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

Customer Release Notes

Extreme Networks NetSight®

Version 6.2
August, 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 6.2, 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 6.2 > NetSight Suite.

Software Enhancements

Enhancements in NetSight 6.2

This section presents the new features and enhancements that were included in NetSight 6.2.

NetSight Suite

- **NetSight/NAC/Purview Virtual Appliance support on HyperV:** An option to install the virtual appliances on HyperV in addition to VMware allows more flexibility to install the virtual appliances on the desired virtual platform.
- **Automatic Trap Configuration by Device Family:** Allows automatic configuration of all supported EXOS and EOS devices to send traps to NetSight. The EXOS SmartTrap feature is also supported.
- **Ridgeline to NetSight Server Migration:** Simplifies the migration process by taking advantage of the configuration already done in Ridgeline by allowing devices and credentials configured in Ridgeline to be migrated to NetSight. The new import feature is accessed from Console File > Device List > Import Devices from Ridgeline DB Backup.
- **OneView NMS-Base License changes:** NMS-Base license upgraded to include the new scripting functionality as well as map support for EAPS, MLAG, EDP, and LLDP. NMS-Base license also includes basic map features and creation of standard maps and wireless client location based on RSS.

Device Support

- **Support for new Extreme switches:** Support for Extreme Summit X430 POE, Summit X460-G2, and Summit X670-G2.

OneView

- **Advanced Scripting Support in OneView:** New scripting functionality built into NetSight OneView allows more flexible configuration and control with devices using CLI. The scripting feature allows creation of script files that contain CLI commands, control structures, and data manipulation functions. NetSight scripts can be executed on one or more devices: simultaneously on multiple devices, or on one device at a time.

- **New OneView Topology Maps:**
  - Topology maps based on EDP and LLDP can be created, edited and displayed in OneView.
  - Logical maps for EAPS domains allow users to visualize the EAPS networks.
  - Logical maps for MLAGs allow users to visualize the network with aggregated links.
- **Network Links View in OneView:** A new Link Summary view in OneView shows link details including EAPS, MLAG, and VPLS links. This is available from OneView > Devices Tab displays inter-switch links and what protocol they were found by.
- **Policy Manager Support in OneView:** New OneView Policy Tab provides basic Policy Manager support allowing migration away from the JNLP-based Policy Manager for many tasks.
- **New Device Tree:** Added a device tree in OneView that allows easy device navigation including displaying alarm status and allowing group creation/deletion via a menu pick or drag and drop.
- **Purview Alarm Management Support:** Allows configuration of Purview alarms in the OneView interface.

Inventory Management

- **Purview/NAC Appliances Upgraded through NetSight:** Improving the ease of administration, Purview and NAC appliances can now be upgraded through Inventory Manager's Firmware Upgrade Wizard.
- **SCP Support for EXOS Firmware & Configuration Management:** Added SCP support allowing EXOS Firmware and Configuration Backup in environments where the SSH XMOD is installed.

Purview™

- **Support for Configuring Purview Threshold Alarms:** The Console Alarms Manager now allows the creation of Purview threshold alarms. A Purview threshold alarm is based on application usage data collected on the Purview appliance.
- **Improved Detection of Client/Server End-Systems:** Improved differentiation of client end-systems from server end-systems seen on the network.

- **Whois Integration from OneView:** Allows easy look-up of server or client IP Addresses found in OneView to better understand who the owner is for that server or client.
- **Enhanced Applications Browser:** Added the ability to specify a Time Range toolbar which allows for a custom range that controls all Applications Browser panels within a custom report created from multiple custom Application Browser-based report components.
- **Fingerprint Creation Enhancement:** Allow more robust fingerprint creation including the ability to create HTTP Header fingerprints, utilize arbitrary pattern matches, utilize PCREs, and multiple pattern/PCRE matching.
- **Support for Appliance Privacy Mode:** The Purview Appliance Advance Configuration Panel now provides support for three appliance privacy levels: Maximum Access (shows and stores all information from Purview), Medium Privacy (Stores but does not display possibly sensitive information from Purview), and Maximum Privacy (Neither displays nor stores possibly sensitive information from Purview). Possibly sensitive information includes User, Hostname, Client Address, Device Family, PCAP data, and Application Metadata.
- **Support for Longer Data Storage:** Increased storage time to one year of data with the default application usage hourly statistics, six months of high-rate (5-minute) application statistics data, and one month of end-system specific data.

IAM/NAC

- **Enhanced NAC Enforce Preview:** The Enforce Preview now provides a more detailed look at the individual changes.
- **NAC Appliance Alarms:** Added alarm notifications for errors on the NAC Appliance. These notifications are sent for errors such encountered from management servers, switches, and the NAC appliances themselves in the NAC system.
- **Added XOS MLAG Support:** Enhanced NAC's port resolution to display MLAG information when an end-system authenticates against an MLAG port.

Wireless

- **Support for IdentiFi Wireless V9.15 Controllers:**
    - The Location Engine now reports location updates for all associated users up to the limit of the wireless appliance.

    - WM supports the deployment of Radar Maintenance and Scan Profile templates to 9.15+ EWCs in High-Availability.
- **Support for IdentiFi Wireless AP3805 i/e APs:**An entry level 802.11ac indoor access point.
- **Locate Threats on OneView Wireless Threats Tab:** Map search for threats are implemented on the OneView > Wireless Threats table and Threat Events table. (EWC V9.01+).
- **Added Configuration Support for:**
    - **Firewall Friendly External Captive Portal (FF-ECP)**: A new WLAN authentication mode which improves the deployment flexibility of an ECP securely across firewall boundaries. This new feature implements a comparable level of control and trust via the use of HTTP redirection between the ECP and EWC that can be 'proxied' by the user's browser. These messages do not require additional ports be open on the firewall. (EWC V9.12+)
    - **'Operator Name' as an Additional RADIUS TLV:** Included in all RADIUS accounting messages for MAC-based, 802.1x and captive portal authentication. (EWC V9.12+)
    - **Location Batch Reporting:** Periodic push of location data over the web for Third Party Location Services and Analytics solutions (e.g. Purple WiFi). (EWC V9.12+)
    - **Primary-Backup RADIUS Server Usage Pattern:** Allows the administrator to configure whether or not the primary RADIUS server should resume client authentication after it has recovered from a failure. (EWC V9.15+)
    - **'Roaming' Location Area:** An area notification feature designed to track client locations within areas identified by the 'Location' property of a client's associated AP. When a client roams between APs, a notification is sent to NAC which can be used to apply different policies to users based on their physical area. The OneView >> Wireless >> 'Clients' and 'Client Events' tabs now show events of type 'Area Change' with the area name being displayed in the 'Details' column. (EWC V9.15+).
    - **Location Engine Globals:** Using a Globals template you can now enable / disable the Location Engine, set the Default AP Height & Environment Model and configure whether or not to 'Locate Active Sessions'. (EWC V8.32+)
    - **RADIUS Globals:** From the 'Authentication Settings' tab of a Globals

template you can configure the following: Strict Mode, and MAC Address Format as well as other advanced settings. (EWC V8.01+)

- **Wireless Advanced Services:** The Wireless Advanced Services (WAS) application is deprecated for new installations of NetSight version 6.2. Users upgrading to version 6.2 from a previous version of NetSight who currently use WAS must configure the WAS IP address in the WAS options prior to upgrading to continue to use WAS functionality.

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.2.0.224:

NetSight Suite Issues Addressed	ID
Corrected an issue where WAS log files were allowed to grow unchecked. Under certain conditions this could lead to a disk full condition.	1123513 1133111 1136648 1136847 1141069
NAC Manager Issues Addressed	**ID**
Improved version detection for the Assessment Agent in Windows 10.	-------
Corrected an issue where NAC authentication would not fail over to a secondary proxy RADIUS server when the primary RADIUS server was not reachable.	-------

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.2.0.221:

NetSight Suite Issues Addressed	ID
Corrected an issue that caused the NetSight TFTPD process to crash on 64-bit Linux operating systems over slower connections.	1122676
Corrected an issue with excessive reads of the licenses from the file system. Additional code was added to ensure that license status is read from a cached value for both licensed and unlicensed features before attempting to read a license from the file system.	-------
Corrected an issue where Captive Portal was not able to scroll on Google Chrome version 43.	1129010 1128911 1130331
Corrected an issue where the presence of a VLAN interface on a DFE prevented any ports from being stored in the network monitor cache, which prevented any port views in NetSight (which rely on the cache) from displaying any ports for that device.	1122621
NetSight now supports Summit X450-G2 devices.	-------
Console Issues Addressed	**ID**
Corrected an issue with processing multi-line syslog messages.	1108739
Policy Manager Issues Addressed	**ID**
Added support for ExtremeXOS 16.1 firmware, which now supports policy.	-------

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.2.0.211:

NetSight Suite Issues Addressed	ID
The SMTP Password in NetSight Suite E-Mail Server options can now be set when running the application in Java JRE version 8.	1110244
Inventory Manager Issues Addressed	**ID**
Corrected an issue where Inventory Manager may stop responding on some versions of Linux on which GNOME is installed.	1093181
NAC Manager Issues Addressed	**ID**
Corrected an issue where existing notification actions stop working when a notification with a Trigger Type of ANY is added after the notification actions and is enabled.	1081855 1106954
Corrected an issue where session detected events cleared the zone.	1097892
Corrected an issue where pre-registered users were not removed when they are expired if multiple captive portals exist for a configuration and the user never logged in.	1105468
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
Purview Issues Addressed	**ID**
Corrected an issue in Purview where incorrectly identified application flows resulted in incorrect user names being extracted from payload data.	------
Corrected a performance issue where entering new Locations into a large list caused a slow response.	------

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.2:

NetSight Suite Issues Addressed	ID
OneView Historical Collection now sends events (1 per day) when the collector has over due targets. This is a sign that expected SNMP is not being completed.	1068918
Corrected an issue when encrypted data (including user name and password) in an https session to the NetSight Server could be converted to plain text via a man-in-the-middle attack if the attacker is in a position to modify packets sent to the server.	------
Corrected problem with processing traps with dollar sign values in trap that caused the Console client to not launch until the server restarted.	------
Corrected an issue causing the VMware tools to re-sync time on a virtual machine back to the ESX server's time after it was synced to an NTP server.	1101314
Console Issues Addressed	**ID**
The product now supports limiting OneView Threshold alarms to port elements in a device group. This only works if the Threshold alarm is associated with a port statistic. For example, if a threshold alarm for interface utilization is associated with a device group containing a port element for fe.1.1, then the alarm can be raised for port fe.1.1 but not for other ports.	1017476
Corrected an issue that caused existing user's authenticated sessions to hang when NetSight lost contact to the back end LDAP server used for authentication.	1041947
The product now retains rsyslog customizations when upgrading.	------
Corrected problem that prevented the user defined trap from being used by an action.	1061688
Corrected an issue where the 'Authenticate to OS on RADIUS failure' and 'Authenticate to OS on LDAP failure' flags were being ignored and NetSight was always falling back to OS authentication when the RADIUS or LDAP login failed. The authenticate to OS fallback will now only occur if the check box is checked.	1067168
Wireless Manager Issues Addressed	**ID**
Added the ability to configure the 'Wireless Advanced Services' (WAS) server using its FQDN or IP address from: "NetSight >> Tools >> Options >> Wireless Advanced Services" or "WAS UI >> Options".	1055540
Inventory Manager Issues Addressed	**ID**

The Inventory Manager Device Family Script files have been fixed to allow upper case characters in the pre-script file creation section.	1058480
Corrected an issue were long files paths would cause Matrix V2 archives to fail.	1077335
NAC Manager Issues Addressed	**ID**
Enhanced NAC's group processing to eliminate trailing spaces errors for different types of NAC rule component groups, LDAP, RADIUS, hostname, etc...	1009008
The OneView Group Editor now restricts access to individual groups based on the permissions of the authorization group of the current user.	1091456
Enhanced NAC's IP resolution to have a new option to always use the IP address from a fully trusted DHCP message.	1020663
Corrected an issue where if the option to disable https for the captive portal administration pages is disabled the user was still being redirected to https.	1023326
NAC Manager now checks html formatting for a valid logo id on captive portal save if a header logo is set, and will provide a warning if correctly formatted html is missing.	1027624
Removed ability to set Port Link Control in NAC Manager UI for Add/Edit RFC3576Configuration, Edit Custom RADIUS Attributes to send, as it does not apply to this feature.	1030482
Corrected an issue in NAC Manager where searching for MAC addresses in end-system groups fails when MAC OUI display property is enabled.	1031544
Corrected an issue where the ES will remain in the Scan state because the Agent-Based Assessment Agent did not provide the MAC Address of the ES.	1026337
Corrected an issue where the NAC process could get locked re-configuring the switches allowed to contact NAC.	1046985
Enhanced NAC's management login events to better handle management logins to an Identifi Wireless Controller.	1048120
Updated NAC Manager to allow setting the RADIUS Accounting (accept packets) feature on switches when access type is set to manual RADIUS configuration.	------
Corrected an issue in NAC Manager where on move of appliances and switches to a new appliance group, the switches would retain the load-balancing setting of the old appliance group.	1052071
Updated NAC end-system moved notification to include moving between Access Points within the same SSID.	------
Corrected an issue where NAC was initiating IP resolution off an accounting stop packet which caused the incorrect IP address to be displayed in NAC in some cases after an end-system left the network.	1062744

Corrected an issue that caused the temporary directory created by a NAC appliance update not to be cleaned up after an upgrade had finished.	1064623
Corrected an issue with SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, using non-deterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack.	1077150
Corrected an issue that was causing an error message to get printed every time the NAC received a RADIUS request from a RADIUS monitor client.	1074403
Addressed an error that could occur in the mobile captive portal not allowing the error page to be displayed to a user.	1072196
Fixed issue in NAC Manager where selected PEP for appliance would get reset to None on save if the switches are displayed by friendly name.	1073299
Corrected an issue that caused the time/date editor for expiration time on pre-registration portal to float on certain browsers.	1074185
Addressed an issue where a device with SNMP timeouts and a large number of RADIUS accounting requests could cause authentications to also timeout.	1074212
Corrected an issue where the NAC appliances default gateway was getting reset after and enforce if the default gateway was configured using the nacconfig script.	1074334
Corrected an issue with the Agent-Based Assessment Agent, where the ScreenSaver assessment check would report incorrectly on Windows 7.	1081344
Addressed an issue that was causing session detected events to be created when switching between host authentication and user authentication.	1082037
Corrected an error that occurred when the pre-registration page when a duplicate user was submitted and the French locale was being used.	1082100
Corrected an issue that caused the NAC to get hung while trying to configure switches via CLI.	1082879
Relabeled NAC Manager Manage Notification Test button to Run Evaluation and updated tooltip to better describe its use as a simulated run of a notification event with user provided data rather than a test of the actions (email, syslog, trap).	1082327
Corrected vulnerability issue with NTP process when configured on a NAC appliance.	1086795
Corrected an issue where an Agent-Based Assessment Agent may not Quarantine an End-System when the Primary NAC is down and the Agent fails over to the Secondary NAC.	1087418
Corrected an issue with the NAC appliance's RADIUS server self signed certificate could not be regenerated, and improved NAC's performance/stability when dealing with devices that are unreachable during SNMP queries.	1089266

Corrected an issue where NAC attempts to maintain sessions from a previous location after moving to a new location that does not support the same authentication types.	1092456
Corrected an issue when registering devices using the Self Registration portal, where users are not able to register up to the maximum number of devices.	1092779
Corrected an issue that caused the NAC appliance to maintain threads that were no longer needed after running "Verify RADIUS Configuration on Switches".	1099049
Corrected an issue in NAC which causes the username to remain in the end-system record even after the registration expires.	------
Fixed an issue where notifications for blacklisted end-systems are not sent if IP resolution on the end-system fails or times out.	1081855
Enhanced operating system detection for Amazon Kindle devices, which were previously detected as Samsung IP cameras.	1091162
Enhanced support to Facebook registration to incorporate changes for the version 2.x API.	1100666
OneView Issues Addressed	**ID**
Corrected OneView AP Up count display to more closely match Wireless Controller WebView where APs in Guardian mode are counted as up.	1015286
Corrected behavior in the syslog event processing to not slowdown if the DNS server is mis-configured or unavailable during event processing.	1058948
Corrected an issue where IE9 could display the display the red, yellow, green application and network response time scales in reverse order.	1058089
OneView Wireless Historical Collection now supports WLAN names that contain ('!').	1063914
Corrected historical collection poll map to verify all outstanding requests are returned else they will be timed out and a counter is incremented to track the issue.	1073486
Corrected an issue where Hostname to IP look-ups reported by DNS become stale and were not cleared. Corrected End-System search by IP to be ordered by time stamp.	1080018
Corrected when a polled wireless controller disabled update the target in poll map set to not polled.	------
Corrected an issue where the most frequent vulnerability reports in OneView Identity and Access Health and in the NAC Manager client statistics charts are incorrect because vulnerability instances with no risk are incorrectly included.	1092629
Policy Manager Issues Addressed	**ID**

Corrected an issue in Policy Manager where the Rule Usage view would show a rule hit as an Unknown rule because UDP/TCP bilateral range rules were not properly matched to the corresponding rule defined in the domain.	1064503
Added a warning message in the import dialog to indicate that appending the imported Class of Service (CoS) data can still affect existing CoS rate limit mappings and to verify the CoS configuration before enforcing to confirm accurate and expected rate limits.	1098143
Corrected an issue where rules defined by one or more automated services are not written during enforce of service(s) specified in two or more network resources that use a location-based topology.	1091871
Purview Issues Addressed	**ID**
The Purview engine will now run in a virtual machine on an AMD processor. Previous versions had Intel-specific instructions and would crash when run on an AMD processor.	------
Resolved issue with encrypted data (including user name and password) in an https session to the NAC or Purview Appliances being converted to plain text via a man-in-the-middle attack if the attacker is in a position to modify packets sent to the appliances.	------
A defect that could cause the Purview engine to hang, resulting in sustained periods of no application identification in the Applications dashboard, has been corrected.	1082109
Corrected an issue that prevented SNMP contact when changing the default parameters.	1063713
Corrected an issue that would cause physical interfaces to be incorrectly ordered if there was a 10 GB card installed. There is a possibility that the monitoring interface has been changed and require adjustment to continue to monitor traffic.	------

Vulnerabilities Addressed

This section presents the Vulnerabilities that were addressed in NetSight 6.2:

- The following vulnerability was addressed in NetSight:
  - CVE-2014-3566
- The following vulnerabilities were addressed in the NetSight, NAC, and Purview appliance image:
  - CVE-2013-6462, CVE-2013-1984, CVE-2014-0106, CVE-2014-0138, CVE-2014-0139, CVE-2014-0224, CVE-2013-2004, CVE-2013-2064, CVE-2013-2003, CVE-2013-1982, CVE-2013-1983, CVE-2013-1985, CVE-2013-2004, CVE-2013-1987, CVE-2013-4244, CVE-2012-6151, CVE-2010-5298, CVE-2014-0198, CVE-2014-0209, CVE-2014-0185, CVE-2014-0237, CVE-2014-5139, CVE-2014-4344, CVE-2014-4345, CVE-2014-6273, CVE-2014-0487, CVE-2014-0488, CVE-2014-0475, CVE-2014-5119, CVE-2014-6277, CVE-2014-6278, CVE-2014-3566, CVE-2014-3637, CVE-2014-3638, CVE-2014-3639, CVE-2013-2002, CVE-2013-2005, CVE-2014-0060, CVE-2014-0061, CVE-2014-0062, CVE-2014-3513, CVE-2014-3567, CVE-2014-3686, CVE-2014-3634, CVE-2014-3683, CVE-2014-4877, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3707, CVE-2014-3158, CVE-2104-9293, CVE-2014-9294, CVE-2014-9296

System Requirements

IMPORTANT: NetSight 6.2 is the last release that will support a 32-bit appliance image. NetSight version 6.3, scheduled for release in July 2015, will only run 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 6.2 > 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.

- **Windows 32-bit** (qualified on the English version of the operating systems)
  - Windows Server® 2003 w/ Service Pack 2
  - 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® 2003 w/ Service Pack 2
  - 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™ 4.0 server
  - VMware ESXi™ 4.1 server
  - VMware ESXi™ 5.0 server
  - VMware ESXi™ 5.1 server
  - VMware ESXi™ 5.5 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	32-bit Windows	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):
  - 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, and 5.5.

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
- Mac OS X - Tiger, Leopard, Snow Leopard, Lion, Mountain Lion, Mavericks, and Yosemite

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:

- McAfee 8.6
- McAfee 9.0
- McAfee 9.5
- Sophos 4.9
- Sophos 7.2
- Norton 11
- Symantec AV 10
- Symantec Endpoint 11
- Symantec Endpoint 12 and 12.1
- ClamX AV 2.2.2

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 will result 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 8.01 or later.

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, you should 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 6.2

Following a new installation of NetSight 6.2 (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 6.2 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. The key will be used 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 6.2 supports upgrades from NetSight 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 6.2.

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 6.2 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 will be disabled on upgrade, and requires a new version in order to operate with NetSight 6.2. You must install an updated module that supports NetSight 6.2. Contact your account team for information on obtaining this update.
    - You must install a NetSight Advanced (NMS-ADV) license with 6.2 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 will 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 will be 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 6.2 NetSight server. If you are using the NAC Request Tool you will need to upgrade the version of NAC Request Tool to version 6.2.

Upgrade Considerations for NAC Manager 6.2

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 will need to review pages, as there will most likely be changes required to allow the custom styles to display correctly with the new page layout. After upgrading, NAC administrators should log on to the screen preview page (https://<NAC appliance IP>/screen_preview) of the NAC captive portal to verify that the portal still looks acceptable for display to end users. If your portal configuration is limited to setting colors and images, there should be no problem with the new portal look and feel, although you may want to set some of the new color options.

General Upgrade Information

When upgrading to NetSight NAC Manager 6.2, you are not required to upgrade your NAC appliance version to 6.2. However, both NetSight NAC Manager and the NAC appliance must be at version 6.2 in order to take advantage of the new NAC 6.2 features. NetSight NAC Manager 6.2 supports managing NAC appliance versions 6.1, 6.0, and 5.1.

NOTE: NAC 6.2 is not supported on the 2S Series and 7S Series NAC Controllers. You cannot upgrade NAC Controllers to version 6.2, but you can use NAC Manager 6.2 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 6.2* document (available on the NetSight Documentation web page > Manuals & Release Notes > NetSight 6.2 > Network Access Control [NAC]) for important information.

In addition, if your NAC solution utilizes a Nessus assessment server, you should also upgrade your assessment agent adapter to version 6.2 if you upgrade to the NAC appliance 6.2.

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 6.2 is 1.14.3.0. 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 6.2 NetSight server. If you are using the NAC Request Tool, you will need to upgrade your version of the NAC Request Tool to version 6.2.

Upgrade Considerations for OneView 6.2

- 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 that were created in NetSight version 4.4 or 5.0 that include both APs and walls will be automatically converted to the Floor Plan Base Map type when the upgrade is performed. This will allow 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 will be updated accordingly.

Upgrade Considerations for Policy Manager 6.2

- Policy Manager 6.2 only supports IdentiFi Wireless Controller version 8.01.03 and higher. If you upgrade to NetSight 6.2 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 6.2 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 will allow the enforce operation to succeed.

Upgrade Considerations for Wireless Manager 6.2

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.
- 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

08/2015
P/N: 9034838-05
Subject to Change Without Notice