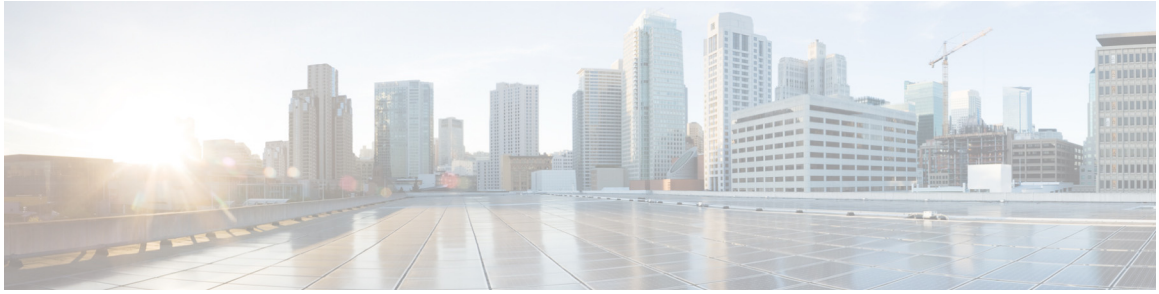

Release Notes for Cisco Prime Network Control System, Release 1.1.3.2

First Published: February, 2013

OL-27687-01

These release notes describe the requirements, features, limitations, restrictions (caveats), and related information for the Cisco Prime Network Control System (NCS) Release 1.1.3.2, 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 1.1.3.2 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 1250 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 1.1.3.2 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 in 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 12.0 or Internet Explorer 8 with the Chrome plugin releases or Google Chrome 18.0.1025.168 m. 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 Wireless Controller on Service Ready Engine (WLCM2 on SRE)	Cisco MSE 3300 Series	Cisco ISE 3300 Series	Cisco 600 Series, Cisco 1040 AP, Cisco 1100 AP, Cisco 1120 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 802 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

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 1.1.3.2	7.2.110.0 7.2.103.0, 7.1.91.0, 7.0.235.0 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	7.2.110.0 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	IOS12.4(25e)JA 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

Installing NCS Software

The following steps summarize how to install new NCS 1.1.3.2 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-1.1.1.X-large/small/medium.ova) and deploy the OVA template.

Note For more information about small, medium, and large deployments, see the following URL: http://www.cisco.com/en/US/docs/wireless/ncs/1.1/configuration/guide/wst.html#wp1379032

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.
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 VUDI is created using the product name, hostname, and serial number. 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.

Note To see the VUDI information, choose **Help > About NCS**.

For more detailed information on license types and obtaining licenses for NCS, see the following URL:

http://www.cisco.com/en/US/docs/wireless/ncs/1.1/configuration/guide/warr.html

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 1.1

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 1.1.3.2.

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:

- Migrating WCS User Data to NCS 1.1 (for Multiple WCS Servers), page 12

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 all/userdata** CLI command is available in WCS Release 7.x and later, which creates the .zip file containing the individual data file.

To export the WCS data, follow these steps:

Step 1 Stop the WCS server.

Step 2 Enter the following command (for Windows) through the script file and provide the path and export filename.

`export.bat all` *`zipfile`*.

all	Exports all WCS data including the entire database, saved reports (if -noreports is not specified), map images, license files, mobility services engine backups, location server backups, accuracy test files, and controller auto provisioning files.
zip file	Full pathname of the compressed .zip file to create.

Note Run this command in the location where the WCS is installed. For example, <Installation Dir>\WCS7.0.x.x\bin (for Windows) or <Installation Dir>/WCS7.0.x.x/bin (for Linux).

Example output

```
C:\Program Files\WCS7.0.230.0\bin>export.bat all c:\testdb
Starting database server ...
Database server is running.
Starting data export.
Creating export configuration files.
Creating database configuration files.
Exporting database data, size = 388.4 MB.
Exported 3% of database.
Exported 7% of database.
Exported 10% of database.
Exported 14% of database.
Exported 18% of database.
Exported 21% of database.
Exported 25% of database.
Exported 29% of database.
Exported 32% of database.
Exported 36% of database.
Exported 40% of database.
```

```
Exported 43% of database.
Exported 47% of database.
Exported 51% of database.
Exported 54% of database.
Exported 58% of database.
Exported 61% of database.
Exported 65% of database.
Exported 69% of database.
Exported 72% of database.
Exported 76% of database.
Exported 80% of database.
Exported 83% of database.
Exported 87% of database.
Exported 91% of database.
Exported 94% of database.
Exported 98% of database.
Completed exporting database data.
Exporting reports, map images, accuracy test files,
          controller auto provisioning files.
Exporting Mobility Service Engine, Location Server backups.
Creating ChecksumFile.
Creating compressed export file.
Shutting down database server ...
Database server successfully shutdown.
Data export completed successfully.
```

Note For Linux, enter the **`export.sh all`** *`zipfile`* command. That is, navigate to the bin directory and enter the ./export.sh all /data/wcs.zip. Run this command from the location where WCS is installed. For example, `#opt/WCS7.0.230.0/bin>`. For an example output, see "Example output" section on page 9.

Migrating WCS Data to NCS

To migrate the 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, the WCS events are not migrated.

The following example shows a sample output.

```
ncs-appliance/admin# ncs migrate wcs-data wcs1.zip repository defaultRepo
Initiating WCS 7x DB restore .  Please wait...
INFO: no staging url defined, using local space.        rval:2
Starting Network Control System...

This may take a few minutes...

Network Control System started successfully.

Stopping Network Control System...

This may take a few minutes...

Network Control System successfully shutdown.

  Stage 1 of 5: Decompressing backup ...
  -- complete.
  Stage 2 of 5: Restoring Support Files ...
              : Restoring the Domain Maps ...
              :  -- complete.
              : Restoring the Report files ...
              :  -- complete.
              : Restoring the License files ...
              :  -- complete.
  -- complete.
  Stage 3 of 5: Restoring Data ...
  -- complete.
  Stage 4 of 5: Updating Database Schema ...
              : This could take long time based on the backup size.
  -- complete.
  Stage 5 of 5: Re-enabling Database Settings ...
  -- complete.
```

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 that 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 1.1.3.2. 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.

Migrating WCS User Data to NCS 1.1 (for Multiple WCS Servers)

When you migrate multiple WCS servers to the NCS, follow these steps:

Step 1 Stop the WCS server.

Step 2 Export data from the WCS server which is running the most critical data. To do this, follow the steps in the "Exporting WCS Data" section on page 9.

Step 3 Export the user data from remaining WCS servers using the following command (for Windows):

```
export.bat userdata zipfile
```

userdata	Exports only user-created data in the database, saved reports (if -noreports is not specified), map images, license files, mobility services engine backups, location server backups, accuracy test files, controller auto provisioning files. **Note** Export userdata is supported only by WCS Release 7.0.172.0 and later.
zip file	Full pathname of the compressed .zip file to create.

Note You need to transfer the exported userdata .zip file from the WCS server to the NCS server.

Note For the remaining WCS servers, except the managed devices and maps, no other userdata (such as config templates, reports, users, virtual-domains, and so on) will not be imported. Also, all network-related data (such as events, alarms, statistics, clients, switches, and so on) will not be imported.

Example output

```
C:\Program Files\WCS7.0.230.0\bin>export.bat userdata c:\jmr3_exportdata
Starting database server ...
Database server is running.
Starting data export.
Initializing PersistenceService. This may take a minute.
PersistenceService initialized. Performing export user data.

Reading file: conf\userDataExportRules\ConfigTemplateExportRules.xml (1/6)
Exporting user data related db tables under group: SECURITY_TEMPLATE_GROUP
Exporting user data related db tables under group: EAP_TEMPLATE_GROUP
Exporting user data related db tables under group: HREAP_TEMPLATE_GROUP
Exporting user data related db tables under group: CLIENT_TEMPLATE_GROUP
Exporting user data related db tables under group: ROGUE_TEMPLATE_GROUP
Exporting user data related db tables under group: CONTROLLER_TEMPLATE_GROUP
Exporting user data related db tables under group: SERVER_TEMPLATE_GROUP
Exporting user data related db tables under group: RADIO_TEMPLATE_GROUP
Exporting user data related db tables under group: MSE_TEMPLATE_GROUP
Exporting user data related db tables under group: LRAD_GENERAL_TEMPLATE_GROUP
Exporting user data related db tables under group: POLICY_TEMPLATE_GROUP
Exporting user data related db tables under group: SNMPANDSYSLOG_TEMPLATE_GROUP
Exporting user data related db tables under group: ACL_TEMPLATE_GROUP
Exporting user data related db tables under group: APGROUP_TEMPLATE_GROUP
Exporting user data related db tables under group: LRAD_TEMPLATE_GROUP
Exporting user data related db tables under group: WLAN_TEMPLATE_GROUP
Exporting user data related db tables under group: CONFIGGROUP_TEMPLATE_GROUP
Exporting user data related db tables under group: MSE_EVENT_GROUP
Exporting user data related db tables under group: SCHEDULER_GROUP

Reading file: conf\userDataExportRules\DeviceExportRules.xml (2/6)
Exporting user data related db tables under group: DEVICE_GROUP
Exporting user data related db tables under group: CREDENTIAL_GROUP
Exporting user data related db tables under group: SCHEDULER_GROUP
Exporting user data related db tables under group: PARTITION_ASSOCIATION_GROUP

Reading file: conf\userDataExportRules\MapExportRules.xml (3/6)
Exporting user data related db tables under group: MAP_GROUP

Reading file: conf\userDataExportRules\ReportExportRules.xml (4/6)
Exporting user data related db tables under group: REPORT_SETTINGS_GROUP
Exporting user data related db tables under group: SCHEDULER_GROUP

Reading file: conf\userDataExportRules\UserExportRules.xml (5/6)
Exporting user data related db tables under group: TEMPUSER_GROUP
Exporting user data related db tables under group: DASHBOARD_GROUP
Exporting user data related db tables under group: SEARCH_GROUP

Reading file: conf\userDataExportRules\VirtualDomainExportRules.xml (6/6)
Exporting user data related db tables under group: PARTITION_GROUP

Exporting map data.
Completed export of user data related db tables.
Exporting reports, map images, accuracy test files,
          controller auto provisioning files.
Exporting Mobility Service Engine, Location Server backups.
Creating ChecksumFile.
Creating compressed export file.
Shutting down database server ...
Database server successfully shutdown.
Data export completed successfully.
```

Step 4 Do the following:

a. To import all the device data from the managed controllers into the NCS (as root user in ROOT-DOMAIN), choose **Configure > Controllers > Add Controllers**, choose **Zip File** from the Add Format Type drop-down list, enter the .zip filename, and then click **Add**.

b. To import all the device data from the managed autonomous APs into the NCS, choose **Configure > Access Points > Add Autonomous Access Points**, choose **Zip File** from the Add Format Type drop-down list, enter the .zip filename, and then click **Add**.

After you add devices, the NCS pulls all inventory/configuration data from the respective devices.

After you add devices, you can export map data from the WCS (choose **Monitor > Maps > Export Map**) and import it into the NCS (**Monitor > Maps > Import Map**).

Upgrading NCS 1.1 to NCS 1.1.3.2

You can upgrade from NCS Releases 1.1.0.58, 1.1.1.24, and 1.1.2.12 to NCS 1.1.3.2. You cannot upgrade NCS Release 1.1.3.2 to Cisco Prime Infrastructure 1.2.

Please download and use NCS 1.1.3.2 only if you are required to run FIPS-certified version of NCS.

Once you install NCS 1.1.3.2 , you will not be able to upgrade to the standard releases such as Cisco Prime Infrastrucgture 1.2.1 or Cisco Prime Infrastrucgture 1.3. Please contact TAC if you have unintentionally downloaded and upgraded to NCS1.1.3.2 or 1.1.2.12. Also, read the following software advisory for more information on how to upgrade.

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.3/software/advisory/Software_Advisory_CPI_1_1_2_and_1_1_3.pdf

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 1.1 to NCS 1.1.3.2:

```
# application upgrade NCS-upgrade-bundle-1.1.3.2.tar.gz ncs-ftp-repo
```

In the preceding command, NCS-upgrade-bundle-1.1.3.2.tar.gz is the upgrade bundle file, which is available for download.

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

Examples of repository configurations follow.

FTP Repository:

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

What's New in This Release?

This is a "Security Hardened" release which is only for customers needing Federal Information Processing Standard (FIPS) compliant software.

Important Notes

This section describes important information about NCS.

This section contains the following topics:

Physical and Virtual Appliance

The 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

The 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 the 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 the 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 that 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 the 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 the 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.

  Note The /opt partition contains the application and the database. There is no estimate of how much space is used by the database. The space occupied by the database depends on the on the data size.

  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

Note All statistics data is part of the data retention period. Statistics data contains only number which can be aggregated such as CPU utilizations, client counts, and so on. All data associated with timestamp is either aggregated data or historical data. Aggregated data consists with numbers that can be aggregated as minimum, maximum, average, and sum. Historical data consists with other information (may also include numbers) that cannot be computed, such as client association history, alarms and events. The reports showing as charts usually are using aggregated data. For example, client count, device utilizations, and so on.

The settings decide how long the NCS retains the aggregated data. The 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.

RADIUS Server Authentication

During the RADIUS Server request and response cycles, the packets size cannot exceed 4096 characters, per IETF RFCs for RADIUS. Because of this reason, the attribute list sent from the RADIUS server may not contain all tasks in the authorization info for user.

Client Association With an 802.11r-enabled WLAN

Legacy clients may not associate with a WLAN which has both 802.11i and 802.11r AKMs enabled. The driver of the supplicant who parses the Robust Security Network Information Element (RSNIE) will be old and hence it will be unaware of the additional AKM suites in the RSNIE. Because of this limitation in the client, it does not send the association request. These clients can associate only with a non-802.11r WLAN.

However, an 802.11r-capable client can associate as an 802.11i client on a WLAN which has both 802.11i and 802.11r Authentication and Key Management (AKM) suites enabled. If the driver of the legacy client is made to understand the new 802.11r AKM, it can send the association request and successfully associate with the previously mentioned WLAN.

Caveats

This section lists open and resolved caveats in the NCS Release 1.1.3.2. 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 20
- Resolved Caveats, page 21

Open Caveats

Table 6 lists the open caveats in NCS Release 1.1.3.2.

Click the identifier to view the impact and workaround for the caveat. This information is displayed in the Bug Toolkit. You can track the status of the open caveats using the Bug Toolkit.

Table 6 Open Caveats

Identifier	Description
CSCtx58026	HA Secondary needs to be able to run a backup and restore to primary
CSCua77597	Discrepancy in TX and RX data from client session report
CSCuc34416	Severity configuration does not prune northbound traps
CSCuc09499	NCS admin user - Permission denied for the MSE Northbound Notifications page
CSCuc06992	Lightweight AP template has country code for Croatia (HR) missing
CSCub91535	During a template push, random exceptions seen from UI on MSE environments
CSCuc13646	NCS Client traffic report Each Floor value & Sum of AP By Floor not same
CSCub61852	NCS reports incorrect MFP validation state for Access points
CSCuc35382	Lost FlexConnect VLAN-Mapping AP Template if not shown in GUI
CSCub56151	Modifying the AP config from static to DHCP Ip address assignment (or vice-versa) via NCS results in the AP coming back with both radios in admin-disable state.
CSCuc78802	Autonomous AP image FTP download by NCS fails due to blank FTP password
CSCud04086	Configuring AP Fast Heartbeat causes Audit Mismatch status
CSCtx66256	Traps and syslogs do not update switch interfaces status
CSCua45993	Issue discovering Cisco 4500 switches
CSCty91309	NCS Backup fails if FTP server password is more than 16 characters
CSCtz37295	Alarm summary panel displays an error for lobby ambassador login
CSCtz44678	decap process will not let NCS start
CSCtz56558	The Lobby Ambassador user gets to the NCS home page by hitting the browser's back button
CSCtz73268	The gain on the NCS and AP are different for 2600i APs for a/n radio
CSCtr93985	Image import from ASR device is not working for size more than 64 MB.
CSCtz43856	Image recommendation is not working for Nexus devices.
CSCtz52220	Single Sign Out is not Working
CSCub95698	WCS apply AP Group template to WLC with random order
CSCuc51508	Client association history in NCS reports incorrect time
CSCud59962	NCS status shows incorrect on CLI after Failback

Resolved Caveats

None.

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 7 provides a list of the documentation for the NCS 1.1.3.2.

Table 7 The 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 1.1	http://www.cisco.com/en/US/docs/wireless/ncs/1.1/command/reference/cli11.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:

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

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

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