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

Customer Release Notes

Extreme Networks NetSight®

Version 6.1.0.182
February, 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 6.1, 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 6.1 > NetSight Suite.

Software Enhancements

Enhancements in NetSight 6.1

This section presents the new features and enhancements that were included in NetSight 6.1.

OneView

- **New DeviceView:** DeviceView is a OneView component that provides a wide range of analysis and troubleshooting information for your network wired and wireless devices, including a device summary, FlexViews, and OneView reports. The primary launch point for DeviceView is from the OneView Devices tab. DeviceView can also be launched from other locations in OneView and Console.
- **Enhanced Extreme Device Support:** The OneView Port Tree now displays additional information for Extreme devices including neighbor link details (EDP) and Multi System Link Aggregation (MLAG). Access from the OneView Devices tab.

Purview™

- **New Data Collection Model:** The Purview appliance now collects application usage data using an improved group-based collection facility that provides:
  - More granular data collection for specific attributes, providing greater resolution when tracking usage over time.
  - Directional flow statistics, letting you view top targets based on bytes sent or received, or flows sent or received.
- **Customizable Dashboard Reports:** The new OneView Report Designer lets you create custom dashboard reports by selecting from a list of available Purview, IAM, Console, and Wireless dashboards, and customizing report components to meet your specific needs. Access from the OneView Administration tab.
- **Enhanced Applications Browser:** The enhanced Browser lets you focus your custom report on application data collected hourly, application data collected at a higher rate (every 5 minutes by default), or end-system data collected hourly.
- **Expanded Application Reports:** The Reports view in the OneView Applications tab offers a wide selection of reports providing detailed information on application usage on your network, as well as network activity statistics based on application, user name, client, and location. Click on an item in a report to view details or right-click an item to select from other focused reports.

- **Info Bar Enhancements:** The Dashboard Info Bar provides a selection of sparkline graphs showing different network statistics for the last 24 hours, with arrows that indicate trends compared to the previous reporting period. Access from the OneView Applications tab.
- **New End-System Applications Summary:** This new OneView report displays application and flow information scoped by end-system. The report is accessed by clicking on a client address in the OneView Applications tab > Application Flows report.
- **DHCP Decoder for Better Detection of MAC, Hostname, and DHCP Options:** Purview now decodes the DHCP protocol and can extract MAC address, hostname, and DHCP options used by the client machine.
- **Improved iCloud Detection:** Enhanced ability to detect iCloud's use of third-party cloud computing and storage services, and fingerprint the flow as iCloud-related.

IAM/NAC

- **Full NAC Support for XOS Devices:** Added support for MAC reauthentication on Extreme devices running ExtremeXOS 15.4.2.
- **Facebook Login for Guest Registration:** The NAC Guest Registration portal now allows end users to log into Facebook to complete the registration process, providing NAC with a higher level of user information as well as an easier registration process for the end user. There are unique deployment requirements for Facebook registration. See *How to Implement Facebook Registration* in the NAC Manager User Guide for more information.
- **OneView Group Editor Tool:** Add, edit, or delete End-System, Location, and User groups from the Identity and Access > End-Systems tab in OneView. The Group Editor also includes a Find in Group function that lets you search your groups for a MAC, IP address, Username, or Hostname.
- **RADIUS Accounting for Extreme XOS:** Added support for RADIUS Accounting configuration on Extreme devices running ExtremeXOS 15.4.2.
- **NAC IP Resolution:** Enhanced IP Resolution for Juniper Wireless Controllers.
- **SMS Credential Enhancements:** New password generation options for authenticated registration and secure guest access, as well as verification code generation options for guest registration and guest web access.
- **Other NAC Enhancements:**
    - Ability to configure RADIUS monitoring tools to monitor NAC appliance performance and availability.

- New "Keep Domain Name for User Lookup" option in the LDAP Configuration allows NAC to do LDAP user group lookups using the principle name.
- Copy and edit entries for Device Type, End-System, Location, and User groups, to quickly add group entries such as MAC addresses by copying a single entry in the table and editing the MAC value.
- Enhanced end-system historical data for better analysis of end-system traffic over time. (OneView > Identity and Access > System tab)
- Ability to view the NAC appliance serial number on the NAC appliance Configuration tab and the NAC Appliances tab in NAC Manager.
- Current and historical data on the number of end-systems per OS family for all appliances. (OneView > Reports > Identity and Access - Dashboard > Device Families report)
- Enhanced NAC Appliance Events in OneView:
  - A new NAC Events tab has been added to the NAC appliance DeviceView, displaying both NAC and NAC appliance events for the selected NAC appliance.
  - A new NAC Appliance events table has been added to the OneView Alarm and Events tab.

Policy

- **View and Set Default Port Policy in OneView:** A new right-click Policy menu in the OneView Devices tab lets you view the current domain, assign a device to a domain, set or clear a device's default role, and perform an Enforce or Verify. From the Port Tree view, you can view the current domain, set or clear the default role, and see role details for the default role.

Wireless

- **Support for IdentiFi Wireless V9.01 and V9.12 Controllers**
- **Support for 38XX (11ac) Family of APs (AP3825i/e, AP3865e)**
- **Rogue Threat Detection and Prevention:** A rogue AP is an unauthorized AP connected to the authorized wired network. Supported by 37xx and 38xx series APs added to In-Service and Guardian Scan Profiles.
- **New Global Template:** A new template used to configure global settings on controllers. These settings are grouped into the following categories which can be independently configured: Administration (Jumbo Frames, System Sync), System Logs, Syslog Settings, Web Settings, and Network Time.

- **Improved configuration of professionally installed APs:** Simplified the configuration of APs with professionally installed antennas by reducing errors in configuring Max Tx Power.
- **Controller License Sharing:** Controllers can now automatically pool Radar and AP capacity licenses if they are in an availability pair (legacy or fast-failover).
- **Support for Link Aggregate Group (LAG/LACP):** LAG allows higher throughput (802.11ac supports radio rates in excess of 1 Gbps, the speed of a single Ethernet port). LACP (Link Aggregation Control Protocol) allows two or more Ethernet ports to be dynamically aggregated. Applies to AP38xx APs.
- **HTTP for Internal Captive Portal:** Allows any type of internal captive portal (ICP, Guest Portal, Guest Splash) to be accessed without requiring HTTPs and certificates.
- **OneView Display Enhancements:**
  - New Wireless Controller and network statistics: APs by Channel, Clients by Protocol (Invalid, Unavailable, Using 802.11 AC).
  - New Wireless Controller DeviceView

Device Support

- **Support for the new AP3825i/e and AP3865e wireless APs.**
- **Support for the new 7148G-F stackable device.**

Known Issues Addressed

This section presents the known issues that were addressed in NetSight 6.1 build 182:

NAC Issues Addressed	ID
Corrected an issue where the setting to tell if NAC should strip the domain name from a username was not being obeyed for RADIUS accounting packets.	------
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 the complete registration page is displayed if no field or acceptable use policy is required.	1084021 1084024 1088186
Corrected problem with processing traps with dollar sign values in trap that caused the Console client to not launch until the server restarted.	1075888
OneView Issues Addressed	**ID**
Fixed issue where most frequent vulnerability reports in OneView Identity and Access Health and in the NAC Manager client statistics charts had incorrect/inconsistent counts due to including vulnerability instances with no risk.	1092629
Fixed a server crash caused by maps with zero length walls. A fix already exists which required the user to edit and save the offending map. This change allows these maps to be used unchanged.	------
Purview Issues Addressed	**ID**
Fixed issue that caused the AppID service to restart when processing SIP traffic.	------
SSL flows on tcp port 5223 will now be labelled 'XMPP/Messaging' instead of 'Apple Push Notifications' as these flows could also be Samsung Push notifications, or encrypted XMMP which many IM apps use.	------
Fixed issue that could cause the Purview engine to hang, resulting in sustained periods of no application identification in the Applications dashboard.	1082109
Policy Manager Issues Addressed	**ID**
Fixed an issue that would cause rules defined by one or more automated services not to be written during enforce. This would occur when the service (s) specified two or more network resources which used a location based topology.	1091871

This section presents the known issues that were addressed in NetSight 6.1 build 171:

NAC Issues Addressed	ID
Corrected an issue where RADIUS accounting packets caused NAC to display the incorrect rule/profile applied in NAC Manager, even though the access control policy was still correctly applied on the device.	1068186 1070701
Enhanced NAC IP resolution to not use full zero IPs (0.0.0.0) from RADIUS accounting.	1066293
Corrected an issue that caused NAC's named lists to not migrate correctly when upgrading from NetSight versions 5.0.0.247 through 5.0.0.259 to NetSight version 6.1.	------
The pre-registration portal now properly presents a voucher regardless of whether any non-required fields are provided.	1068847
Corrected 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 a pre-install check was preventing the Agent-Based Assessment Agent from installing on some OS X 10.8 (Mountain Lion) systems.	------
Updated process used to sign the Agent-Based Assessment Agent on OS X 10.9 (Mavericks) and 10.10 (Yosemite) to pass the Gatekeeper security check.	------
OneView Issues Addressed	**ID**
Added support for the AP 3805 i/e in OneView Reporting.	------
Corrected an issue where APs that were SNMP unreachable appeared in the AP Down report. Increased the default number of Wireless targets that are polled in a minute from 300 to 600.	1068899
Corrected historical interface collection issues caused by sparse OID support on different Cisco devices.	1060771
Corrected an issue with the time-lapse location threats search performed in the Wireless tab Threats table. Searching for threats outside of the Threats table (for example, searching from Maps) should be avoided.	------
Purview Issues Addressed	**ID**
Extended the carrier detection signature set to more completely capture AT&T and T-Mobile traffic.	1068697
Identified wireless carriers are now normalized and grouped together for simpler analysis.	------
Corrected a defect that led to incorrect characterization of client and server flows, that also affected operating system assignments.	------
Wireless Manager Issues Addressed	**ID**
Improved support for 9.15 controllers. In particular, Wireless Manager now supports the configuration of 3805 APs, and the deployment of Radar Maintenance and Scan Profile templates to 9.15 controllers in high availability.	------

This section presents the known issues that were addressed in NetSight 6.1 build 159:

NAC Issues Addressed	ID
Enhanced NAC's web service to handle incomplete LocalUser objects when adding a local user to the Local Password Repository.	------
Corrected an issue where the Agent-Based assessment agent would not install on OS X Yosemite 10.10. This fix removes a dependency on the system requiring that Java 6 be installed.	------
Corrected an issue where the NAC process could get locked while reconfiguring the switches allowed to contact NAC.	1046985
OneView Issues Addressed	**ID**
Corrected an issue with OneView map elements to allow Wireless Coverage features to continue to work.	1060361
Modified the OneView map threat event tracking and search so that threat events are uniquely identifiable, allowing the historic threat search and location probability to display correctly. Also, the tooltip now reflects that the search result is a Threat, not a Client.	------

This section presents the known issues that were addressed in NetSight 6.1 build 157:

NetSight Suite Issues Addressed	ID
Addressed multiple CVEs by upgrading the Java version used with the NetSight, NAC, and Purview products to version 1.7.0_67.	------
Appliance Issues Addressed	**ID**
Addressed vulnerabilities CVE-2014-6271, CVE-2014-6277, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187 in NetSight, NAC, and Purview 64-bit (Ubuntu) appliances. These vulnerabilities will not be addressed in the 32-bit (Slackware) appliances. It is recommended that users re-image the 32-bit appliances to be 64-bit for the most up-to-date security patches.	------
NAC Issues Addressed	**ID**
Enhanced NAC's web services to allow a caller to get a PKCS5 hash for a plain text password via a web service call.	------
Corrected a timing issue that caused a NAC appliance's status to show as unlicensed for one poll cycle following a restart of the appliance.	------
Corrected an issue where devices modeled without SNMP would not use the RFC3576 configuration set in the advanced configuration of the switch.	1057596
Corrected an issue where the NAC assessment license check could run out of memory if run against a database with a large amount of historical scan data.	------
Enhanced NAC's DHCP fingerprint library to correctly identify an Axis network camera.	1019354

Corrected an Out Of Memory exception by upgrading Java on NAC installations.	1012458
Corrected a JMS queue deadlock issue by upgrading Java on NAC installations.	------
OneView Issues Addressed	**ID**
Corrected syslog event processing behavior to prevent a slowdown if the DNS server is mis-configured or unavailable during event processing.	1058948
Corrected two OneView Wireless pie charts (Wireless Dashboard Clients by Protocol and APs by Channel) to use the latest available raw data instead of hourly data, to closer approximate what is reported by the Wireless Overview panel.	------

This section presents the known issues that were addressed in NetSight 6.1 build 147:

NetSight Suite Issues Addressed	**ID**
Fixed an issue with the device cache that could cause continual slow memory growth in the NetSight server if there were several thousand devices modeled with LLDP enabled.	------
Appliance Issues Addressed	**ID**
Addressed vulnerability CVE-2014-5139 in NetSight, NAC, and Purview appliances.	------
Console Issues Addressed	**ID**
Corrected an issue with the Console Basic Policy tab where the last port on a G3 would not correctly report the default role.	1019914
NAC Issues Addressed	**ID**
Enhanced NAC's re-authentication capabilities to allow dynamic switching of the security policy on an XOS switch without having to toggle the port.	------
Corrected an issue that caused the username to persist in the end-system record even after the registration expired.	------
Added an option to the Captive Portal redirect functionality to optimize the redirection time by not using the DHCP delay when the option to redirect immediately.	------
Enhanced NAC's integration with EXOS to better handle switching the UPM on 802.1x authenticated end-system on the fly.	------
OneView Issues Addressed	**ID**
Corrected a FlexView issue where the Interface, Instance, and Slot columns were sorted by ASCII string value instead of numeric value.	------
Corrected an issue where the Show Support diagnostic feature did not gather all information if older collector status report targets without a create time were present.	------
Corrected an issue with OneView maps where changing radio bands could cause the slider position to become invalid.	------

Corrected an issue with OneView maps where the drawing tools allowed a wall to be created with the same endpoints (i.e., a dot), causing the heatmap library to crash. OneView now filters out such walls from the FXML. The following action is required before using wireless coverage: 1. Delete all *.fxml files in the NetSight <install directory>/appdata/OneView/MyMaps folder. Do not delete any subfolders. 2. In OneView, for each map that causes this problem, click **Edit**, then click **Save** without making any changes.	------
Corrected an issue with device icon sizing in OneView maps.	1044960
Corrected an issue with the OneView maps Wall menu where the wall material was not set correctly.	1039164-
Corrected an issue in OneView maps where the client's distance was not being used during a map search.	------
Policy Manager Issues Addressed	**ID**
Added support for 7100 Series firmware update 08.03.01 which altered the manner in which rate limits are associated to classes of service. Upgrading to this firmware may require an enforce in Policy Manager if inbound rate limits are in use.	------
Corrected an issue with the Ports tab in the Device View that caused ports to be sorted in the incorrect order.	------
Purview Issues Addressed	**ID**
Corrected an issue with data not displaying in the End-System Applications Summary view when multiple Purview appliances were present.	------
Corrected an issue in the Purview engine where a data race condition could result in a crash when decoding FTP traffic.	------
Corrected a sensor defect that could cause an incorrect assignment of server operating system to client flows, and vice-versa. This would result in the over-representation of server operating systems in the reports that break down traffic by client.	------

This section presents the known issues that were addressed in NetSight 6.1 build 137:

NetSight Install Issues Addressed	**ID**
Corrected an issue that caused an exception in the NetSight server.log file when the server is started for the first time after a fresh install. This happened when the NAC plugin was not licensed yet.	------
Corrected an issue where permissions were not set on install for a non-root user to be able to run ipmitool.	------
Inventory Manager Issues Addressed	**ID**

Corrected an issue with the archive script for XOS device types. The script will now run correctly if the device's primary configuration is not being used.	------

NAC Manager Issues Addressed	**ID**
Corrected an issue where an invalid accounting request from a Cisco switch caused NAC to be unable to process requests.	1044195 1044216 1044221
Corrected a NetSight upgrade issue that caused the Distributed End-System Cache to not be initialized properly after the upgrade.	------
The MySQL innodb_flush_log_at_trx_commit value has been changed from enabled to disabled to correct a performance problem in the captive portal.	------

This section presents the known issues that were addressed in NetSight 6.1 build 135:

NetSight Suite Issues Addressed	**ID**
Corrected an issue where a clean installation of NetSight on an Ubuntu system could fail to install and start the MySQL database if the system host name could not be resolved via DNS.	------
Appliance Issues Addressed	**ID**
Corrected vulnerabilities in NetSight, NAC, and Purview appliances for USN-2192-1, CVE-2010-5298, and CVE-2014-0198.	------
Corrected vulnerabilities in NetSight, NAC, and Purview appliances for USN-2232-1, USN-2232-2, and CVE-2014-0224.	1026924
Console Issues Addressed	**ID**
Corrected a database restore issue where existing alarms were removed if they were named Device Status Change, Fan Failure, AP Down, AP Online, AP Radio Change, or AP Radio OnOff.	------
NAC Manager Issues Addressed	**ID**
Corrected an issue where an end-system failing over to a secondary NAC appliance could have an extra toggle link performed due to port link control seeing the authentication as a new authentication.	1035695
Corrected an issue with NAC appliance upgrades where OpenSSL was upgraded that caused a failure when attempting to create a client certificate request.	1035967
Added support for parsing ifIndex from NAS-Port on H3C S3100 switches.	1037857
Corrected an issue where the end-system remained in the Scan state because the assessment agent did not provide the end-system's MAC address.	1026337
Enhanced NAC's OS detection via DHCP so that devices running OS X 10.7 and above will be detected as "Mac OS X 10.7+". This will include the new Mac OS Yosemite.	------
Corrected an issue with NAC's OS detection via DHCP that caused Nintendo Wii U devices to be detected as Blackberry.	------

Policy Manager Issues Addressed	ID
Corrected an issue where editing a rule's traffic description from the parent service's Details View did not trigger the Save icon indicating the domain data had been changed, and for global services the change was not saved to the database after a manual save.	1038463
Purview Issues Addressed	**ID**
Corrected an issue where bad data in the Purview Locations configuration caused exceptions in the server.log and prevented the NetSight server from restarting.	------
Corrected an issue that prevented the Purview sensor from sending IPFIX records to the collector after properly identifying applications.	------
Wireless Manager Issues Addressed	**ID**
Added support for IdentiFi Wireless V9.12 Controllers, the AP3865e wireless AP, and rogue AP detection for Guardian scan profiles.	------

This section presents the known issues that were addressed in NetSight 6.1 build 127:

NetSight Suite Issues Addressed	ID
Corrected an issue that prevented the JBOSS_HOSTNAME from being used as the server address.	------
NetSight Appliance Issues Addressed	**ID**
Corrected an issue where an error was reported to the NetSight server.log file for a non-root user being unable to run the ipmitool to get hardware events from a NetSight appliance.	------
NAC Manager Issues Addressed	**ID**
Corrected an issue where too many concurrent agent-less assessment scans could cause performance issues on a NAC appliance.	------
Policy Manager Issues Addressed	**ID**
Corrected an issue where Policy Manager could hang during a Verify when the Transmit Queue Port Groups Arbiter Mode was set to "Use Per-Port Type Arbiter Mode" but nothing was configured.	------
Corrected an issue where Policy Manager could fail to launch the Class of Service Configuration View when the Transmit Queue Port Groups Arbiter Mode was set to "Use Per-Port Type Arbiter Mode" and a port type was undefined.	------
Corrected an issue where MAC to Role mappings were not being imported from the device correctly, causing the mappings to be removed after an Enforce was done.	------
PurView Issues Addressed	**ID**
Corrected an issue where the report showing total bandwidth over time was not properly reporting bandwidth received and bandwidth transmitted, although the total bandwidth was correct.	------

Corrected an issue where the Purview appliance could not recover its connection to the NetSight server when there were frequent connection problems.	------
Corrected an issue where a missing Applications Browser component name would cause OneView to fail to load reports.	------
Corrected an issue where a null pointer exception was displayed in the server log when an Applications Browser based custom report was selected in the Reports tree.	------

This section presents the known issues that were addressed in NetSight 6.1:

NetSight Suite Issues Addressed	**ID**
Corrected an issue that prevented the import of a database where the invconfigurations table was large.	------
Corrected an issue where some devices with large entity MIBs (Bonded S-Series S8 and others) were not discovering serial number or Boot PROM.	1015901
Console Issues Addressed	**ID**
Corrected an issue with incorrect filtering of IPv6 addresses in Compass.	1016052
Corrected an issue with resolving vendors if MAC address delimiters other than a colon were used in Compass.	1017366
Corrected an issue with the Console Basic Policy tab showing the incorrect default Role for some devices.	1019914
Inventory Manager Issues Addressed	**ID**
Corrected the Capacity Planning "Ports Used" PDF report to show the correct data.	1011248
Corrected an issue where the File Transfer Method was set from a device in the Device Tree, but the value was not saved.	1023513
NAC Manager Issues Addressed	**ID**
Corrected an issue with the Agent-Based Assessment agent that caused excessive memory growth on some Windows XP systems.	916835
Corrected an issue where Custom Information for entries in an End-System group would disappear from display when adding/editing/deleting entries from the group.	997897
Enhanced the export feature for End-System groups to also export custom information, if present.	999100
Corrected an issue where the timeout value on an existing LDAP configuration could not be modified.	------
Enhanced IP resolution for Juniper wireless controllers.	------
Corrected an issue where the precedence order was incorrect due to NAC not taking into account the AP information of the location of a policy mapping.	1006646

NAC now supports detection of Symantec Endpoint Protection 12 and 12.1 with the Agent-Based Assessment agent on Mac OS X.	1007902
Corrected an issue where the Used-By check for a rule failed when an Advanced AAA rule had the User/MAC/Host criteria set to Group and Local Password Repository Users.	------
Search functionality is now available in the OneView Group Editor to search for entries within groups. Partial and full MAC addresses, usernames, and locations can be queried to find the groups to which they belong.	1009526
Enhanced the NAC captive portal to allow User groups to provide an override look and feel for certain users.	1009873 1009902
Corrected an issue where the NAC DNS proxy responded to an IPv6 DNS request with an IPv4 response	1011501
Corrected an issue where exceptions occurred when launching the Edit Policy Mapping window against a policy mapping in the Advanced Configuration > Policy Mapping panel.	1016724 1026608
Added a feature that allows copy and edit of entries in a Rule Component group via a Copy menu item, to facilitate adding new entries.	994325
Enhanced NAC to allow for RADIUS monitoring of NAC appliances.	1013968
Enhanced NAC's IP resolution to fall back to a switch-specified IP subnet or the global IP subnet if a VLAN is used for access control for an end-system but there was no IP subnet defined for that VLAN.	1018440
Fixed issue where an authorized user with a dash (-) in the user name could not move an end-system from one group to another in the OneView Identity and Access tab.	1021159
Enhanced the NAC captive portal to display the self-registration portal if any location enables it.	1021834
Corrected an issue where the NAC DNS proxy was not responding to requests that should be redirected when the back-end DNS server was not reachable.	1022912
Corrected an issue with the NAC web service API addMACToEndSystemGroup which was causing extra notifications to be generated.	-----
Corrected a problem in NAC Enforce Audit which was causing an error condition to occur and prevent the Audit from completing successfully.	1015113
Corrected NAC's OS Detection to make the detection consistent across various models of Cisco IP Phones.	1016679
Corrected an issue with NAC's OS Detection which caused Samsung IP Cameras to be detected as Vizio IPTV.	-----
Enhanced NAC's OS Detection by adding a new DHCP fingerprint for detecting Chromebook devices.	1016426
Corrected an issue where NAC could take too long processing periodic RADIUS requests when SNMP contact to a device is lost.	1027167

OneView Issues Addressed	ID
The OneView Group Editor lets you add, edit, or delete End-System, Location, and User groups from the Identity and Access > End-Systems tab in OneView.	994683
Corrected an issue where Purview data could be displayed in the End-Systems Details window for users without Purview privileges.	10114444
Corrected an issue with the bandwidth reporting on the Interface Details PDF report.	1016513
Enhanced wireless client count accuracy by collecting new wireless controller 9.01 firmware data, creating controller and network-level statistics.	------
Corrected an issue where guardian mode APs were not showing the correct alarm status in the OneView Wireless Access Points view.	1010628
Corrected a problem in the OneView Search where a match of multiple end-systems by IP address could return a stale MAC address.	1013867
Corrected the Wireless Details Radio Details SSID Name and added the BSSID MAC address.	1016463
Corrected an issue where a map image could not be deleted after the map that used the image was deleted.	1013468
Changed the Add Map Link feature in OneView Maps to remove a capability requirement for Purview Read Access. Purview restricted content is now hidden from the view if the capability is not enabled.	1021810
Enhanced OneView Maps display name to match the name shown in OneView Devices, not just the IP address.	1023036
Policy Manager Issues Addressed	**ID**
Corrected an issue where the rule count in the Role Details View was inaccurate when automated services existing in the role were counted more than once.	985769
Corrected an issue where a service would be added to a role just by opening Enforce Preview when two rules exist in the role with the same traffic description, and one is local and the other global.	1006783
Corrected an issue where a Java exception occurred in the client log when a device was unassigned from a domain while it was currently selected in the Device Tree.	1010856
Corrected an issue preventing authentication settings from being set on LAG ports on 7100 Series devices.	1016039
Corrected an issue that would cause the client to hang when retrieving port-level session information on S- Series and K-Series devices running 7.73 firmware.	1018208
Corrected an issue that caused a rule to be omitted from Enforce Preview and Enforce when another rule of the same name existed in a different service.	1023337
Purview Issues Addressed	**ID**

The OneView Applications Browser now supports saving different configurations as a Report Designer component. The feature provides the ability to choose selected Applications Browser configuration fields to create a custom interface, or no fields to create a view-only report.	------

System Requirements

IMPORTANT: Beginning in NetSight version 6.3, the 32-bit appliance image will no longer be supported. 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 6.1 > Network Access Control (NAC) and NetSight Appliances. Please contact GTAC 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
  - Windows Server® 2008 R2
  - Windows Server® 2012

    - 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
- **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

	Minimum	Medium	Large	Enterprise
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 or version 7 update 40 (also referred to as 1.6 or 1.7).
- Supported Web Browsers:
  - Internet Explorer versions 9, 10, and 11
  - Mozilla Firefox 26 and 27
  - Google Chrome 32.0

Virtual Appliance Requirements

A virtual appliance is a software image that runs on a virtual machine. 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.

IMPORTANT: For ESX 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, and Mavericks

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 9, 10, and 11
- Mozilla Firefox 26 and 27
- Google Chrome 32.0

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 6.1

Following a new installation of NetSight 6.1 (not an upgrade), if you restore a database from NetSight version 5.1 or earlier, you will need to go to the Inventory Manager Tools > Options > Data Storage Directory Path option and modify the path to point to the new NetSight 6.1 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 6.1 supports upgrades from NetSight 6.0, 5.1, and 5.0. If you are upgrading from a NetSight version prior to 5.0, you must perform an intermediate upgrade. For example, if you are upgrading from NetSight 4.4, you must first upgrade to NetSight 5.1, and then upgrade to NetSight 6.1.

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 (Tools > Server Information > Database tab).

Important Upgrade Considerations

- If your network is using Purview appliances, you must first perform the NetSight upgrade to version 6.1 and then upgrade the Purview appliances.
- 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 6.1. You must install an updated module that supports NetSight 6.1. Contact your account team for information on obtaining this update.
    - You must install a NetSight Advanced (NMS-ADV) license with 6.1 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 6.1 NetSight server. If you are using the NAC Request Tool you will need to upgrade the version of NAC Request Tool to version 6.1.

Upgrade Considerations for NAC Manager 6.1

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 6.1, you are not required to upgrade your NAC appliance version to 6.1. However, both NetSight NAC Manager and the NAC appliance must be at version 6.1 in order to take advantage of the new NAC 6.1 features. NetSight NAC Manager 6.1 supports managing NAC appliance versions 6.1, 6.0, 5.1, and 5.0.

NOTE: NAC 6.1 is not supported on the 2S Series and 7S Series NAC Controllers. You cannot upgrade NAC Controllers to version 6.1, but you can use NAC Manager 6.1 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 6.1 document (available on the NetSight Documentation web page > Manuals & Release Notes > NetSight 6.1 > 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 6.1 if you upgrade to the NAC appliance 6.1.

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 6.1 is 1.13.0.0. 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 6.1 NetSight server. If you are using the NAC Request Tool, you will need to upgrade your version of

the NAC Request Tool to version 6.1.

Upgrade Considerations for OneView 6.1

- 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 6.1

- Policy Manager 6.1 only supports IdentiFi Wireless Controller version 8.01.03 and higher. If you upgrade to NetSight 6.1 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 6.1 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 6.1

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/enterasys-support/mibs/.

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

02/2015
P/N: 9038812-08