Release Notes for Cisco Prime Network Control System, Release 1.1.0.58

February 2012

These release notes describe the requirements, features, limitations, restrictions (caveats), and related information for the Cisco Prime Network Control System (NCS) Release 1.1.0.58, which is a part of the Cisco Unified Network Solution. These release notes supplement the Cisco NCS documentation that is included with the product hardware and software release.

Contents

These release notes contain the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The NCS is the next generation network management platform for managing both wired and wireless access networks. NCS delivers converged user, access, and identity management, with complete visibility into endpoint connectivity regardless of the device, network, or location. NCS speeds up the troubleshooting of network problems related to client devices, which is one of the most reported customer pain points. NCS also provides identity security policy monitoring through integration with Cisco Identity Services Engine (ISE) to deliver visibility into compliance based on real-time contextual information from the network, users, and devices across the entire wired and wireless access network.

NCS is a scalable platform that meets the needs of small, mid-sized, and large-scale wired and wireless LANs across local, remote, national, and international locations. NCS gives IT managers immediate access to the tools they need, when they need them, so that they can more efficiently implement and maintain secure wireless LANs, monitor wired and wireless LANs, and view users and endpoints across both networks all from a centralized location.

Operational costs are significantly reduced through the workflow-oriented, simplified, and intuitive user experience of the platform, as well as built-in tools that improve IT efficiency, lower IT training costs, and minimize IT staffing requirements, even as the network grows. Unlike overlay management tools, NCS incorporates the full breadth of management requirements from radio frequency, to controllers, switches, endpoints, and users on wired and wireless networks, and to mobility and identity services to deliver a scalable and unified platform.

Key benefits of NCS 1.1.0.58 include the following:

- Ease of Use—Simple, intuitive user interface designed with focus on workflow management. It supports user-defined customization to display only the most relevant information.
- Scalability—Manages complete lifecycle management of hundreds of Cisco wireless LAN controllers and 15,000 of Cisco Aironet lightweight access points from a centralized location. Additionally, NCS can also manage up to 5000 autonomous Cisco Aironet access points.

Note Each stack or chassis is counted as a single device.

- Wired Management—Comprehensive monitoring and troubleshooting support for maximum of 5000 Cisco Catalyst switches, which allows visibility into critical performance metrics for interfaces, ports, endpoints, users, and basic switch inventory.
- WLAN Lifecycle Management—Comprehensive wireless LAN lifecycle management includes a full range of planning, deployment, monitoring, troubleshooting, remediation, and optimization capabilities.
- Planning and deployment—Built-in planning and design tools simplify defining access point placement and coverage. Information from third-party site survey tools can be easily imported and integrated into NCS to aid in WLAN design and deployment. A broad array of integrated controller, access point, and command-line interface (CLI) configuration templates deliver quick and cost-effective deployment.
- Delivery Modes—Delivered as a physical or a virtual appliance allowing deployment scalability to help customers meet various deployment models.

In addition to these, NCS 1.1.0.58 supports non-English characters and provides greater stability.

Requirements

This section contains the following topics:

Supported Hardware

NCS software is packaged with your physical appliance, can be downloaded as an image for installation, or can be downloaded as a software image to run as a virtual appliance on a customer-supplied server. The NCS virtual appliance can be deployed on any of the platforms listed in Table 1.

Table 1 Supported Hardware

Hardware Platform	Configuration
Cisco Prime NCS High-End Virtual Appliance (physical/virtual appliance)	• Supports up to 15,000 Cisco Aironet lightweight access points, 5,000 autonomous access points, 5000 switches, and 1200 Cisco wireless LAN controllers. • Supports up to 100,000 unified wireless clients, 50,000 wired clients, and 20,000 autonomous clients. • Processor Cores: 8, at 2.93 GHz or better. • Minimum RAM:16 GB. • Minimum hard disk space allocation: 400 GB.
Cisco Prime NCS Standard Virtual Appliance	• Supports up to 7,500 Cisco Aironet lightweight access points, 2,500 autonomous access points, 2,500 switches, and 600 Cisco wireless LAN controllers. • Supports up to 50,000 unified wireless clients, 25,000 wired clients, and 10,000 autonomous clients. • Processor Cores: 4, at 2.93 GHz or better. • Minimum RAM: 12 GB. • Minimum hard disk space allocation: 300 GB.

Table 1 Supported Hardware (continued)

Hardware Platform	Configuration
Cisco Prime NCS Low-End Virtual Appliance	• Supports up to 3,000 Cisco Aironet lightweight access points, 1,000 autonomous access points, 1,000 switches, and 240 Cisco wireless LAN controllers. • Supports up to 25,000 unified wireless clients, 10,000 wired clients, and 5,000 autonomous clients. • Processor Cores: 2, at 2.93 GHz or better. • Minimum RAM: 8 GB. • Minimum hard disk space allocation: 200 GB.
VMware ESX and ESXi Versions (Virtual Appliance on a Customer-Supplied Server)	• If deploying NCS as a virtual appliance on a customer-supplied server, one of the following versions of VMware ESX or ESXi may be used: – VMware ESX or VMware ESXi version 4.0 – VMware ESX or VMware ESXi version 4.1 – VMware ESXi version 5.0 **Note** VMware Tools version 4.1 is preinstalled in the NCS virtual appliance.

Note If you want to use a Cisco UCS server to deploy a virtual appliance for NCS, you can use the UCS C-Series or B-Series. Make sure the server you select matches the processor, RAM and hard disk requirements specified in the "Supported Hardware" section on page 3.

Note Non-English characters are supported from Cisco Prime Network Control System, Release 1.0.1.4.

Note These specifications relating to the number of clients supported on different NCS configurations are based on combination of internal lab tests and our experience with large customer installations.

Supported Browsers

The NCS user interface requires Mozilla Firefox 3.6 or later minor version and Internet Explorer 8.x with the Chrome plugin releases or Google Chrome 12.0.742.x. The Internet Explorer versions less than 8 are not recommended. The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Supported Devices

Table 2 lists the NCS supported devices for controllers, access point images, Identity Services Engine (ISE), and mobility services engines (MSE).

Table 2 Supported Device Matrix

Supported Switches	Supported Controllers	Supported MSE Devices[1]	Supported ISE Devices	Supported Lightweight APs	Supported Autonomous APs
Cisco Catalyst 2960, 2975 Switches [IOS12.2(50) SE], Cisco Catalyst 3560 Switches [IOS12.2(50) SE], Cisco Catalyst 3750 Switches [IOS12.2(50) SE], Cisco Catalyst 4500 Switches [IOS12.2(50) SG], Cisco Catalyst 6500 Switches [IOS12.2(33) SXI].	Cisco 2100 Series Cisco 2500 Series Cisco 4400 Series Cisco 5500 Series Cisco Flex 7500 Series Wireless LAN Controllers Cisco Catalyst 3750G Series Integrated Wireless LAN Controllers Cisco Catalyst 6500 Series Wireless Services Modules (WiSM/WiSM2) Cisco Wireless LAN Controller Module on SRE Cisco Wireless LAN Controller Module (WLCM and WLCM-E) for Integrated Services Routers	Cisco MSE 3300 Series	Cisco ISE 3300 Series	Cisco 600 Series, Cisco 1040 AP, Cisco 1130 AP, Cisco 1140 AP, Cisco 1200 AP, Cisco 1230 AP, Cisco 1240 AP, Cisco 1250 AP, Cisco 1260 AP, Cisco 1500 AP, Cisco 1524 AP, Cisco 1552 AP, Cisco 3500i AP, Cisco 3500e AP, Cisco 3500p AP, Cisco 3600i AP, Cisco 3600e AP, Cisco 801 AP.	Cisco 1130 AP, Cisco 1200 AP, Cisco 1230 AP, Cisco 1240 AP, Cisco 1250 AP, Cisco 1260 AP, Cisco 1141 AP, Cisco 1142 AP, Cisco 1800 and Cisco 800 ISR Series. Cisco Aironet 1310 and 1410 Bridges

1. NCS does not support Cisco 2700 or 2710 Location Appliance.

Supported Versions

Table 3 lists the NCS supported versions of controllers, access point images, Identity Services Engine (ISE), and mobility services engines (MSE).

Table 3 Supported Version Matrix

NCS Version	Supported Controller Version	Supported MSE Version	Supported ISE Version	Supported Cisco IOS Switch Version	Operating System Requirements	Supported ACS Server Version
NCS 1.1.0.58	7.2.103.0, 7.0.230.0, 7.1.91.0, 7.0.220.0, 7.0.116.0, 7.0.98.218, 7.0.98.0, 6.0.202.0, 6.0.199.4, 6.0.196.0, 6.0.188.0, 6.0.182.0, 6.0.108.0, 4.2.209.0, 4.2.207.0, 4.2.205.0, 4.2.176.0, 4.2.173.0, 4.2.130.0, 4.2.112.0, 4.2.99.0, 4.2.61.0	7.2.103.0, 7.0.230.0, 7.0.220.0, 7.0.201.204, 7.0.112.0, 7.0.105.0, 6.0.202.0, 6.0.103.0, 6.0.105.0 (LBS).	ISE 1.0 ISE 1.1	IOS12.2(50)SE, IOS12.2(50)SG, IOS12.2(33)SXI	VMWare ESX or VMWare ESXi Version 4.0 VMWare ESX or VMWare ESXi Version 4.1 VMware ESXi version 5.0	ACS 4.1, ACS 4.2, ACS 5.1, ACS 5.2, ACS 5.3
NCS 1.0.2.29	7.1.91.0, 7.0.230.0, 7.0.220.0, 7.0.116.0, 7.0.98.218, 7.0.98.0, 6.0.202.0, 6.0.199.4, 6.0.196.0, 6.0.188.0, 6.0.182.0, 6.0.108.0, 4.2.209.0, 4.2.207.0, 4.2.205.0, 4.2.176.0, 4.2.173.0, 4.2.130.0, 4.2.112.0, 4.2.99.0, 4.2.61.0	7.0.230.0, 7.0.220.0, 7.0.201.204, 6.0.202.0, 6.0.103.0, 6.0.105.0 (LBS).	ISE 1.0	IOS12.2(50)SE, IOS12.2(50)SG, IOS12.2(33)SXI	VMWare ESX or VMWare ESXi Version 4.0 VMWare ESX or VMWare ESXi Version 4.1	ACS 4.1, ACS 4.2, ACS 5.1, ACS 5.2

Table 3 Supported Version Matrix (continued)

NCS Version	Supported Controller Version	Supported MSE Version	Supported ISE Version	Supported Cisco IOS Switch Version	Operating System Requirements	Supported ACS Server Version
NCS 1.0.1.4	7.0.220.0, 7.0.116.0, 7.0.98.218, 7.0.98.0, 6.0.202.0, 6.0.199.4, 6.0.196.0, 6.0.188.0, 6.0.182.0, 6.0.108.0, 4.2.209.0, 4.2.207.0, 4.2.205.0, 4.2.176.0, 4.2.173.0, 4.2.130.0, 4.2.112.0, 4.2.99.0, 4.2.61.0	7.0.201.204, 6.0.202.0, 6.0.103.0, 6.0.105.0 (LBS).	ISE 1.0	IOS12.2(50)SE, IOS12.2(50)SG, IOS12.2(33)SXI	VMWare ESX or VMWare ESXi Version 4.0 VMWare ESX or VMWare ESXi Version 4.1	ACS 4.1, ACS 4.2, ACS 5.1, ACS 5.2
NCS 1.0.0.96	7.0.116.0, 7.0.98.218, 7.0.98.0, 6.0.202.0, 6.0.199.4, 6.0.196.0, 6.0.188.0, 6.0.182.0, 6.0.108.0, 4.2.209.0, 4.2.207.0, 4.2.205.0, 4.2.176.0, 4.2.173.0, 4.2.130.0, 4.2.112.0, 4.2.99.0, 4.2.61.0	7.0.201.204, 6.0.202.0, 6.0.103.0, 6.0.105.0 (LBS).	ISE 1.0	IOS12.2(50)SE, IOS12.2(50)SG, IOS12.2(33)SXI	VMWare ESX or VMWare ESXi Version 4.0 VMWare ESX or VMWare ESXi Version 4.1	ACS 4.1, ACS 4.2, ACS 5.1, ACS 5.2

Installing NCS Software

The following steps summarize how to install new NCS 1.1.0.58 software on supported hardware platforms (see the "Supported Hardware" section on page 3 for support details).

Step 1 Click **Cisco Download Software** at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm. You might be required to provide your Cisco.com login credentials.

Step 2 Choose **Products > Wireless > Wireless LAN Management > Network Control > Cisco Prime Network Control System**.

Step 3 Download the appropriate NCS software version .ova image (for example. NCS-VA-1.1.0.X-large/small/medium.ova) and deploy the OVA template.

Step 4 Reboot the virtual appliance to initiate the NCS installation process.

Step 5 Perform the initial NCS configuration according to the instructions in the *Cisco Prime Network Control System Configuration Guide, Release 1.1.* Before you run the setup program, ensure that you know the configuration parameters listed in Table 4.

Table 4 Initial Configuration Parameters

Parameter	Description
Hostname	Must not exceed 19 characters. Valid characters include alphanumeric (A-Z, a-z, 0-9), hyphen (-), with a requirement that the first character must be an alphabetic character. **Note** We do not recommend using mixed case and hyphens in the hostname.
IP address	Must be a valid IPv4 address for the eth0 Ethernet interface.
Netmask	Must be a valid IPv4 address for the netmask.
Default gateway	Must be a valid IPv4 address for the default gateway.
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numbers, hyphen (-), and period (.).
Primary name server	Must be a valid IPv4 address for an additional Name server.
Add/Edit another name server	Must be a valid IPv4 address for an additional Name server.
Primary NTP server	Must be a valid NTP domain.
Add/Edit another NTP server	Must be a valid NTP domain.
System Time Zone	Must be a valid time zone. The default value is UTC.

Table 4 Initial Configuration Parameters (continued)

Parameter	Description
Username	Identifies the administrative username used for access to the NCS system. If you choose not to use the default, you must create a new username, which must be from 3 to 8 characters in length, and be composed of valid alphanumeric characters (A-Z, a-z, or 0-9).
Password	Identifies the administrative password used for access to the NCS system. You must create this password (there is no default), and it must be composed of a minimum of six characters in length, include at least one lowercase letter (a-z), at least one uppercase letter (A-Z), and at least one number (0-9).
High Availability Role	Enter **Yes**, if you want to specify the server as the secondary server for high availability. Enter **No**, if you do not want to specify the server as the secondary server for high availability.
Web Interface Root Password	Enter the root password for the web interface or the NCS root password.
FTP Password	Enter the FTP password.

This section contains the following topics:

NCS License Information

NCS is deployed through a physical or virtual appliance. Use the standard License Center Graphical User Interface to add new licenses, which are locked by the standard Cisco Unique Device Identifier (UDI). When NCS is deployed on a virtual appliance, the licensing is similar to a physical appliance, except instead of using a UDI, you use a Virtual Unique Device Identifier (VUDI). The NCS license is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package is purchased by a customer.

For more detailed information on license types and obtaining licenses for NCS, see the "NCS and End User License" chapter of the *Cisco Prime Network Control System Configuration Guide, Release 1.1.*

For detailed information and license part numbers available for NCS, including licensing options for new installations as well as migration from an existing Cisco product like Cisco Wireless Control System, see the Cisco Network Control System Ordering Guidelines at the following URL: http://www.cisco.com/web/ordering/root/index.html.

Finding the Software Release

If NCS is already installed and connected, verify the software release by choosing **Help > About Cisco NCS**. To find more information on the software release that NCS is running, see the *Cisco Prime Network Control System Configuration Guide, Release 1.1.*

Migrating WCS to NCS

Note You must upgrade your Cisco WCS deployment to Release 7.0.164.3 or 7.0.172.0 or 7.0.220.0 or 7.0.230.0 before you attempt to perform the migration process to NCS 1.1.0.58.

This section provides instructions for migrating the WCS on either a Windows or Linux server to NCS. The NCS release is a major release to provide for converged management of wired and wireless devices, and increased scalability. The NCS platform is based on Linux 64 bit OS, and the backend database is Oracle DBMS. The existing WCS platforms are either Windows or Linux 32 bit and the backend database is Solid DB.

This section contains the following topics:

Note For steps on migrating NCS in a high availability environment, see Chapter 4, "Performing Maintenance Operations" of the *Cisco Prime Network Control System Configuration Guide, Release 1.1.*

Exporting WCS Data

Note There is no GUI for exporting data from WCS 7.x. The **export userdata** CLI command is available in WCS Release 7.x and later, which creates the .zip file containing the individual data file. The CLI does not provide any option to customize what can be exported; all non-global user-defined items are exported.

To export WCS data, follow these steps:

Step 1 Stop the WCS server.

Step 2 Enter the **export** command through the script file and provide the path and export filename when prompted.

Step 3 For Linux, enter the **export.sh all /data/wcs.zip** command. For Windows, enter the **export.bat all \data\wcs.zip** command.

Migrating WCS Data to NCS

To migrate WCS data, follow these steps:

Step 1 Place the WCS export .zip file (for example, wcs.zip) in a repository or folder (for example, repositories).

Step 2 Log in as admin user and stop the NCS server by entering the **ncs stop** command.

Step 3 Configure the FTP repository on the NCS appliance by entering the **repository** command:

```
ncs-appliance/admin#configure
ncs-appliance/admin(config)#repository ncs-ftp-repo
ncs-appliance/admin(config-Repository)#url ftp://209.165.200.227//
ncs-appliance/admin(config-Repository)#user ftp-user password plain ftp-user
```

Note Make sure the archived file is available using the **show repository** *repositoryname* command.

Step 4 Enter the **ncs migrate** command to restore the WCS database:

```
ncs-appliance/admin# ncs migrate wcs-data wcs.zip repository ncs-ftp-repo
```

By default, no WCS events are migrated.

Step 5 Enter the **ncs start** command to start the NCS server after the upgrade is completed.

Step 6 Log in to the NCS user interface using the root login and the root password.

Non-upgradable Data

The following data are not upgradable from WCS to NCS:

- Certain Reports (AP Image Predownload, AP Profile Status, AP Summary, Client Count, Client Summary, Client Traffic, PCI Report, PCI Compliance Detailed and Summary reports, Preferred Call Network Summary report, Rogue APs, Adhoc Rogues, New Adhoc Rogues, Security Summary, and Guest Session reports).
- Dashboard customization
- Client Station Statistics information is not populated with old WCS data in clients charts, client details page, dashboards, and reports.
- Client historical session information does get upgraded.
- All events from WCS Release 7.0 are completely dropped and are not migrated to NCS.
- RADIUS/TACACS server IP and credentials are not migrated and need to be added again after the migration is complete. You need to copy the latest custom attributes from NCS and include them in AAA server for user authentication/authorization in TACACS+/RADIUS.

Note Make sure you enable the RADIUS/TACACS server as AAA mode in the **Administration > AAA > AAA Mode Settings** page, and click **Save**.

- Only alarms with Root Virtual Domain are migrated from WCS Release 7.0 to NCS.

Note All WCS Release 7.0 alarms and event data are stored as CSV files along with other data in a .zip file during upgrade.

- The root password is not migrated from the WCS releases to NCS Release 1.1.0.58. The user must change the root password during the installation of the application. Non root users and their credentials are migrated during migration.
- Alarm categories and subcategories are not restored after migration to NCS Alarm Summary.

Upgrading NCS 1.0 to NCS 1.1.0.58

You can upgrade from NCS Releases 1.0.0.96, 1.0.1.4, 1.0.2.28, and 1.0.2.29 to NCS 1.1.0.58.

Caution Ensure that you perform a backup before attempting to upgrade.

Caution Remove high availability before performing the upgrade.

Note For the TACACS+/RADIUS user authentication, the custom attributes related to the new features are required to be added/appended to the existing set of attributes in AAA server to access certain pages/views. For example, Monitor Media Stream page, Virtual Domain List (to view the list of virtual domains from the Create Report page), and so on.

Note Shut down NCS before performing the upgrade. To stop NCS, enter the **ncs stop** command.

Use the following command to upgrade from NCS 1.0 to NCS 1.1.0.58:

```
# application upgrade NCS-upgrade-bundle-1.1.0.58.tar.gz wcs-ftp-repo
```

In the preceding command, NCS-upgrade-bundle-1.1.0.58.tar.gz is the upgrade bundle file, which is available for download.

The repository used in the example, **wcs-ftp-repo**, can be any valid repository.

Examples of repository configurations follow.

FTP Repository:

```
# configure
(config)# repository wcs-ftp-repo
(config-Repository)# url ftp://ip-address
(config-Repository)# user ftp-user password plain ftp-user
(config-Repository)# exit
(config)# exit
#
```

SFTP Repository:

```
# configure
(config)# repository wcs-sftp-repo
```

```
(config-Repository)# url sftp://ip-address
(config-Repository)# user ftp-user password plain ftp-user
(config-Repository)# exit
(config)# exit
#
```

TFTP Repository:

```
# configure
(config)# repository wcs-tftp-repo
(config-Repository)# url tftp://ip-address
(config-Repository)# exit
(config)# exit
#
```

NCS Features

This release includes the following new features and enhancements, which may be configured and managed through NCS:

Note For more details on the new features, see the *Cisco Prime Network Control System Configuration Guide, Release 1.1*.

IPv6

The following new features have been introduced as part of the IPv6 feature enhancements:

IPv6 Dual-Stack Client Support

Intelligent IPv6 packet processing to enable seamless Layer 3 roaming for IPv6 and dual-stack client support. This feature enables reliable connectivity while roaming.

IPv6 Security

First hop security features including RA Guard which automatically blocks rogue router announcements from the access point, source guard, and DHCP guard. This feature enables increased network availability and lower operational cost by proactive blocking of known threats.

IPv6 Client Management

Enables administrators for IPv6 address planning, client traceability, and so on. The IPv6 (wired and wireless client) addresses visibility on a per client basis; system-wide IP version distribution, and trending from NCS.

IPv6 Packet Optimization

Intelligent packet processing through NDP proxy and rate limiting of chatty IPv6 packets. This feature enables increased radio efficiency and reduced CPU utilization in the router.

FlexConnect

This section describes the FlexConnect enhancements that have been introduced.

FlexConnect Rebranding

Beginning with this release, the Hybrid REAP (Hybrid Remote Edge Access Points) feature is referred to as FlexConnect.

Improved FlexConnect Upgrade Process

This feature enables administrators to more effectively perform AP upgrades. This enhancement enables one FlexConnect AP per branch to act as the master AP and download the image from the controller and then APs of the same model in the same branch can then predownload the image from the master AP.

This feature enables local distribution of software images from master to other APs in a branch, speeding up the upgrade, therefore minimizing traffic over the WAN and providing increased reliability.

FlexConnect ACLs

Allows filtering of client traffic that is locally switched on the FlexConnect AP. This feature enables protection and integrity of locally switched data traffic at the FlexConnect AP.

FlexConnect AAA Override

Allows dynamic VLAN assignment of AAA for locally switched clients on a FlexConnect access point. This feature enables deployment flexibility for VLAN assignments for locally switched clients.

FlexConnect-Fast Roaming for Voice Clients in a FlexConnect Group

This feature removes WAN link dependency by handling mobility events at the FlexConnect access points. This feature enables reduced roaming delay for fast roaming clients.

FlexConnect - L2 Security for Centrally Switched Users on Cisco Flex 7500 Controller

Provides full range of authentication mechanisms with 802.1x for centrally switched users. This feature enables a Flex 7500 controller to support 802.1x authentication for centrally switched users.

FlexConnect Peer-to-Peer Blocking

Administrators now have the ability to disable peer-to-peer communications for FlexConnect APs. Once enabled, peer-to-peer communication on the WLAN is blocked. This feature limits vulnerabilities from insecure peer-to-peer client communication.

Rogue Enhancements

This feature provides the ability to configure a minimum RSSI value for rogue clients, report after a minimum time, ignore transient rogue, and not track friendly rogue. The benefits of this feature include advanced controls for rogue monitoring, detection, and management.

Note This feature is applicable for rogue APs only. Rogue clients and ad hoc clients are not considered.

Note Only monitor mode APs can be configured with transient rogue interval.

Rogue AP Alarm Severity Customization

This feature provides the ability to customize rogue AP alarm severity so that it can be tied to e-mail notifications in NCS. When this happens, you can choose receive alerts for malicious rogues only.

KTS-based CAC Support for NEC

Key Telephone System (KTS)-based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the controller to support CAC on KTS-based SIP clients, to process bandwidth request message from such clients, to allocate the required bandwidth on the AP radio, and to handle other messages that are part of the protocol.

Multi-level Filters in Client Reports

This feature enables you to use more than one filter in reports.

Advanced Filters in Client and Users Page

This feature supports advanced filters in the Clients and Users page, which is similar to the Alarms page.

Graphical Display of Historical Client

This feature provides the ability to show graphical charts to trend client counts on the Access Points Detail page.

Batch Reports and Templates

This feature provides the ability to create a report template at the root domain, and turn it into a template for all member domains so that a report can be created and populated to all domains under it.

Wi-Fi Direct Client Management

The Wi-Fi Direct Client Management feature is a flexible architecture used to support and detect Wi-Fi direct clients; therefore, it prevents enterprise vulnerability with this new technology.

TPCv2 Support

This feature enables you to optimize the coverage and the interference in a coordinated way based on the measurement readings from APs. TPCv2 identifies the deployment density that each AP experiences and determines TxPower for that AP.

RF Profiles

In NCS 1.1, the existing AP Groups are extended to support different configuration profiles called RF Profiles. An RF Profile is a group of related parameters that can be applied to one or more AP Groups. RF Profiles allow the administrator to tune groups of APs sharing a common coverage zone together.

Alloy WLAN QoS

The Alloy WLAN QoS feature provides the capability to properly prioritize the multiple traffic types that a multifunction device sends across the same WLAN. Under Alloy WLAN, the metal names Platinum, Gold, Silver, and Bronze are now treated as a profile name. Alloy WLAN QoS solves the multicast-unicast priority problem by placing non-WMM clients in the default multicast QoS priority queue.

CleanAir Phase 2 Enhancements

As part of the CleanAir Phase 2 Enhancements, the following functionalites are added to NCS:

- Persistent Device avoidance
  - Minimizes the use of channels affected by persistent interferences.
  - Persistent devices are detected by local and monitor mode AP propagated to both CleanAir and non-CleanAir APs.
- Custom Event Driven RRM Threshold
  - Ability for the radio to change channel in reaction to strong interference reported in the form of Air Quality Index.
- Air Quality Unclassified
  - New alarm triggered by the severity of unclassified category going above a configured threshold.

ISE 1.1 Enhancements

The enhancements for ISE 1.1 for this release include support for Local Web Authentication (LWA) and Central Web Authentication (CWA). This feature enables RADIUS NAC enabled WLAN to support additional configuration using Open Authentication and MAC filtering enabling devices like smart phones and tablets to connect to the corporate wireless network. For local web authentication with RADIUS NAC, web-auth is also supported.

Important Notes

This section describes important information about NCS.

This section contains the following topics:

Physical and Virtual Appliance

NCS is available as a physical or virtual appliance. Both are self-contained, and include the operating system, application, and database. These availability options speed up deployments and deliver greater deployment flexibility.

New License Structure

NCS is deployed through physical or virtual appliances. Use the License Center Graphical User Interface (Choose **Administration > License Center** from the NCS home page) to add new licenses, which is locked by the Cisco Unique Device Identifier (UDI). When NCS is deployed on a virtual appliance, the licensing is similar to a physical appliance, except instead of using a UDI, you use a Virtual Unique Device Identifier (VUDI). The NCS license is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package is purchased by a customer. For more information about UDI or VUDI, see the *Cisco Prime Network Control System Configuration Guide, Release 1.1*.

Wired Client Discovery

Wired client discovery depends on the Content Address Memory (CAM) table on the switch and this table is populated with the clients data. When a wired client is not active (not sending traffic) for a certain amount of time, usually five minutes, the corresponding client entry in the CAM table times out and is removed. In this case, the client is not discovered in NCS.

Autonomous AP Migration Analysis

Migration Analysis used to run autonomous AP during discovery can be configured by selecting the **Run Autonomous AP Migration Analysis on discovery** check box in the Administrator > Settings > CLI Session page. By default, this option is disabled.

Importing Maps

The Aeroscout engine fails to start MSE if the importing map names contain special characters such as '&'.

Monitoring Disk Usage

You can monitor the current disk usage from the **NCS > Administration > Appliance** page.

When the NCS backup background task fails, it indicates there is an issue with disk space. Choose **NCS > Administration > Background Tasks** to check the status of the NCS Backup Task.

Recommendations for Managing Disk Usage

We recommend the following to effectively utilize and manage disk space in the NCS server:

- Clean up some of the old files in the /dev/mapper/smosvg-localdiskvol partition so that there is some space available in this partition. This partition is the user-accessible area of the disk where any reports, FTP files, and local repository files are stored. This partition should have some free space so that files can be stored in this location. If this partition is full then any attempt to store files will fail.

  There are two ways to clean up the files located in this partition:

  - Log in to NCS CLI as an admin User and enter the **delete disk:/dir/filename** command to delete files from the /dev/mapper/smosvg-localdiskvol partition.
  - Log in to NCS CLI as an admin User and enter the **ncs cleanup** command. You are prompted to confirm if you want to delete all files in the local disk partition.
- Configure the NCS backup background task so that it uses a remote repository. This helps you to manage the space in the local disk partition effectively. You can configure a remote repository using any of the following protocols:
  - FTP
  - NFS
  - SFTP
  - TFTP

  Example remote repository configuration:

```
ncs-appliance/admin# configure
Enter configuration commands, one per line.  End with CNTL/Z.
ncs-appliance/admin(config)# repository remote_repository
ncs-appliance/admin(config-Repository)# url ?
  <WORD>  Enter repository URL, including server and path info (Max Size - 80)
  cdrom:  Local CD-ROM drive (read only)
  disk:   Local hard disk storage
```

```
  ftp:    URL using a FTP server
  http: URL using a HTTP server (read only)
  https: URL using a HTTPS server (read only)
  nfs:    URL using a NFS server
  sftp:   URL using a SFTP server
  tftp:   URL using a TFTP server
ncs-appliance/admin(config-Repository)# url ftp://hostname/rootDir.
```

- Ensure the used disk space in the /dev/mapper/smosvg-optvol partition is below 70% so that the backup attempts do not fail. If you encounter backup failures then you can configure a remote NFS mount for the backup task. This remote NFS mount should be an open share with read and write permissions.

  Example remote staging area configuration:

```
ncs-appliance/admin# configure
Enter configuration commands, one per line.  End with CNTL/Z.
ncs-appliance/admin(config)# backup-staging-url ?
  <WORD>  NFS URL for staging area (Max Size - 2048)
ncs-appliance/admin(config)# backup-staging-url nfs://hostname:/mount
ncs-appliance/admin(config)# exit
ncs-appliance/admin#
```

- Add additional disk space in a virtual appliance if you encounter disk space issues.

  If you have additional disk space available with your deployed virtual appliance, you can modify that virtual appliance to use more of that space. For this release, contact Cisco TAC to help in increasing the disk space available to the Virtual Appliance.

- Change the data retention period for aggregated data if you want to manage the disk space. To change the retention period for aggregated data, choose **NCS > Administration > Settings > Data Management** and change the values.

  Table 5 provides the recommendations for changing the data retention period for aggregated data.

Table 5 Data Retention Period for Aggregated Data - Recommendations

Aggregation	Default	Recommendation for systems with more than 5000 clients
Hourly	31 days	15 days
Daily	90 days	60 days
Weekly	54 weeks	54 weeks

The settings decide how long NCS retains the aggregated data. NCS polls for statistics data every hour, day, and week. The statistics data is used to generate trending charts or reports. You can significantly reduce the size of many aggregated tables by reducing the size of the aggregation period. The drawback being the granularity of trending charts or reports might be bigger.

For example, if you create a four weeks long Client Count chart, with the default setting, the hourly data is used. It means it has 4*7*24=672 data points (samples). With the new setting, the daily data is used and it has 4*7=28 data points. You see no change if you create a chart or report for less than 2 weeks.

Caveats

This section lists open and resolved caveats in NCS Release 1.1.0.58. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are taken directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website: http://tools.cisco.com/Support/BugToolKit/

Note To become a registered cisco.com user, go to the following website: http://tools.cisco.com/RPF/register/register.do

This section contains the following topics:

- Open Caveats, page 21
- Resolved Caveats, page 40

Open Caveats

Caveats Associated with Release 1.1.0.58

Table 6 lists the open caveats in NCS Release 1.1.0.58.

Table 6 Open Caveats

ID Number	Caveat Title
CSCtx28409	**The default client graph options do not show correctly.** **Symptom:** Default "overlaid" option for client related graphs in home page does not show correctly. **Conditions:** Client graphs such as "Client Count By Association/Authentication", "Client Count By Wireless/Wired" and "Client Count By IP Address Type" in dashboard shows by default in "stacked" format but the selected option shows as "overlaid". **Workaround:** Try to save the filter again so that the options appear correctly.

Table 6 Open Caveats (continued)

CSCtw86460	**Floor view map is truncated.** **Symptom:** Floor View AP pop-up not fully visible. **Conditions:** Floor View AP pop-up not fully visible in maximized mode **Workaround:** Keep browser in normal mode.
CSCtq53528	**SPT is not working in a virtual domain environment** **Symptom:** Switch Port Tracing (SPT) does not work properly in a virtual domain. **Conditions:** NCS will use all the switches and APs to perform SPT even though SPT request is issued from a certain virtual domain. **Workaround:** None.
CSCtr04327	**Export option for the Client Session Report may take 30 minutes to a few hours** **Symptom:** Exporting Client Sessions report in CSV or PDF format might take long time if the network has lot of mobile clients resulting in millions of sessions over a period of time. The interactive export operation might take anywhere from 30 minutes to a few hours. **Conditions:** Select long period of reporting time, for example, 4 weeks A lot of sessions in the database Data Cleanup task is running or the database is busy **Workaround:** Select shorter period of time to run. Schedule to run the report in less busy time. Schedule to run a few hour before you need the report.
CSCtt08852	**No recurrence Interval warning for > 10 virtual domain scheduled reports** **Symptom:** If recurrence is hourly, the warning message should be displayed if there are more than 10 sub Virtual Domains, but no warning message appears even if sub domains are more than 10. **Conditions:** When virtual domain based sub reports option is selected on report details page along with scheduling enabled, recurrence interval selections should display appropriate messages. **Workaround:** None.
CSCtu42661	**Issues in Rogue AP Report Run Result page navigation** **Symptom:** In Rogue AP Report Run Result, the last page of navigation shows no data available. **Conditions:** Create a report with the report result should contain at least 2 pages, click the last page link in the report, and then run result. **Workaround:** None.
CSCtx28949	**NCS showing switches as unknown device but reachable.** **Symptom:** NCS is showing switches as unknown device but reachable. **Conditions:** Switch Cat6k **Workaround:** None.

Table 6 Open Caveats (continued)

CSCtq94128	**Expanded row with detail shown in Event Page is not fixed on the top** **Symptom:** When clicking row expander to view detail in Event/Alarm page, the expanded row is not highlighted or fixed on the top of the table. **Conditions:** If the total number of events/alarms in the scope changes when user clicks the row, the expanded row may no longer be in focus. **Workaround:** User may need to scroll down the table to find the expanded row with detail shown.
CSCtq94148	**Alarm detail view is closed after failure to launch location history** **Symptom:** When user clicks the 'Location History' link inside Rogue AP Alarm detail panel, warning dialog may pop up if location page cannot be launched. After clicking the 'ok' button in the warning dialog, the alarm detail panel will be closed. **Conditions:** When failure to launch the 'Location History' page from Rogue AP Alarm Detail, the alarm detail panel will be closed. **Workaround:** User may need to find and click the row expander to reopen the alarm detail.
CSCtq39816	**Default values should exist for QoS template** **Symptom:** QoS template should have valid default values for all the attributes. **Conditions:** When editing the QoS template for first time. **Workaround:** None.
CSCtt52659	**No AP Config template for Venue to apply a mass config to a number of APs** **Symptom:** Cannot use template to apply Venue type config on APs at scale **Conditions:** Using AP template, the below parameters cannot be configured. Venue Group Venue Type Venue Name **Workaround:** Manually configure these parameters
CSCtw66830	**Mesh detecting APs RBAC domain handling is wrong** **Symptom:** Detecting AP information for mesh is only available in root domain, regardless of domain membership of mesh APs. **Conditions:** Mesh APs belong to a non-root RBAC domain, and user is viewing that non-root domain. **Workaround:** Only view mesh detecting AP information from the root domain.

Table 6 Open Caveats (continued)

CSCtw69878	**Unable to modify date in guest user account in Japanese XP client** **Symptom:** Unable to modify the date in create guest user account page in Japanese XP OS. **Conditions:** Date format is not displaying properly in NCS after logging in as guest user. Steps to reproduce: 1) Create a new guest user (Lobby user) 2) Log in to NCS as a guest user 3) Choose "Add Guest user" from the drop-down list 4) Click the Advanced tab 5) Change the life-time to "Limited" 6) Change the date and year to any date after the current date. This issue is specific to Japanese OS. **Workaround:** None.
CSCtw74599	**Date format is not proper in the WLAN configuration page** **Symptom:** Date format is not proper in the WLAN config page **Conditions:** When you try to schedule date for a particular WLAN profile, the selected date appears as yyyy/mm/dd but when you click the submit button the error message is appearing as “the valid date should be in mm/dd/yyyy format. This is specific to Japanese XP OS (client) Steps to reproduce: 1) Choose Configure > Controller 2) Select any one of the controller 3) Choose WLAN > WLAN configuration from the left side menu 4) Select any one of the WLAN profile and select "Schedule Status" from the right side drop-down list. 5) Enter the schedule task name, schedule time and date. The date format appears in yyyy/mm/dd format in GUI (only in Japanese XP client) 6) Click the Submit button. 7) Error message appears as "please enter valid date in mm/dd/yyyy format” **Workaround:** None.
CSCtw76483	**db_migration.log grows unbounded with trace enabled** **Symptom:** When trace logging enabled on the NCS, the db_migration.log can keep growing until it takes up all the disk space. **Conditions:** Observed on NCS 1.0.1.4 and 1.0.2.29 releases. **Workaround:** Install root patch for NCS and manually clear the log.

Table 6 Open Caveats (continued)

CSCtw89860	**Not able to apply channel width to AP602i -AP template** **Symptom:** Issue1: NCS shows error message "Not applicable when try to apply channel width 20/40 MHz for radio 802.11a/n via ap template". Issue2: Link latency is not supported for AP 602i running 7.0.220.0 version. NCS shows SNMP error on AP602i configuration page. Issue3: NCS allows to disable Admin status of radio 802.11a/n or 802.11b/g/n for AP602i running 7.0.220.0 version. **Conditions:** same as symptom **Workaround:** Issue1: NCS allows configuration of channel width 20 or 40 MHz on 802.11a/n radio of AP 602i on configuration page. Issue2: NCS shows correct error msg when applied via AP template. Issue3: This works fine via AP template
CSCtw98787	**The ncs password ftpuser CLI command should enforce ftp-user parameter** **Symptom:** The ncs password ftpuser command allows the username input to be anything and will accept that input without error: snx1-ncs-1/opsadmin# ncs password ftpuser testacct password Hello123 Initializing... Updating FTP password. This may take a few minutes... Successfully updated location ftp user But then attempt to login with that information, you get this: ftp snx1-ncs-1 Connected to snx1-ncs-1.cisco.com. 220 Service ready for new user User (snx1-ncs-1.cisco.com:(none)): testacct 331 User name okay, need password for testacct Password: 530 Access denied Connection closed by remote host. **Conditions:** ncs cli command, seen in versions 1.0.1.4, 1.0.2.28 and 1.0.2.29 **Workaround:** Must use the ncs passowrd ftpuser ftp-user password <password> syntax to update the ftp-user account. While other input for username is allowed, it has no effect.
CSCtx05881	**MIB object cWNotificationSpecialAttributes is not populated all the time** **Symptom:** MIB object cWNotificationSpecialAttributes (1.3.6.1.4.1.9.9.199991.1.1.2.1.12) is not populated for all the alarm conditions. **Conditions:** NCS 1.0.2.29. When northbound messages are generated. For certain alarm conditions which are sent Northbound, the SNMP MIB object - cWNotificationSpecialAttributes (1.3.6.1.4.1.9.9.199991.1.1.2.1.12) does not get populated.
CSCtx07978	**Select all button is not working in FlexConnect AP Groups > template page** **Symptom:** The Select all button is not working in Configure > Controller Template Launch Pad > FlexConnect > FlexConnect AP Groups > New Controller Template. **Conditions:** When template is not saved after entering template name and then selecting select all button in FlexConnect AP tab. **Workaround:** User can select individual APs instead of select all without saving template or create FlexConnect AP groups template with name and save it. Then click FlexConnect AP, click add AP, and then click the Select all button.

Table 6 Open Caveats (continued)

CSCtx29822	**NCS does not support rendering new lines** **Symptom:** For the guest account details report under Disclaimer, message is sent in one line. No carriage return is accepted in the disclaimer message. If Line1/Line2 were added on separate lines, but from guest account details report we have it on the same Disclaimer line **Conditions:** None. **Workaround:** None.
CSCtx32180	Cannot save WLAN configuration (with webpolicy disabled) on WLC 7500 **Symptom:** Cannot save WLAN config (with webpolicy disabled) on WLC 7500 **Conditions:** Trying to edit and save a WLAN Config on a WLC 7500 with Web policy unchecked from Configure > Controllers > <ip> > WLANs > WLAN Configuration > WLAN Configuration Details page. **Workaround:** Edit the WLAN template and apply it to the WLC. To do this, navigate to Configure > Controller Template Launch Pad > WLANs > WLAN Configuration, select a WLAN template, edit the config, save the changes and apply it to WLC. Also, you can create a CLI template for editing WLAN Config and apply it to WLC. To do this, choose Configure > Controller Template Launch Pad > CLI > General, create a CLI template with config wlan command and apply it to WLC.
CSCtx38131	**AP template schedule cannot be disabled** **Symptom:** Scheduled AP template cannot be disabled. **Conditions:** Choose Configure > Lightweight AP Templates. Create an AP template and schedule the template for future date/time. Open the template and unselect schedule check box and click the save button. The template still shows as scheduled. Expected Result: The template should disable the schedule functionality. **Workaround:** Method 1: Disable the scheduled AP template from Configure > Scheduled Configuration tasks > select template > Disable schedule Method 2: Delete AP template to disable AP template schedule and create another one for use.
CSCtq26535	**Remove buttons at external webauth config** **Symptom:** Save and Audit buttons found in External Webauth Config page **Conditions:** This is always found **Workaround:** None. Buttons work. Since the external web auth server cannot be changed after configuring, there is no necessity for the Save and Audit buttons.
CSCtr17338	**Modifying Legacy User password not displaying policy failure error** **Symptom:** After migrating to NCS from previous releases, modifying Migrated/Legacy Users with some invalid password not matching existing password policies, no error is getting displayed. **Conditions:** Users are migrated from a previous version of WCS **Workaround:** Password policy failure errors are displayed for Newly created users in NCS. Its not displaying for only Legacy / Migrated users.

Table 6 Open Caveats (continued)

CSCtr24105	**On interim upgraded NCS some user cannot switch between multiple virtual domains** **Symptom:** User cannot switch from one virtual domain to other. **Conditions:** This happens in NCS that has undergone interim release upgrade (for example, NCS 1.0.0.69 to NCS 1.0.0.94). This happens for user who does not have root privilege or superuser privilege. **Workaround:** None.
CSCtt00458	**Unable to download the file after device data collector Background task.** **Symptom:** Unable to download file after Device Data Collector Background task execution **Conditions:** 1. Administration > Background Tasks > Other Background Tasks > Device Data Collector 2.Select the Controller by specifying IP address and enter CLI commands. 3. Save the config and then execute the "Device data collector" task. Click the download the file link. It throws error and file is not downloaded. **Workaround:** None.
CSCtw99434	**Incorrect time zone shown in NCS** **Symptom:** Customer configure NCS and WLC with MST time zone. However from NCS > Monitor > Clients and Users show in UTC time zone. **Conditions:** NCS version1.0.1.4. Users and client monitor does not sync with the time zone that has been configured on NCS. **Workaround:** None.
CSCtx09586	**"Copy And Replace AP" function does not work** **Symptom:** The "Copy And Replace AP" function does not work in NCS. Error pop-up shows the following message: `Error : COMMON-1 : Some Unexpected internal error has occured. If the problem pesists please report to the Tech Support. Error : Detail : errorID=12, componentName=CRUD Error update Failed` **Conditions:** Only NCS is affected. WCS 7.0.220.0 does not experience this symptom. **Workaround:** None.
CSCtx15383	**Audit Trail logs for unlock user has incorrect reason** **Symptom:** Audit Trail logs for unlock user operation has incorrect reason **Conditions:** When user is unlocked by root user and Audit trail logs are viewed for the same user. **Workaround:** None.
CSCtq71784	**Special Characters should not be allowed while creating AP Groups** **Symptom:** When AP group name is created, Question mark (?) character is allowed in the name field. **Conditions:** This happens while creating a AP group. **Workaround:** None

Table 6 Open Caveats (continued)

CSCts79048	**Not all Virtual domains listed for AAA Radius Authenticated user** **Symptom:** Not all Virtual domains are displayed in Home Page for AAA Radius Authenticated user by which the user can switch between Virtual domains. **Conditions:** When AAA user authentication is performed using ACS 4.2 and Radius protocol with custom attributes size greater than 4096 bytes **Workaround:** Remove some data from AAA server Radius Custom attributes list. Else try AAA TACACS user authentication to check if all the Virtual domains are displayed.
CSCtu08116	**Audit status is not changing for one controller** **Symptom:** The Audit status was not changing for one controller on doing on demand refresh also. While checked the background task, config sync was failed for 1 device that could be the reason for not updating status. **Conditions:** When the config sync background task failed for controller. **Workaround:** None
CSCtw23482	**Apply CLI template with Config commands fails with Null PointerException** **Symptom:** Apply CLI template with several 11u commands fails with null pointer exception in Apply template result page **Conditions:** Under Administration > Settings > CLI Session, SSH is used to communicate with Controller, a CLI template with several 11u CLI commands are applied onto 7.2.x controller. **Workaround:** Break these large suite of CLI commands into smaller suite of CLI template having fewer commands (say 3-5) and try to apply them onto controller
CSCtx28185	**Improper login credential message coming on applying CLI template** **Symptom:** Improper login credential message coming **Conditions:** On applying CLI template **Workaround:** Retry is helping in some cases.
CSCtu57130	Failed to load data for tables: ADLRADIFVOICESTATS error on WCS 7x to NCS migration **Symptom:** During WCS to NCS migration, the following error messages were thrown in the terminal: Stage 3 of 5: Restoring Data ... Failed to load data for these tables: ADLRADIFVOICESTATS (OR) Stage 3 of 5: Restoring Data ... Failed to load data for these tables: BASESERVICEDOMAIN **Conditions:** WCS 7x to NCS Migration **Workaround:** User needs to share the WCS7x export zip file. Then, Dev engineer will fix the issue and provide share fixed WCS7x export zip.

Table 6 Open Caveats (continued)

CSCtu34859	**NCS should validate KTS CAC with QoS profile** **Symptom:** NCS fails to validate saving KTS CAC without Plantinum QoS Profile on WLAN Configuration page. **Conditions:** Configure KTS CAC on WLAN Configuration page without selecting QoS Profile as platinum **Workaround:** Enabling the same from WLAN Template throws the correct error message.
CSCtw71445	**Resequence Rules in ACL Templates doesn't work.** **Symptom:** The "Resequence Rules" option is not working in ACL template and FlexConnect ACL templates **Conditions:** Try to resequence the rules of acl using "Resequence Rules" option in ACL template or FexConnect ACL template **Workaround:** Delete and add rules again according to the new sequence.
CSCtu22859	**Stranded APs, worst node hops getting failure on customization** **Symptom:** Stranded APs, worst node hops getting failure on customization of rep **Conditions:** Click the customize button. In Data field sorting, select "sort by" option =MAC Address. and select "then by" option. Apply the customize and run the report. **Workaround:** Run the report without customiztion.
CSCtw89678	**NCS web session timeout redirects to login page without any notification** **Symptom:** NCS web session timeout redirects to login page without any message alert or notification **Conditions:** Under Administration > User Preferences for Root/admin user, Logout idle user is enabled and "Logout idle user after" is set for 15 mins. NCS web session is kept idle for above configured duration. **Workaround:** None.
CSCtw94866	**Not all mesh aps is shown in Report > Mesh > Link Stats > Report Criteria** **Symptom:** Have a controller with Mesh APs added to the NCS. Navigate to Report -> Report Launch Pad -> Mesh -> Link Stats Create a new report. report type as LINK STATS report by option as AP by Controller Report Criteria > click -> edit in > Filter Criteria > Controller > select the controller which has mesh APS. in access point only ONE mesh aps is seen. other mesh aps are not listed. **Workaround:** BUT in report type > NODE HOPS report by option > AP by Controller Report Criteria > click > edit in > Filter Criteria > Controller > select the controller which has mesh APs. In access point all mesh aps are listed.

Table 6 Open Caveats (continued)

CSCtx14181	**Unable to UPDATE AND SYNC controller in unknown devices page with V3 version** **Symptom:** UPDATE AND SYNC controller in unknown devices page with V3 version through error (asking for community field) **Conditions:** While updating the controller credentials in unknown devices page with V3 version **Workaround:** From the unknown devices page, remove the controller and add it again
CSCtw53357	**Timestamp error in preset filter in Alarms and Events page** **Symptom:** Timestamp error in preset filter in Alarms and Events page. **Conditions:** In Alarms and Events page, for any selected filter (for example, Alarms in last 8/24 hours), when preset filter option is clicked, it shows Timestamp as Last 5 minutes for any filtered list of alarms or events. **Workaround:** None
CSCtu07020	**Monitor > Google Earth Maps Import CSV shows error** **Symptom:** Monitor > Google Earth Maps Import CSV shows error. **Conditions:** When reimporting the CSV file, getting error message which states that `"Error: Saving Folder details to the database. COMMON-1"` **Workaround:** Remove all the APs and reimport.
CSCtx01075	**Incorrect Target Client/AP IP address data for wIPS alarm 138** **Symptom:** When wIPS contains IPv6 address, NCS will not be able to display is properly. **Conditions:** None. **Workaround:** None.
CSCtw75535	**Virtual Domains not showing maps, WLCs, APs - DB corruption** **Symptom:** NCS 1.0.1.4 may not show available APs, WLCs and maps to add them in the Virtual Domain configuration **Conditions:** NCS 1.0.1.4 with virtual domains configured **Workaround:** none.
CSCtq84181	**Assigning selected devices to a virtual domain takes long time** **Symptom:** NCS takes long time to add selected controllers or access points in a virtual domain. **Conditions:** When a large number of controllers or access points are selected to be part of a virtual domain, NCS takes long time (of the order of minutes) to add them in the virtual domain. This slowness is observed when the number of controllers is above 100 or the number of access points is above 1000. **Workaround:** Add small number of controllers or access points to a virtual domain at a time.

Table 6 Open Caveats (continued)

CSCtq94229	**Adding Switch (SPT mode only) to virtual domain throws exception** **Symptom:** Adding Switch (with SPT mode only) to Virtual Domain throws internal exception error. **Conditions:** Whenever we have a switch added with license level SPT-only, associating the switch to any virtual domain throws internal exception error **Workaround:** None.
CSCtw97140	**Filter "All Campuses" for Client Counts chart show wrong data** **Symptom:** In Client Counts chart: 1. "All Campuses" shows total client counts for both floors and outdoors, irrespective of "Search By" option set to "Floor Area" or "Outdoor Area". Also same results shown for root virtual domain or non-root virtual domain. 2. Selecting a specific campus with "All Buildings" or "All Outdoors" will show total client counts for both floors and outdoors, irrespective of "Search By" option set to "Floor Area" or "Outdoor Area". Also same results are shown for root virtual domain or non-root virtual domain. **Conditions:** Expected Behavior: When "Search By" option is set to "Floor Area", client counts chart will show all clients from all the floors in its virtual domain. Similarly, When "Search By" option is set to "Outdoor Area", clientCounts chart will show all clients from all the outdoors in its virtual domain. Same thing should happen when a campus is selected. **Workaround:**None.
CSCtu24003	**In Non-Root VD, Switch Location config Template not seen in list page** **Symptom:** Switch Location Configuration template created in non-root virtual domain is not getting displayed in the list page **Conditions:** User belonging to non-root virtual domain tries to create a Switch Location configuration template **Workaround:** Login to ROOT-DOMAIN, the switch location configuration template is visible
CSCto36340	**Session timeout popup appears twice** **Symptom:** Session Timeout pop up appears twice after configured User idle timeout. **Conditions:** Under Administration > User Preferences, the Logout idle user flag is enabled & configured with Idle time. **Workaround:** Have the Logout idle user flag disabled
CSCtu16596	**client delist trap - reason code changes** **Symptom:** Client Delist information does not get populated even if Media client has delisted. **Conditions:** When Media client gets delisted **Workaround:** None.

Table 6 Open Caveats (continued)

CSCtw66822	**addObjectsWithOverrideWithoutUpdate still calls validation** **Symptom:** High CPU utilization during Radio Statistics polling, especially when controllers have a large number of APs associated. **Conditions:** Controllers have a large number of APs associated. **Workaround:** None.

CSCtx06624	**System loses RAID configuration after power interruption**
	Symptom: The analysis and solution described below apply to the following platforms and products:
	• Cisco Flex 7500 with IBM M1015 RAID card
	• Cisco Mobility Services Engine - MSE-3355 with IBM 5015 RAID card
	• Cisco Prime NCS Appliance with IBM 5015 RAID card
	While booting up, the following error message appears on the attached monitor or on serial console.
	`"All the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your system and check your cables to ensure all disks are present. Press any key to continue or C to load the configuration utility"`
	When Space key is pressed the system is unable to boot from disk. During bootup, the LSI WebBIOS loads fine and shows two physical disks being present but no virtual (logical) disks. The behavior points to a loss of the RAID configuration that was present on the system.
	Cause/Analysis: Most likely, the box went through an accidental power interruption (i.e., the power was interrupted while the system was operational). Upon reboot, the RAID card could not find its configuration in the non-volatile memory and therefore it could not boot. Basically, the configuration stored in non-volatile memory was corrupted/erased due to the power interruption. The RAID card does keep a backup of the configuration on the hard drives too. However, when the card loses the configuration information stored in the non-volatile memory, it does not automatically pickup the backup configuration information from the hard drives. The information on the hard drives is considered a "foreign configuration" that requires explicit user intervention before it can be loaded. At this time, the system will wait for the user to take action. Remember that all the data on the hard drives are still intact.
	Action/Remedy: When this situation is encountered, the user/administrator must enter the RAID management tool. There are two version of this tool - one that uses extensive menus and requires an attached monitor and another that is completely based on the command lines (CLI). The CLI version can be accessed from the serial console or from a directly connected monitor. During the bootup process, you'll see a message for invoking the CLI based RAID management tool, right after the error message Press Ctrl-H for WbeBIOS or Ctrl-Y for Preboot-CLI. Enter the CLI version of the utility by pressing Ctrl-Y and then type in the following command
	`-CfgForeign -Import -a0`
	Next, reboot the server and everything should be back to normal

Table 6 Open Caveats (continued)

CSCtq10930	**Time period for saved search is not retained after upgrade** **Symptom:** Time period for saved search is lost after upgrade. **Conditions:** None. **Workaround:** None.
CSCtq98064	**All Legends show when there is no data for Non-WiFi ChannelUtlil. Chart** **Symptom:** Radio Detail page for CleanAir is showing all legends when there is no data for Non-WiFi Channel Utilization **Conditions:** There is no AirQuality Classification Data, that is, there are no interferers contributing to AirQuality. **Workaround:** None.
CSCtw84513	**NCS Some AP information pop-ups open in non-viewable space** **Symptom:** In NCS 1.0.2.29, when a user navigates to a floor plan map and mouses over an AP on the right hand side of the page, the information popup will open in non-viewable space, causing scroll bars to be used. **Conditions:** None. **Workaround:** At this time, there is no workaround other than to use the scroll bars when presented.
CSCtw87328	**Client list, quick search, and advanced search takes too long to complete** **Symptom:** Loading of Client List page or response for Quick search and Advanced Search for a specific client may take quite long time. **Conditions:** This issue may occur in a very rare scenario, when after fresh installation the user tries to bring up Monitor Clients and Users page, or launches Quick or Advanced Client search, during a short interval when Client Status polling background task discovers first set of clients. **Workaround:** This issue gets resolved after some time without any further action required from the user. Restarting NCS server would also resolve this issue.
CSCtx32223	**Save on Monitor Media Stream task not working on upgraded NCS.** **Symptom:** After upgrading NCS 1.0.1.4 to NCS 1.1.0.54, the Monitor Media Streams task from User Group details page is not getting saved. **Conditions:** NCS is upgraded from previous release to 1.1 either using application upgrade command or restoring earlier NCS version DB onto NCS 1.1 **Workaround:** Login to NCS 1.1 DB and update the xmpprivelege table “instancename” column value to remove the extra white space for “Monitor Media Streams” value, after which the User is able to save the task from User Group details page.

Table 6 Open Caveats (continued)

CSCtl77129	**User authentication via TACACS+ shows Access denied in dual network** **Symptom:** User authentication via TACACS displays Access denied page when used for a particular interface in a Dual NIC NCS and ACS server. **Conditions:** Both NCS and ACS servers have Dual NIC support and these are reachable to each other. In the Administration > AAA > AAA Mode Settings page, the TACACS option is selected and "Enable fallback to Local" is selected with default option. **Workaround:** Works correctly with one of the 2 interfaces
CSCto13373	**The "ncs start" command on a running NCS reports an incorrect message.** **Symptom:** The "ncs start" command on an already running NCS reports an incorrect message. **Conditions:** NCS 1.0.2.29 **Workaround:** If NCS is already running and if you enter the command "ncs start", it would report the following message. ncs-lab/admin# ncs start Starting Network Control System... This may take a few minutes... Health Monitor is already running. Failure during Network Control System startup. Check launchout.log for details. ncs-lab/admin#
CSCto36542	**Proper error required during AAA user login** **Symptom:** NCS should display proper error message during login indicating reason for failure whenever an AAA user with certain custom attributes tries to login which does not match the AAA mode set in NCS, that is, when AAA mode is set as TACACS and Radius user tries to login and vice versa. Currently NCS displays the Access Denied page. **Conditions:** Under Administration > AAA > AAA Mode Settings page, TACACS option is selected. However Radius User tries to Login to NCS and vice versa. **Workaround:** None.
CSCto44918	**AAA Radius/TACACS+ servers are not migrated from WCS to NCS.** **Symptom:** The Radius/TACACS servers created in previous release of WCS are not getting migrated to NCS. **Conditions:** Radius / TACACS servers are created in previous releases of WCS, restoring data from these releases onto NCS does not migrate AAA serverstouchbacks **Workaround:** Create Radius / TACACS servers again in NCS and navigate to Administration > AAA > AAA Mode Settings page, reconfirm the Mode set. Save the settings and perform AAA user authentication.
CSCtq32125	**Planning mode > Add APs, Override... option includes other services** **Symptom:** While using the Planning Tool to automatically add APs to a floor, if you choose the option "Override Coverage Per AP Per AP Area," all of the options for Data, Voice, etc. are disabled. However, if you checked them prior to checking "Override Coverage Per AP Per AP Area," those options will still be part of the calculation when you click on Calculate. **Conditions:** This applies to version 1.0 of the Cisco Prime Network Control System. **Workaround:** Uncheck all of the Services options before selecting Override Coverage Per AP Per AP Area.

Table 6 Open Caveats (continued)

CSCtq53132	**AP Summary pop-up appears out of bounds** **Symptom:** When you hover your mouse cursor over an object on a floor or outdoor area page, the informational popup appears partially off-screen. **Conditions:** This affects version 1.0 of the Cisco Network Control System. This occurs most frequently when the object is in the lower-right corner of the map. **Workaround:** Use your middle mouse button to scroll with your mouse, and scroll to reveal the rest of the popup. This may also work with a multi-finger drag on certain touchpads.
CSCtq67819	**Audit in RF group page should open a popup even if there are no mismatches** **Symptom:** Choose Configure > Controllers > 802.11a/n > RRM > RF Grouping. If there are no mismatches then a popup should open with the following text should appear "No differences found between NCS and device values". **Conditions:** When there are no mismatches between NCS RF Grouping Config and WLC RF Grouping config **Workaround:** None.
CSCtq79369	**Monitor > SE showing different count for alarms on clicking hyperlink** **Symptom:** Alarms shown on clicking the alarm count link on Monitor > SE page shows all SE alarms and not just the alarms specific to the current SE. **Conditions:** More than one SE connected to WCS **Workaround:** None.
CSCtq81553	**Wi-Fi invalid category is shown as SuperAG in SE detected interferers** **Symptom:** Wi-Fi invalid category is shown as SuperAG in Monitor > SE detected interferers **Conditions:** Have Wi-Fi Invalid interferer **Workaround:** None.
CSCtq81833	**SE becomes unreachable after some time but alarms keep coming** **Symptom:** Issues with adding SE or after adding SE, connection terminates. **Conditions:** None. **Workaround:** None
CSCtq82216	**Virtual Domain: Cannot open maps tab- if user is logged in with R/W Maps user group** **Symptom:** Permission denied page is seen for maps tab if user is logged in with R/W Maps user group **Conditions:** It is not reproducible currently. **Workaround:** None.

Table 6 Open Caveats (continued)

CSCtq84792	**DB server cannot start if restore server timestamp is behind backup server.** **Symptom:** 1. Take a NCS Server backup from Server running on timestamp-B. 2. Now, change the NCS date/time to timestamp-A such that timestamp-A < timestamp-B. 3. Restore NCS backup taken from step 2 on NCS Server running on timestamp-A. NCS fails to start and throws error as mentioned in the bug. **Conditions:** NCS 1.0.0.94 and NCS is running behind date/time which is in the DB backup. **Workaround:** Configure and set the correct date/time on NCS.
CSCtq92772	**EventWriter throws exceptions for IDR when controller is rebooted** **Symptom:** When a controller having Clean-air APs associated to it is rebooted, EventWriter related exceptions are seen in the log. **Conditions:** A controller having CleanAir APs associated to it is rebooted **Workaround:** None.
CSCtq96037	**Added controller is found in switch list page in a NAT setup** **Symptom:** When attempting to add a controller, it shows up as a switch in the switch pages. **Conditions:** This has been seen in the test environment on two systems that are on the same subnet, but both have NAT addresses for outside access to the devices. When adding the controller to the NCS using the internal lab address, everything works fine. When you try to add the controller using the NAT address, the IP gets associated to the switch, and added as a switch. **Workaround:** Add the controller using the internal lab address.
CSCtq96208	**User without planning mode permissions is able to launch planning tool** **Symptom:** Users without the Planning Mode permission are able to launch the Planning Tool. **Conditions:** This affects version 1.0 of the Cisco Prime Network Control System. **Workaround:** None.
CSCtq98554	**Annotation is not working for virtual domain on restored DB** **Symptom:** With restored database from NCS upgrade, adding annotation on alarm will not work for virtual domains other than ‘root’. **Conditions:** If NCS is upgraded from beta release or from WCS 7x release, the above issue on adding annotation may occur with restored database. **Workaround:** To add annotation on alarm after NCS is upgraded from previous release and database is restored, login as ‘root’ user and use root virtual domain.
CSCtr00084	**Invalid parameter “Dynamic Tx Power Control” in config RRM TPC** **Symptom:** Invalid parameter “Dynamic Tx Power Control” shows up in Config RRM TPC **Conditions:** All Configure RRM TPC will show this **Workaround:** None.

Table 6 Open Caveats (continued)

CSCtr00174	**DCA Channel Width parameter is not present in RRM templates.** **Symptom:** DCA Channel Width parameter is not present in RRM templates. **Conditions:** Configure > Controller Template Launch Pad > 802.11a/n > DCA > Controller Template. The DCA Channel Width is not available for RRM 802.11a template. **Workaround:** Manually go to each Controller page's DCA Section and configure Channel Width.
CSCtr04897	**SPT switches have a few issues after upgrade** **Symptom:** After NCS upgraded from WCS7.x. For Switches upgraded from WCS 7.x will not have model name, description, software version, and so on in Inventory Reports and the reachability status is missing as well. Inventory reports do not show all the information for SPT switches. Shows only "Device Name and IP Address". Need to show all other information such as model name, description, software version, and so on. **Conditions:** Upgrade switches from WCS 7.x to NCS. **Workaround:** Perform a manual switch sync from NCS will trigger the switch reachability status update.
CSCtr08989	**ncs db sql query command throws error when run for a single column select** **Symptom:** When executing 'ncs db sql "select <specificcolumn> from <tablename>" NCS CAR CLI command on NCS appliance box. avansamb-vm2/admin# ncs db sql "select buildversion from applicationversion" BUILDVERSION ---------- 1.0.0.92 % Internal error during command execution avansamb-vm2/admin# The query returns the correct results on the console even there is an error. **Conditions:** This happens only when executing the sql query to retrieve specific column data. For 'select * from <tablename>' , ie., all columns data retrieval, this does not happen. **Workaround:** Use * to retrieve all columns data instead of a single column, that is, use 'select * from <tablename>' command.
CSCtr11492	**Password policy mismatch in GUI page and server side after upgrade** **Symptom:** Create/Edit user display password policy error even for those which are not turned on. This happens when few of Local Password policy are turned off in earlier release of Wireless Control System & after migration to NCS, even though the user sees them as disabled in Administration > AAA > Local Password Policy page, but all the password policies are actually enabled by default at server side. **Conditions:** Whenever Few Local Password policies are turned off in earlier release of Wireless Control System & data migrated to NCS. Trying to create User / Edit User password with passwords matching those policies shall fail with appropriate Error. **Workaround:** Navigate to Administration > AAA > Local Password Policy page, Enable/Disable the required policies & Save. After which try creating / editing user password

Table 6 Open Caveats (continued)

CSCtr29255	**Enlarge Map issues with Location History pages** **Symptom:** The enlarged location history map does not display properly. The map appears off to one side, and the position of the element does not update on the enlarged map. **Conditions:** This applies to viewing the location history of an element tracked by an MSE. This affects version 1.0 of the Cisco Prime Network Control System. **Workaround:** None.
CSCtx35805	**IPv6 support is unavailable for Media Stream.** **Symptom:** IPv6 support is unavailable for Media Stream. **Conditions:** If Media stream is configured with IPV6 IP, media stream client info. might not display in NCS. **Workaround:** Use IPv4 IP to configure media stream.
CSCtq82314	**Maps tree view is not highlighting the selected Map.** **Symptom:** When you view the Map Tree View from a map page in the Cisco Prime Network Control System, the tree view provides no indication of what map you are viewing. **Conditions:** This affects Cisco Prime Network Control System, Release 1.0. **Workaround:** Use the breadcrumb above the map to figure out which map you are looking at.
CSCtw98436	**AAA user in 2nd TACACS+ server fails to login with defferent AAA mode setting** **Symptom:** AAA users configured in Second/Third TACACS+ server are unable to login with valid credentials when Enable fallback to Local is selected with default option "Only on no server response”. **Conditions:** Under Administration > AAA > AAA Mode Settings, Enable fallback to Local is selected with option "Only on no server response". **Workaround:** Modify the AAA mode enable fallback to local option to "on Auth failure or no server response". Save and Re-login with same user.
CSCtx27746	**Error opening Event Details when accessing from RRM > Channel Change** **Symptom:** Error dialog pops up when clicking Event Details via the RRM Page > Channel Change APs **Conditions:** Occurs when a heavily loaded System is run for long time **Workaround:** None
CSCtr86264	**Oracle crashed at customer site** **Symptom:** Oracle database crashed. **Conditions:** This is due to an existing Oracle database bug **Workaround:** Restart NCS server fixes the problem

Table 6 Open Caveats (continued)

CSCtu07154	**NCS RRM templates is not properly highlighted in LHS menu** **Symptom:** RRM templates is not properly highlighted in LHS **Conditions:** In configure > controller template page, when go to the RRM template, its not highlighted the correct templatein LHS. **Workaround:** Cross verify with the breadcrumb
CSCtu32372	Monitor lite rogue ap search issue **Symptom:** Monitor lite search issue **Conditions:** Login to ncs with monitor lite user. In search filed, provide name as 'rogue' and search it. Rogue AP count would be shown in search list. Click on rogue ap count. The permission denied message shows as "you dont have access to the page 'Alarms'". When doing the same search second time, no message is thrown. **Workaround:** None.
CSCtu76201	Failing to add all 100 APs on a floor on first attempt; only 24/25 **Symptom:** Cannot add the full 100 APs on a floor after adding the 6th & 7th floors **Conditions:** Already added 500 APs across 5 floors with 100 APs each. We already have many buildings and APs on different floors. Just started to see this issue as of late. **Workaround:** Re-add the remaining APs that didn't make it the first time
CSCtw51046	VD changed as Root-domain in all reports after upgrade by defaul **Symptom:** In VD by default shows as Root-domain in all reports after upgrade. **Conditions:** Create and save some reports in VD. upgrade the NCS build. **Workaround:** Delete the report and create anew report.
CSCtw59460	DB restore failed with rman error message in log **Symptom:** NCS restore failed **Conditions:** This happens due to existing bug in Oracle database. **Workaround:** Take another backup. Optionally we have other scripts using other Oracle tools to take a backup, which we can restore without any problems.
CSCtx03365	Word 'WCS' to be replaced in mouse over msg of 'Rogue AP events' report **Symptom:** Mouse over Rogue AP events report, it refers WCS instead of NCS. **Conditions:** None. **Workaround:** None.

Table 6 Open Caveats (continued)

CSCtt94177	If application bundle file is corrupt need appropriate message to user
	Symptom: When there is any kind of bundle installation failure, the users sees the following message, which is not very clear:
	`ncs/admin# application install NCS-upgrade-bundle-1.1.0.57.tar.gz ftp-repo`
	`Save the current ADE-OS running configuration? (yes/no) [yes] ?`
	`Generating configuration...`
	`Saved the ADE-OS running configuration to startup successfully`
	`Initiating Application installation...`
	`% Manifest file not found in the bundle`
	`ncs/admin#`
	Conditions: The two common conditions for this are;
	1. Mis-spelling in the bundle name
	2. Corrupt bundle
	Workaround: For the common issues above the workarounds are:
	1. Verify Spelling
	2. Verify bundle integrity.

CSCtu06012	NCS1.1- FFT :Administration >Settings does not show the save success msg **Symptom:** Administration > settings does not show the successful save message **Conditions:** In Administration > settings, make the changes for any options, except login disclaimer **Workaround:** For save the changes successful, save the changes once again.
CSCtx38608	Unable to add Spectrum Expert to NCS **Symptom:** NCS 1.0.2.29 adding a Spectrum Expert client running SE 4.0.68 getting a generic "An internal error occurred while performing the action." message. **Conditions:** None. **Workaround:** None.

Resolved Caveats

Table 7 lists caveats resolved in NCS 1.1.0.58.

Table 7 Resolved Caveats

ID Number	Caveat Title
CSCtr98051	The Copy and replace AP function does not update the information in the map.
CSCts48582	Support for different Mac address format in Advanced search
CSCtv21726	Logged in user session times out even if the session is actively used
CSCtw74389	NullPointerException in XmpRbacServiceUtil.getPrivilegesForUserGroup
CSCtu24864	Slow loading of Monitor->RRM page
CSCtr27032	NCS fails to start after failing back from the secondary
CSCtt94353	Heatmaps are not drawn after migration from WCS to NCS

Table 7 Resolved Caveats (continued) (continued)

ID Number	Caveat Title
CSCts41176	need to add more Apple's MAC prefix to vendorMacs.xml file
CSCtr88095	Template-based audit fails for Rogue AP rules templates
CSCts00814	TACACS/RADIUS authentication fails after failover to secondary
CSCtu04020	Clear config / Reset AP throws permission denied on AP config page

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. See the following URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website: http://www.cisco.com/en/US/support/index.html

Click **Wireless** and **Wireless LAN Management** and then choose **Network Control System**.

Related Documentation

For information on the Cisco Unified Network Solution and for instructions on how to configure and use the NCS, see the *Cisco Prime Network Control System Configuration Guide* and the *Cisco Wireless LAN Controller Configuration Guide.*

Table 8 provides a list of the documentation for NCS 1.1.0.58.

Table 8 NCS Documentation

Documentation Title	URL
Cisco Prime Network Control System Configuration Guide, Release 1.1	http://www.cisco.com/en/US/docs/wireless/ncs/1.1/configuration/guide/NCS11cg.html
Cisco Prime Network Control System Command Reference Guide, Release 1.0	http://www.cisco.com/en/US/docs/wireless/ncs/1.0/command/reference/cli_pref.html
Cisco Prime Network Control System Appliance Getting Started Guide, Release 1.0	http://www.cisco.com/en/US/docs/wireless/ncs/appliance/install/guide/primencs_qsg.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.