145 Rio Robles
San Jose, CA 95134
+1 408-579-2800

Customer Release Notes

Extreme Networks Extreme Control Center (formerly NetSight)®

Version 7.0.0.139
April, 2016

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

Extreme Control Center (ECC) is distinguished by its web-based, unified control interface. Graphical and exceptionally easy-to-use, OneView 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.

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

The ECC 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 Control 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 > Extreme Control Center (NetSight) (NMS) > Documentation > Manuals & Release Notes > Extreme Control Center (NetSight) 7.0 > Extreme Control Center (NetSight) Suite.

Software Enhancements

Enhancements in Extreme Control Center 7.0

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

OneView

- 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: Extreme Control Center now limits the historical statistical records saved to the database in a low disk space condition.
- .

Application Analytics/Purview™

- Increased search capability for locations: The algorithm for location search has been 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 appliance: Added the ability to limit the number of end systems reported per appliance to ensure

the database does not fill with data from one appliance and not persist data from the other appliances.

- 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 has 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.

Identity and Access/NAC

- 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.
- 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 Identity and Access reporting: Updated the Total End-Systems Seen Last 24 Hrs chart in the Identity and Access 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: Extreme Control Center now prompts users 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 NAC Appliances: NAC Appliances now support the RADIUS dictionary file for Checkpoint Firewalls.
- 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.
- Improvement to Identity and Access email functionality: Identity and Access 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: Identity and Access now differentiates between the DHCP fingerprint for Apple TV and the fingerprint for iOS.
- Support for legacy devices deprecated in ECC version 7.0 release: The following end-of-service legacy devices are no longer being supported in Extreme Control Center version 7.0:
  - SNS-TAG-LPA
  - SNS-TAG-HPA
  - SNS-TAG-ITA

Wireless

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

Known Issues Addressed

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

Extreme Control 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 has been disabled on upgrade due to PCI compliance vulnerability.	------
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
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 has been 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
Identity and Access/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
Identity and Access 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.	------
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 OneView 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 OneView 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
Application Analytics 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 appliances 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.	------
Wireless Manager Issues Addressed	**ID**
Failure to process client events occasionally caused high memory utilization on the server.	01175837 1174756

Vulnerabilities Addressed

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

- The following vulnerabilities were addressed in the Extreme Control Center, Identity and Access, and Application Analytics appliance 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-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 Control Center (ECC) version 7.0 only runs on a 64-bit appliance image. Any ECC or Identity and Access (I&A) appliance 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 appliance OS and upgrade procedures can be found in the *Migrating or Upgrading to a 64-bit Extreme Control Center Appliance* document or the *Upgrading to a 64-bit Identity and Access Appliance* document available on the ECC (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 > ECC (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 Control Center Server and Client OS Requirements

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

IMPORTANT: Beginning in ECC version 7.0, only 64-bit operating systems are officially supported on the ECC server and remote ECC client machines. Any ECC server or client machine currently running a 32-bit OS must be upgraded to a 64-bit OS.

- Windows 64-bit (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 64-bit
  - 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® 64-bit (remote ECC client only)
  - Lion
  - Mountain Lion
  - Mavericks
  - Yosemite
- VMware® (64-bit ECC Virtual Appliance)
  - VMware ESXi™ 5.0 server
  - VMware ESXi™ 5.1 server
  - VMware ESXi™ 5.5 server
  - VMware ESXi™ 6.0 server

Extreme Control Center Server and Client Hardware Requirements

These are the hardware requirements for the ECC server and ECC client machines.

Extreme Control Center Server

	Minimum	Medium	Large	Enterprise
Operating System	64-bit Desktop • Windows • Ubuntu • Red Hat • SUSE	64-bit Desktop • Windows • Ubuntu • Red Hat • SUSE	64-bit Server • Ubuntu • Red Hat • SUSE	64-bit Ubuntu Server
CPU	Dual Core	Quad Core	Dual Quad Core	Dual Hex Core
Memory	2 GB	8 GB	12 GB	24 GB
Free Disk Space	10 GB	40 GB	100 GB	Greater than 100 GB
Storage Capacity	NA	NA	NA	Dual 1 TB hard drives with RAID controller

Extreme Control 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

Virtual Appliance Requirements

VMWare:

The ECC, I&A, and Application Analytics virtual appliance 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.

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

The ECC, I&A, and Application Analytics virtual appliances support a disk format of VHDX.

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

The ECC, I&A, and Application Analytics virtual appliances use the following resources from the server on which they are installed:

- I&A virtual appliance — configured with 12 GB of memory, four CPUs, two network adapters, and 40 GB of thick-provisioned hard drive space.
- ECC virtual appliance — configured with 8 GB of memory, four CPUs, one network adapter, and 100 GB of thick-provisioned hard drive space.

- Application Analytics virtual appliance — configured with 8 GB of memory, four 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 appliance.

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.

Identity and Access Agent OS Requirements

These are the supported operating systems for end-systems connecting to the network through an Extreme Networks I&A 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

Identity and Access Appliance Version Requirements

For complete information on I&A appliance version requirements, see the Upgrade Information section of these Release Notes.

Identity and Access VPN Integration Requirements

This section lists the VPN concentrators that are supported for use in I&A 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 I&A 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.

Identity and Access SMS Gateway Requirements

The following SMS Gateways have been tested for interoperability with I&A:

- Clickatell
- Mobile Pronto

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

Identity and Access SMS Text Messaging Requirements

The following mobile service providers are supported by default for SMS text messaging in a I&A 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 Control Center Browser Requirements

The following web browsers are supported for ECC:

- Internet Explorer versions 10 and 11
- Mozilla Firefox 34 and later
- Google Chrome 33.0 and later

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.

Extreme Control Center and Wireless Manager Requirements

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

IMPORTANT: ECC 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 ECC license.

Installation Information

When you purchased Extreme Control Center (ECC), you received a Licensed Product Entitlement ID that allows you to generate a product license key. Prior to installing ECC, 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 ECC (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 ECC 7.0 (not an upgrade), if you restore a database from ECC 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 ECC 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 ECC Console, the installation program saves copies of any FlexViews that you have created or modified in the <install directory>\NetSight\.installer\backup\current\appdata\System\FlexViews folder.

Evaluation License

If you have requested a ECC 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 Control Center Installation Guide* for instructions on upgrading your evaluation license.

Upgrade Information

Extreme Control Center (ECC) 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 ECC 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 appliances, you must first perform the ECC upgrade to version 7.0 and then add the Application Analytics appliances.
- If you are running Data Center Manager (DCM), a Mobile Device Management (MDM) integration, or other OneFabric Connect or Fusion integration with ECC:
    - The OneFabric connect module is disabled after upgrading and requires a new version in order to operate with ECC 7.0. You must install an updated module that supports ECC 7.0. Contact your account team for information on obtaining this update.
    - You must install a ECC (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 ECC (NetSight) Advanced (NMS-ADV) license. Contact your account team for information on obtaining this license.
- When upgrading a 64-bit ECC server or when upgrading from a 32-bit to a 64-bit ECC server, if the -Xmx setting is set below 1536m, it increases to 1536m.
- Older ECC licensing keys (starting with INCREMENT) are no longer supported as of ECC 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 ECC 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 ECC 6.1, the I&A captive portal was enhanced to provide a more modern look and feel. If you have 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 a I&A administrators to the screen preview page (https://<I&A appliance IP>/screen_preview) of the I&A 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 ECC NAC Manager 7.0, you are not required to upgrade your I&A appliance version to 7.0. However, both ECC NAC Manager and the I&A appliance must be at version 7.0 in order to take advantage of the new I&A 7.0 features. ECC NAC Manager 7.0 supports managing I&A appliance versions 6.3, 6.2, 6.1, 6.0, and 5.1.

NOTE: I&A 7.0 is not supported on the 2S Series and 7S Series I&A Controllers. You cannot upgrade I&A Controllers to version 7.0, but you can use NAC Manager 7.0 to manage controllers running version 4.3.xx.

You can download the latest I&A appliance version at the ECC (NetSight) (NMS) Download web page http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx. Be sure to read through the *Upgrading to Identity and Access7.0* document (available on the ECC (NetSight) Documentation web page > Manuals & Release Notes > NetSight 7.0 > Network Access Control [NAC]) for important information.

In addition, if your I&A solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 7.0 if you upgrade to the I&A appliance 7.0. Version 7.0 of the assessment agent adapter requires an operating system with a 64-bit architecture.

Agent Version for Identity and Access Agent-Based Assessment

If you are using onboard agent-based assessment, be aware that the agent version is upgraded during the I&A appliance 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 I&A appliance 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 ECC server. If you are using the NAC Request Tool, you will need to upgrade your version of the NAC Request Tool to version 7.0.

Upgrade Considerations for OneView 7.0

- Beginning in 5.1, all OneView 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. OneView maps created in ECC 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 OneView 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 ECC 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 ECC client.

Configuration Considerations

Firewall Considerations

- The Extreme Control Center (ECC) 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 ECC client applications.
- Port 8443 (Default HTTPS traffic) must be accessible through firewalls for clients to access the ECC Server Administration web pages, ECC, and Identity and Access (I&A) Dashboard.
- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the I&A Appliance Administration web pages.
- The following ports must be accessible through firewalls for the ECC Server and a I&A appliance 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 I&A appliance to I&A appliance communication:
  TCP: 8444
- The following ports must be accessible through firewalls for I&A appliance-to-I&A appliance 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 I&A assessment agent to every I&A appliance in order to support agent mobility:
  TCP: 8080, 8443

- The following ports must be accessible through firewalls for the ECC Server and Wireless Controllers to communicate:
  SSH: 22
  SNMP: 161, 162
  Langley: 20506
- The following ports must be accessible through firewalls for the ECC Server and WAS to communicate:
  TCP: Port 8443 — Used by WAS to authenticate ECC users. This port corresponds to ECC's HTTPs Web Server port.
  TCP: Port 443 — Import data from ECC into WAS.
  TCP: Port 8080 — Upgrade WAS from WAS UI.
- The following ports must be accessible (bi-directionally) through firewalls for the ECC Server and an Application Analytics appliance to communicate:
  TCP: Ports 4530-4533, 4589, 8080, 8443
  UDP: Ports 161, 162
  To Application Analytics appliance:
  UDP: Port 2055 (NetFlow)
  TCP: 22, 8443

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

Supported MIBs

The following directory contains the IETF and Private Enterprise MIBs supported by Extreme Control Center applications:
<install directory>\NetSight\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 Control Center software products and product information.

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

Extreme Networks Support

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods.

Web	www.extremenetworks.com/support/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks Support phone number in your country: www.extremenetworks.com/support/contact/
Email	support@extremenetworks.com

04/2016
P/N: 9034967
Subject to Change Without Notice