CHAPTER 4

Performing Maintenance Operations

You can perform the actions at the system level, such as updating system softwares or downloading certificates that can be used with many items.

This chapter describes the system level tasks to perform with Cisco NCS. It contains the following sections:

Information About Maintenance Operations

A system-level task is a collection of tasks that relate to operations that apply to the NCS database as a whole. System tasks also include restoring the NCS database. For more information, see the "Restoring the NCS Database" section on page 4-8.

Performing System Tasks

This sections describes how to use the NCS to perform system-level tasks. This section contains the following topics:

Adding a Controller to the NCS Database

To add a controller to the NCS database, follow these steps:

Note We recommend that you manage controllers through the controller dedicated service port for improved security. However, when you manage controllers that do not have a service port (such as 2000 series controllers) or for which the service port is disabled, you must manage those controllers through the controller management interface.

Step 1 Log into the NCS user interface.

Step 2 Choose **Configure > Controllers** to display the All Controllers page.

Step 3 From the Select a command drop-down list, choose **Add Controller**, and click **Go**.

Step 4 In the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.

Step 5 Click **OK**. The NCS displays a Please Wait dialog box while it contacts the controller and adds the current controller configuration to the NCS database. It then returns you to the Add Controller page.

Step 6 If the NCS does not find a controller at the IP address that you entered for the controller, the Discovery Status dialog displays this message:

```
No response from device, check SNMP.
```

Check these settings to correct the problem:

- The controller service port IP address might be set incorrectly. Check the service port setting on the controller.
- The NCS might not have been able to contact the controller. Make sure that you can ping the controller from the NCS server.
- The SNMP settings on the controller might not match the SNMP settings that you entered in the NCS. Make sure that the SNMP settings configured on the controller match the settings that you entered in the NCS.

Step 7 Add additional controllers if desired.

Using the NCS to Update System Software

To update controller (and access point) software using the NCS, follow these steps:

Step 1 Enter the **ping** *ip-address* command to be sure that the NCS server can contact the controller. If you use an external TFTP server, enter the **ping** *ip-address* command to be sure that the NCS server can contact the TFTP server.

Note When you are downloading through a controller distribution system (DS) network port, the TFTP server can be on the same or a different subnet because the DS port is routable.

Step 2 Choose **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Select the check box of the desired controller, choose **Download Software (TFTP or FTP)** from the Select a command drop-down list, and click **Go**. The NCS displays the Download Software to Controller page.

Step 4 If you use the built-in NCS TFTP server, choose **Default Server** from the Server Name drop-down list box. If you use an external TFTP server, choose **New** from the Server Name drop-down list box and add the external TFTP server IP address.

Step 5 Enter the file path and server file name in their respective text boxes (for example, AS_2000_*release*.aes for 2000 series controllers). The files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory.

Note Be sure that you have the correct software file for your controller.

Step 6 Click **Download**. The NCS downloads the software to the controller, and the controller writes the code to flash RAM. As the NCS performs this function, it displays its progress in the Status field.

Downloading Vendor Device Certificates

Each wireless device (controller, access point, and client) has its own device certificates. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

To download a vendor-specific device certificate to the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificates in one of two ways:

a. Select the check box of the controller you choose.

b. Choose **Download Vendor Device Certificate** from the Select a command drop-down list, and click **Go**.

or

a. Click the URL of the desired controller in the IP Address column.

b. Choose **System > Commands** from the left sidebar menu.

c. Choose **TFTP** or **FTP** in the Upload/Download Command section.

d. Choose **Download Vendor Device Certificate** from the Upload/Download Commands drop-down list, and click **Go**.

Step 3 In the Certificate Password text box, enter the password which was used to protect the certificate.

Step 4 Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name field. If the certificate is on the local machine, you must specify the file path in the Local File Name field using the **Choose File** button.

Step 5 Enter the TFTP server name in the Server Name field. The default is for the NCS server to act as the TFTP server.

Step 6 Enter the server IP address.

Step 7 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 8 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 9 In the Local File Name text box, enter the directory path of the certificate.

Step 10 Click **OK**.

Downloading Vendor CA Certificates

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller. To download vendor CA certificate to the controller, follow the instructions:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificates in one of two ways:

a. Select the check box of the controller you choose.

b. Choose **Download Vendor CA Certificate** from the Select a command drop-down list, and click **Go**.

or

a. Click the URL of the desired controller in the IP Address column.

b. Choose **System > Commands** from the left sidebar menu.

c. Choose **Download Vendor CA Certificate** from the Upload/Download Commands drop-down list, and click **Go**.

Step 3 Specify if the certificate to download is on the TFTP server or on the local machine. If it is on the TFTP server, the name must be supplied in the Server File Name field in Step 9. If the certificate is on the local machine, you must specify the file path in the Local File Name field in Step 8 using the Browse button.

Step 4 Enter the TFTP server name in the Server Name field. The default is for the NCS server to act as the TFTP server.

Step 5 Enter the server IP address.

Step 6 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 7 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 8 In the Local File Name text box, enter the directory path of the certificate.

Step 9 Click **OK**.

Using the NCS to Enable Long Preambles for SpectraLink NetLink Phones

A radio preamble (sometimes called a *header*) is a section of data at the head of a packet. It contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

To optimize the operation of SpectraLink NetLink phones on your wireless LAN, to use the NCS to enable long preambles, follow these steps:

Step 1 Log into the NCS user interface.

Step 2 Choose **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Click the IP address of the desired controller.

Step 4 From the left sidebar menu, choose **802.11b/g/n > Parameters**.

Step 5 If the *IP Address* > 802.11b/g/n Parameters page shows that short preambles are enabled, continue to the next step. However, if short preambles are disabled, which means that long preambles are enabled, the controller is already optimized for SpectraLink NetLink phones, and you do not need to continue this procedure.

Step 6 Enable long preambles by unselecting the **Short Preamble** check box.

Step 7 Click **Save** to update the controller configuration.

Step 8 To save the controller configuration, choose **System > Commands** from the left sidebar menu, choose **Save Config To Flash** from the Administrative Commands drop-down list, and click **Go**.

Step 9 To reboot the controller, choose **Reboot** from the Administrative Commands drop-down list and click **Go**.

Step 10 Click **OK** when the following message appears.

```
Please save configuration by clicking "Save Config to flash". Do you want to continue
rebooting anyways?
```

The controller reboots. This process might take some time, during which the NCS loses its connection to the controller.

Note You can view the controller reboot process with a command-line interface session.

Creating an RF Calibration Model

If you would like to further refine the NCS Location tracking of client and rogue access points across one or more floors of a building, you have the option of creating an RF calibration model that uses physically collected RF measurements to fine-tune the location algorithm. When you have multiple floors in a building with the same physical layout as the calibrated floor, you can save time calibrating the remaining floors by using the same RF calibration model for the remaining floors.

The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This allows the Cisco Unified Wireless Network Solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure and save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

Performing the NCS Operations

This section contains the following topics:

Verifying the Status of the NCS

This section provides instructions for checking the status of the NCS. To check the status of the NCS. You can check the status at any time, follow these steps:

Step 1 Log into the system as admin.

Step 2 Using the CARS command-line interface, enter the **NCS status** command.

The command-line interface displays messages indicating the status of the NCS.

Stopping the NCS

This section provides instructions for stopping the NCS. You can stop the NCS at any time. To stop the NCS, follow these steps:

Note If any users are logged in when you stop the NCS, their NCS sessions stop functioning.

Step 1 Log into the system as admin.

Note To see which version of NCS you currently have installed, enter **show application version NCS**.

Step 2 Using the CARS command-line interface, enter the **NCS stop** command.

The command-line interface displays messages indicating that NCS is stopping.

Backing Up the NCS Database

This section provides instructions for backing up the NCS database. You can schedule regular backups through the NCS user interface or manually initiate a backup. The following files are backed up using, both the NCS user interface and command-line interface:

- Oracle database
- Maps
- Report files
- Accuracy files used for generating reports
- USERMGT file

The device configurations are obtained from the devices in the back up files.

Note Machine specific settings (such as FTP enable and disable, FTP port, FTP root directory, TFTP enable and disable, TFTP port, TFTP root directory, HTTP forward enable and disable, HTTP port, HTTPS port, report repository directory, and all high availability settings) are not included in the backup and restore function if the backup is restored to a different device.

This section contains the following topics:

- Scheduling Automatic Backups, page 4-7
- Performing a Manual Backup, page 4-8

Scheduling Automatic Backups

To schedule automatic backups of the NCS database, follow these steps:

Step 1 Log into the NCS user interface.

Step 2 Choose **Administration > Background Tasks** to display the Scheduled Tasks page.

Step 3 Click the **NCS Server Backup** task to display the NCS Server Backup page.

Step 4 Select the **Enabled** check box.

Step 5 At the Backup Repository field, Choose an existing backup repository, or click **Create** to create a new repository.

Step 6 If you are backing up in remote location, select the **FTP Repository** check box. You need to enter the FTP location, username, and password of the remote machine.

Step 7 In the Interval (Days) text box, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 8 In the Time of Day text box, enter the time when you want the backup to start. It must be in this format: *hh*:*mm* AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the NCS server. Therefore, we recommend that you schedule backups to run when the NCS server is idle (for example, in the middle of the night).

Step 9 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/admin/NCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Performing a Manual Backup

To back up the NCS database, follow these steps:

Note You do not need to shut down Oracle or the platform to perform a backup.

Step 1 Log into the system as admin.

Step 2 Create a local or remote backup directory for the NCS database with no spaces in the name (for example, mkdir NCS1.0.X.X_Backup).

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Note If it is a remote backup location, you MUST specify the correct FTP location (For example, ftp://hostname/location) and user credentials.

Step 3 You can perform a backup using the command-line interface.

Step 4 Run either of these commands to perform a manual backup:

- Back up the appliance and application to the repository (local or remote) by entering the following command:

  backup *testbackup* repository *backup_repo*

- Back up the application only to the repository (local or remote) by entering the following command:

  backup *testbackup* repository *backup_repo* application *NCS*

The command-line interface displays messages indicating the status of the backup.

Restoring the NCS Database

This section provides instructions for restoring the NCS database. This section contains the following topics:

Restoring the NCS Database

If you are restoring the NCS database in a high availability environment, see the "Restoring the NCS Database in a High Availability Environment" section on page 4-9. To restore the NCS database from a backup file. follow these steps:

Step 1 To view all local repository backups, enter the following command:

```
show repository backup_repo
```

Note If possible, stop all the NCS user interfaces to stabilize the database.

Step 2 Manually shut down the platform.

Step 3 Using the command-line interface, perform one of the following:

- Restore the appliance and application backup by entering the following command:

  restore testbackup-yymmdd-xxxx.tar.gpg repository backup_repo

- Restore only the application backup by entering the following command:

  restore testbackup-yymmdd-xxxx.tar.gpg repository backup_repo application NCS

Step 4 Click **Yes** if a message appears indicating that the NCS is running and needs to be shut down.

Note If the restore process shuts down the NCS, a restart is attempted after a successful restore. The appliance then restarts and you have to again login and restart the dbserver and the platform manually as admin (make sure you do not start with dbclean, else you lose your recently restored data).

The command-line interface displays messages indicating that the NCS database is being restored.

Restoring the NCS Database in a High Availability Environment

During installation, you were prompted to determine if a secondary NCS server would be used for high availability support to the primary NCS server. If you opted for this high availability environment and enabled it in the Administration > High Availability page, the status appears as HA enabled. Before restoring a database, you must convert the status to HA not configured.

Note If you attempt to restore the database while the status is set to HA enabled, unexpected results might occur.

To change the status from HA enabled to HA not configured, follow one of these procedures:

- Click the **Remove** button in the HA Configuration page (Administration > High Availability).

- Restart the primary server. Go to the secondary HealthMonitor graphical user interface (https://<SecondaryNCS>:8082), and click **Failback**.
  - Use this method when one of the following instances has occurred:

    The primary server is down and failover has not been executed, so then the secondary server is in SecondaryLostPrimary state.

    or

    The primary server is down and failover has already executed, so then the secondary server is in the SecondaryActive state.

The primary server is now in HA Not Configured mode, and you can safely restore the database.

Uninstalling NCS

This section provides instructions for uninstalling the NCS. You can uninstall the NCS at any time, even while the NCS is running.

To uninstall the NCS, follow these steps:

Step 1 Stop the NCS.

Step 2 Log into the system as admin.

Step 3 Using the CARS command-line interface, enter the **application remove NCS** command.

Step 4 Click **Yes** to continue the uninstall process.

Upgrading WCS to NCS

This section provides instructions for upgrading to the NCS. If you are upgrading to the NCS in a high availability environment, see the "Upgrading the NCS in a High Availability Environment" section on page 4-11.

Note The NCS supports data migration in the WCS Releases 7.0.164.3, 7.0.172.0, and 7.0.220.0. If you do not have either release of the WCS, you must upgrade to either the WCS 7.0.164.3 or 7.0.172.0 or 7.0.220.0 first and then follow the migration steps.

To Upgrade from the WCS to the NCS, perform the following:

Step 1 Stop the WCS server.

Step 2 Enter the export command to export all the WCS data in to a export file. For Linux, enter the **export.sh all** command and for windows enter the **export.bat all** command.

Note While upgrading from the WCS to the NCS, on running the export command, you might encounter a "could not reserve enough space" error. If you encounter this error then access either the export.bat (for Windows OS) or export.sh (for Linux OS) file and replace the instance of -Xmx1024m with -Xmx512m.

Step 3 Copy the export .zip file (for example, wcs.zip) in to a local repository folder.

Step 4 Log in to the NCS as admin and stop the NCS server using the **NCS stop** command.

Step 5 Configure the repository in the NCS appliance using the repository command:

```
ncs-appliance/admin# configure
ncs-appliance/admin(config)# repository wcs-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 wcs.zip is listed for the **show repository repositoryname** command. For tftp, if directory listing is not enabled, then restore fails. This is an expected behavior and the **show repository** command produces an error message.

```
ncs-appliance/admin# show repository wcs-ftp-repo
wcs.zip
ncs-appliance/admin# show repository wcs-tftp-repo
% Protocol does not support listing directories
```

Step 6 Enter the **NCS migrate** command to restore the WCS database.

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

Using the noclientstats option, no client count and client statistics data are migrated to the NCS. By default no WCS events are migrated.

Step 7 Run the **NCS start** command to start the NCS server after the upgrade is completed.

Step 8 Login to the NCS User Interface using the admin and the admin password.

Note The client count, client summary, client throughput, client traffic, rogue AP, adhoc rogues, new adhoc rogues, PCI details, PCI summary and security summary reports, dashboard customizations, client station information and its statistics, all WCS events, RADIUS/TACACS server IP and credentials, and the admin password are not migrated from the WCS to the NCS. Make sure you enable the RADIUS/TACACS server as AAA mode in **Administration > AAA > AAA Mode Settings** page and click **Save**.

Upgrading the NCS in a High Availability Environment

If you have a primary and secondary NCS, follow these steps for a successful upgrade:

Step 1 You must first remove the HA configuration with the following steps:

a. Log in to the primary NCS server.

b. Choose **Administration > High Availability**, and choose HA Configuration from the left sidebar menu.

c. Click **Remove** to remove the HA configuration.

Note It might take a few minutes for the remove to complete.

Step 2 You must first upgrade the secondary NCS with the following steps:

a. Shut down the secondary NCS. See the "Stopping the NCS" section on page 4-6 for more information.

Note You can use **NCS stop** for a graceful shut down. A graceful shut down does not trigger the automatic failover.

b. Perform an upgrade on the secondary NCS.

c. Start the secondary NCS.

Note It attempts to reconnect to the primary NCS, but a version mismatch error is returned.

Step 3 Upgrade the primary NCS.

a. Shut down the primary NCS. See the "Stopping the NCS" section on page 4-6 for more information.

b. Perform an upgrade on the primary NCS.

c. Start the primary NCS.

Step 4 Enable HA again on the primary NCS.

a. Login to the primary NCS server.

b. Choose Administration > High Availability and select HA Configuration from the left sidebar menu.

c. Enter the HA configuration settings and click **Save** to enable high availability.

Upgrading the Network

Network upgrades must follow a recommended procedure so that databases can remain synchronized with each other. For example, You cannot upgrade the controller portion of the network to a newer release but maintain the current NCS version and not upgrade it. The supported order of upgrade is NCS first, followed by the controller, and then any additional devices.

Reinitializing the Database

If you need to reset the database because of a synchronization problem or a corruption of some type, enter **NCS db reinitdb** to reinitialize the database.

Recovering the NCS Password

You can change the NCS application root user or FTP user password. This option provides a safeguard if you lose the root password. An executable was added to the installer /bin directory (passwd.bat for Windows and passwd.sh for Linux). For password recovery on a wireless location device, refer to Chapters 8 or 9 of the *Cisco 2700 Series Location Appliance Configuration Guide*. To recover the passwords and regain access to NCS, follow these steps:

Note If you are a Linux user, you must be the root user to run the command.

Note In Linux, use the ***passwd.sh*** to change the NCS password. The ***passwd*** is a built-in Linux command to change the OS password.

Step 1 Log in to the NCS command-line interface as an admin user.

Step 2 Run the following command:

ncs password root password *password*

Where *password* is the root user login password. You can enter a password not exceeding 80 characters.

Example of the command usage:

```
ncs-appliance/admin# ncs password root password ?

<WORD>  Type in root user login password (Max Size - 80)
```

You should now be able to login to NCS web interface with the new root password.