Title	**Release Notes for NSE 2400, 2500, 5800, 5900 and 6000**
Abstract	This document captures the changes made to the NSE operating code from release **8.1** to release **8.12**
Originator	NSE Product Management
Author	Nomadix, Inc
Date	August 28, 2018

Contents

New Features and Enhancements Added

Release 8.12 August 2018

Description of Feature / Enhancement Added
Support for the latest AG6000 platform. The basic configuration has been expanded to support 6 GbE ports, 2 Small Form-Factor Pluggable (SFP) fiber ports and an option for 2 additional SFP+ (10G) fiber ports. The AG 6000 offers 6Gbps of sustained bandwidth, making it the highest-performing platform in the Nomadix family of bandwidth management and access gateways.
This release introduces a new, simplified method of calculating the number of licenses in use on any NSE. All entries in the Current Table, regardless of status (i.e., Pending or Valid subscribers, or Devices) will count against the license total – and that's it. Saved profiles are not counted separately.
The General Data Protection Regulation (GDPR) mandate, which became effective May 25, 2018, unifies the data protection rules across Europe and strengthens the rights of EU citizens by emphasizing transparency, fairness and accountability. This version is compliant with GDPR requirements.
When using class-based queueing, classes can now be configured to set bandwidth limits that constitute a percentage of the throughput available on the interface, or of the parent class (for sub-classes), rather than by explicit Kbps values. This allows ratios between classes to be maintained even if the overall interface throughput changes. (Note that these two methods are mutually exclusive - the feature cannot be configured so that some classes use percentages and others use Kbps.)
AAA (Authentication Authorization and Accounting Setting) The Default Logout IP address has been modified from 1.1.1.1 to 198.51.100.10. The remaining selectable addresses (2.2.2.3, 3.3.4.5, 4.5.6.7 and 5.0.0.5) are unchanged.

Release 8.11 January 2018

Description of Feature / Enhancement Added
Removed mandatory email address field from Nomadix web management interface (WMI) -

-> Configuration --> Location, and from the new gateway installation process for GDPR compliance. For currently installed gateways, please update the email address to support@nomadix.com manually by logging on to the NSE for GDPR compliance.
Template files have been created that can be used for a Local Web Server portal (these are currently limited to use with 2-way PMS).
A Default Group Bandwidth Management Policy can now be configured by Port Location. Subscribers connected to the port on which these defaults are defined and enabled will be assigned the Default Policy values, unless a different policy or individual bandwidth limits are explicitly assigned to the subscriber via some other mechanism (i.e., via the Nomadix RADIUS Group Bandwidth VSA's, Up /Down Bandwidth VSA's, Billing Plan, etc). Such explicit assignments will override the port-based defaults.
When Class-Based Queueing is enabled, a Default CBQ Class can now be assigned to subscribers by port location. Subscribers connected to the port on which the default class is defined will be assigned to that class, unless a different class is explicitly assigned to the subscriber via some other mechanism (i.e., via the Nomadix RADIUS Class VSA, Billing Plan setting, etc). Such an explicit assignment will override the port-based default.
The NSE's Failover functionality can now be configured via SNMP.
This release includes a number of IPv6 WAN-side additional features and enhancements. The NSE now supports receiving its IPv6 address and DNS configuration from DHCPv6 as well as supporting SLAAC or manual configuration. In addition IPv6 support is now included for the XML interface server addresses, RADIUS servers, Portal Page servers, Portal XML POST URL's, SNMP (including traps), Syslog servers, and NTP servers.
Changes to the NSE's Local Web Server (LWS) content no longer require a reboot of NSE to put new content into effect. This can now be done using an XML Command, through SNMP, or through the Web UI.

Release 8.10 September 2017

Description of Feature / Enhancement Added
With this release the NSE now supports external access to subscriber-side IPv6 devices. The basic functionality is equivalent to IPv4 static port mapping, but the underlying mechanism is somewhat different, as follows: ○ The feature is provided by routing, not NAT. External computers will access the device's IPv6 address directly. ○ Access is given ONLY to the IPv6 addresses that have been entered in the Access Control List. ○ Devices must be statically configured to an address in a specific IPv6 subnet. For more information regarding this feature, consult the most recent version of the User Guide.
The NSE now supports Link Aggregation via LACP (Link Aggregation Control Protocol). This can provide improved throughput and link redundancy by combining two or more physical links into a single virtual link. Two Link Aggregation Groups (LAGs) are available, and can be used for WAN-side or Subscriber-side connections as desired.
This release introduces NSE support for PayPal payments, which also includes standard credit card authorization through the Payflow system in several countries (U.S. & Canada for all versions). PayPal support essentially replaces support for the Authorize.net Credit Card feature, which has been removed from the NSE.
The NSE's subscriber-side DHCP feature has been enhanced to provide support for up to 500 DHCP pools (the previous limit was 200).
A "Suppress posting of zero payment amount" option has been added for Micros and Micros Fidelio PMS. In previous releases, when issuing XML USER_PAYMENT or USER_PURCHASE commands with these PMS types, the NSE always sent a POST even if the amount was free (Zero). Now, if the "suppress posting" option is enabled, when a zero amount is charged, the PMS query will still take place, but no POST will be sent.
For Micros Emulation PMS, a configurable parameter has been added so that, if desired, the "Sales 1 Total" field can be filled in with the transaction sub-total value.
The Local Web Server can now be refreshed with a click of a button (instead of requiring a reboot) to read in any page changes that have been made.

Release 8.9 May 2017

Description of Feature / Enhancement Added
The Nomadix Access Gateway Model 2500 (AG 2500) is supported by this release.
The NSE now supports a "Primary WAN Interface Watchdog" setting which is accessible via the System menu (in both WMI and CLI). When enabled, the watchdog will monitor the network connection on the Primary WAN interface by pinging the default gateway that is configured on that interface at specific intervals. If for some reason there is no response from the gateway, after a certain period of time, the watchdog will reboot the system (both the ping intervals and the reboot period are set internally by the system – they are not administratively configurable at this time). Which interface constitutes the "Primary" WAN is determined as follows: ○ If only one interface on the NSE is configured in the WAN role, that interface is Primary. ○ In a Multi-WAN configuration, the Primary is the interface with the "lowest" reference (i.e., the labeled WAN interface, followed by Eth1, Eth2, etc, in that order). However, on an AG 5900 that includes the fiber module, if either of the fiber interfaces are enabled and configured to the WAN role, then that interface becomes the Primary. In the event both fiber ports are enabled and set to WAN, the SFP0+ interface will be Primary.
An additional Unique Identifier field has been added for Subscriber Tracking ("Lawful Intercept") syslogs. This is now the final field (or column) in the syslog content, and consists of a sixteen character hexadecimal string. The value of this field is algorithmically generated in a manner that is designed to ensure that no repetition of values can occur for at least a year. Use of the field is enabled / disabled via a parameter that has been added to the WMI logging configuration page called "Include Unique Session IDs". The parameter can also be set via CLI or SNMP.

Release 8.8 January 2017

Description of Feature / Enhancement Added
The NSE software now supports an updated version of the AG 5900 hardware that includes a plug-in module containing two SFP+ 10 Gigabit fiber interface ports. The module may be initially shipped with the unit, or can be inserted later as an add-on. There are several points to keep in mind regarding this feature: ○ The system MUST be powered down, and the power cord unplugged from the unit, prior to insertion or removal of the module. Severe damage to the module and/or the NSE could result if the module is inserted or removed while power is applied. (NOTE: Due to a minor change in power management required to support the module, when shutting down the system, it may be necessary to hold down the power button on the unit for a few seconds in order for the process to initiate.) ○ The requirement to power off the system does not apply to insertion and removal of transceivers from the SFP+ ports. This can be done with power either on or off. ○ The 10G SFP+ ports only support 10 Gigabit transceivers at this time. 1G standard SFP transceivers are not supported. ○ When the SFP+ ports are present and configured in the WAN role, they become the highest priority interfaces on the system. For example, if the SFP+0 slot is configured as WAN, system traffic will be routed through that interface.
The NSE now supports a Fast Forwarding mode. When enabled, overall throughput for the total system is enhanced, offering significant improvement over the maximum rate that could previously be achieved on the specific NSE platform being used. Items to note about this feature: ○ On higher-end NSE platforms, the maximum rate the system can achieve may be limited by the line rate of the interfaces used. In order to benefit from the Fast Forwarding feature on these platforms, it will be necessary to use either the fiber interfaces, if present (discussed above), or to use multiple 1G standard ethernet interfaces (both on the network and subscriber sides) with the Load Balancing feature enabled. ○ Weighted Fair Queueing (WFQ) must be enabled for the Fast Forwarding feature to be used. If an attempt is made to enable Fast Forwarding while WFQ is disabled, a pop-up warning will be displayed. ○ Due to the mechanism used to achieve the greater data rate, events triggered from accounting statistics (bytes sent / received, for instance) could be delayed by up to 5 seconds. Thus, volume-based billing quotas could be overrun by approximately 5 seconds.
The NSE now includes IPv6 configuration options for interfaces set to the WAN role, which allows administrative control and system traffic over IPv6. The global IPv6 enable selection

has been removed, and replaced with a *per-interface* IPv6 enable/disable. (Please note, however, that ***subscriber*** traffic over IPv6 is not yet supported. This is expected in a future release).
"Device Add" and "Device Delete" XML commands are now available to add/delete Devices to/from the NSE's internal database (in the same manner as the User Add and Delete commands are used for regular subscribers).
When multiple interfaces are configured in the WAN role and Load Balancing is enabled, DNS requests issued by VALID subscribers will now be forwarded from the WAN interface to which the subscriber is assigned, and thus to the DNS server address(es) specifically configured for that interface (previously, all DNS requests were considered system traffic, and were always sent from the highest priority WAN interface).
Subscriber tracking ("Lawful Intercept") is now supported for non-translated subscribers. A number of functional and aesthetic improvements have been made to the Web Management Interface.
The RADIUS Acct-Terminate-Cause code sent in accounting stop packets triggered by zone migration is now customizable.

Release 8.7 October 2016

Description of Feature / Enhancement Added
Weighted Fair Queueing can now be used in conjunction with Class Based Queueing. This provides the ability to weight users according to their configured individual limits while also assigned to a class, and the Fair Queueing ratio(s) between users will then apply within that class. This will work as well with multiple classes, and the relative class priorities will still be applied.
Bandwidth Management now includes a "Share Unused Bandwidth" option. This allows the WFQ feature to proportionally increase subscriber bandwidth allocations when excess bandwidth is available. In other words, when there is still excess bandwidth on the system, users will be allowed to receive more bandwidth than their individually configured maximums, in the same proportion as their relative upper limits dictate, until such time as the total aggregate bandwidth demand of all the users maximum values exceeds the total bandwidth available on the system.
A Default Bandwidth Limit setting has been added to the bandwidth management parameters. This provides the ability to configure a default bandwidth limit for authorized (i.e. "valid" AAA state) subscribers. Authorized subscribers with bandwidth limits set to 0 are currently treated as having unlimited bandwidth. Such behavior may not be desirable when subscribers with different limits are mixed. For example, a user on a NO CHARGE port by default would have unlimited bandwidth and thus could achieve higher effective throughput than an authorized premium subscriber with defined limits. The new capability allows the administrator to override the per-subscriber bandwidth value of 0 with a global default. The new value will take effect whenever the per-subscriber limits are set to 0, which could be due to either missing authorization parameters (e.g. missing RADIUS attributes) or when the per-subscriber limits are explicitly set to 0.
The subscriber statistics page (Subscriber Administration / Statistics) now includes a "Subscriber Licenses in Use" field. This can be helpful is determining actual license usage when, for example, a significant number of subscriber-side Devices are configured.
The SNMP listening port value is now configurable.
Support has been added for DHCP Option 82 (Relay Agent Information) embellishment of DHCP transactions between an NSE operating as DHCP Relay Agent and its associated external DHCP server.
The XML Portal Sub ID length value has been increased to 36 bytes.
The User Definable fields in the NSE's internal database have been extended to 128 bytes.
The NSE's time zone database has been updated to reflect current changes.

Release 8.6 March 2016

Description of Feature / Enhancement Added
The NSE's time configuration now includes support for automatic daylight Savings Time adjustment and official IANA time zones.
The QoS feature has been expanded to include support for DSCP (Differentiated Services Code Point) marking along with the existing 802.1p support.
A maximum retry limit can now be set for MAC authentication requests.
A quick utility that can verify if the PMS port is working has been added to the PMS interface.

Release 8.5 August 2015

Description of Feature / Enhancement Added
Automatic RADIUS re-authentication can now be restricted to the initial login zone via Zone Migration.
Subscriber login can now be performed using Facebook® credentials.
Group accounts can now be configured with an overall account time limit.
DHCP pools can now be enabled / disabled via a configuration setting.
The PMS Serial Redirector can now be implemented over TCP/IP.
Weighted Fair Queueing.
With this release, the AAA configuration screen has been changed to a tabular format. Simply select the desired tab in order to access the AAA section you need to configure. Note that when the "Submit" button on any of the tabs is clicked, the configuration settings for all tabs are submitted simultaneously.

Release 8.4 April 2015

Description of Feature / Enhancement Added
Class-based queuing.
Destination based WAN selection

Per-port subscriber-side DHCP enable / disable

Release 8.3 June 2014

Description of Feature / Enhancement Added
Subscriber Intra-Port Communication.
Metaphone 3 support for Micros, Micros Fidelio, and Marriot WFB & FOSSE PMS systems.
Subscriber DHCP improvements, including increase of DHCP lease limit to 25,000.
User-definable RADIUS attributes.
Pending subscribers will now generate MAC authentication requests upon migration if port / zone migration is enabled.

Release 8.2 April 2013

Description of Feature / Enhancement Added
Multiple WAN Interface Support. The NSE can now support up to five (AG5800) WAN interfaces at once, using completely independent network settings for each. Each WAN port has independent Mode, IP, DNS, iNAT, Monitoring, Additional NAT addresses, 802.1Q tagging, and bandwidth settings. Roles for most ports (those marked either EthX or AuxX) are unrestricted; that is, each port can be set to WAN, SUB (Subscriber), or OOS (Out Of Service). However, designated WAN or LAN ports cannot be set to the opposite role, but can be set to OOS. Each configured and active WAN port can be used for NSE Management activity, and the WMI is available on that address. Multiple WAN interfaces may be configured and used for management activity (but not subscriber traffic), even without the Load Balancing license feature (or with the feature disabled). Out of the box, the NSE will boot with one WAN port and one LAN port enabled, and the remaining ports set to OOS. With multiple WAN ports enabled, how does the NSE chose which interface to send traffic out? (Note that this discussion does not apply to SUBSCRIBER traffic, the NSE deals with

that separately.)

- The NSE's own traffic is primarily directed by clever routing. A default route is created for each enabled WAN interface, but with a different metric for each. Eth0 is assigned a metric of 1, Eth1 is assigned 2, and so on through Eth5. The route with the lowest metric has priority if both could be used to reach the same destination.

- Setting a WAN port to OOS removes the route(s) for that port from the routing table.

The metrics are shown in Network Info -> Routing.

There is an additional rule for incoming TCP and ICMP traffic to the NSE management interfaces. This rule was added because (particularly when 8.2 is run without a Load Balancing license , which removes much of the logic that routes traffic) - with multiple WAN interfaces assigned, packets are not always sent to an interface that allows the reply to get back to the sender. To correct this we have a special rule that says, "send the response back out the interface from where it came".

Load Balancing and WAN link Failover.

In the 8.2 release the NSE can balance subscriber assignment between all active WAN interfaces when Load Balancing mode is enabled. Note that it is SUBSCRIBERS that are balanced, not traffic.

As subscribers go valid, they will be assigned to a WAN interface, taking account of both the Uplink bandwidth settings of the interfaces and the number of subscribers currently using each interface. Higher bandwidth settings will mean more subscribers will be assigned to that interface. The subscriber will use the assigned interface for all traffic.

If a WAN interface goes down, the subscribers currently assigned to that interface will be re-assigned to the remaining interfaces. How that interface will behave once the interface is restored is selectable. With Active Rebalancing enabled (it is on by default), the NSE will respond to a link restoration by reassigning the smallest possible number of subscribers needed to get the links back into balance. This will make the bandwidth of the restored link available to subscribers as quickly as possible without unnecessarily affecting the connection of more subscribers than required. If the restored link affects subscribers that were assigned by the Preferred WAN VSA they will be reassigned back to their preferred link once it is restored.

If Active Rebalancing is not selected current subscribers will NOT be re-assigned, but new subscribers will be assigned to that interface (in accordance with the load balancing algorithm) until that link is again in balance. In this mode subscribers using the Preferred WAN RADIUS VSA will not be assigned back to their preferred WAN connection once it is restored.

An NSE reboot will rebalance all subscribers.

Subscribers will use the IP address of their WAN port (or assigned additional NAT address) for their DAT sessions.

Run Time Status gives a useful summary of all Load Balancing settings and subscriber distribution.

As a complementary feature to Load Balancing, 8.2 can now actively monitor each WAN connection to assure that full network functionality exists.

Interface Monitoring must be enabled - it is off by default. It is set separately for each configured WAN interface.

Three failures must occur before the system sets the port status to Unavailable and re-assigns subscribers.

Monitoring may be configured for both the Monitoring Interval (default is 60 seconds) and for three different methods as required by the network:

- The default method (Automatic) will generate a random DNS query to each configured DNS server. Receiving an "Error" back from the server(s) verifies full network connectivity.
- Host Probing (Ping) - A Host or IP address can be pinged to verify connectivity via ICMP response.
- Host Probing (HTTP) will generate an HTTP GET to the configured Web address. The HTTP response will verify network connectivity.

New Consolidated Routing Interface. All Routing configuration additions and deletions are now made on the same page. Manually added routes (Static/Persistent) are now shown in their own section for easy reference and modification.

A new separate iNAT interface page shows the settings for each port in either WAN or OOS modes. Ports in SUB mode are not shown.

Each of the displayed ports has individual iNAT / Subscriber tunnel settings accessible by clicking on that port's link.

A new improved interface allows easy deletion of any iNAT address range.

New Current Subscriber Table.

Display of system information on LCD

• Platform and Firmware Version Installed • Primary IP Address of the NSE • NSE ID • Active Subscribers
Beginning in 8.2, the NSE now has support for switching the WMI interface itself to a different language. Initially, support is provided for English and Simplified Chinese.

Release 8.1 December 2012

Description of Feature / Enhancement Added
Micros Fidelio Query and Post over TCP is now supported.
NSE now supports query only to enable "Free for user" support - the query is done but no billing occurs (for both Micros and Micros Fidelio).
"Dynamic" Bandwidth Management – It is no longer necessary to reboot the system to enable/disable Bandwidth management.
DHCP pool count increase. The NSE now supports up to 10,000 individual DHCP pools.
Potential system time "drift" has been greatly reduced.

Bugs and Issues Fixed

The issues described below have been corrected in the releases specified.

Release 8.12 August 2018

Description of Bugs / Issues Fixed
Using the pre-defined PMS template, guests with the NPY flag set were not able to gain internet access, even if the "Free for PMS Use" option was selected in the billing plan.
When using Micros Fidelio, the NSE did not support 40 characters for the Guest Name field.
Several RADIUS options did not have corresponding OID's in the MIB table: Enable Automatic Subscriber Reauthentication; Automatic Subscriber Reauthentication Timeout; Restrict Reauthentication to Originally Authenticated Zone; Enable Session-Terminate-End-Of-Day When Authorized; Enable Byte Count Reset On Account Start.
Subscriber up/down byte counts were not updating properly when Fast Path is enabled.
When using LAG's, the source MAC address (for traffic originating from the NSE) in the LAG traffic was incorrect.
Parameter signing was not working correctly when used with Hyatt Freebird.

Release 8.11 January 2018

Description of Bugs / Issues Fixed
If a change or addition was made to the PMS redirector configuration (link records were added or modified, etc), when the updated configuration was saved, the changes were written to nseconf.txt, but were not read back into the configuration unless the redirector feature was enabled. Enabling the feature shouldn't be necessary to view the actual state of the configuration.
Subscribers using "Public" subnets would have their address translated (i.e., were being NAT'd) if that subnet was different from the WAN port subnet (this was incorrect because subscribers on a NSE Public subnet should never be translated).
The WAN interface default gateway could "oscillate" between old/new value after being modified.
The XML SUBSCRIBER_QUERY_CURRENT command was not returning bandwidth values correctly in the MAX_BW_UP and MAX_BW_DOWN elements.

In network configurations where the NSE is behind a NAT, IPsec was not invoking connections over UDP port 4500 (for NAT traversal) correctly.
When sending an XML command to the NSE over a secure connection using wget, the connection was not terminated properly.
When the "later login supersedes previous" RADIUS option is enabled, if the NSE received two XML RADIUS login requests very close together in time for the same subscriber, the accounting packets for the session that results could contain an empty value in the "acct-session-id" attribute.

Release 8.10 September 2017

Description of Bugs / Issues Fixed
When the "Later login supersedes previous" RADIUS client option was enabled, a timing problem could occur that resulted in loss of the Session ID value in some accounting packets.
LACP LAG connections were not connecting successfully to some Cisco switches.
PPPoE connections were not connecting successfully with the WAN-side VLAN option enabled.
DNS names with a single character in the most specific name field (such as "q.mycompany.com" or "s.example.com" would not resolve properly when entered on the NSE's System / ICMP page.
On the AG 2500, after a reboot, an intermittent problem could occur such that the administrative interfaces could not be reached over the network. This was due to a boot sequence timing issue.
Problem on the AG 5900 where SNMP octet and packet count values for the fiber interfaces were not reporting correctly.
On the configuration page for the PMS redirector, some records in the Link Initialization and Expected Responses sections were displaying incorrectly, and the field content could not be modified.
When using system failover, on the AG 5900 platform, if the subscriber count was very large, the authfile.dat file that holds the subscriber profiles was not being transferred successfully from the Primary to the Secondary.

Release 8.9 May 2017

Description of Bugs / Issues Fixed
The XML API and Port Location tables did not handle embedded special characters in certain fields.
Use of the CLASS_NAME element in an XML Group Add command now works correctly.
In the 8.8 release, in the WMI, the "Cascading" buttons in the Port Location configuration "Access Concentrator" section did not work properly (although the configuration could still be performed via the CLI).
In a Port Location table entry, if either Credit Card, PMS, or Facebook Login (or any combination thereof) was selected, and the Billing Plan option was set to "No plans," an error message would be generated when saving the page (since all of those login types require at least one plan). However, if RADIUS login was also selected, the error message would not appear (though it still should have).
Use of a colon character (':') in a RADIUS shared secret string now works correctly (previously this could cause the string to be truncated).
A condition existed where logging out of a serial CLI session immediately following a soft reboot of the NSE could result in a subsequent "silent" reboot.
When an entry in the NSE's internal database contained no expiration time, and then that record was modified via SNMP, upon reboot the record would be lost.
Minor issues with the Trap Recipient IP and DAT Trap Interval fields on the WMI SNMP page.
Under certain conditions some syslogs could be lost, and overall syslog throughput was limited. Syslog processing has been considerably improved to alleviate this.
Changes made by Facebook in their login mechanism had resulted in problems with the NSE's Facebook Login feature. The NSE code has been updated so that it now operates correctly with these changes.

Release 8.8 January 2017

Description of Bugs / Issues Fixed
Enabling the NSE's DNSSEC feature could potentially result in a lockup condition.
A link negotiation problem with certain Cisco switches has been corrected (this may also correct similar issues with other switches / interfaces if such symptoms are observed using

earlier NSE builds).
When using the NSE's Local Web Server (LWS) feature, if a landing page was referenced by an "?OS=" parameter in a secure URL string (i.e., https), the redirect to that page was not handled properly.
Use of the CLASS_NAME element in an XML Group Add command did not work correctly.
A condition existed where logging out of a serial CLI session immediately following a soft reboot of the NSE could result in a subsequent "silent" reboot.
Tables displayed in the Web Management Interface will now scroll properly on Apple iOS devices.
Under certain conditions, the NSE could stop sending XML Portal Post messages.
PPPoE authentication using PAP could fail.
An interface set to PPPoE will now operate properly immediately after being changed to WAN from OOS (previously the system could require a reboot before the PPPoE connection could be successfully established).
Command Line Interface settings for the Bandwidth Management feature are now located in their own sub-menu (under Configuration).
Using the RADIUS "Remember Me" login option could result in an endless loop if no credentials were entered.
Routing for multiple WAN ports now works correctly when Load Balancing is disabled.
The character limit for Facebook App IDs has been increased.

Release 8.7 October 2016

Description of Bugs / Issues Fixed
A reboot could affect RADIUS subscribers with individual bandwidth caps. Specifically, authenticated RADIUS subscribers could be improperly placed in bandwidth groups. The issue did not affect subscribers already assigned to group bandwidth policies, nor subscribers authenticated with PMS, Credit Card, or XML (auth file entries).
Connection issues existed when using the Microsoft Edge browser to make secure (HTTPS) connections to the NSE's WMI interface.
Improved ability of AG 5800 to auto-negotiate Gigabit Ethernet parameters with Cisco WS-

C2960X-PS-L hardware version V02.
When using MAC authentication, if the MAC authentication transaction had already occurred before a browser (or other web app) was launched, the user would be re-directed to a message saying "You have been logged in by MAC authentication" before the desired destination page was reached. This sometimes caused problems for certain devices, so this behavior has been removed.
Problems with loss of MAC Authentication configuration settings after performing an upgrade.
Some issues that were occurring with PPPoE negotiation have been addressed.
Intermittently, the VLAN ID could be lost when adding a pending subscriber to the NSE database (via the "Add to Database" button) for the purpose of configuring it as a Device.
When using the NSE's Local Web Server (LWS) option, if a local page was configured to redirect to a secure site after the completion of a login, the redirect to the intended site could fail and instead display a message stating "You are already logged in."
On the Subscriber Administration / Statistics page, the "Subscriber Licenses in Use" field could give an incorrect count of the number of licenses used in the event that AAA was disabled (entries in the NSE database were included in the total even though they are not effective in this situation). Now if AAA is off, the database entries are omitted from the total.
It was found that some enhancements to the Web Management Interface had the effect of preventing scrolling on iOS devices (iPhone, iPad).
Radius Service Profiles could be incorrectly displayed as plaintext in the Web Management Interface.
If a Realm Routing Profile was created using a DNS-based radius profile, after submission the Realm profile could appear as empty.
When the HTTPS redirect feature is enabled, a few sites have experienced pagefault / reboot problems. Code improvements have been made to address this situation.
When using the Automatic Subscriber Re-authentication feature for RADIUS users, if during the initial login as Portal ID was included, it could be lost when the automatic re-authentication took place (after a session timeout, for example).
If the configured credentials for the Radius Remote Test Login feature were identical to those used for manager login, then administrative access to the system via the Command Line Interface or FTP would not succeed. This has been corrected by requiring that the different login types configured on the System/Login page must have unique usernames.

In a Multi-WAN setup, Static Port Mappings could in some cases become non-functional.
In some cases, connections to a PMS from the system over TCP could become unstable.
A problem existed when trying to set the secret key for a secondary authentication server in a RADIUS profile via SNMP.
When logging users in via the XML RADIUS_LOGIN command, if the PORTAL_SUB_ID element was included and the Radius Automatic Subscriber Re-authentication feature was enabled, when an automatic re-authentication took place, the portal sub ID value would be lost and set back to zero.

Release 8.6 March 2016

Description of Bugs / Issues Fixed
A condition in which an SNMP page fault could occur while accessing the aaaAuthSubTable OID.
If the login credentials defined for the NSE contained certain special characters, the login to the NSE flash via FTP would fail.
Occasionally, after logging in, a PMS subscriber would get redirected to a message reading "You are already logged in!" instead of the original target URL.
Previously, if a subscriber had logged via a method that does not support logging out (such as a Credit Card login), if an attempt was then made to logout via the configured logout IP, a message indicating the user was not logged in could be displayed. This was confusing, and has been corrected to display a more accurate message.
A problem existed when trying to set the secret key for a secondary authentication server in a RADIUS profile via SNMP.
In a Multi-WAN setup, Static Port Mappings could in some cases become non-functional.

Release 8.5 August 2015

Description of Bugs / Issues Fixed
Under certain conditions, a situation could occur in which some RADIUS attributes were intermittently missing from Access Request packets.
An issue was discovered in which a Routed Subscriber configuration would fail to pass traffic if IPv6 was disabled.
X over Y users are now properly removed from the NSE's internal database when the Y time expires.
A situation in which credentials that are used with the RADIUS Termination Action attribute were not being retained properly.
Previously, it was possible to create a DHCP pool in which the scope included some blacklisted (i.e., reserved) addresses. The administrator is now notified via a warning message if the submitted configuration would create such a condition (see additional information in the "Known Issues" section below).
A situation existed in which a "Subnet" reference in a port location entry could be "orphaned" if the DHCP pool to which it referred was deleted. Now, if an attempt is now made to delete such a pool, the deletion will not be allowed.
A condition could occur in which an SNMP pagefault could occur while accessing the aaaAuthSubTable OID.

Release 8.4 April 2015

Description of Bugs / Issues Fixed
A condition could occur in which fragmented UDP packets arriving from a subscriber could trigger erroneous iNAT sessions.
When upgrading from release 8.2 or earlier to the current build, it was possible that stored RADIUS accounting data (from any transactions that had not succeeded and were still being retried) would be lost.
Connections from SSLv2 and SSLv3 clients will be disallowed by default to address the POODLE attack vulnerability. A check box that will allow access from these clients is now added to the Access Control page.
A situation in which RADIUS accounting messages could be delayed.
In system failover mode, if iNAT was enabled on the secondary and addresses were defined, those addresses would inadvertently respond to pings.
A condition could occur in which SSH socket connections on the WAN side of the system would not succeed.
Occasionally, when operating as a DHCP client, an NSE WAN interface would fail to obtain a default gateway value.

Release 8.3 June 2014

Description of Bugs / Issues Fixed
Room numbers that include a leading zero are now supported by the PMS interface for Marriot Wired-For-Business and FOSSE systems.
Billing Plan bandwidth limits could not be set to a value greater than 1500kbps.
In certain situations, it was possible for an entry to be registered in the current table with a broadcast IP address (255.255.255.255), which then could cause other issues. This is no longer allowed.
A condition could occur in which an erroneous syslog was sent with respect to ESP sessions.
In some cases, static or persistent routes entered into the routing table for which the subnet was not on an even class boundary would have an incorrect mask value.
ICC now handles plan definitions correctly even if the first plans in the numerical sequence are defined as X over Y.

Release 8.2 April 2013

Description of Bugs / Issues Fixed
When using the system failover, the NSE can send status messages between the primary and secondary on the subscriber side to convey status information in the event of a link loss on the primary. This mechanism was not working properly.
Certain issues could cause transaction failures when using the PMS Serial Redirector.
In some cases, static port mappings to devices would not work immediately after a reboot until some traffic was generated by the device itself.
When using RADIUS Automatic Subscriber Reauthentication, a situation could occur where expired Wireless devices would not be able to reconnect successfully.
In some cases, the “"Maximum TCP MSS" setting for PPPoE was not being applied.
Improvements have been made to the NSE’s subscriber-side DHCP service. This corrects certain cases in which it was seen that DHCP pools were no longer handing out leases as expected.
In some cases, when RADIUS authentication is in use and subscribers were using Google Chrome, URL redirection via the Nomadix URL redirection VSA would fail.
When administratively adding a subscriber, device, or group account, the bandwidth limit is now correctly set at 1000000K.
Previously, if the Portal Post URL was configured using a DNS name, if the resolution during the initial boot of the system failed, no retries were performed unless the Portal Post value was administratively re-entered or changed. As a result, Portal Post messages could not be sent. This has been modified so that if the resolution fails, the NSE will re-try at periodic intervals until it succeeds.
A condition could occur in which the NSE was sending a non-standard EOL sequence during telnet connections.
The Network Info > Interfaces page now correctly displays the interface link speed and duplex status.

Release 8.1 December 2012

Description of Bugs / Issues Fixed
Quality of Service (QoS) policies assigned via port location will now be applied even if the port is set to "No Charge."
In previous versions, when using IPSec, the NSE would allow IPSec global settings to be enabled even if no tunnel peer or tunnel policy configurations were yet defined. Now at least one peer definition and one policy definition must exist before IPSec can be enabled.
A memory depletion issue could occur when QoS is enabled.
A condition could occur in which Subscriber Tracking syslogs were missing the timestamp value.
Administrative access to the NSE via secure https connections no longer generates error syslogs.
The syslog to file operation now works even if no external syslog server is being used (i.e., even if no value is entered in the Server IP field for the given syslog type).
In 8.0 builds, a problem was found in which status messages were not sent to the Portal Post URL in the event of RADIUS session or idle timeout.
In some cases, if the NSE was unable to resolve a Portal Post URL DNS name at system boot time (perhaps due to intermittent network problems), Portal Post messages could not be sent. The NSE now periodically refreshes this value, and will retry at a brief interval if the initial attempt fails until a successful resolution is achieved.
When using an IPSec tunnel connected to a single remote host (i.e., utilizing a 32-bit mask), it was found that SNMP packets were not being successfully transferred.
When using of MAC filtering, if a large number of MAC addresses were entered in the filtering table, ad problem could occur.
In 8.0 and later releases, SIP ALG processing has been removed. The NSE utilizes Endpoint-Independent Mapping for UDP traffic; thus, allowing SIP clients to successfully negotiate connections through the gateway without a need for the internal SIP ALG processing that the NSE previously provided (the "SIP" checkbox does still appear on the iNAT page, but its use has been deprecated and the checkbox will be removed in a future release).

Known Bugs and Issues

Release 8.12 July 2018

Known Bugs / Issues
When using one of the SFP+ ports as a WAN interface, if Class Based Queueing is also enabled and a given class is invoked for a subscriber that is assigned to that interface, the class name will display in the current table with an asterisk (*). This normally indicates that the class be assigned does not exist on the interface (i.e., the subscriber's class assignment is erroneous), but on the SFP+ interfaces, this indication is displayed even when the assignment is valid. This condition is expected to be corrected in a subsequent release.
Currently, the Bill Record Mirroring feature only supports PMS charges. Credit Card transactions performed using PayPal will not be mirrored to the configured Bill Record Mirroring servers.
Subscribers with an IP address on the same subnet as a Remote IPSec subnet do not get redirected to the splash and login page correctly.
There are certain addresses on the NSE that are considered "blacklisted" – that is, they are defined for specific purposes and are reserved, and therefore unavailable for use by subscribers (these include WAN interface addresses, DNS server entries, iNAT pool addresses, and some others). In previous builds, a defect existed in which it was possible to configure a DHCP pool such that the pool scope could overlap these addresses, and the conflict was not caught. This was corrected in the 8.5 release. However, if while on a build prior to 8.5 such a situation did exist, and the system is then upgraded to 8.5 or later, after the upgrade, the "offending" DHCP pool will be deleted, and a DHCP-related syslog will be sent. If this occurs, it will be necessary to re-create the pool (and if while creating the new definition the same conflict arises, the system will now catch this and not allow the pool to be created incorrectly as before).
When using Micros Fidelio PMS, an option now exists to disable the need to enter the Registration Number (configured on the WMI PMS page). If this option is used, administrators will also want to modify the prompt string that appears on the page on which subscriber enter the PMS login credentials, so that it doesn't refer to the registration number field. This can be done by modifying the string in the "Micros Fidelio Login Message" field, located on the Subscriber Interface \ Login UI page.
The NSE Hyatt Freebird feature requires authorization from the Hyatt Corporation in order to be used. It is a licensed feature. Please contact Hyatt for inquiries regarding availability of the Freebird functionality.

Known Caveats for Deployment

1. On the AG 5900 and AG 2500, power management constraints require that the power switch be depressed for several seconds to shut down the unit.

2. When configuring any of the physical Ethernet ports other than the labeled WAN interface to function in WAN mode, care should be taken by administrators to insure that a given port that has been functioning in the WAN role is *not* inadvertently changed to the Subscriber role while a physical connection to a WAN-side subnet is still in place. If that occurs, and the NSE's subscriber-side DHCP service is running, hosts on the WAN subnet may begin to pick up addresses from the NSE's subscriber pool(s), and find that web requests are being re-directed to the NSE's login page.

3. The support for multiple WAN ports provides the ability to balance subscriber traffic between two or more WAN ports. However, these features are not all available after a software upgrade without additional actions. Load balancing and failover of subscriber and administrative network traffic require upgrading the per-unit license to include the Load Balancing feature. Without this feature, support for multiple WAN interfaces is strictly limited. Subscriber traffic will be able to use only a single WAN port, and the system will have no ability to automatically direct traffic to alternate WAN ports in response to a network link outage. This behavior will also be seen if a license upgrade has been performed but Load Balancing is disabled, which in large part restricts the NSE's WAN functionality to that of previous software releases. If you wish to use multiple network WAN links, Nomadix strongly recommends purchasing the Load Balancing upgrade, and for full functionality Load Balancing should be configured in either Failover or Load Balancing modes.

4. If two or more NSE interfaces are set to the WAN role and are configured such that they are attached to the same local subnet, if there is a port failover event for one of those ports, packets will then be sent using a different source address. Therefore, any systems or devices on that subnet that invoke processing decisions based on packet *source* addresses (such as RADIUS servers) should be configured so that they will respond to any of the NSE interface addresses that are configured on that subnet. For example, if two NSE WAN ports having addresses of 205.5.6.10 and 205.5.6.20, respectively, are directly connected to the 205.5.6.0 subnet, and a RADIUS server is located directly on the 205.5.6.0 subnet, the server should have both 205.5.6.10 and 205.5.6.20 configured as valid RADIUS client addresses in order to guarantee that any RADIUS requests originating from the NSE for that server will be accepted.

5. If two or more Ethernet interfaces are configured in the WAN role, and both Load Balancing and Class-Based Queueing are enabled, when a subscriber logs in via RADIUS to an account that returns both the Preferred WAN and Class attributes, that subscriber will be assigned to the correct WAN port and class accordingly, and will be shown as such in the current table. However, if subsequently internet access becomes unavailable for the WAN interface to which the subscriber is assigned, the

subscriber's traffic should be routed out through a different available WAN interface, but the current table will not accurately indicate this (i.e., the preferred WAN port will still be shown as the active primary, and the class information will not display the asterisk that indicates that the class cannot currently be applied to the subscriber's traffic).

6. When configuring two NSE's to operate in system failover mode, it is important to remember that the Ethernet Port settings are NOT transferred from the Primary to the Secondary. This includes not only the IP address information (including DNS), but the port role settings as well (i.e., WAN, SUB, or OOS). This can become an issue if the NSE is configured with multiple WAN or subscriber ports, or any other changes from the default port roles. Therefore, assuming that it is desired for both the Primary and Secondary to have the same logical port role setup, the port role configuration on the secondary NSE should be manually configured to match that of the primary prior to enabling the failover operation.

7. The clustering feature provides a means to spread a large number of subscribers across multiple NSE's. However, there is a limitation with regard to the number of defined port locations that can be configured. A given NSE does not support more defined port locations than the number of licensed users on that unit, and the port location configuration will need to be common to all units in the cluster. Therefore, the maximum number of port locations that can be defined will be equal to the number of licensed users on a single NSE in the cluster. For example, if a cluster is set up using two AG5800's, each of which has a license key enabling 4000 users, the maximum user count will be 8000, but the maximum number of port locations that can be defined will be 4000.

8. When initially configuring the clustering feature in an existing installation (which will normally involve adding one or more additional NSE's and then enabling the feature), if certain users appear to lose access, this can be corrected by having those users disconnect and then reconnect again.

9. When configuring multiple WAN interfaces, please note that explicitly labeled ports (WAN and LAN) cannot be configured to the opposite role. Such ports may set to Out Of Service, but explicitly labeled WAN ports may not be configured to the SUB role, and vice versa. Ports labeled Eth(X) or Aux(X) may be configured to any role.

10. The Information Control Console / Logout Console feature (ICC/LC) consists of a pop-up window that allows subscribers the option to log out of their current access plan, and also provides a means to display time usage information and a certain amount of advertising space. Because of the different ways that current generation browsers support pop-up windows (in addition to the multitude of blocking mechanisms that are available on the open market), there may be differences in the display, or the ability of the ICC/LC to appear for the subscribers.

11. When the NSE is placed in bridge mode, all packets that arrive at any interface will automatically be propagated to all other interfaces, unless those interfaces are

currently set to OOS (Out of Service). Therefore, if the NSE is configured to use multiple WAN interfaces that connect to different subnets, entering bridge mode has the effect of creating direct connections between those subnets. This is usually an undesirable condition. It is recommended that only one WAN interface should be active before placing the NSE in bridge mode (either by placing all other WAN interfaces into the OOS role, or by physically disconnecting them).

12. When using a routed subscriber configuration, if Cisco HSRP (Hot Standby Router Protocol) is being used for routers on the subscriber side of the NSE, there are some additional issues to consider. HSRP routers are normally configured to use virtual MAC and IP addresses, and these defined values must be entered into the NSE's ARP and routing tables as appropriate. However, for certain functions (such as ARP requests), the HSRP routers use the physical source MAC and source IP of its NSE-facing interface, instead of the virtual values. For this reason, it is necessary to configure the NSE to add persistent ARP entries for physical IP and MAC addresses of each NSE-facing router interface of all directly connected routers on the subscriber side.

13. In 8.0 and later releases, SIP ALG processing has been removed. The NSE utilizes Endpoint-Independent Mapping for UDP traffic; thus, allowing SIP clients to successfully negotiate connections through the gateway without a need for the internal SIP ALG processing that the NSE previously provided.

14. Certain features in this release (SSL, HTTPS Redirection, and HTTPS management connections to the Web Management Interface) require that a working set of certificate files (consisting of cakey.pem, cacert.pem, and server.pem) is installed on the flash. This release ships with a "dummy" set of these files that will allow these features to be enabled; however, if these dummy files are used, any systems that attempt to connect to the NSE using such connections will receive security warnings. Please see the section in the User Guide that covers the set up of the SSL feature for instructions on how to configure a properly working set of certificate files for your specific installation.

15. The NSE's IPSec feature now includes a NAT Traversal option. This can be used in cases where there are one or more NAT's between the NSE and the IPSec tunnel endpoint that are unable to translate IPSec traffic. It should be noted that in such situations, if NAT Traversal is *not* used initially, the NSE may still report that tunnel(s) are up, but actual tunneled traffic will not get through (this is because the negotiation phase may not be able to directly detect the presence of the NAT's in the path). If this occurs, it is recommended to enable NAT Traversal and see if this corrects the difficulty.

16. Connections from mis-configured (i.e., translated) subscribers that run over UDP do not support UDP fragmentation. If transactions from such users (such as TFTP connections) are not successful, it may be necessary to adjust the endpoint configurations so that fragmentation is not invoked.

17. If a user is entered via the XML User Payment Plan command and a defined X-over-Y plan is specified, then the Current Plan field in the authorization database will be set to -1 (simply denoting entry via XML), instead of flagging the XoverY plan properly. This prevents the logout / log-back-in feature from working. However, if the user is added via the XML Add User X-over-Y command and the same plan is specified, the user will be entered with the Current Plan field flagged correctly (as *n, where n is the plan number). The logout function will then work properly.

18. When the NSE is configured to use GRE tunneling and GRE is enabled, any servers / hosts that provide essential network services (such as DNS, RADIUS, FTP, Portal Page / Post, or other services that need be accessed through connections originated by subscribers or by the NSE itself) SHOULD NOT be configured with non-tunneled local addresses (i.e. on the same subnet as the NSE WAN interface). Access to devices / hosts on the immediate non-tunneled local subnet is undefined for NSE-initiated connections when GRE is enabled. The NSE's management interfaces will continue to be accessible from systems on the local subnet via the NSE's WAN IP, *provided that those devices are initiating the transaction*, but it should be assumed that traffic originating from or "through" the NSE will be routed through the GRE tunnel.

19. Changing the PMS payment mode (from pre-pay to post-pay, or vice versa) while PMS subscribers are currently in a valid state may result in erroneous charge and/or logout behavior for those subscribers. It is recommended that if a configuration change of the payment mode is required, the operation should be performed when no PMS subscribers are logged in.

20. ICC does not support changing billing plans if subscribers purchased access with Post-Paid PMS.

21. When the NSE is configured to use a dynamic address (whether via DHCP or PPPoE), but for some reason is unable to obtain one (such as a link-down condition on the network side) subscriber-side access to the unit will succeed only if the subscriber system is on the same subnet as the NSE's Administrative IP.

22. The SNMP MIB contains SNMP objects for all major NSE features running on the Access Gateway. If your current license does not contain a particular feature, you will not be able to GET or SET the object for the feature.

23. You cannot configure Auto-Configuration using SNMP.

24. You cannot Delete All DAT Sessions using SNMP.

25. You cannot configure PMS interface settings using SNMP

26. The Administrative interface that displays the DAT sessions for the Nomadix NSE shows both Active and Inactive sessions at the same time. While the DAT session cleanup

routine is working, there will still be inactive sessions on a unit that are displayed in the management interface.