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

Customer Release Notes

Extreme Networks NetSight®

Version 6.3.0.168
October, 2015

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

NetSight is distinguished by web-based OneView™, the unified control interface. Graphical and exceptionally easy-to-use, OneView simplifies troubleshooting, help desk support tasks, problem-solving and reporting. Its Identity and Access interface provides specialized visibility and control for managed and unmanaged devices connecting to the network.

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

The NetSight Release Notes provide information on the new features and enhancements included in version 6.3, 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 NetSight 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 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 > NetSight (NMS) > Documentation > Manuals & Release Notes > NetSight 6.3 > NetSight Suite.

Software Enhancements

Enhancements in NetSight 6.3

This section presents the new features and enhancements that were included in NetSight 6.3.

NetSight Suite

- **Deprecated 32-bit appliance installers:** Discontinued build and release of 32-bit appliance installers for NetSight, NAC, and Purview.
- **Upgrade warning:** Added a warning to protect against invalid upgrades from 32-bit server installations to 64-bit server installation on Windows operating systems.
- **OneView NMS-BASE License changes:** NMS-BASE license upgraded to include the application-level Search feature, accessed by clicking on the magnifying glass icon in the main toolbar. Additionally, the End-Systems table, End-Systems Events view, and a limited End-Systems Details view in the Identity and Access tab are now available with the NMS-BASE license.
- **OneView NMS-XX License change:** NMS-XX license upgraded to include support for virtual NAC appliances.
- **New Basic OneView license type:** A new basic OneView license type (NMS-BASE-5) is added. This license provides support for management of 5 devices and 50 APs.
- **Trap processing:** Improved trap processing to make traps easier to read.
- **VMWare ESXi 6.0:** Added support for VMWare ESXi version 6.0.

Device Support

- **Support for new Extreme access point:** Added support for Extreme AP 3801i.
- **Support for new Extreme controller:** Added support for Extreme controller C35.
- **Support for new Extreme switch:** Added support for Extreme Summit X450G2.

OneView

- **Stack modules displayed in Device Summary in DeviceView:** The Device Summary section of DeviceView now displays the names of all modules in stacks.

- **Ability to view VLAN data in OneView:** OneView can now display VLAN data from devices. Additionally, selecting a VLAN associated with devices added to a map highlights the devices within the map.
- **VLAN provisioning for ExtremeXOS devices in OneView:** OneView now contains VLAN provisioning functionality for ExtremeXOS devices.
- **Improvement to viewing EAPS data in OneView:** Added the EAPS detail view, which displays all EAPS data from the EAPS tab of the Network Details section within a map.
- **Viewing shared and blocked EAPS links in maps:** Shared and blocked EAPS links are now highlighted in maps when highlighting EAPS domains.
- **Improved map links:** Improved map links to represent the state of links/ports in a map, which are updated dynamically.
- **EAPS topology map links:** Topology map links included in EAPS rings are now highlighted when selecting the EAPS ring.
- **MLAG pair searching:** Searching for an end-system to which a pair of MLAG-connected switches are connected now highlights both switches in a map, if the switches are added to the map.
- **Alarm Manager functionality in OneView:** OneView now allow configuration of all alarm types available in Alarm Manager.
- **Define areas in maps:** Added support for defining areas on a map to enable the area location feature on the wireless controller.
- **Export maps in SVG format:** Added the ability to export that which is currently visible in a map viewpoint to an SVG image format.
- **Improved device upgrade functionality in OneView:**
  - **Ability to upgrade Firmware:** Added the ability to upgrade device Firmware on the Devices tab in OneView. You can perform upgrades immediately or schedule it at a later time. Additionally, multiple ExtremeXOS devices can be updated simultaneously.
  - **Ability to upgrade BootPROM:** Added the ability to upgrade BootPROM on the OneView Devices tab.
  - **Ability to configure firmware download options:** Added the ability to configure the following for a device in OneView:
    - The file transfer mode.
    - The MIB and Script File settings for firmware and configuration.
    - The firmware download server.

- **OneView theme improvements:** OneView now features improved load and response time performances, as well as theming and usability enhancements to provide a better overall user experience.
- **Improved controller and Purview appliance integration:** OneView now allows you to enable or disable the integration of a controller with a Purview appliance to provide application visibility into the wireless network. This enables customers to understand the user, device, and application without the need of adding specialized equipment into the network.
- **Enhanced OneView reporting capabilities:** Enhanced reporting capabilities in OneView to allow the addition of items to the primary navigation bar.
- **New OneView reports:** Added new OneView reports:
  - Added Top 100 Interfaces by Bandwidth Daily report.
  - Added **Weekly** option for the Master Detail report.
- **Ability to add ports in DeviceView:** Ports can now be added to device groups from the DeviceView/Port Tree view in the OneView Devices tab.
- **Support for Ekahau Floor Plan map format:** OneView maps now support Floor Plan maps imported from Ekahau version 7.x.
- **Enhanced Wireless Controller Summary:** The OneView Wireless Controller Summary Report on the Wireless tab in OneView now contains a pie chart displaying the top Clients by WLAN.
- **Improvement to retrieving information:** Added NetSightDeviceWebService methods for retrieving switch and port information from NetSight nsportdata table, allowing users to query ports by serial number or by an nsportdata column-specific filter.
- **Configure devices in OneView:** OneView now allows you to change the device profile setting for selected devices in the device table.

Inventory Management

- **Improvement to retrieving information:** Added NetSightDeviceWebService methods for retrieving port and module information from devices modeled in NetSight.

Policy Manager

- **Policy Manager support for ExtremeXOS:** Added Policy Manager support for the new ExtremeXOS 16.1 firmware, which adds support for policy. This includes policy profile management, as well as QoS (class of service), authentication, and RADIUS configuration.

- **Policy Manager support for RADIUS MIB functionality:** Added Policy Manager support for RADIUS MIB enhancements made to support existing ExtremeXOS features. This includes the ability to add DNS servers, realm-specific status and settings (Network Access/Management), and specifying a management interface (Virtual Router) to egress the RADIUS requests.
- **Policy Manager rule enhancements:** Added Policy Manager rule and role default support for for firstN traffic mirrors to physical ports on wireless controllers running v9.21 FW and later. Note, only a single physical port may be specified in the mirror configuration. VNS and multiple physical ports are unsupported, as is mirroring all packets.

Purview™

- **Reputation Feed in Purview:** A new report in Purview displays IP addresses of end-systems to which your trusted devices connect a reputation feed identifies as untrustworthy. The reputation feed classifies IP addresses based on the reason they are suspicious.
- **Application ID Browser export as CSV:** Enhanced the OneView Application Browser view to export results in CSV format.
- **Policy rule creation enhancements in Purview:** Added the ability to provide a rule name when creating a Policy Manager rule from a flow on the Application > Flows tab in OneView. Leaving the name blank uses the traffic description as the name. Additionally, once the rule is created, the success dialog window now contains a button to open the domain in a new tab, which automatically opens the new rule.
- **Controllers included as flow sources:** Extreme Wireless Controllers are now supported as Purview flow sources.

IAM/NAC

- **Send messages from NAC Manager to end-systems:** Added the ability to send a message via a drop-down menu in the NetSight NAC Manager's End-System table to one or more end-systems with agent-based assessment configured.
- **Bypass Welcome Page:** Added the ability to bypass the NAC Captive Portal Welcome Page via a new checkbox in the Network Settings panel in NAC Manager.
- **Improved ability to manage NAC functionality in OneView:** Added the ability to manage the following NAC functionality on the Identity and Access tab in OneView:
    - RADIUS servers
    - LDAP configurations

  - Basic and advanced AAA configurations
  - Editing and deleting switches
  - LDAP OU imports for LDAP user groups
  - LDAP host groups
- **Improvement to the Mobile Captive Portal:** The Mobile Captive Portal now provides an improved experience on phones with the Windows 8.x operating system.
- **Inject RADIUS attributes:** Added the ability to configure the injection of attributes into RADIUS requests or accounting packets.
- **Improved reporting in NAC end-system tables:** NAC end-system tables now display information from OneFabric Connect.
- **Enhanced Agent detection for installed programs:** The Assessment Agent can now detect installed programs registered in the Add/Remove Programs or Programs and Features list on a Windows operating system or in standard install locations the on a Mac operating system.
- **RADIUS configuration on ExtremeXOS switches:** Added support for RADIUS configuration via NAC Manager on ExtremeXOS switches running firmware version 16.1 or later.
- **NAC appliance alarms:** Added a feature to monitor NAC appliance certificates that generates a NetSight alarm notice when a certificate is 30 days from expiring, an alarm warning when the certificate is 7 days from expiring and a critical alarm when the certificate expires. The notice and warning times can be overridden via NAC properties and the Certificate monitor runs when the appliance is initialization or is enforced and reschedules itself to run weekly or shortly after the next alarm time is expected.
- **Enhanced NAC Manager interface:** When adding APs to a location based group in NAC Manager, the entry area is now resizable and scrollable to facilitate adding a large number of AP IDs to the group.
- **Added Policy support in Identity and Access tab:** Policy configuration support is now available in the Configuration view on the Identity and Access tab in OneView. Policy is accessed via a right-click menu on a selected switch.
- **NAC LDAP enhancement:** Enhanced NAC's LDAP configuration to automatically disable de-referencing aliases when connecting to Novel E-Directory.
- **Session timeout support:** Added support to NAC to allow session timeouts to be applied via CoA if the device is an IdentiFi wireless controller running firmware version 9.21 or higher.

- **New Captive Portal languages:** Added Captive Portal language files for Russian and Romanian.
- **Enhanced Captive Portal diagnostics:** NAC Captive Portal now contains enhanced diagnostics for customers with advanced location portals.

Wireless

- **Support for additional statistics:** OneView Wireless now provides support for 10 additional bandwidth statistics.
- **Increased client support:** OneView and Wireless Manager now support 30,000 clients.
- **NetSight support for controllers:** NetSight version 6.3 only supports the configuration of 8.32 or later controllers and now supports controllers running IdentiFi Wireless version 9.21.
- **Simplified certificate workaround for Adaptive UI:** When accessing the controller GUI through the Adaptive UI from either OV or Wireless Manager a 'Fix' button has been added to help automate the changes needed to resolve the the certificate warnings for Google Chrome and Mozilla Firefox browsers.
- **IdentiFi Wireless C35 Controller:** A high performance mid-level wireless appliance capable of managing 125 APs and 2,000 users in standalone mode, and 250 APs and 4,000 users in availability mode. Intended to replace the C25.
- **Support for IdentiFi Wireless AP3801i i/e APs:** A fully featured 2x2:2 single radio 802.11 ac/an/bgn AP with configurable single radio (2.4GHz or 5GHz), 1 GE interface, and 802.3af/PoE compliant.
- **Elastic Virtual IdentiFi Wireless Appliance for VMware:** Added support for the elastic virtual appliance that can be scaled in terms of users and APs by adjusting the resources allocated to it by the host system. Supports up to 525 APs and 4,096 users in standalone mode, and 1,050 and 8,192 users in availability mode.
- **Added Configuration Support for the following:**
  - **802.11k Radio Management:** Enables client stations to understand the radio environment in which they exist so they have more information to make decisions about roaming and performance, improving the distribution of traffic within the wireless network. Supported on 37xx and 38xx series APs.
  - **'Triangulated' Location Area:** An area notification feature designed to work in conjunction with the new area notification feature that tracks client locations within areas defined on maps in OneView. Now when a client roams between areas you define, the controller can be configured to send a notification to NAC so it can be used to apply different policies to users

based on their physical area. These events can also be seen from the OneView >> Wireless >> ‘Clients’ and ‘Client Events’ tabs.

- **Intelligent RF Medium Control:** Reduces the aggregate amount of probe responses transmitted by APs through inter-AP communication improving network performance. Designed for use in high density wireless deployments like stadiums, arenas, lecture halls, lobbies, and large common areas
- **WMM-Admission control:** Added additional support for 'best effort' and 'background' access categories for prioritizing traffic to provide enhanced multimedia support. Using WMM-Admission Control improves the reliability of multimedia applications such as VoIP and video by preventing over subscription of bandwidth.
- **VLAN Pooling on IdentiFi Controllers:** Introduces the ability to distribute wireless load across subnets via multiple selection mechanisms reducing the broadcast domain and improving performance. This new capability is useful in high density deployments that are using a centralized topology. Supported for 'routed' and 'bridged-at-controller' topologies.
- **802.11r Fast Transition:** Eliminates much of the handshaking overhead while roaming, reducing the handoff times between APs while providing security and QoS. Useful for client devices with delay-sensitive applications that use voice and/or video. Supported on 37xx and 38xx series APs.
- **802.11w WiFi Protected Management Frames:** Improves security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection. Supported on 37xx and 38xx series APs.
- **RADIUS enhancements:** Added the ability to configure whether:
  - The RADIUS accounting is disabled globally on a controller regardless of the RADIUS accounting settings of individual WLAN services.
  - The start of RADIUS accounting is taken to be from the moment the client authenticates or from when the client gets an IP address.
  - The Service-Type attribute in the RADIUS Access-Request message should be set to 'Framed' or 'Login'.
  - The 'Framed-IP-Netmask' attribute should be added to all RADIUS accounting requests.
  - The Chargeable-User-Identity is included in RADIUS Access-Request messages and whether to treat and Access-Accept without a CUI attribute as an Access-Reject.

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.3.0.168:

NAC Manager Issues Addressed	ID
Corrected a problem with Facebook Registration where the user's information could not be retrieved and causing the Registration to only contain the user's Facebook identifier.	------
Fixed an issue where on enabling network access for RADIUS on switch, and no management servers are configured, management was not being disabled, and if enabling management without configuring servers through NAC, management was NOT being enabled.	01157133
Fixed an issue where deleted end-systems reappear if the deleted events are received before a local cached has removed those end-systems.	------
OneView Issues Addressed	**ID**
Added new [XOS System Configuration] FlexView allowing read/write support for this MIB table.	01145287
Corrected an issue where renderers reused model names, causing an error when combining FlexView reports.	1147459
Updated 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.	------
Fixed an issue where a null pointer exception would occur when sorting by response times in the Application(Analytics) reports.	------
Policy Manager Issues Addressed	**ID**
Fixed an issue with Policy Manager enforce of UDP/TCP source/destination rules that contained an IPv4 address. The rule would be written with an incorrect address and significant bits mask.	01158869
Fixed an issue where enabling PWA authentication and opting to set uplink ports to inactive/default role would set drop VLAN tagged frames to enabled. This could cause loss of connectivity from the device to the network.	------
Purview Issues Addressed	**ID**
Corrected an issue where some of the top clients for the top 100 applications were not persisted in the NetSight database for any hour.	------

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.3.0.162:

OneView Issues Addressed	ID
Corrected a problem where a error/exception on the server would cause stale data on the server.	01148219
Corrected a problem in VLAN Provisioning where a VLAN could not be modified.	1149354

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.3.0.158:

NetSight Suite Issues Addressed	ID
Corrected Network Monitor Cache interface parse out of bounds caused by varbind level error that is now checked before parsing the results.	1141655
Inventory Manager Issues Addressed	**ID**
Corrected an issue with firmware discovery with the 800-series firmware.	1141047
Policy Manager Issues Addressed	**ID**
Added support for dashes in VLAN names when written to ExtremeXOS devices, which now display a warning dialog when other unsupported characters are removed.	1145660
Fixed an issue that prevented rules from being successfully enforced to legacy devices.	------
NAC Manager Issues Addressed	**ID**
Corrected an issue where the Policy Domain field would be grayed out for ExtremeXOS switches.	01146034
Corrected an agent-based test-set editing issue where test-sets created for Windows 10 in NetSight 6.2 could not be edited.	------
Corrected an issue where NAC authentication would not fail over to a secondary proxy RADIUS server when the primary RADIUS server was not reachable.	------
Extreme AP38251's are now detected properly with DHCP fingerprinting and are no longer detected as an Amazon Kindle.	1141055
Janam barcode scanners are now detected properly with DHCP fingerprinting and are no longer detected as a Slingbox.	01141094
OneView Issues Addressed	**ID**
Corrected a formatting issue seen when displaying DHCP Fingerprints in OneView.	1141194

This section presents the known issues that were addressed in NetSight 6.3.0.142:

NetSight Suite Issues Addressed	ID
Corrected an issue where physical interfaces were incorrectly ordered if a 10 GB fiber card was installed.	------

Corrected an issue where the presence of a VLAN interface on a DFE prevented any ports from being stored in the network monitor cache. This prevented any port views in NetSight relying on the cache from displaying the ports for that device.	1122621
Corrected an issue with excessive reads of licenses from the file system. Additional code was added to ensure that a license status is read from a cached value for both licensed and unlicensed features before attempting to read the license from the file system.	------
Corrected an issue where RedHat version 7 installations were selecting the wrong atlas file.	------
Console Issues Addressed	**ID**
Corrected NetSight/OneView FlexView export issue where HTML export did not match CSV export. Both formats now contain identical data, as the CSV export contains data that was previously missing.	1095501 1096203
Corrected an issue where the source column in SysLog messages was not populating due to name resolution.	1095805
Corrected a problem with processing multi-line SysLog messages.	1108739
Inventory Manager Issues Addressed	**ID**
Corrected an issue where the NetSight TFTPD process crashed on 64-bit Linux operating systems with slower connections.	1122676
Corrected an issue with Inventory Manager Configuration Archive where some devices failed because a directory was not created.	01108306
Corrected an issue where Linux systems running the GNOME desktop crashed.	01108306
NAC Manager Issues Addressed	**ID**
Corrected an issue where NAC's port link control was causing NAC to re-enable ports that were disabled due to BPDUGuard.	01018380
Corrected an issue where the zone was getting cleared by session detected events.	1097892
Corrected an issue where a change to the force HTTPS option for the captive portal was not being applied when in multi-interface mode.	1082561
Corrected an issue on HPA Appliances running the Ubuntu operating system where the LCP display was not updating correctly.	------
Corrected an issue where NAC queried the entire LDAP user database when testing a restored LDAP server connection. It now correctly queries for a single user to verify the connection is restored.	1118325
Corrected an issue in the NAC AAA configuration entry editor where an AAA rule was not saved properly when changing the existing User/MAC/Host field of the AAA from the Group 'Local Repository Users' to Pattern.	------

OneView Issues Addressed	**ID**
Corrected a weak ephemeral key issue when connecting to OneView using the Developer version of Mozilla Firefox or Google Chrome version 45.	01135710
Corrected AP Summary panel data displayed for APs in Sensor or Guardian mode.	------
Corrected a problem in Scripting where output from a command was detected as a prompt, causing some of the output to be truncated.	1107077
Corrected NetSight/OneView Interface utilization calculation to include 'Duplex' mode.	1093355
Corrected rendering issues for the 'Bridge Spanning Tree' in NetSight/OneView FlexView.	01118710
Corrected an issue in the OneView End-System Seen Last 24 Hours report where end-systems were counted for the 24 hours of the previous day as well as any end-systems seen in the current day. The report now only displays end-systems within 24 hours of the current time.	------
Corrected an issue where the Device Archive report was sorting based on the time, not on the date the report was run.	1091462
Purview Issues Addressed	**ID**
Corrected an issue where misidentified flows led to incorrect usernames being extracted from the payload data.	------
Corrected an issue where Purview incorrectly calculated the average network and application response times over a period of time. For some targets, the value stored in the database was incorrect, resulting in incorrect data.	1126851
Wireless Manager Issues Addressed	**IDs**
Corrected a problem for customers using WAS in which large files ('puna_trace.xml.#') in the 'NetSight\appdata\logs\bk_third_party' folder were consuming excessive disk space.	1123513 1129072 1133111 1136648 1136847

Vulnerabilities Addressed

This section presents the Vulnerabilities that were addressed in NetSight 6.3.0.168:

- The following vulnerabilities were addressed in the NetSight, NAC, and Purview appliance images:
  - CVE-2014-9087, CVE-2012-6656, CVE-2014-6040, CVE-2014-7817, CVE-2014-8767, CVE-2014-8768, CVE-2014-8769, CVE-2014-9140, CVE-2014-2653, CVE-2014-7209, CVE-2014-2532, CVE-2010-0624, CVE-2014-9112, CVE-2009-4135, CVE-2014-9471, CVE-2014-9447, CVE-2014-8142, CVE-2014-9427, CVE-2014-9652, CVE-2015-0231, CVE-2015-0232, CVE-2015-1351, CVE-2015-1352, CVE-2014-9656, CVE-2014-9657, CVE-2014-9658, CVE-2014-9659, CVE-2014-9660, CVE-2014-9661, CVE-2014-9662, CVE-2014-9663, CVE-2014-9664, CVE-2014-9665, CVE-2014-9666, CVE-2014-9667, CVE-2014-9668, CVE-2014-9669, CVE-2014-9670, CVE-2014-9671, CVE-2014-9672, CVE-2014-9673, CVE-2014-9674, CVE-2014-9675, CVE-2015-1315, CVE-2014-5351, CVE-2014-5352, CVE-2014-5353, CVE-2014-5354, CVE-2014-9421, CVE-2014-9422, CVE-2014-9423, CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2013-7439, CVE-2015-0261, CVE-2015-2153, CVE-2015-2154, CVE-2015-2155, CVE-2014-0191, CVE-2014-4617, CVE-2013-7345, CVE-2014-0207, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3538, CVE-2014-5461, CVE-2014-5270, CVE-2014-3587, CVE-2014-3660, CVE-2014-9029, CVE-2014-7824, CVE-2013-6629, CVE-2013-6630, CVE-2014-5270, CVE-2012-1571, CVE-2014-1943, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206, CVE-2014-8139, CVE-2014-8140, CVE-2014-8141, CVE-2014-8150, CVE-2014-6272, CVE-2013-4576, CVE-2012-0950, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4147, CVE-2015-4148, CVE-2015-4598, CVE-2015-4599, CVE-2015-4600, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE-2015-4643, CVE-2015-4644, CVE-2010-4651, CVE-2014-9637, CVE-2015-1196, CVE-2015-1395, CVE-2015-1396, CVE-2015-0247, CVE-2015-1572, CVE-2013-1064, CVE-2013-1752, CVE-2013-1753, CVE-2014-4616, CVE-2014-4650, CVE-2014-7185, CVE-2014-3565, CVE-2015-5621, CVE-2015-5352, CVE-2015-5600, CVE-2013-7443, CVE-2015-3414, CVE-2015-3415 CVE-2015-3416, CVE-2013-1066, CVE-2013-4314

This section presents the Vulnerabilities that were addressed in NetSight 6.3:

- The following vulnerabilities were addressed in the NAC appliance image:
    - CVE-2012-3509, CVE-2014-8484, CVE-2014-8485, CVE-2014-8501, CVE-2014-8502, CVE-2014-8503, CVE-2014-8504, CVE-2014-8737, CVE-2014-8738, CVE-2010-2810, CVE-2012-5821
- The following vulnerabilities were addressed in the NAC and Purview appliance images:
    - CVE-2014-8161, CVE-2015-0241, CVE-2015-0243, CVE-2015-0244, CVE-2015-1802, CVE-2015-1803, CVE-2015-1804, CVE-2014-0075, CVE-2014-0096, CVE-2014-0099, CVE-2014-0119, CVE-2013-2067
- The following vulnerabilities were addressed in the NetSight, NAC, and Purview appliance images:
    - CVE-2014-9087, CVE-2012-6656, CVE-2014-6040, CVE-2014-7817, CVE-2014-8767, CVE-2014-8768, CVE-2014-8769, CVE-2014-9140, CVE-2014-2653, CVE-2014-7209, CVE-2014-2532, CVE-2010-0624, CVE-2014-9112, CVE-2009-4135, CVE-2014-9471, CVE-2014-9447, CVE-2014-8142, CVE-2014-9427, CVE-2014-9652, CVE-2015-0231, CVE-2015-0232, CVE-2015-1351, CVE-2015-1352, CVE-2014-9656, CVE-2014-9657, CVE-2014-9658, CVE-2014-9659, CVE-2014-9660, CVE-2014-9661, CVE-2014-9662, CVE-2014-9663, CVE-2014-9664, CVE-2014-9665, CVE-2014-9666, CVE-2014-9667, CVE-2014-9668, CVE-2014-9669, CVE-2014-9670, CVE-2014-9671, CVE-2014-9672, CVE-2014-9673, CVE-2014-9674, CVE-2014-9675, CVE-2015-1315, CVE-2014-5351, CVE-2014-5352, CVE-2014-5353, CVE-2014-5354, CVE-2014-9421, CVE-2014-9422, CVE-2014-9423, CVE-2015-0209, CVE-2015-0286, CVE-2015-0287, CVE-2015-0288, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2013-7439, CVE-2015-0261, CVE-2015-2153, CVE-2015-2154, CVE-2015-2155, CVE-2014-0191, CVE-2014-4617, CVE-2013-7345, CVE-2014-0207, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3538, CVE-2014-5461, CVE-2014-5270, CVE-2014-3587, CVE-2014-3660, CVE-2014-9029, CVE-2014-7824, CVE-2013-6629, CVE-2013-6630, CVE-2014-5270, CVE-2012-1571, CVE-2014-1943, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206, CVE-2014-8139, CVE-2014-8140, CVE-2014-8141, CVE-2014-8150, CVE-2014-6272, CVE-2013-4576, CVE-2012-0950, CVE-2015-3411, CVE-2015-3412, CVE-2015-4021, CVE-2015-4022, CVE-2015-4024, CVE-2015-4025, CVE-2015-4026, CVE-2015-4147, CVE-2015-4148, CVE-2015-4598, CVE-2015-4599, CVE-2015-4600, CVE-2015-4601, CVE-2015-4602, CVE-2015-4603, CVE-2015-4604, CVE-2015-4605, CVE-2015-4643, CVE-2015-4644, CVE-2010-4651, CVE-2014-9637, CVE-2015-1196, CVE-2015-1395, CVE-2015-1396, CVE-2015-0247, CVE-2015-1572, CVE-2013-1064, CVE-2013-1752, CVE-2013-

1753, CVE-2014-4616, CVE-2014-4650, CVE-2014-7185, CVE-2014-3565, CVE-2015-5621, CVE-2015-5352, CVE-2015-5600, CVE-2013-7443, CVE-2015-3414, CVE-2015-3415 CVE-2015-3416

System Requirements

IMPORTANT: NetSight version 6.3 only runs on a 64-bit appliance image. Any NetSight or NAC appliance currently running a 32-bit OS image must be upgraded to the newer 64-bit image prior to upgrading to 6.3.

Instructions on determining your appliance OS and upgrade procedures can be found in the *Migrating or Upgrading to a 64-bit NetSight Appliance* document or the *Upgrading to a 64-bit NAC Appliance* document available on the 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 > NetSight (NMS) > Documentation > Manuals & Release notes > NetSight 6.3 > Network Access Control (NAC) and NetSight Appliances. Please contact Extreme Networks Support with any questions.

NetSight Server and Client OS Requirements

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

IMPORTANT: Beginning in NetSight version 6.4, only 64-bit operating systems will be officially supported on the NetSight server and remote NetSight client machines. Any NetSight server or client machine currently running a 32-bit OS must be upgraded to a 64-bit OS.

- **Windows 32-bit** (qualified on the English version of the operating systems)
  - Windows Server® 2008 Enterprise
  - Windows Server® 2008 R2
  - Windows® 7
  - Windows® 8 and 8.1
- **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 32-bit**
  - Red Hat Enterprise Linux WS and ES v5 and v6
  - SuSE Linux versions 10, 11, and 12.3
  - Ubuntu 11.10 Desktop version (remote NetSight client only)
- **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 NetSight client only)
  - Lion
  - Mountain Lion
  - Mavericks
  - Yosemite
- **VMware®** (64-bit NetSight Virtual Appliance)
  - VMware ESXi™ 5.0 server
  - VMware ESXi™ 5.1 server
  - VMware ESXi™ 5.5 server
  - VMware ESXi™ 6.0 server

NetSight Server and Client Hardware Requirements

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

NetSight Server

	Minimum	Medium	Large	Enterprise
Operating System	64-bit Desktop • Windows • Ubuntu • Red Hat • SUSE 32-bit Windows (support is deprecated after release 6.3).	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

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

Virtual Appliance Requirements

VMWare:

The NetSight, NAC, and Purview 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: 4.0, 4.1, 5.0, 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 NetSight, NAC and Purview virtual appliances support a disk format of VHDX.

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

The NetSight, NAC, and Purview virtual appliances use the following resources from the server they are installed on:

- NAC virtual appliance – configured with 12 GB of memory, four CPUs, two network adapters, and 40 GB of thick-provisioned hard drive space.
- NetSight virtual appliance – configured with 8 GB of memory, four CPUs, one network adapter, and 100 GB of thick-provisioned hard drive space.
- Purview 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.

NAC Agent OS Requirements

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

NAC Appliance Version Requirements

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

NAC VPN Integration Requirements

This section lists the VPN concentrators that are supported for use in NAC 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 NAC 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.

NAC SMS Gateway Requirements

The following SMS Gateways have been tested for interoperability with NAC:

- Clickatell
- Mobile Pronto

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

NAC SMS Text Messaging Requirements

The following mobile service providers are supported by default for SMS text messaging in a NAC 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	

OneView Browser Requirements

The following web browsers are supported for OneView:

- 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.

OneView and Wireless Manager Requirements

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

IMPORTANT: NetSight version 6.3 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 NetSight license.

Installation Information

When you purchased NetSight, you received a Licensed Product Entitlement ID that allows you to generate a product license key. Prior to installing NetSight, 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 NetSight (NMS) Documentation web page: http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx.

Important Installation Considerations

Important Requirement for Inventory Manager 6.3

Following a new installation of NetSight 6.3 (not an upgrade), if you restore a database from NetSight version 5.1 or earlier, you will 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 NetSight 6.3 installation directory. If you don't do this, your Inventory Manager data including capacity reports, configuration templates, and property files will be stored in the wrong directory.

Custom FlexViews

When re-installing NetSight 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 NetSight evaluation license, you will 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 *NetSight Installation Guide* for instructions on upgrading your evaluation license.

Upgrade Information

NetSight 6.3 supports upgrades from NetSight 6.2, 6.1, 6.0, and 5.1. If you are upgrading from a NetSight version prior to 5.1, you must perform an intermediate upgrade. For example, if you are upgrading from NetSight 5.0, you must first upgrade to NetSight 5.1, and then upgrade to NetSight 6.3.

IMPORTANT: When performing an upgrade, be sure to backup the NetSight 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 Purview appliances, you must first perform the NetSight upgrade to version 6.3 and then add the Purview appliances in OneView.
- If you are running Data Center Manager (DCM), a Mobile Device Management (MDM) integration, or other OneFabric Connect or Fusion integration with NetSight:
    - The OneFabric connect module is disabled after upgrading and requires a new version in order to operate with NetSight 6.3. You must install an updated module that supports NetSight 6.3. Contact your account team for information on obtaining this update.
    - You must install a NetSight Advanced (NMS-ADV) license with 6.3 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 NetSight Advanced (NMS-ADV) license. Contact your account team for information on obtaining this license.
- When upgrading a 64-bit NetSight server or when upgrading from a 32-bit to a 64-bit NetSight server, if the -Xmx setting is set below 1536m, it is increased to 1536m.
- Older NetSight 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 4.xx version of the NAC Request Tool is not compatible with the 6.3 NetSight server. If you are using the NAC Request Tool you will need to upgrade the version of NAC Request Tool to version 6.3.

Upgrade Considerations for NAC Manager 6.3

Important Captive Portal Changes

In NetSight 6.1, the NAC 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 NAC administrators to the screen preview page (https://<NAC appliance IP>/screen_preview) of the NAC 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 NetSight NAC Manager 6.3, you are not required to upgrade your NAC appliance version to 6.3. However, both NetSight NAC Manager and the NAC appliance must be at version 6.3 in order to take advantage of the new NAC 6.3 features. NetSight NAC Manager 6.3 supports managing NAC appliance versions 6.2, 6.1, 6.0, and 5.1.

NOTE: NAC 6.3 is not supported on the 2S Series and 7S Series NAC Controllers. You cannot upgrade NAC Controllers to version 6.3, but you can use NAC Manager 6.3 to manage controllers running version 4.3.xx.

You can download the latest NAC appliance version at the NetSight (NMS) Download web page http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx. Be sure to read through the *Upgrading to NAC 6.3* document (available on the NetSight Documentation web page > Manuals & Release Notes > NetSight 6.3 > Network Access Control [NAC]) for important information.

In addition, if your NAC solution utilizes a Nessus assessment server, upgrade your assessment agent adapter to version 6.3 if you upgrade to the NAC appliance 6.3.

Agent Version for NAC Agent-Based Assessment

If you are using onboard agent-based assessment, be aware that the agent version is upgraded during the NAC 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 NAC appliance version 6.3 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 6.3 NetSight server. If you are using the NAC Request Tool, you will need to upgrade your version of the NAC Request Tool to version 6.3.

Upgrade Considerations for OneView 6.3

- 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 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 OneView maps is not consistent with data on the controller, the controller updates accordingly.

Upgrade Considerations for Policy Manager 6.3

- Policy Manager 6.3 only supports IdentiFi Wireless Controller version 8.01.03 and later. If you upgrade to NetSight 6.3 prior to upgrading your controllers, then Policy Manager will not allow you to open a domain where the controllers already exist or add them to a domain. You will see a dialog indicating that your controllers do not meet minimum version requirements and that 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 6.3 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 IdentiFi Wireless Controller version 8.31 and higher, a Policy Manager enforce will fail 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 6.3

Following a Wireless Manager upgrade, you should clear the Java Cache before starting the NetSight client.

Configuration Considerations

Firewall Considerations

- The NetSight 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 NetSight client applications.
- Port 8443 (Default HTTPS traffic) must be accessible through firewalls for clients to access the NetSight Server Administration web pages, NetSight OneView, and NAC Dashboard.
- Port 8444 (Default HTTPS traffic) must be accessible through firewalls for clients to access the NAC Appliance Administration web pages.
- The following ports must be accessible through firewalls for the NetSight Server and a NAC 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 NAC appliance to NAC appliance communication:
  TCP: 8444
- The following ports must be accessible through firewalls for NAC appliance-to-NAC 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 NAC assessment agent to every NAC appliance in order to support agent mobility:
  TCP: 8080, 8443
- The following ports must be accessible through firewalls for the NetSight Server and Wireless Controllers to communicate:
  SSH: 22
  SNMP: 161, 162
  Langley: 20506

- The following ports must be accessible through firewalls for the NetSight Server and WAS to communicate:
  TCP: Port 8443 – Used by WAS to authenticate NetSight users. This port corresponds to NetSight's HTTPs Web Server port.
  TCP: Port 443 – Import data from NetSight into WAS.
  TCP: Port 8080 – Upgrade WAS from WAS UI.
- The following ports must be accessible (bi-directionally) through firewalls for the NetSight Server and a Purview appliance to communicate:
  TCP: Ports 4530-4533, 4589, 8080, 8443
  UDP: Ports 161, 162
  To Purview appliance:
  UDP: Port 2055 (NetFlow)
  TCP: 22, 8443

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

Supported MIBs

The following directory contains the IETF and Private Enterprise MIBs supported by NetSight 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 NetSight software products and product information.

- For information on product licensing, visit https://extranet.extremenetworks.com/Pages/default.aspx.
- To download the latest NetSight software products, visit the NetSight (NMS) web page: http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx.
- To download previously released NetSight products, visit the NetSight (NMS) web page: http://extranet.extremenetworks.com/downloads/Pages/NMS.aspx.

- To register any NetSight 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

10/2015
P/N: 9034882-03
Subject to Change Without Notice