Release Notes for the Cisco Prime Network Control System, Release 1.0.0.96

July 2011

These release notes describe the requirements, features, limitations, restrictions (caveats), and related information for the Cisco Prime Network Control System, Release 1.0 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. The Cisco Prime Network Control System hereafter is referred to as *NCS*.

Contents

These release notes contain the following sections:

Introduction

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

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

of network problems related to client devices which is one of the most reported customer pain points. NCS also provides monitoring of identity security policy 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 platform's workflow-oriented, simplified, and intuitive user experience, 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, Cisco 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 1.0 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.
- 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 Cisco Prime 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.

Requirements

This section contains the following topics:

Supported Hardware

NCS software is packaged with your physical appliance, or 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 15000 Cisco Aironet lightweight access points, 5000 autonomous access points, 5000 switches and 1200 Cisco wireless LAN controllers. • Processors: 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 7500 Cisco Aironet lightweight access points, 2500 autonomous access points, 2500 Switches and 600 Cisco wireless LAN controllers. • Processors: 4, at 2.93 GHz or better. • Minimum RAM: 12 GB. • Minimum Hard disk space allocation: 300 GB.
Cisco Prime NCS Low-End Virtual Appliance	• Supports up to 3000 Cisco Aironet lightweight access points, 1000 autonomous access points, 1000 Switches and 240 Cisco wireless LAN controllers. • Processors: 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

Note If you want to use a Cisco UCS Server to deploy a virtual appliance for Cisco Prime NCS, you can use the UCS C-Series or B-Series. Make sure the server you pick matches to the Processor, RAM and Hard Disk requirements specified in "Supported Hardware" section on page 3 section on page 2-2 deployment.

Note Non-English characters are not supported in *Cisco Prime Network Control System, Release 1.0*. Use only English keyboard layouts.

Supported Browsers

The NCS user interface requires Mozilla Firefox 3.6 or later and Internet Explorer 8.0 or later with the Chrome plugin releases or Google Chrome 12.0.742.x. Internet Explorer 6.0 is not supported. 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 controller, access point images, Identity Services Engine (ISE), and Mobility Services Engines (MSE).

Table 2 Supported Device Matrix

Supported Switches	Supported Controllers	Supported MSE Devices	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 1000 AP, Cisco 1040 AP, Cisco 1100 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 3500i AP, Cisco 3500e AP, Cisco 3500p AP	Cisco 801 AP, Cisco 1100 AP, Cisco 1130 AP, Cisco 1200 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

Supported Versions

Table 3 lists the NCS supported versions of controller, 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 switch IOS Version	Operating System Requirements
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

Installing Cisco NCS Software

The following steps summarize how to install new Cisco NCS Release 1.0 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 > Unified Wireless LAN Management > Cisco Prime Network Control System**.

Step 3 Download the appropriate Cisco NCS software version .OVA image (for example. NCS-VA-1.0.0.X-large/small/medium.ova) and deploy the OVA template.

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

Step 5 Perform NCS initial configuration according to the instructions in the *Cisco Prime Network Control System Configuration Guide, Release 1.0*. 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. Default value is UTC.
Username	Identifies the administrative username used for access to the Cisco 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 Cisco 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).

This section contains the following topics:

NCS License Information

NCS is deployed through 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 physical appliance, except instead of using a UDI, you will 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 Cisco NCS, see the "NCS and End User License" chapter of the *Cisco Prime Network Control System Configuration Guide, Release1.0.*

For detailed information and license part numbers available for Cisco 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 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 Network Control System Configuration Guide, Release 1.0.*

Migrating WCS to NCS

Note You must upgrade your Cisco WCS deployment to Release 7.0.164.3 or 7.0.172.0 before you attempt to perform the migration process to Cisco NCS Release 1.0.

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:

- Exporting WCS Data, page 9
- Migrating WCS Data to NCS, page 9
- Non-upgradable Data, page 10

Note For steps on migrating NCS in a high availability environment, see Chapter 4, “Performing Maintenance Operations” of the *Cisco Network Control System Configuration Guide, Release 1.0.*

Exporting WCS Data

Note There is no GUI for exporting data from WCS 7.x. A new CLI "export userdata" is available in WCS 7.x which creates the .zip file containing the individual data files. 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 Run the **export** command through the script file and provide the path and export file name when prompted.

Step 3 For Linux, run export.sh all /data/wcs.zip. For Windows, run export.bat all \data\wcs.zip.

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://172.19.28.229//
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.

Note When migrating from WCS to NCS, Non-English characters do not display correctly, appear corrupted and is un-readable. For more information, see Bug CSCtq88498 in "Open Caveats" section on page 19.

Non-upgradable Data

The following data are not upgradable from WCS to NCS:

- Certain Reports (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 and Security Summary reports).
- Dashboard customization
- Client Station Statistics information will not be populated with old WCS data in clients charts, client details page, dashboards and reports.
- Client historical session information does get upgraded.
- All events from 7.0 are completely dropped and are not migrated to NCS.
- RADIUS/TACACS server IP and credentials are not migrated and need to be readded again after migration is complete.

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 7.0 to NCS.

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

- The root password is not migrated from 7.0.164.3 or 7.0.172.0 to NCS 1.0 and user needs to change the root password during the installation of the application. Non root users and their credential are migrated during migration.
- Alarm categories and Sub categories are not restored after migration to NCS Alarm Summary.
- When migrating from WCS to NCS, existing non-English characters gets corrupted.

NCS Features

Cisco NCS release 1.0 is Cisco's next generation network management platform for managing wired and wireless networks. This is a major upgrade to Cisco WCS Release 7.0. For more information about new features and enhancements, see the "What's New" section on page 15.

NCS is the ideal platform for eliminating the complexity of converged wired and wireless user and access network management. This platform provides clear visibility and control of the wireless LAN and user access environment from an easy-to-use, centralized interface. It simplifies all LAN and WLAN problem resolution by providing visibility into all connected endpoints with built-in tools to remediate client connectivity issues, helping to ensure smooth Wi-Fi performance, RF interference mitigation with Cisco CleanAir, enhanced network security, and an optimal experience for all fixed and mobile end

users. Cisco NCS requires minimal IT staffing to meet the most demanding operational requirements and is the ideal platform for maintaining a cost-effective, business-ready, converged access Cisco Unified Network.

Table 5 NCS Features

Feature	Description
Simplicity	The NCS User Interface is very simple and intuitive, eliminating complexity. The modularized interface supports user-defined customization to display only the most relevant information. Flexible platform accommodates new and experienced IT administrators.
Scalability	NCS manages lifecycle management of 1200 of Cisco wireless LAN controllers and 15,000 of Cisco Aironet lightweight access points from a centralized location. Additionally, manage up to 5000 autonomous Cisco Aironet access points. Additionally NCS manages up to 5000 switches for monitoring and troubleshooting functions. Scalable mobility and Identity service management are delivered through integration with the Cisco MSE and the Cisco ISE, respectively. Delivered as a physical or a virtual appliance allowing deployment scalability to help customers meet various deployment models.
Centralized Monitoring	Centralized monitoring of the wired and wireless network helps maintain robust performance and an optimal access connectivity experience. Unified switch inventory, dashboard components, reports, and monitoring views help you quickly monitor the access network from a single pane. NCS integration of Cisco Identity Services Engine (ISE) provides monitoring of endpoint security policy 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.
Planning	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 Cisco Prime NCS to aid in WLAN design and deployment. Specialized tools enable immediate assessment of the WLAN's readiness to support VoWLAN and context-aware (location) services. Support for on-demand coverage reassessments helps mitigate the effects of - and in many cases eliminate - improper RF designs and coverage problems.

Table 5 NCS Features (continued)

Feature	Description
Deployment	A broad array of integrated controller, access point, and command-line interface (CLI) configuration templates deliver quick and cost-effective deployments. Network auditing is supported for effective configuration compliance and management. Tools and processes support monitoring, upgrading, and migrating selected Cisco Aironet standalone (autonomous) access points to operate as lightweight access points and run Control and Provisioning of Wireless Access Points (CAPWAP). Role-based Access Control provides flexibility to segment the wireless network into one or more virtual domains controlled by a single Cisco Prime NCS platform. Power savings are delivered through Cisco Energy Wise technology with adaptive WLAN power management. Cisco Prime NCS maps, hierarchies, and network designs can be easily exported and imported between one or more Cisco Prime NCS servers. Virtual domains help deploy large, multi-site networks and managed-services alike.
Troubleshooting	NCS helps in troubleshooting large-scale wired and wireless networks with minimal IT staffing. Integrated workflows and tools help IT administrators quickly assess service disruptions, receive notices about performance degradation, research resolutions, and take action to remedy non-optimal situations. The Alarm Summary provides robust fault, event, and alarm management is now on every NCS page at the bottom, which makes it easy for the administrators to constantly know at-a-glance the working state and therefore support quicker resolution. The Client Troubleshooting tool supports a step-by-step method to analyze problems and configuration issues for all client devices across all connection media, with support to troubleshoot issues such as 802.1X (for wired and wireless networks), and identify RF interferers that are affecting client devices. The ever-present search tool facilitates cross-network access to immediate and historic information. Integration with Cisco ISE 1.0 and Cisco Secure Access Control Server (ACS 4.2, 5.1 and 5.2) View provides a simple way to collect and analyze additional data relevant to endpoints. Specialized diagnostic tools support enhanced analysis of connection problems occurring with Cisco Compatible Extensions clients Version 5 or later. Radio Resource Management (RRM) tools provide visibility into performance, RF statistics, and air quality.

Table 5 NCS Features (continued)

Feature	Description
Reporting	Extensive on-demand and automated reports can be run on immediate and historic network activity, performance, usage, devices, inventory, compliance, security. CleanAir report data, time frame, and format are customizable and output reports in CSV or PDF format is supported and can be saved as a file or attached to an email. NCS integration to Cisco Identity Services Engine (ISE) helps to cross-launch new ISE reports.
CleanAir	Cisco CleanAir technology provides detailed information about RF interference events, air quality, and interference security threats to help more efficiently assess, prioritize, and manage RF interference issues. Easy-to-use graphical displays serve as a starting point for maintenance, security, troubleshooting, and future capacity planning. This feature provides detailed information about RF interference events, air quality, and interference security threats to help more efficiently assess, prioritize, and manage RF interference issues.
High Availability	Built-in, software-based High-Availability maximizes uptime for services delivery and improves operational efficiency. This feature reduces client downtime and results in higher network availability. Access point and client downtime are reduced by shortening the failure detection time, avoiding the restart of the Dynamic Host Configuration Protocol (DHCP) process by reusing the same IP address to re initiate the discovery process, and enhancing the access point discovery process. **Note** High Availability is provided on a 1X1 basis (that is, one secondary NCS can provide failover support to only one primary NCS).
Unique Device Identifier Support	This feature provides the capability to uniquely identify Cisco wireless LAN controllers and LWAPP access points. The wireless LAN controller and the access points Unique Device Identifier (UDI) is retrievable through the CLI and GUI of the wireless LAN controller. The UDI is imprinted in the device and can be viewed from NCS for wireless LAN controller, switches, lightweight and autonomous access points. This information is used for RMA, inventory control and Cisco manufacturing processes.
Autonomous AP Management	Autonomous access points are based on Cisco IOS Software and these devices act as regular APs in terms of processing for all features. Standalone (autonomous) access points are managed by NCS, that is, NCS uses a Telnet-based connection to upgrade the access point firmware. NCS supports easy upgrade or migration of standalone (autonomous) access points.
Context Aware Service	Location tracking allows organizations to more easily find equipment within a data center environment and make business decisions more quickly. Now the MSE platform locates wired and wireless information so that businesses can make decisions based on both wired and wireless business assets.
Cisco NCS mobility group templates	Users can assign a template to all of the elements in a mobility group. Users can select the mobility group name, and then apply the template across the entire mobility group domain. Users still have the option to assign templates to specific network elements.
Management Frame Protection (MFP)	This is for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points.

Table 5 NCS Features (continued)

Feature	Description
Enhanced WLAN Security	With expanded intrusion detection and new rogue classification capabilities, the security on both the wired and wireless networks is increased, false alarms are reduced, and more granular control over detection, policies, and reporting is provided.
Hybrid Remote Edge Access Point (H-REAP)	Hybrid REAP capabilities help IT managers to centrally control Service Set Identifiers (SSIDs), security parameters, software loads, facilitating unified, and enterprise wide wireless LAN services.
Improved guest user management	Secure wired and wireless guest access gives controlled wireless access to customers, vendors, visitors, and partners, while keeping the network secure. You can customize a login failure message and a logout verification message web page. Additionally, you can enhance overall security by introducing guest account creation limits and extending investment protection with the support of LD authentication.
Enhanced voice over WLAN capabilities	Organizations can improve the quality of voice calls and reduce dropped calls. The new audit tool automates configuration checks by allowing customers to define a set of rules in the NCS to validate the configuration of a group of controllers based on the VoWLAN deployment guide recommendations. Violations of the configuration can be presented in the form of a report and/or alarm.
Auto-provisioning of wireless LAN controllers	Cisco NCS can automatically configure a new Cisco wireless LAN controller when it is detected on the wireless network.
Diagnostic channel security enhancements	Cisco Compatible Extensions version 5 client devices can request diagnostic channel association to the unified network to assist with troubleshooting.
Tracking Optimized Monitor Mode	Tracking Optimized Monitor Mode is a new access point configuration that enables the detection of Wi-Fi tags even if a wireless network is not actively deployed. TOMM access points can be easily added exactly where they are needed to provide ideal coverage and location accuracy without disrupting existing network configurations.
Automated client troubleshooting	When a Cisco Compatible Extension version 5 client gets associated to the WLAN diagnostic channel on WLC, a diagnostic trap is raised. If you choose to automatically troubleshoot the client, a series of version 5 tests are carried out on the client upon trap arrival, and the client is updated with the test status via pop-up messages. The report is placed in the logs directory. You have the option to export all of the automated troubleshooting logs.
wIPS ELM	wIPS now includes the ability to visualize, analyze, and pro-actively prevent attacks on customer networks and equipment. The objective of the ELM (Enhanced Local Mode) is the ability to detect on-channel attacks while simultaneously providing client access and services. The feature offers full 802.11, nonstandard channel and non-Wi-Fi threat detection. It uses an extensive threat library and supports forensics and reporting. Pre-processing at the access points minimizes the data backhaul because it works over very low bandwidth links.

Table 5 NCS Features (continued)

Feature	Description
RF Grouping	This feature provides wireless controller enhancements to Radio Resource Management (RRM). An RF grouping algorithm provides optimal channel allocation and power settings for access points in a network.
3500P AP Support	Support for a 3500P AP has been added in NCS. The 3500P APs are 802.11n access points that have narrow beam and highly directional antennas.
VLAN Select	Integration of the VLAN Select feature in 7.0.114.82 release enables WLAN to be mapped to multiple interfaces using an interface group. Wireless clients associating to this WLAN will get an IP address from pool of subnets identified by the interfaces in round-robin fashion.
Web Auth Proxy	This feature enables clients that have manual web proxy enabled in the browser to facilitate authentication with the controller.
FIPS Support	Cisco Controller Release 7.0.98.0 has been awarded Federal Information Processing Standard (FIPS) 140-2 validation.
Google Earth Integration	Google Earth can be launched and used from Cisco NCS to correlate the location and define the RF coverage area of a Cisco Aironet lightweight outdoor mesh access point using the Google Earth map feature. Google Earth must be installed to enable this feature.
Spectrum Management	Cisco Spectrum Expert can be utilized for Cisco Aironet access points that are enabled with Cisco CleanAir technology and configured for Cisco Spectrum Expert.

What's New

This release includes the following new features and enhancements:

Note For more details on the new features, refer the *Cisco Prime Network Control System Configuration Guide, Release 1.0*.

- Converged Access Management—Single view of wired and wireless clients, monitoring of controllers and switches and more. Comprehensive monitoring and troubleshooting support for Cisco Catalyst switches allows for visibility into critical performance metrics for interfaces, ports, endpoints and users, and basic switch inventory.
- User Services—Monitor or list pages for clients, detail pages (client, controller, switch).
- Identity Services Engine (ISE) integration—ISE provides the functions of Cisco ACS and Cisco NAC in one integrated platform. Its unique architecture allows enterprise networks to gather real-time contextual information from the network users and devices. It then uses this information to make proactive governance decisions by tying identity back into various network elements including access switches, wireless controllers, Virtual Private Network (VPN) gateways, and data center switches. Prior to Cisco ISE, the network connected to several devices in order to provide AAA services, user and device compliance, device discovery and profiling, and guest lifecycle management. With Cisco ISE, one device contains all of these functions.
- New User Experience—New home page (components, customization of components and home page), navigation/customization within client/device list and detail pages.

- Other salient features—Advanced searching, filtering and listing of alarms and search results.
- CleanAir Support—Monitoring and reporting of CleanAir.
- Autonomous AP Support—Monitoring and reporting of Autonomous AP support. Autonomous AP client management is also supported in NCS.
- Deployment Modes—NCS has two deployment options: physical appliance and virtual appliance. The virtual appliance is an OVA file that can be deployed on VMware ESX/ESXi 4.x. The physical appliance is a physical device.
- Adding and configuring switches—Switches can be added to your network. Switches can be added individually or multiple switches can be imported via CSV file. You can also associate switches with the maps so that the maps provide context regarding where the wired endpoint resides. However, the switches will not appear on the map.
- Enhanced Dashboards—Dashboard components have been enhanced with intuitive flows, ease of customization. Administrators can now create their own dashboard so the information that is most relevant to them can be quickly displayed.
- Monitoring Client and Users—NCS provides the ability to monitor both wired and wireless clients. This provides a unified view of all clients on the network.
- Wired and Wireless Client Troubleshooting—Both wired and wireless monitoring and troubleshooting have been integrated with identity services.
- Tracking Clients—A network administrator can track specific clients and be notified when these clients connect to the network.
- Dynamic Heatmaps—Displays real-time heat maps.
- Reports—NCS provides integrated management of wired and wireless devices/clients. SNMP is used to collect client data. Cisco ISE is polled periodically to collect client statistics and other attributes to populate related reports.
- Alarms and Events—NCS provide a single page view of alarms and events for wired and wireless devices. The alarm summary and the alarm browser is displayed in the bottom right of the screen regardless of what screen the user is on. Quick and Advanced filter options provide greater search capability.
- New License Structure— New licensing structure has been introduced in NCS. This is a simpler licensing structure and protects the customer's current license investment. You can migrate the existing WCS licenses to NCS.
- Unknown Devices—NCS labels a device that is not communicating with NCS as an unknown device. This device could be a device that has just been added to NCS that has not yet communicated with NCS or it could be another device that has not been added to the system. If the device attempts and is able to communicate with NCS, it is removed from the "unknown device" list. The Monitor > Unknown Device page provides information regarding the device and any errors associated with it. The Config > Unknown Device page enables the administrator to remove the device or update the device's credentials.

Important Notes

This section describes important information about NCS.

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 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 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 physical appliance, except instead of using a UDI, you will 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, refer to the *Cisco Prime Network Control System Configuration Guide, Release 1.0*.

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 will get timed-out and be removed. In that case, the client will not be discovered in NCS.

Autonomous AP Migration Analysis

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

Importing Maps

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

Old Features Not Supported

The following list of features is not supported in the current NCS 1.0 release:

- Monitor RRM Enhancements
- WEB-auth on MAC filter failure
- NAC 802.11 disassociation trap-webauth proxy
- 11-N Mesh support
- NEC Phase III enhancements/Preferred Call
- Voice Diagnostics

- General Video Support

Caveats

This section lists open and resolved caveats in Cisco NCS 1.0. 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: https://tools.cisco.com/RPF/register/register.do

Open Caveats

Caveats Associated with Release 1.0

Table 6 lists the open caveats in NCS 1.0.

Table 6 Open Caveats

ID Number	Caveat Title
CSCtn70913	The state column in the stranded AP report is incorrect. **Symptom**: Stranded APs do not show proper value in the state column. When ever the mesh APs go stranded, NCS shows the mesh AP in the stranded AP report, but the State column does not show the correct value. **Conditions**: When Mesh controller is added to NCS and associated Mesh APs have gone stranded for some reason. **Workaround**: None.
CSCtq09640	Sometimes Switch Location Configuration Template apply gives error. **Symptom**: Sometimes Switch Location Configuration Template apply gives error **Conditions**: When using the switch location configuration template to apply template to a large number of ports, telnet connection to the switch might time out. When you choose Configure > Switch Location Configuration Template, create a template and apply to switch interface, it shows 'EXCEPTION_THROWN'. **Workaround**: Apply template to a couple of ports at a time.
CSCtq56961	CCXv5 profiles are incorrectly reported for V5 clients. **Symptom**: CCXv5 profiles are shown for some clients although the client does not have any profile associated to it. **Conditions**: Sometimes there is a data discrepancy seen between Controller GUI and NCS UI. NCS reports CCXv5 profiles for some V5 clients which perhaps do not have any associated profiles. **Workaround**: None.
CSCtq71119	Saved Report Templates are missing in Virtual Domain when NCS is upgraded from WCS. **Symptom**: ClientCount, Client Summary, Report BandwidthUtilization report templates are missing in a virtual domain. **Conditions**: This condition happens when database is upgraded from WCS to NCS. **Workaround**: None. These three types of report template settings will not be upgraded from WCS to NCS.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq78026	After upgrade from WCS, root user cannot switch to other allowed Virtual Domains. **Symptom**: Allowed virtual domains for a root user are missing when database is upgraded. **Conditions**: This condition happens when database is upgraded from WCS to NCS. **Workaround**: Assign the missing allowed virtual domains for a root user from the root-domain. The page to be used for setting a user to virtual domains is: Administration > AAA > Users > User Details.
CSCtq78807	Incorrect Rogue Alarms reported from a virtual domain. **Symptom**: Incorrect rogue alarms are reported in a virtual domain. **Conditions**: When user logged into virtual domain, the rogue alarms counts is seen in the detailed alarm summary and the rogue alarms are seen in Monitor > Alarms page. In a virtual domain, NCS reports rogue alarms from controllers that are not part of this virtual domain. **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.
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 is less than timestamp-B. 3. Restore NCS backup taken from step2 on NCS Server running on timestamp-A, NCS fails to start and throws error. **Conditions**: NCS 1.0 is running behind date/time which is in the DB backup. **Workaround**: Configure and Set the correct date/time on NCS.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq87447	Exception when you add autonomous AP once deleted from Virtual Domain. **Symptom**: NCS failed to delete an autonomous AP from a virtual domain. **Conditions**: This happens when an autonomous AP is first added into the root domain and then assigned it to a virtual domain. Later, the user logged into the same virtual domain, deleted the autonomous AP and then re-added it with wrong credentials. **Workaround**: Delete the autonomous AP from the root domain.
CSCtq87805	Sorting ethernet switches by IP address does not work. **Symptom**: Sorting ethernet switches by IP address does not work on **Monitor > Switches** page. **Conditions**: When user reaches the **Monitor > Switches** page by clicking on the pie chart on the NCS home page. **Workaround**: Go to the **Monitor > Switches** page from the top Menu.
CSCtq91517	Audit trail logs are empty for non root users after data migration. **Symptom**: After migrating users from earlier version of WCS to NCS, clicking on Audit trail for non-root users in NCS displays empty records. **Conditions**: Audit trail records are populated for non-root users in earlier version of WCS. **Workaround**: None
CSCtq92214	Delete or Edit Dynamic Interface associated with WLAN Multicast VLAN throws error. **Symptom**: Deleting a dynamic interface which is associated to WLAN Multicast VLAN interface is throwing an unknown error; Similarly editing the same associated dynamic interface throws a SNMP error. **Conditions**: Multicast is enabled on the controller and a dynamic interface is associated to WLAN Multicast VLAN interface. **Workaround**: Remove the association and edit the dynamic interface.
CSCtq92383	PDF Report export for large data set can take from 30 minutes to few hours. **Symptom**: Interactive Save and export operation for report containing large data set can take a long time. **Conditions**: Run Save and Export for a report containing large data set and set the export format to PDF. The operation can take anywhere from few minutes to hours. **Workaround**: The same report can be scheduled instead of doing an interactive report generation through Save and Export. **Further Problem Description**: The amount of time taken for a report generation in PDF format is dependent upon the data set for the report, time taken by data retrieval from db which in turn depends among other things upon how busy the db is and JasperReport generation time.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq94128	Expanded row with detail shown in Event Page is not fixed on the top. **Symptom**: When clicking the row expander to view detail in Event or Alarm page, the expanded row is not highlighted or fixed on the top of the table. **Conditions**: If the total number of events or 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 'Location History' link inside Rogue AP Alarm detail panel, warning dialog may pop up if location page can't be launched. After the 'ok' button in the warning dialog is clicked, alarm detail panel will be closed. **Conditions**: When failure to launch '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 re-open the alarm detail.
CSCtq94153	**Monitor > Controller**: clicking on port link on WLC image throws error. **Symptom**: Click on a controller on the Monitor > Controllers page to view its Controller Details page. On the Controller Details page, clicking on a port in the controller image takes you to a page without the navigation header. Links on this page may not work. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. This applies to monitoring 7500, 2500, or 2106 Wireless LAN Controller models. **Workaround**: Reach the Port Detail page from the **Ports > General** menu option on the left-hand side of the Controller Detail page.
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.
CSCtq94255	Certain links in the security dashboard are not working. **Symptom**: issue1: Click Home > Security dashboard and detach Security Index dashlet. The "View All" and "Devices" links are not working. issue2: After acknowledged security issues from "View All" on Home > Security dashboard page under Security Index dashlet, from "Devices" list the security issues counts do not reflect the changes. Ideally the counts should only show unacknowledged issues. **Conditions**: None. **Workaround**: None.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq95461	Time is not properly displayed correctly for Pre Coverage Hole events. **Symptom**: In an Event list, Pre Coverage Hole events have a large number listed for the Time, and no value for the Radio Type.You can view a list of Pre Coverage Hole events by performing an Advanced Search for Events, where the Event Category is "Pre Coverage Hole". **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: Click on the event to view its details. This will show you which radio band the event affects, and a human-readable value for the time at which the Pre Coverage Hole was detected.
CSCtq96037	Added controller is found in switch list page in a NAT setup. **Symptom**: When you restore customer DB backup from NCS, and adding couple of controllers. Both the controllers show up in configure > Switch list page. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: None.
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.
CSCtq97889	Admin user seeing Access denied for wIPS alarm information display. **Symptom**: The help content related to wIPS alarms in wIPS Profile Configuration page are not getting displayed for Admin or Config Manager users. **Conditions**: Issue seen for Admin or Config Managers users, where in the information for wIPS alarms are not loaded earlier by root/super user. **Workaround**: Using root user, all wIPS alarms are accessed to load the information content; Then login as admin user solves the problem.
CSCtq99699	Changing ethernet bridging VLAN access mode configuration throws error for Mesh APs. **Symptom**: When you change ethernet interface access mode from access to trunk or trunk to access mode, it throws up SNMP exception. **Conditions**: When Mesh APs are added to NCS. **Workaround**: None. **Further Description**: The changes are reflected in the controller.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq99992	The Mesh Alarm page does not display the generated mesh alarms when navigated from mesh dashlet. **Symptom**: In alarm dashlets, you have the number of mesh alarms as a hyperlink. On click of that it takes you to the Mesh alarms page. This link shows there are 'n' number of alarms but when you click on it, it does not show any alarms. **Conditions**: NCS with Mesh controllers added to it, and mesh alarms are generated. **Workaround**: Check the Monitor > Alarms page.
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 shows this error. **Workaround**: None.
CSCtr00174	DCA Channel Width parameter is not present in RRM templates. **Symptom**: DCA Channel Width parameter is not present in RRM templates. **Conditions**: Choose 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.
CSCtr01285	Not able to delete maps in a Virtual Domain. **Symptom**: Floor map or building map cannot be deleted when user logged in a virtual domain. **Conditions**: For floor map delete case, this happens when its parent building-map is also in the same virtual domain. For building map delete case, this happens when its parent campus-map is also in the same virtual domain. **Workaround**: If user in a virtual domain does not need to access all floor maps in a building, do not assign the parent campus and the parent building to the same virtual domain. Assign the allowed floor maps only to this virtual domain.
CSCtj99108	Client computer/physical port name in controller CLI session page shows incorrect value. **Symptom**: Client computer/physical port name in controller CLI session page shows incorrect value. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: Look at the controller page under **Management -> User sessions** to see the correct value.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtj99119	Last request sent parameter in the DHCP statistics shows incorrect value. **Symptom**: Last request sent parameter in Controller > System > DHCP statistics page shows incorrect value. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: The value can be obtained through the CLI command show dhcp stats in NCS.
CSCtk65012	Guest count does not include wired guest counts in the guest user count dashlet. **Symptom**: Wired Guest count are not included in the home page guest user count dashlet. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: Query for wired guest clients from the Advanced Search tool.
CSCtl77129	User authentication through 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 is reachable to each other. Under Administration > AAA > AAA Mode Settings page, TACACS+ option is selected and "Enable fallback to Local" is checked with default option. **Workaround**: Works well with one of the two interfaces **Further Problem Description**: NCS Box has two interfaces - 10 N/w (10.x.x.x) & 9 N/w IP(9.x.x.x); (With default route on 10 N/w) Similarly ACS server has above two interfaces. In NCS, you can create AAA TACACS+ server selecting 10 N/w interface. AAA user authentication works fine. However when you create AAA TACACS+ server selecting 9 N/w interface, AAA user authentication is failing.
CSCtl97650	Virtual domain count is incorrect in the child partitions for applied templates in the restored setup. **Symptom**: Virtual domain count is incorrect in the child partitions for applied templates in the restored setup. **Conditions**: In a WCS to NCS upgraded setup. **Workaround**: None.
CSCtn16860	No valid error alert seen for North bound API user login through web. **Symptom**: Seeing Invalid username / password alert pop up whenever North bound API user tries to login via web whenever AAA mode set to local. NCS redirects user to Access Denied Page whenever AAA is set for Radius or TACACS+. **Conditions**: Issue seen for North Bound API user login via Web with different AAA mode options. **Workaround**: None

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtn56637	Link to a report in an email goes to the login page instead of report. **Symptom**: NCS EMail report links - do not directly go to the report link if clicked instead it goes to dashboard. **Conditions**: Issue seen when user gets email report link. **Workaround**: As of now user need to manually go to the report launch pad to see the specific category reports.
CSCto16463	Software version column sorting in controller page is incorrect. **Symptom**: Try sorting on Software Version column on Controllers List Page. The sorting happens with digit by digit comparison and not as octets. For example, 7.0.98.1 falls higher than 7.0.114.0 though 98 is less than 114. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: None. **Further Problem Description**: Considering versions as 7.0.114.102, 4.2.212.0, 7.0.98.0, 7.0.114.97 NCS sorts as 4.2.212.0 7.0.114.102 7.0.114.97 7.0.98.0 The correct sorting should be 4.2.212.0 7.0.98.0 7.0.114.97 7.0.114.102
CSCto26967	IE8 64 bit flash plugin download URL is incorrectly shown on the charts. **Symptom**: Charts are not seen when using IE8+Chrome 64 bit browser. The same content works ok on Firefox and IE8 32 bit. **Conditions**: The download URL provided for flash plugin is not correct when using IE8 64+ chrome browser. **Workaround**: Use the following URL to download the flash plugin manually: http://helpx.adobe.com/flash-player/kb/flash-player-64-bit-operating.html

Table 6 Open Caveats (continued)

ID Number	Caveat Title
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 servers. **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.
CSCto56706	Not all failed password policies are displayed. **Symptom**: Only one failure reason displayed instead of displaying all password rules which failed to adhere in Add user / change password page. **Conditions**: Under Local password policy, all the password rules are checked or enabled. Whenever the password specified contains username, you can see only one error - User password should not contain the associated user name and the user name reversed, Instead of displaying all password rules which failed to adhere in this case. **Workaround**: You will be able to see Password failure errors one at a time and all together in this particular case when password contains user name.
CSCto60695	Port Detail Alarms link is not filtering alarms. **Symptom**: Click Monitor > Controllers, select a controller, select Ports >General from the left-hand menu, then click on a port to view the Port Details page for a controller's port. If you click on the Alarms link at the top of the page, the resulting list of alarms will not be filtered with alarms specific to that port. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: None.
CSCto78497	CleanAir AP count in inventory report when it is run in a Virtual Domain is displayed incorrectly. **Symptom**: CleanAir AP count in the inventory report is displayed incorrect. **Conditions**: If user is logged into a virtual domain and inventory report is run, the CleanAir AP count shown is wrong. **Workaround**: None.
CSCto96526	User Group Audit trail does not display AAA auth. user operations. **Symptom**: When AAA users belonging to a particular User group login to NCS, the audit trail logs for that particular User group doesn't display any information on these AAA users login / logout operation. **Conditions**: User Group Audit trail missing for AAA authenticated users only. **Workaround**: However the audit trail is displayed from Active Sessions page for the AAA logged in user.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq04302	The Channel Utilization chart should be renamed in the Radio Monitoring Page. **Symptom**: Channel Utilization chart on the Radio Monitoring Page is different from Channel Utilization under Load Statistics. They should not be correlated. **Conditions**: Navigate to Radio Monitoring Page **Workaround**: None.
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.
CSCtq11177	OfficeExtend AP settings are not retained after upgrade for air quality report. **Symptom**: OfficeExtend AP settings are not retained after upgrade for air quality Vs time report. **Conditions**: Air Quality Vs time report created in WCS 7.0 with settings as All Controllers > All Office Extend APs gets reset to All Controllers > All Access Points when backed up and restored in NCS. **Workaround**: Change the report settings back to All Controllers > All OfficeExtend APs.
CSCtq18725	Advanced search is not showing all RRM CleanAir channel change events. **Symptom**: Advanced search is not showing all RRM CleanAir channel change events. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: Go to the Monitor > RRM page to look at the CleanAir channel change events.
CSCtq24859	Security risk alarm count does not match with the list shown on security tab. **Symptom**: Security risk alarm count obtained by searching alarms does not match with the list shown on security tab. The CleanAir security section in Security tab on homepage shows the incorrect count. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: Use advanced search to find the security risk alarms.
CSCtq29277	Interface Group Template can select quarantine and non-quarantine interfaces. **Symptom**: Able to select mixture of both quarantine and non-quarantine interfaces in Interface Group. Ideally you should not be able to select both mixture of quarantine and non-quarantine interfaces. **Conditions**: This happens while trying to edit the interface group for quarantine state and include quarantine interfaces to the interface group. **Workaround**: Explicitly remove unwanted dynamic interfaces.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq31584	Duplication of RRM > TPC configuration parameters in different places. **Symptom**: Duplication of RRM > TPC configuration parameters in different places. The transmit power threshold configuration is present in two different paths in NCS. If one is updated then the other link shows a mismatch. **Conditions**: Appears at 802.11 (a/n and b/g/n) RRM > TPC and 802.11 (a/n and b/g/n) > Parameters. **Workaround**: Just configure RRM TPC Parameters at RRM > TPC page and ignore settings at 802.11 (a/n and b/g/n) > Parameters.
CSCtq31784	Discrepancy in RRM > DCA > Channel Update Interval. **Symptom**: The 'Channel Update Interval' interval is not getting updated on NCS. It always shows the default value of 600 seconds. Audit will not show a mismatch if controller is configured with a different value. Refresh Config from controller is also not updating the DCA update interval on NCS. **Conditions**: When Controller is configured with a different value. **Workaround**: None.
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.
CSCtq34227	Invalid trap log message in Monitor > events for signal change. **Symptom**: If an AP changes channel due to signal strength, the Event as it appears in the Monitor > Events list may incorrectly state the reason as "Load or Channel changed by neighboring AP". **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: If you view the trap log on the originating controller, you may see that the reason should actually be: (your-controller) > show traplog Number of Traps Since Last Reset ..... 1 Number of Traps Since Log Last Displayed .... 1 Log System Time Trap --- ---------- ---------- 0 Tue May 17 06:40:55 2011 Channel changed for Base Radio MAC: aa:bb:cc:dd:ee:ff on 802.11a radio. Old Channel: 1. New Channel: 2. Why: Signal Strength. Energy before/after change: 2/3. Noise before/after change: 4/5. Inter ference before/after change: -56/56.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq35642	Cannot add Spectrum Expert 4.0 using FireFox in MAC Operating System. **Symptom**: Spectrum Expert 4.0 cannot be added to NCS when using Firefox on MAC Operating System. **Conditions**: This affects version 1.0 of the Cisco Network Control System. **Workaround**: Add using Internet Explorer 8 with Chrome plugin or Firefox on windows Operating System.
CSCtq37807	The RSSI graph of RX Neighbors in the AP Radio page does not show the scale information. **Symptom**: The RSSI graph of RX Neighbors in the AP Radio page does not show any kind of scale. **Conditions**: Monitor > AP - Radio page (On demand RSSI-statistics graph) **Workaround**: None.
CSCtq40098	In the Guest Association report, the same guest user in two different sessions is shown as one entry. **Symptom**: If two or more users use the same Guest User account to log into the network, NCS reports only one of these. **Conditions**: This happens when the client polling cycle has missed to fetch the client information. **Workaround**: None.
CSCtq53132	AP Summary pop-up appears out of bounds. **Symptom**: When you hover your mouse over an object on a floor or outdoor area page, the informational popup appears partially off-screen. **Conditions**: 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.
CSCtq57832	TACACS+ users does not remember the last logged in Virtual Domain. **Symptom**: TACACS+ users does not login into their last active virtual domain unlike Radius users who login correctly into their last active virtual domain. **Conditions**: TACACS+ users who belong to multiple virtual domains. **Workaround**: After login, switch to the desired virtual domain.
CSCtq64164	Mobility groups shows controllers that do not belong to current active Virtual Domain. **Symptom**: When Adding Mobility group members, NCS lists the controllers that do not belong to the current active virtual domain. **Conditions**: Atleast one controllers should be a member of a non root virtual domain. **Workaround**: None.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq67819	Audit in RF group page should open a popup even if their are no mismatches. **Symptom**: Navigate to Configure > Controllers > 802.11a/n > RRM > RF Grouping. If there are no mismatches then a popup should open with the following text "No differences found between NCS and device values". **Conditions**: When there are no mismatches between NCS RF Grouping Config and WLC RF Grouping config, No popup opens to mention the there were no differences. **Workaround**: None
CSCtq70306	Alarm mismatch between Maps Tree view and Floor view. **Symptom**: View the Maps Tree view for a particular floor area. The icon for the floor indicates that there is a Critical alarm present. Similarly, that floor's entry on the map list page may show a critical radio alarm. However, when you view the floor, all of the access point icons show only yellow for Major alarms. **Conditions**: This affects version 1.0 of the Cisco Network Control System. It also affects all versions of the Cisco Wireless Control System. **Workaround**: Use the Floor Settings menu to display the AP status instead of the radio status. Click on the arrow '>' for Access Points to display the Access Points filter, and select AP Status. You can save this preference with the Save Settings button.
CSCtq79221	SPT issues after upgrade. **Symptom**: The following issues seen for the saved SPT results after upgrade from WCS 7.x: 1. In Annotation, Data or Time is missing. 2. Enable/Disable port link doesn't work properly. **Conditions**: None **Workaround**: Perform another SPT in NCS.
CSCtq79369	Monitor > Spectrum Expert shows different count for alarms on clicking the 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**: This affects version 1.0 of the Cisco Network Control System. It shows WI-FI Invalid interferer. **Workaround**: None.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq81833	SE becomes unreachable after some time but alarms keep coming. **Symptom**: Issues with adding SE or after adding SE, connection terminates. **Conditions**: This affects version 1.0 of the Cisco Network Control System. **Workaround**: None.
CSCtr08113	Switches added for SPT shows up under client report filters. **Symptom**: Switches that are added for SPT (Switch Port Tracing) and are not managed by NCS, show up under the client report filters. For these switches, the data is empty and no client related statistics is collected. **Conditions**: When switches are added for SPT but are not managed by NCS. **Workaround**: None.The switches can be ignored or filtered out from the list of selected devices for the reports.
CSCtr04327	Export operations for ClientSessionReport may take from 30 minutes to 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 few hours. **Conditions**: - Select long period of reporting time (say 4 weeks) - A lot 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 **Further Problem Description**: The problem is observed in a database having over 10 million sessions.
CSCto07596	Exception is seen in the log while deleting a controller. **Symptom**: Delete controller fails with exception in the log. **Conditions**: This affects version 1.0 of the Cisco Network Control System. **Workaround**: Try the delete again.
CSCto46112	Virtual Domain tree does not give any indication if there are sub-domain under parent. **Symptom**: There is no visual indication that a virtual domain has children. **Conditions**: This is seen in the virtual domain tree (left hand pane) in Administration > Virtual Domains page. **Workaround**: Click on any Virtual Domain name in the tree to check that it has children.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq00666	Root domain is shown twice on upgraded NCS server. **Symptom**: Root domain is shown twice in virtual domain drop-down list for the root user **Conditions**: This happens when NCS is upgraded from WCS. **Workaround**: Go to the Administration > AAA > Users > User Details page. Remove the additional ROOT-DOMAIN from the selected Virtual Domain section and Save.
CSCtq10886	Not getting results for AP summary report if run by Floor Map in a Virtual Domain. **Symptom**: Not getting results for AP summary report if run by Floor Map in a virtual domain. **Conditions**: This happens when the parent campus-maps and the parent building-maps are not present in the same virtual domain where their children floor-maps are present. **Workaround**: Add the parent campus-maps and the parent building-maps for all the floor-maps that are in a virtual domain.
CSCtq22201	**Symptom**: When NCS is unlicensed, clicking on Advanced search gives error dialog with content "Error while parsing rendering content.....". **Conditions**: NCS is unlicensed. **Workaround**: Add a NCS license.
CSCtq37281	No link to cross launch AP details from AP alarm detail panel. **Symptom**: Unlike previous releases of WCS, there's no hyper link to cross launch AP Details from AP alarm detail panel in Alarm Page. **Conditions**: When view AP alarm detail in Alarm Page, user may not see hyper link to cross launch AP details. **Workaround**: Use AP page launched from other points to view AP details.
CSCtq37963	Idle timeout happens even if it is not enabled. **Symptom**: Session gets timed out even when the idle timeout in user preferences is disabled. **Conditions**: This issue happens only for the following condition: - idle timeout is enabled and user log out of the session. - after logging back in user disable the idle timeout and save the setting however the session still gets timed out. **Workaround**: If user logs out again and log back in then the idle timeout setting is correctly persisted.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq39369	Exception is thrown when you add a virtual domain to user in Non-root Virtual Domain. **Symptom**: Cannot assign virtual domain to user in a non-root virtual domain **Conditions**: User logs into a non-root virtual domain, and creates some new virtual domains. Now, when creating a new user and assigning the newly created virtual domain(s) will throw exception error. **Workaround**: Logout and re-login to this virtual domain. Then add a a new user and assign the virtual domain(s) that were created previously.
CSCtq53528	SPT is not working in VD 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.
CSCtq55227	Update Device Credential Page does not show the correct values. **Symptom**: UpdateDevice Credential Page does not show the correct values. **Conditions**: In Unknown device page. **Workaround**: Enter the credentials for the device again. Use bulk update to update the credentials for the device.
CSCtq66036	Template Virtual Domain propagation does not happen when it gets applied to a controller. **Symptom**: Applied template to a controller cannot be seen in the relevant virtual domains. **Conditions**: When a template is applied to a controller, this template is not seen in all the virtual domains where this controller is a member. **Workaround**: From the root domain, first remove the controller from all the assigned virtual domains, and then re-add the same controller to these virtual domains.
CSCtq68680	RF Group Summary lacking link to detailed Summary under RRM Dashboard. **Symptom**: There is no way of knowing RF Group summary- only count will be seen like 10. It should be click-able and allows user to further look at summary a/n, bg/n groups with IP address and more information. **Conditions**: Click Monitor > RRM Dashboard. **Workaround**: None.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq76735	Switch and NCS category NB traps is not supported in Netcool. **Symptom**: • NCS and Switch category traps cannot be processed correctly by Netcool application. • When AP is disassociated, the NB will receive, a AP down critical trap and then Radio clear traps, though radio is not up. When AP comes back up, then AP up clear alarm is received in the NB. **Conditions**: When NCS generates, NCS and Switch category alarms, corresponding NB traps will be generated. But Netcool will not be able to process these traps correctly. It will be shown as unknown categories. **Workaround**: None. **Further Problem Description**: 1. When NCS generates, NCS and Switch category alarms, corresponding NB traps will be generated, if the user has chosen those categories in the UI. But Netcool will not be able to process these traps correctly. It will be shown as unknown categories as the MIB does not support them yet. 2. When AP is disassociated, the NB will receive, a AP down critical trap and then Radio clear traps, though radio is not up. When AP comes back up, then AP up clear alarm is received in the NB. This is a side effect of the radio alarm suppression logic in NCS.
CSCtq76770	Unresponsive script warning in selecting AP's for Virtual Domain. **Symptom:** Unresponsive script warning in selecting AP's for adding them into a virtual domain. **Conditions:** This happens when total number of controllers, access points, switches and maps that are managed by the NCS becomes high (when the total number is greater than 7K). **Workaround:** Click to continue wait (may take couple of minutes to complete).
CSCtr16514	Unacknowledged tasks are accessible to all users on alarm detail page. **Symptom**: Unacknowledged task is accessible to all users on alarm detail page irrespective of acknowledge/unacknowledge rights. **Conditions**: This affects version 1.0 of the Cisco Network Control System. **Workaround**: None.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtr00667	All columns are not sortable in Monitor > Clients > Clients by MSE. **Symptom**: Some of the sort columns are not sortable in the client list for clients detected by MSE. **Conditions**: This happens when the user is trying to sort based on columns which are not present on the MSE. The following is the columns which are not sortable: 1. Posture Status 2. Speed 3. Traffic 4. Throughput 5. RSSI 6. SNR 7. Auth Policy 8. HREAP Auth 9. AP Name 10. AP IP 11. Switch Name 12. Hostname 13. AP type 14. Auth time stamp 15. Authorized by 16. Bytes received 17. Bytes sent 18. Vendor 19. ISE Name **Workaround**: None **Further Problem Description**: Sorting on unsupported columns leads to a default sort by mac address.
CSCtq53283	Inspect Location Quality tool page scrolling issue when using Firefox. **Symptom**: Using Firefox browser, open an 'RF Calibration' page and launch 'Inspect Location Quality'. Select a data point and hover over it. All details for the point should be shown and additional detail is obtained by scrolling to the bottom of the screen. **Conditions**: Scrolling is not successful in the normal page view mode. **Workaround**: Select 'Full View' from the firefox browser tool window. This will bring the full page and data can be seen this way.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtq30464	MSE installer file size preventing download. **Symptom**: When you try to download an MSE software image from NCS to the MSE using the GUI; it fails when the chosen file is the image with database bundled in it. This is a tar file posted on CCO along with the regular binary installer. **Conditions**: The failure occurs because the size of this tar file is > 2GB. NCS has a check which limits the maximum size to 2GB for downloads. **Workaround**: Manually FTP OR SCP this file to the MSE and place it under /opt/installers folder.
CSCtr19220	Cleared alarms cannot be deleted by the data cleanup background task. **Symptom**: Data clean background task could not perform the following pruning: 1. Delete cleared non-security alarm after 7 days. 2. Delete cleared security alarm after 30 days. 3. Deleted alarms based on GUI setting (user could chose to say that delete all the alarms older than 30 days old). Hourly based alarm table pruning could not delete cleared alarms when alarm table has more than 300000 entries. **Conditions**: This affects version 1.0 of the Cisco Network Control System **Workaround**: User could take proactive actions to maintain the alarm table size by deleting unwanted cleared alarms from NCS User Interface.
CSCtr13005	Interferer location history page does not show the icon and enlarge option. **Symptom**: Interferer Location History does not show the Enlarge Icon and the "Enlarge Map" option. **Conditions**: Choose Monitor > Interferer, click on Interferer Details. From the Drop-down list, select Interferer History. **Workaround**: None.
CSCtr13833	Switch Inventory and Autonomous AP task execution history is missing. **Symptom**: The task execution history for Autonomous AP inventory and Switch inventory gets removed from Administration > Background Tasks page. **Conditions**: This happens everytime when Data Cleanup background task runs. **Workaround**: None
CSCtr16460	Charts are not visible on chrome browser for Monitor > radio details. **Symptom**: On the Radio Details page for a radio interface, the charts on the General tab do not appear. **Conditions**: This affects users of the Chrome browser and Chrome Frame plug-in. This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: Use Mozilla Firefox browser version 3.6 or later to access the Radio Details page.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtr19310	UDI gets removed from the secondary configuration file. **Symptom**: NCS fails to start on secondary when attempting to become the active server. One of the failure messages seen during this failure is: “Unable to start secondary Reason: ORA-01665: control file is not a standby control file”. Other failure messages may also be seen but the initial condition of the failure is due to a license validation failure on startup of the NCS services. **Conditions**: The issue is seen when NCS attempts to start on the secondary during a failover. When starting the NCS server a license validation is done and the validation fails on the server. **Workaround**: Reboot the primary server. After the server restarts and NCS is running. Navigate to Administration > High Availability. Remove the current secondary NCS. After successfully removing the server then add the NCS server back again. If the problem occurs again then repeat the proceeding steps.
CSCtr19389	Database server does not start after failover. **Symptom**: On the Secondary server when NCS is active the "ncs status" command will display the database server as stopped. **Conditions**: Failover from Primary NCS server to Secondary NCS server. NCS is active on the server and started successfully. From the command line run the "ncs status" command. **Workaround**: Log into the web interface of NCS. If this is successful then the database is running and the message can be ignored.
CSCtr04897	SPT switches information not visible after upgrade. **Symptom**: For Switches upgraded from WCS 7.x will not have model name, description, software version, and so on in the Inventory Reports and the reachability status is missing as well. Inventory reports does not show all the information for SPT switches. Shows only "Device Name and IP Address". It has to show all other information like: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.
CSCtr05965	'Logged in Guest User' Dashlet do not show all guest clients sometimes. **Symptom**: Logged in Guest Dashlet does not show the Apple client information. **Conditions**: This affects version 1.0 of the Cisco Prime Network Control System. **Workaround**: The Monitor client list shows the client successfully.

Table 6 Open Caveats (continued)

ID Number	Caveat Title
CSCtr08968	Running Profiles on disassociated CCXv5Client leads to Unknown exception. **Symptom**: Running profiles on disassociated CCXv5 clients leads to Unknown Exception in NCS. **Conditions**: Profile information not available for CCXv5 client in a disassociated state. The application is not presenting a meaningful error message to the end user. **Workaround**: There is no workaround for this issue. Users can retrieve profile information for associated clients. Since the application go to the WLC directly to fetch this information, the data cannot be viewed for disassociated clients.
CSCtr09038	Failure in migration certain models of Autonomous AP. **Symptom**: While migrating certain models of Autonomous AP, the migration process fails in the step 'Copying environmental variables'. **Conditions**: This scenario is faced when trying the conversion on high latency networks. **Workaround**: None. Trying multiple times sometimes results in successful migration.
CSCtr09048	NCS displays error message if the ACL has 64 ACL rules. **Symptom**: When you create an ACL template with 64 rules and try to apply to the controller. NCS shows an error that the ACL has maximum limit. **Conditions**: While creating a rule, configure DSCP value as any, and apply to the controller. For example, Go to configuration page of applied ACL, select DSCP value as specified. NCS shows 256, but the value range is between 0 to 63. If you check on controller, it shows specified value and default as 0. **Workaround**: None.
CSCtq88498	Only English characters are supported. **Symptom**: Non-English characters in NCS, do not display correctly, and appear corrupted and is un-readable. **Conditions**: If you use non-English characters in NCS, the text appears to be corrupted and may impact network configuration if changes with such characters are pushed to the network. Additionally, when migrating from Wireless Control System to Network Control System, existing non-English characters will get corrupted. If the devices managed by NCS have non-English characters in the configuration, when the inventory tasks collect these data and stores in NCS database, these characters will be corrupted. **Workaround**: Use English characters with NCS. Customers with non-English keyboards may also use English keyboard layouts.

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. Click this 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 at the following location: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 Cisco Network, see the *Cisco Network Control System Configuration Guide* and the *Cisco Wireless LAN Controller Configuration Guide.*

Table 7 provides a list of the documentation for Cisco Prime Network Control System 1.0.

Table 7 NCS Documentation List

Documentation Title	URL
Cisco Prime Network Control System Configuration Guide, Release 1.0	http://www.cisco.com/en/US/docs/wireless/ncs/1.0/configuration/guide/NCS10cg.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.