to a policy domain
            - Ability to add device to Access Control Engine Group
            - Ability to enable port authentication on a device

WARNING: Configuring the authentication could affect communication to a device and result in loss of connectivity through the interswitch link ports, if not detected or configured properly during the discovery process. If you are configuring the policy and authentication on the interswitch link, it's strongly recommended to ensure neighbor discovery protocols such as LLDP, EDP, and CDP are enabled before enabling the authentication using port templates.

- Improvement to layer 7 application rule type: Added support for enhancements to layer 7 application rule type, which classifies traffic by application, determined by deep packet inspection of flows on the wireless access point.
- Ability to pre-register devices by scanning QR (Quick Response) code or barcode: Added a new mobile application that allows you to pre-register switches by scanning the QR code or barcode. Additionally, devices you pre-register can be added to a site, allowing the site configuration to be assigned to the device automatically.
- Added new ExtremeXOS FlexView: Added new ExtremeXOS System Configuration FlexView allowing read/write support for this MIB table.
- Enhanced MLAG maps: Highlighting in MLAG map now includes the connected switch if it is displayed on the map. Additionally, the MLAG grid table data now includes the connected switch IP address.
- Improvement to Traps: Traps sent as Alarm Manager actions have been enhanced to include more detailed information that can be better parsed by trap receivers.
- Improved ability to configure alarm actions: Multiple trap receivers can now be configured in a single alarm action.
- Improvement to statistical record storage: Management Center now limits the historical statistical records saved to the database in a low disk space condition.
- Ability to customize dashboards: Dashboards in Management Center are now customizable, allowing you to display the most important information for your network.
- Enhancement to PortView: Search results viewed in PortView now contain an application summary and map information.
- Improved reporting capabilities: A **Reports** sub-tab is now available in the **Network**, **Control**, **Analytics**, and **Wireless** tabs. These tabs contain pre-

defined reports that can be customized displaying information relating to the information contained on each tab. Additionally, events are now stored in the database, providing more information and more complete reporting as more data is retained.

- Integration of Extreme Access Control with Policy Manager: The following tasks are now available when using both Extreme Access Control and policy functionality:
  - Map policy domains to engine groups
  - Automatically create profiles and roles
  - Create profiles, rules, roles, and named lists from Extreme Access Control configuration
  - Centralized configuration workflow from Extreme Access Control configuration

Application Analytics/Purview™

- Additional Application Analytics Support for Wireless Controllers: Updated the Application Analytics Wireless Controller Flow Source UI to support 10.21 Wireless Controllers IPFIX Flow export.

NOTE: Rx Packets and **Rx Bytes** may incorrectly be **0** when flow data is gathered via a wireless controller running version 10.21 or higher. Additionally, application response times and some meta data may be blank. This is a known issue and will be addressed in a future release.

- Improvement to Fingerprint Identification: The Flow Collector now uses port information to improve Fingerprint identification.
- Added a Network Services Dashboard: The Analytics Dashboard now has a Network Service dashboard. This view shows the performance of LDAP, RADIUS, Kerberos, DHCP, and DNS for each location in one-minute intervals.
- Increased search capability for locations: The algorithm for location search is optimized to support up to 64k locations.
- Improvement to high-rate data collector: The high rate collector now stores Client count, Flow count, Bytes, Received bytes, Sent bytes, App response time and Network response time indexed by combination key of location and application ID.
- Ability to limit number of end-systems reported per engine: Added the ability to limit the number of end systems reported per engine to ensure the

database does not fill with data from one engine and not persist data from the other engines.

- Improvement to flow record storage: Application Analytics now limits the flow records saved to the database in a low disk space condition.
- Improvement to syslog export: Updated the Analytics Engine syslog export to include the source and destination MAC address.
- Enhanced NetFlow record exporting: Application Analytics now supports exporting enhanced NetFlow records containing both identification and traffic information to external SIEM(s).
- Ability to view real-time network and application response times: Network and Application response times can now be tracked in near real-time using the newly added Response Time Dashboard.
- Improvement to application response time reporting: Application Analytics now contains an option for storing additional client data for the 10 slowest clients for each of the worst 100 applications by application response time per hour.
- Added new address lookup option: X-Force Exchange is added as an option for performing an address look-up.
- Ability to import/export location definitions: Application Analytics now allows exporting location definitions for Purview into a CSV file and importing saved location definitions.

Extreme Access Control/NAC

- Enhancement to freeRADIUS dictionary: Added additional trapeze RADIUS attributes to the freeRADIUS dictionary, which are now available in Access Control.
- Improvements to Access Control functionality in Management Center: The following functionality is now available in Management Center:
    - General Administration and Administrative Role configuration for Access Control Portal Configurations is now available via Extreme Management Center.
    - Assessment and Remediation configuration for Access Control Portal Configurations is now available via Management Center
- Improvement to Location Groups: Location groups can be associated with an IP Subnet mapping, so that same VLAN ID can be used in multiple IP Subnet mappings.

- Ability to detect third-party firewalls on the Windows operating system: Extreme Access Control can now detect third-party firewalls on Windows systems, proving better visibility and more control for end-systems using Windows.
- Improved ability to monitor end-systems per end-system group: Added a new threshold alarm that warns if number of entries in an end-system group exceeds 50,000.
- Improvement to Extreme Access Control reporting: Updated the Total End-Systems Seen Last 24 Hrs chart in the Extreme Access Control System report to an hourly format, displaying peak values rather than average, to better reflect current end-system usage.
- Ability to prompt users to change password: Management Center now prompts users to change their password when the client is configured to manually enter their network authentication and the password expires or for new accounts that require a password change.
- Added RADIUS dictionary to Extreme Access Control Engines: Extreme Access Control Engines now support the RADIUS dictionary file for Checkpoint Firewalls.
- Added RADIUS server load balancing functionality: Extreme Access Control can now load balance among RADIUS servers.
- Improvement to expiration timer: The account expiration timer for pre-registered guest users can now be configured to start counting down at the occurrence of the user's first login attempt.
- Ability to configure guest registration expiration of less than one day: Added the ability to set the default guest registration to less than one day to provide better control of guests on the network.
- Improvement to Extreme Access Control email functionality: Extreme Access Control now supports the ability to perform variable substitution in the Secure Guest SendTo email field to support functionality needed with some SMS Gateways.
- Added fingerprint for Windows 10 devices: Added an additional DHCP Fingerprint discovered for Windows 10 devices.
- Added fingerprint for Apple TV: Extreme Access Control now differentiates between the DHCP fingerprint for Apple TV and the fingerprint for iOS.
- Support for legacy devices deprecated in Management Center version 7.0 release: The following end-of-service legacy devices are no longer being supported in Management Center version 7.0:

- SNS-TAG-LPA
- SNS-TAG-HPA
- SNS-TAG-ITA

Wireless

- Support for WAS deprecated on EWC in version 10: ExtremeWireless Controllers running version 10 do not support Wireless Advanced Services.

Known Issues Addressed

This section presents the known issues that were addressed in Extreme Management Center 7.0.9.4:

Extreme Access Control/NAC Manager Issues Addressed	ID
Injection of RADIUS accounting attributes by the proxy server was occasionally failing when the newly injected attribute was comprised of data from existing attributes in the frame.	01271388
The Management Center version was displayed in some places when backing up and restoring the `snmpd.conf` file during a Management Center upgrade.	1264237

This section presents the known issues that were addressed in Extreme Management Center 7.0.8.34:

Extreme Management Center Suite Issues Addressed	ID
When adding new users to Management Center, User Names could not include periods (.).	1258335 01262468
The Administrator Password in LDAP Configuration cannot consistently handle the Euro sign character (€), as a result it may not be possible to connect to an LDAP server which has a Euro sign in the password.	01235954
The Management Center server was failing to start in environments where a firewall blocks internet access, preventing the URL connection socket timeout from being received.	1248929
Modifying the `/etc/samba/smb.conf` file and then upgrading the Management Center server from version 6.3 to version 7.0 was causing the upgrade to fail.	01245348
All syslog messages were displaying with a severity of **Info**, regardless of the severity with which they were configured.	1144968
Extreme Access Control/NAC Manager Issues Addressed	**ID**
Access Control Captive Portal was not supported on servers using AMD processors.	01245267 01251356
Injection of proxy RADIUS attributes were not being handled correctly on redundant Access Control engines.	1254555
Importing a pre-registered user .CSV file when the Captive Portal was configured to use the German locale was causing a message string parsing error.	01231061
Rotate squid cache and log files to reduce disk space consumption.	01151070 01202480

When determining end-system device types via DHCP fingerprinting, Vizio televisions were incorrectly listed as Amazon Kindles.	01245679
Virtual Access Control Engines with a NAC-V-20 license were not properly updating using an Enterprise license (e.g. IA-ES-3K).	1250445
Importing a pre-registered user .CSV file with an empty column representing an optional field value followed by a populated column representing a required field value was causing the file to be imported improperly.	01233530
Application Analytics/Purview Issues Addressed	**ID**
Enforcing an Application Analytics engine from Management Center with interfaces eth4 or eth5 configured was causing manually configured interfaces to be removed from the engine.	1263225
Policy/Policy Manager Issues Addressed	**ID**
The Policy Manager legacy java application would run out of memory when retrieving port information via the **Ports** tab for stacked 440-series Summit devices configured in large stacks.	------

This section presents the known issues that were addressed in Extreme Management Center 7.0.6.27:

Extreme Access Control/NAC Manager Issues Addressed	**ID**
NTLM authorization rejects were incorrectly being reported as a RADIUS reject.	1160538 1213189 1226892
Access Control now saves the TLS Client Certificate Issuer and Expiration as part of the End System data for applicable end-systems.	------
Enforcing to an Access Control engine was changing SNMP RW credentials to be the same as RO when the RW credentials are set to <no access>.	1230105
A shared secret containing a comma in Access Control was causing RADIUS authentication to fail due to mismatched shared secret.	01235771

This section presents the known issues that were addressed in Extreme Management Center 7.0.5.12:

Extreme Management Center Suite Issues Addressed	**ID**
Devices automatically added by Management Center (**Automatically Add Devices** is selected for the Site) were incorrectly duplicated in the Management Center database, which resulted in the Device Tree device count not matching.	**------**
Multiple "Task Engine Queue Timer" threads were incorrectly being created.	------

Putty 0.6 uses weak ciphers that are unable to be used with Management Center. Management Center now ships with Putty 0.67.	
Extreme Access Control/NAC Manager Issues Addressed	**ID**
Access Control was incorrectly identifying 38xx ExtremeWireless access points as a Windows device.	01234777
Downloading and installing the Assessment Agent via Microsoft Internet Explorer or Edge was giving a corrupt or invalid certificate error.	1234200 01235098 01237000

This section presents the known issues that were addressed in Extreme Management Center 7.0.4.29:

Extreme Management Center Suite Issues Addressed	**ID**
Management Center server upgrades were not completing properly when a corrupted end-system event log file was read.	1223391
Extreme Management Center (formerly OneView) Issues Addressed	**ID**
MapQuest discontinued direct tile access to maps and, as a result, geographic maps were not displaying properly.	**------**
Displaying the wireless signal strength of the APs on a Floorplan map with a large number of cells was loading slowly.	**------**
Compass searches were not displaying all matches if the filter was IP Address.	1214178
AP serial numbers could not be edited via a floorplan map.	1227111

This section presents the known issues that were addressed in Extreme Management Center 7.0.3.12:

Extreme Management Center Suite Issues Addressed	**ID**
Clicking on an Application Analytics alarm in the **Analytics** > **Configuration** tab was not launching an alarm list.	------
Filtered alarm lists occasionally incorrectly become unfiltered when reloading.	------

This section presents the known issues that were addressed in Extreme Management Center 7.0.2.33:

Extreme Management Center Suite Issues Addressed	**ID**
The Management Center Help System did not display when viewed using Internet Explorer.	------
Custom alarms were not triggering when one of the matching criteria was an IP Address.	1182906

Security layer was not permitting ZTP+ device application to connect to server for device registration.	------
Extreme Management Center (formerly OneView) Issues Addressed	**ID**
LLDP links for third-party devices were not displaying in maps.	01192299
Extreme Access Control/NAC Manager Issues Addressed	**ID**
Access Control engines were incorrectly managing the PMIP6-Home-HN-Prefix radius accounting attribute.	------
Access Control engines were not being detected by the assessment server and were not appearing in the assessment server table.	------
The Access Control distributed end-system cache is now enabled by default in new installations of Management Center.	------
Application Analytics (formerly Purview) Issues Addressed	**ID**
When the appid process on the Application Analytics engine encountered a malformed UDP packet, it was allocating a potentially large amount of memory (causing excessive swapping) or performing a core dump. Malformed UDP packets where the IPv4 header indicates there is a UDP layer when there is no UDP layer are now ignored.	1211563
The same flow was being duplicated on multiple switches. Feedback to help debugging misconfigured switches was added. This includes alarms for the same flow being duplicated by multiple switches, and alarm for a switch only mirroring half of a session, and the ability to search for duplicated flows with a new search "flowsource=multiple".	------

This section presents the known issues that were addressed in Extreme Management Center 7.0.1.13:

Extreme Management Center (formerly OneView) Issues Addressed	**ID**
The resolution of large maps was decreasing when imported into Management Center.	1173132

This section presents the known issues that were addressed in Extreme Management Center 7.0.0.139:

Extreme Management Center Suite Issues Addressed	**ID**
The custom fingerprint template contained a hard-coded creation and modification date of Dec 31, 2013 rather than the current date.	------
Portmap service is disabled on upgrade due to PCI compliance vulnerability.	------
Extreme Management Center (formerly OneView) Issues Addressed	**ID**

Interface history for XSR products occasionally reported an error when displaying the interface view.	1173132
An exception was thrown when a PDF report was generated if packages required by the PDF generation tool were not present in the system.	------
Serial numbers were truncated or not displayed correctly in the DeviceView and FlexViews.	1147459
The Interface Details reported Half Duplex on new port types that were Full Duplex.	01163855
A user logging in may have been directed to a view for which they do not have privileges, resulting in an authorization error.	1195166
An error/exception on the server caused status information for a Map to fail to be updated when conditions changed.	01148219
The "Parameter definition" and "Conditional statements" example scripts contained syntax errors.	1200110
Inventory manager added duplicate scheduled entries for firmware downloads, when multiple devices were selected for upgrade.	1163679
Inventory manager schedule dates were incorrect if the user specified a date and time in a format other than the default MM/DD/YYYY.	1177915
When right clicking a device in the left Device Tree in Management Center and selecting Configuration/Firmware -> Restore Configuration -> Clone, the device type was displayed as undefined and it also incorrectly showed no saved configuration files.	1184794
When failing to login on the Management Center login page, the failed password was return in the response and may have remained cached in the browser.	------
The Protocol Address field was missing in the OneView VLAN summary table.	1149624
When selecting Application Browser from the Analytics dashboard occasionally resulted in a "could not load report" error.	------
Selecting the Enable and Disable All functions in OneView caused the status to indicate that it had been changed, but functionally the status was not changed.	
Application Analytics (formerly Purview) Issues Addressed	**ID**
Syslog messages were displaying with a **Severity** of **Info** for installations on the Windows operating system.	1144968
When sorting by response times in Application Analytics, a null pointer exception error occasionally occurred.	------
It was not possible to enter a non-standard netmask while configuring the network address.	1188109

The interface configuration section of the setup script was called 'Tunnel Configuration', which was confusing.	01190063
Purview engines could not be deployed behind a NAT router.	------
In certain cases, some of top 100 applications for an hour showed no clients in the reports or application browser.	------
Extreme Access Control/NAC Manager Issues Addressed	**ID**
User customized fields were not included in the email body of a notification test.	------
Disabled configuration rules were being included in the enforce audit verification.	------
Advanced location portals in the configuration feature panel could not be edited when the number of locations exceeded the space available on the panel.	------
Management was not being disabled when enabling network access for RADIUS on a switch with no management servers configured. Additionally, if enabling management without configuring servers through NAC, management was not enabling.	01157133
NAC CLI-based RADIUS configuration on Extreme devices was failing to configure accounting if the save from RADIUS authentication sets was not completed.	------
The username for end-systems was being cleared for users that authenticated via 802.1x and subsequently registered once the registration expired.	1160869
The German locale message string for Password Repository (domainName) was incorrectly labeled "Domain-Name" (and was changed to "Passwortdatenbank").	01186624
Windows 10 802.1x authorization was failing due to MD5 signature algorithm. New installations now use SHA256 as the signature algorithm for RADIUS self-signed certificates.	1170459 1170452 1173204
Extreme Access Control captive portal was using a deprecated SHA-1 certificate that caused the Chrome browser to warn that the site is untrustworthy. New installations now use SHA256 as the signature algorithm for captive portal self-signed certificates.	01195188
Third-Party Firewalls were not being detected by the Assessment Agent on Windows operating systems.	1041024 1164987
The Installed Program assessment check was not displaying application details when the program was discovered in the file system, but not discovered in the registry.	01152990
A topology change that occurred simultaneously with a client registration caused the user to not be redirected out of the captive portal.	01159640

If a user disconnected or used a different SSID, their Verify Pin no longer worked in the captive portal.	1180995
Incoming NAC Notification Events were occasionally not processed.	------
NAC authentication did not fail over to a secondary proxy RADIUS server when the primary RADIUS server was not reachable.	------
NAC Request tool now only runs on 64 bit Windows or Linux.	------
Policy Manager Issues Addressed	**ID**
Configuring MAC authentication on an ExtremeXOS device did not work properly in Policy Manager if no password was configured. Added a dialog message notification when enabling MAC authentication on Extreme devices and no MAC password is configured, indicating that the password must be set before MAC authentication is successful.	1159682
When modifying the role and selecting "Add/Remove Services" view, if the service name is longer than 12 character, the pull down menu did not display the entire name.	1181139
In the role "Add/Remove Services" view in the Policy Manager java application, role names longer than 12 characters were truncated.	1181306
Wireless Manager Issues Addressed	**ID**
Failure to process client events occasionally caused high memory utilization on the server.	01175837 1174756
Inventory Manager Issues Addressed	**ID**
Configuration restore was not working with 800-Series devices.	1146083
The Configuration Template Wizard stopped responding when certain special characters were used in variables.	1148471

Vulnerabilities Addressed

This section presents the Vulnerabilities that were addressed in Extreme Management Center 7.0:

- The following vulnerabilities were addressed in the Extreme Management Center, Extreme Access Control, and Application Analytics engine image:
    - CVE-2002-2443, CVE-2012-2417, CVE-2012-3425, CVE-2012-4428, CVE-2013-6425, CVE-2013-7422, CVE-2013-7447, CVE-2014-3591, CVE-2014-4330, CVE-2014-5355, CVE-2014-8161, CVE-2014-8964, CVE-2014-9512, CVE-2014-9745, CVE-2014-9766, CVE-2015-0241, CVE-2015-0243, CVE-2015-0244, CVE-2015-0837, CVE-2015-0860, CVE-2015-1197, CVE-2015-1283, CVE-2015-1794, CVE-2015-1819, CVE-2015-2325, CVE-2015-2326, CVE-2015-2590, CVE-2015-2596, CVE-2015-2597, CVE-2015-2601, CVE-2015-2613, CVE-2015-2619, CVE-2015-2621, CVE-2015-2625, CVE-2015-2627, CVE-2015-2628, CVE-2015-2632, CVE-2015-2637, CVE-2015-2638, CVE-2015-2659, CVE-2015-2664, CVE-2015-2694, CVE-2015-2695, CVE-2015-2696, CVE-2015-2697, CVE-2015-2698, CVE-2015-2808, CVE-2015-3165, CVE-2015-3166, CVE-2015-3167, CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2015-3210, CVE-2015-4000, CVE-2015-4141, CVE-2015-4142, CVE-2015-4143, CVE-2015-4144, CVE-2015-4145, CVE-2015-4146, CVE-2015-4491, CVE-2015-4729, CVE-2015-4731, CVE-2015-4732, CVE-2015-4733, CVE-2015-4736, CVE-2015-4748, CVE-2015-4749, CVE-2015-4760, CVE-2015-5073, CVE-2015-5177, CVE-2015-5288, CVE-2015-5289, CVE-2015-5312, CVE-2015-5589, CVE-2015-5590, CVE-2015-6831, CVE-2015-6832, CVE-2015-6833, CVE-2015-6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838, CVE-2015-7236, CVE-2015-7497, CVE-2015-7498, CVE-2015-7499, CVE-2015-7500, CVE-2015-7511, CVE-2016-7547, CVE-2015-7575, CVE-2015-7673, CVE-2015-7674, CVE-2015-7696, CVE-2015-7697, CVE-2015-7803, CVE-2015-7804, CVE-2015-7941, CVE-2015-7942, CVE-2015-7981, CVE-2015-8035, CVE-2015-8126, CVE-2015-8241, CVE-2015-8242, CVE-2015-8317, CVE-2015-8370, CVE-2015-8472, CVE-2015-8605, CVE-2015-8710, CVE-2016-0402, CVE-2016-0448, CVE-2016-0466, CVE-2016-0475, CVE-2016-0483, CVE-2016-0494, CVE-2016-0755, CVE-2016-0766, CVE-2016-0773, CVE-2016-0777, CVE-2016-0778, CVE-2016-1577, CVE-2016-2037, CVE-2016-2116, CVE-2016-2381

System Requirements

IMPORTANT: Extreme Management Center version 7.0 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 7.0.

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 7.0 > 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: Beginning in Management Center version 7.0, 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® 2008 Enterprise and 2008 R2
  - Windows Server® 2012 and 2012 R2
  - Windows® 7
  - Windows® 8 and 8.1
- Linux
  - Red Hat Enterprise Linux WS and ES v5 and v6
  - SuSE Linux versions 10, 11, and 12.3
  - Ubuntu 11.10, 12.04, and 13.04

- Mac OS X® (remote Management Center client only)
  - Lion
  - Mountain Lion
  - Mavericks
  - Yosemite
- VMware® (Management Center Virtual Engine)
  - VMware ESXi™ 5.1 server
  - VMware ESXi™ 5.5 server
  - VMware ESXi™ 6.0 server
- Hyper-V (Management Center Virtual Engine)
  - Hyper-V Server 2012

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	Large	Enterprise
Operating System	64-bit Desktop • Windows • Ubuntu • Red Hat • SUSE	64-bit Server • Ubuntu • Red Hat • SUSE	64-bit Ubuntu Server
CPU	Quad Core	Dual Quad Core	Dual Hex Core
Memory	8 GB	12 GB	24 GB
Free Disk Space	40 GB	100 GB	Greater than 100 GB
Storage Capacity	NA	NA	Dual 1 TB hard drives with RAID controller

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, and El Capitan

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 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 that are 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	

Extreme Management Center and Wireless Manager Requirements

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

IMPORTANT: Management Center version 7.0 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 that was 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 Installation Considerations

Important Requirement for Inventory Manager 7.0

Following a new installation of Management Center 7.0 (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 7.0 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 that you have 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 7.0 supports upgrades from NetSight 6.3, 6.2. If you are upgrading from a NetSight version prior to 6.2, you must perform an intermediate upgrade. For example, if you are upgrading from NetSight 6.0, you must first upgrade to NetSight 6.2, and then upgrade to Management Center 7.0.

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 **Server Information** window to perform the backup. From the menu bar, access **Tools > Server Information** and select the **Database** tab.

Important Upgrade Considerations

- If your network is using Application Analytics engines, you must first perform the Management Center upgrade to version 7.0 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 7.0. You must install an updated module that supports Management Center 7.0. Contact your account team for information on obtaining this update.
    - You must install a Management Center (NetSight) Advanced (NMS-ADV) license with 7.0 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 7.0 Management Center server. If you are using the NAC Request Tool you need to upgrade the version of NAC Request Tool to version 7.0.

Upgrade Considerations for NAC Manager 7.0

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 7.0, you are not required to upgrade your Access Control engine version to 7.0. However, both Management Center NAC Manager and the Access Control engine must be at version 7.0 in order to take advantage of the new Access Control 7.0 features. Management Center NAC Manager 7.0 supports managing Access Control engine versions 7.0, 6.3, and 6.2.

NOTE: Access Control 7.0 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 7.0* document (available on the Management Center (NetSight) Documentation web page > Manuals & Release Notes > NetSight 7.0 > 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 7.0 if you upgrade to the Access Control engine 7.0. Version 7.0 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 7.0 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 7.0 Management Center server. If you are using the NAC Request Tool, you need to upgrade your version of the NAC Request Tool to version 7.0.

Upgrade Considerations for Management Center 7.0

- 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 7.0

- Policy Manager 7.0 only supports ExtremeWireless Controller version 8.01.03 and later. If you upgrade to Management Center 7.0 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 7.0 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 7.0

Following a Wireless Manager upgrade, you should 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

01/2017
P/N: 9034967-09
Subject to Change Without Notice