CHAPTER 17

Tools

The Tools menu provides access to the Voice Audit, Location Accuracy Tool, Configuration Audit Summary, and Migration Analysis features of the Cisco NCS. This chapter contains the following sections:

Running Voice Audits

The NCS provides voice auditing mechanism to check the controller configuration and to ensure that any deviations from the deployment guidelines are highlighted as an Audit Violation.

To access the Voice Audit feature, choose **Tools > Voice Audit**. The Voice Audit Report page appears.

This page contains three tabs: Controllers, Rules, and Reports.

- The Controllers tab allows you to choose the controller(s) on which to run the voice audit.
- The Rules tab allows you to indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.
- The Report tab provides a summary of the voice audit details and report results.

To access the Voice Audit feature, choose **Tools > Voice Audit**.

This section contains the following topics:

Running Voice Audits on Controllers

The Controllers tab allows you to choose the controller(s) on which to run the voice audit.

Note You can run the voice audit on a maximum of 50 controllers in a single operation.

To select the controller(s) for the voice audit, follow these steps:

Step 1 Choose **Tools > Voice Audit**.

Step 2 Click the **Controllers** tab.

Step 3 From the Run audit on drop-down list, choose **All Controllers**, **A Floor Area**, or **A Single Controller**.

- All Controllers—No additional Controller information is necessary.
- A Floor Area—From the drop-down lists, choose the applicable campus, building, floor, and controller.
- A Single Controller—Choose the applicable controller from the drop-down list.

Step 4 Click the **Rules** tab to determine the rules for this voice audit. See the "Choosing Voice Audit Rules" section on page 17-2 for more information.

Choosing Voice Audit Rules

The Rules tab allows you to indicate the applicable VoWLAN SSID and the applicable rules for this voice audit.

To indicate the rules for the voice audit, follow these steps:

Step 1 In the Tools > Voice Audit page, click the **Rules** tab.

Step 2 Type the applicable VoWLAN SSID in the **VoWLAN SSID** text box.

Step 3 From the **Rules List**, select the check boxes of the applicable rules for this voice audit (see Table 17-1).

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Table 17-1 Rules List for Voice Audit

Rule	Rule Details
VoWLAN SSID	Description—Checks whether or not the VoWLAN SSID exists. Rule validity—User-defined VoWLAN SSID.
CAC: 7920	Description—Checks whether or not 7920 AP CAC is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CAC: 7920 Clients	Description—Checks whether or not the 7920 Client CAC is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.

Table 17-1 Rules List for Voice Audit (continued)

Rule	Rule Details
DHCP Assignment	Description—Checks whether or not DHCP assignment is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
MFP Client	Description—Checks whether or not MFP Client protection is not set to **Required** for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Platinum QoS	Description—Checks whether or not QoS is set to Platinum (Voice) for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Non Platinum QoS	Description—Checks that QoS is not set to Platinum for non-VoWLAN. Rule validity—User-defined VoWLAN SSID.
WMM	Description—Checks whether or not WMM is enabled for VoWLAN. Rule data—Choose **Allowed** or **Required** from the drop-down list. Rule validity—User-defined VoWLAN SSID.
CCKM	Description—Checks whether or not CCKM is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CCKM With No AES- for 792x phones	Description—Check that AES encryption is not enabled with Cisco Centralized Key Management (CCKM) for VoWLAN. This rule is only for 792x phones. Rule validity—User-defined VoWLAN SSID.
TSM	Description—Check that Traffic Stream Metrics (TSM) is Enabled. Rule data—Choose **802.11a/n TSM**, **802.11b/g/n TSM**, or both check boxes. Rule validity—At least one band must be selected.
DFS	Description—Checks whether the Channel Announcement and Channel Quite Mode are Enabled for Dynamic Frequency Selection (DFS).
ACM	Description—Checks whether or not Admission Control is enabled. Rule data—Choose **802.11a/n ACM**, **802.11b/g/n ACM**, or both check boxes. Rule validity—At least one band must be selected.
DTPC	Description—Checks whether or not Dynamic Transmit Power Control is enabled. Rule data—Select **802.11a/n DTPC**, **802.11b/g/n DTPC**, or both check boxes. Rule validity—At least one band must be selected.

Table 17-1 Rules List for Voice Audit (continued)

Rule	Rule Details
Expedited Bandwidth	Description—Checks whether or not Expedited Bandwidth is enabled. Rule data—Select **802.11a/n Expedited Bandwidth**, **802.11b/g/n Expedited Bandwidth**, or both check boxes. Rule validity—At least one band must be selected.
Load Based CAC	Description—Checks whether or not Load Based Admission Control (CAC) is enabled. Rule data—Select **802.11a/n Load Based CAC**, **802.11b/g/n Load Based CAC (LBCAC)**, or both check boxes. Rule validity—At least one band must be selected.
CAC: Max Bandwidth	Description—Checks whether or not Maximum RF Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Allowed Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0—100%.
CAC: Reserved Roaming Bandwidth	Description—Checks whether or not Reserved Roaming Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Reserved Roaming Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0—100%.
Pico Cell mode	Description—Checks whether or not Pico Cell mode is disabled. Rule data—Select **802.11a/n Pico Cell mode**, **802.11b/g/n Pico Cell mode**, or both check boxes. Rule validity—At least one band must be selected.
Beacon Period	Description—Checks whether or not Beacon Period is configured properly. Rule data—Enter the time (ms) in the text boxes for Beacon Period for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 20—1000. Enter 0 or keep it empty if a band should not be checked.
Short Preamble	Description—Checks whether or not Short Preamble is enabled for 11b/g.

Table 17-1 Rules List for Voice Audit (continued)

Rule	Rule Details
Fragmentation Threshold	Description—Checks whether or not Fragmentation Threshold is configured properly. Rule data—Enter the threshold amount (bytes) in the text boxes for Fragmentation Threshold for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 256—2346. Enter 0 or keep it empty if a band should not be checked.
Data Rate	Description—Checks whether or not Data Rates are configured properly. Data Rate configuration for 11b/g—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category. Data Rate configuration for 11a—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category.
Aggressive Load Balancing	Description—Checks whether or not Aggressive Load Balancing is disable.
QoS Profile	Description—Checks that QoS Profiles are not altered from default values.
EAP Request Timeout	Description—Checks whether or not EAP Request Timeout is configured properly. Rule data—Enter the time limit (sec) for the EAP Request Timeout. Rule validity—Data cannot be left blank or as zero. The valid range is 1—120.
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Note Click **Reset** to reset the rules to the default configuration.

Step 4 When the rules are configured for this voice audit, click **Save** to save the current configuration or **Save and Run** to save the configuration and run the report.

Step 5 Click the **Report** tab to view the Report results. See the "Voice Audit Report Details" section on page 17-5 for more information.

Voice Audit Report Details

The Voice Audit details provides the following information:

- Audit Status—Indicates whether or not the audit is complete.
- Start Time and End Times—Indicates the time at which the voice audit starts and ends.
- # Total Devices—Indicates the number of devices involved in the voice audit.
- # Completed Devices—Indicates the number of devices the tool attempted to audit.

Note If a controller is unreachable, the audit skips it. The Voice Audit does not complete any rule checks for that controller.

- # Rules—Indicates the number of rules selected for the voice audit.

Voice Audit Report Results

The Voice Audit Report results include the following information:

- IP Address—Indicates the IP address for the controller involved in the voice audit.
- Rule—Indicates the rule that was applied for this controller.
- Result—Indicates the result (Skipped, Violation, Unreachable) of the applied rule.

Note If there is no mismatch between the current configuration and a rule value, no results are displayed for that rule.

- Details—Defines an explanation for the rule results.

Note If the applied rule results in a Violation, the Details link provides additional information including Name, the Device Value, and the Rule Value. Hover your mouse cursor over the link to view the additional details.

- Time—Provides a timestamp for the voice audit.

Configuring the Location Accuracy Tools

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy Tools.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy Tools enable you to run either of the following tests:

There are two ways to test location accuracy:

- **Scheduled Accuracy Testing**—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already pre-positioned so that the test can be run on a regularly scheduled basis.
- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

This section contains the following topics:

- Enabling the Location Accuracy Tool, page 17-7

Enabling the Location Accuracy Tool

Note You must enable the **Advanced Debug** option in the NCS to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy Tool does not appear as an option on the Tools menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in the NCS, follow these steps:

Step 1 In the NCS, choose **Monitor > Maps**.

Step 2 Choose **Properties** from the Select a command drop-down list, and click **Go**.

Step 3 In the page that appears, select the **Enabled** check box to enable the Advanced Debug Mode. Click **OK**.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

You can now run location accuracy tests on the mobility services engine using the Location Accuracy Tool.

Proceed to either the "Using Scheduled Accuracy Testing to Verify Accuracy of Current Location" section on page 17-8 or "Using On-demand Accuracy Testing to Test Location Accuracy" section on page 17-10.

Viewing Currently Scheduled Accuracy Tests

To view the currently scheduled location accuracy tests, follow these steps:

Step 1 Select **Tools > Location Accuracy Tool**.

Step 2 The Accuracy Tests page displays all currently scheduled accuracy tests. The page displays the following information:

- Test Name—Click the Name to view details regarding this accuracy test.
- Test Type
- Floor or Outdoor Area—Displays the location of this test.
- Status
- Accuracy %
- Average Errors (m)

Use the Select a command drop-down list to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.

Note

- You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either **Download Logs** or **Download Logs for Last Run**. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Viewing Accuracy Test Details

To view details regarding a current accuracy test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 Click the name of the accuracy test for which you want to access details.

In the Accuracy Test Details page, you can position test points or delete the accuracy test.

Step 3 Click **Cancel** to return to the Accuracy Test overview page.

Using Scheduled Accuracy Testing to Verify Accuracy of Current Location

To configure a scheduled accuracy test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 Choose **New Scheduled Accuracy Test** from the Select a command drop-down list.

Step 3 Enter a Test Name.

Step 4 Choose the **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the begin and end time of the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.

Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 9 Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.

Note If you choose the e-mail option, an SMTP Mail Server must first be defined for the target e-mail address. Choose **Administrator > Settings > Mail Server** to enter the appropriate information.

Step 10 Click **Position Testpoints**. The floor map appears with a list of all clients, tags, and interferers on that floor with their MAC addresses.

Step 11 Select the check box next to each client, tag, and interferer for which you want to check the location accuracy.

When you select a MAC address check box, two icons appear on the map. One icon represents the actual location and the other represents the reported location.

Note To enter a MAC address for a client or tag or interferer that is not listed, select the **Add New MAC** check box, enter the MAC address, and click **Go**. An icon for the element appears on the map. If the newly added element is on the location server but on a different floor, the icon is displayed in the left-most corner (0,0 position).

Step 12 If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. Only the actual location icon can be dragged.

Step 13 Click **Save** when all elements are positioned. A dialog box appears confirming successful accuracy testing.

Step 14 Click **OK** to close the confirmation dialog box. You are returned to the Accuracy Tests summary page.

Note The accuracy test status is displayed as Scheduled when the test is about to execute. A status of Running is displayed when the test is in process and Idle when the test is complete. A Failure status appears when the test is not successful.

Step 15 To view the results of the location accuracy test, click the test name and then click the **Results** tab in the page that appears.

Step 16 In the Results page, click the **Download** link under the Saved Report heading to view the report.

The Scheduled Location Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

Using On-demand Accuracy Testing to Test Location Accuracy

An On demand Accuracy Test is run when elements are associated but not pre-positioned. On demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

To run an On-demand Accuracy Test, follow these steps:

Step 1 Choose **Tools > Location Accuracy Tool**.

Step 2 From the Select a command drop-down list, choose **New On demand Accuracy Test**.

Step 3 Enter a Test Name.

Step 4 Choose **Area Type** from the drop-down list.

Step 5 Campus is configured as Root Area, by default. There is no need to change this setting.

Step 6 Choose the Building from the drop-down list.

Step 7 Choose the Floor from the drop-down list.

Step 8 Choose the Destination point for the test results. Test results are viewed in the Accuracy Tests > Results page. Reports are in PDF format.

Step 9 Click **Position Testpoints**. The floor map appears with a red crosshair at the (0,0) coordinate.

Step 10 To test the location accuracy and RSSI of a particular location, select either client or tag or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client or tag or interferer) displays in a drop-down list to its right.

Step 11 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 12 From the Zoom percentage drop-down list, choose the zoom percentage for the map.

The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.

Step 13 Click **Start** to begin collection of accuracy data.

Step 14 Click **Stop** to finish collection. You should allow the test to run for at least two minutes before clicking Stop.

Step 15 Repeat Step 11 to Step 14 for each testpoint that you want to plot on the map.

Step 16 Click **Analyze Results** when you are finished mapping the testpoints.

Step 17 Click the **Results** tab in the page that appears.

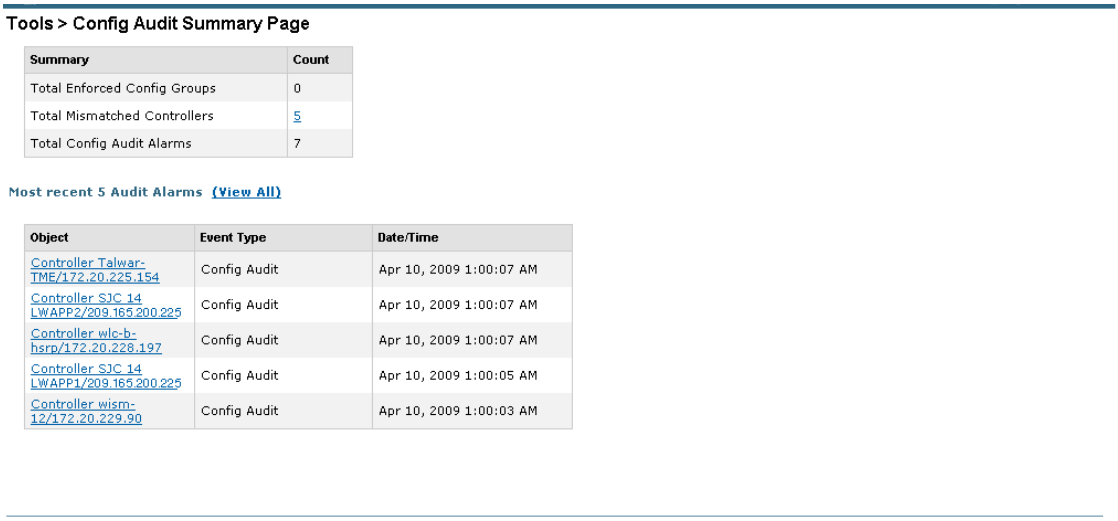
The On-demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph

Configuring Audit Summary

Choose **Tools > Config Audit** to launch the Config Audit Summary page (see Figure 17-1).

Figure 17-1 Tools > Config Audit Summary Page



This page provides a summary of the following:

- Total Enforced Config Groups—Identifies the count of config group templates, which are configured for Background Audit and are enforcement enabled.

  Click the link to launch the Config Group page to view config groups with Enforce Configuration enabled.

- Total Mismatched Controllers—Identifies the number of mismatched controllers. Mismatched controllers indicate that there were configuration differences found between the NCS and the controller during the last audit.

  Click the link to launch the controller list sorted in the mismatched audit status column. Click an item in the Audit Status column to view the audit report for this controller.

- Total Config Audit Alarms—Identifies the number of alarms generated when audit discrepancies are enforced on config groups.

  Click the link to view all config audit alarm details.

  Note If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Most recent 5 config audit alarms—Lists the most recent configuration audit alarms including the object name, event type, date, and time for the audit alarm.

Click **View All** to view the applicable Alarm page that includes all configuration audit alarms.

Configuring Migration Analysis

Choose **Tools > Migration Analysis** to launch the Migration Analysis Summary page.

Note You can also access the migration analysis summary by choosing **Configure > Autonomous AP > Migration Templates** and choosing **View Migration Analysis Summary** from the Select a command drop-down list.

The autonomous access points are eligible for migration only if all the criteria has a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version—Conversion is supported only from 12.3(7)JA releases excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only

Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

This section contains the following topics:

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. In the Migration Analysis page, you can select the access point with the software version listed as failed and choose **Upgrade Firmware (Manual or Automatic)** from the Select a command drop-down list. This process upgrades the autonomous firmware image of the Cisco IOS access point to a supported version.

The NCS uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in the NCS. The default images per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar

- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional page with TFTP server IP, file path, and file pathname appears. The final page is the Report page.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, choose **Change Station Role to Root Mode** from the Select a command drop-down list to change the mode.

Running Migration Analysis

Choose **Run Migration Analysis** from the Select a command drop-down list of the Migration Analysis Summary page. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Viewing the Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down list of the Migration Analysis Summary page to generate a report. The report includes the following:

- Access point address
- Status
- Timestamp
- Access point logs

Viewing a Firmware Upgrade Report

Choose **View Firmware Upgrade Report** from the Select a command drop-down list to view a current report of the upgrade status for the selected access point.

The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the firmware upgrade.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

See the "Upgrading Autonomous Access Points" section on page 17-12 for more information.

Viewing a Role Change Report

Because a wired connection between the access point and controller is required to send the association request, the autonomous access point must be assigned the appropriate role.

To view a report of these role changes, choose **View Role Change Report** from the Select a command drop-down list. The following information is displayed:

- AP Address—IP address of the access point.
- Status—Current status of the role change.
- TimeStamp—Indicates the date and time of the upgrade.
- AP Logs

Click **OK** to return to the Migration Analysis Summary page.

Configuring TAC Case Attachments

Note You must configure a valid mail server before configuring TAC case attachments.

The TAC Case Attachment tool helps you easily attach all the relevant controller TAC case information in one step. This tool provides two options:

- Send—Sends an e-mail to attach@cisco.com.
- Download—Downloads the information to a local computer. You must manually e-mail the data to attach@cisco.com. This option is handy if there is no e-mail connectivity between the NCS server and Cisco or if the information is too large to be attached through e-mail.

This tool sends the following information:

- Network Information—Sends device inventory details and the client types.
- Controller Information—Sends running configuration details, tech-support, message logs, trap logs, and the controller crash files.
- Access Point Information—Sends crash files and radio core dumps.

To Send or Download information, you must enter the following details:

- Enter a valid TAC Case Number.
- Select a controller if you want to send the controller or AP information.

Note You can also send additional information using the additional comments text box. After sending the information, you can verify whether the data has reached Cisco by looking at the attachment section in the Case tool.

Note This tool requires read-write access on the controller to collect and upload controller or access point information.