CHAPTER 15

Running Reports

WCS reporting is necessary to monitor the system and network health as well as troubleshoot problems. A number of reports can be generated to run on an immediate and scheduled basis. Each report type has a number of user-defined criteria to aid in the defining of the reports. The reports are formatted as a summary, tabular, or graphical layout. Once defined, the reports can be saved for future diagnostic use or scheduled to run and report on a regular basis.

Reports are saved in either CSV or PDF format and are either saved to a file on WCS for later download or e-mailed to a specific e-mail address.

The reporting types include the following:

- Current, which provides a snap shot of the data from the last polling cycle without continuously polling
- Historical, which retrieves data from the device periodically and stores it in the WCS database
- Trend, which generates a report using aggregated data. Data can be periodically collected based from devices on user-defined intervals, and a schedule can be established for report generation.

With WCS, you also have the ability to export any report that you can view, sort reports into logical groups, and archive for long-term storage.

Note If you want the report to print as it appears on the window display, you must choose landscape mode.

From the Reports menu, you can access any of the following types:

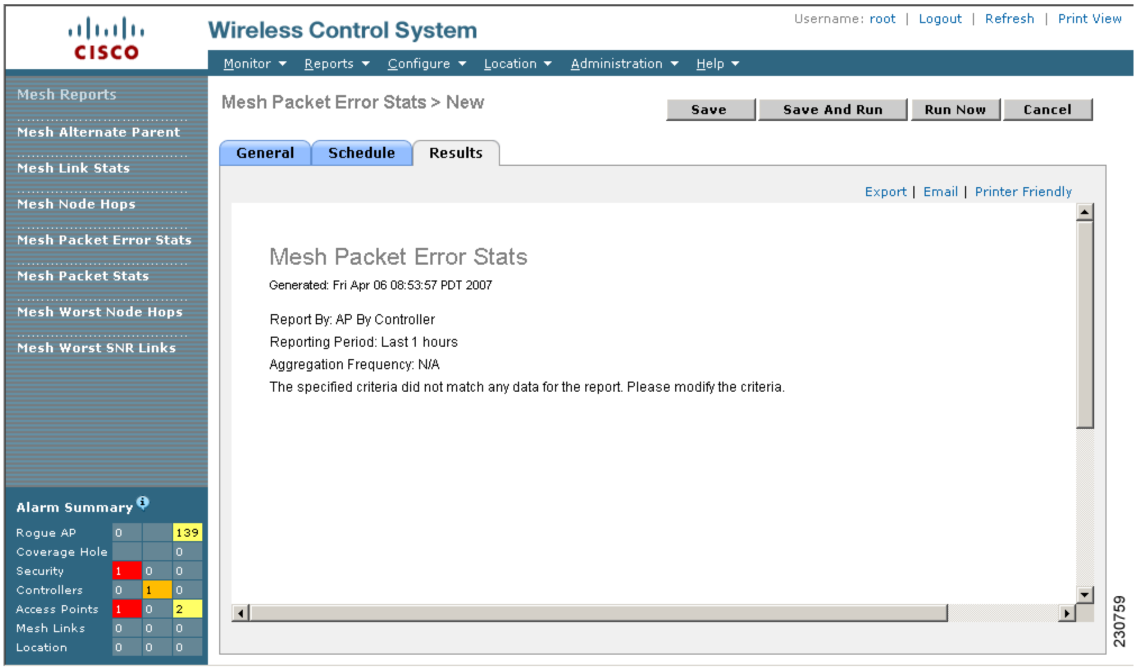
Choosing a Report

If you choose one of the above options from the Reports menu, a window with a list of created report tasks appears. Perform one of the following operations:

- If you want to enable or disable a report schedule, refer to the "Enabling or Disabling a Schedule" section on page 15-2.
- If you want to delete a report, refer to the "Deleting a Report" section on page 15-3.
- If no reports are defined, you can create a report by selecting **New** from the Select a command menu. After clicking **GO**, two new panels appear: General and Schedule. The General panel allows you to configure data gathering parameters. The Schedule panel allows you to control when and how often the report runs, based on what you specify. Refer to the "Accessing the Schedule Panel" section on page 15-4.

  After running the report, a Results tab shows the report data (see Figure 15-1).

Figure 15-1 Results Tab



Mesh Packet Error Stats

Generated: Fri Apr 06 08:53:57 PDT 2007

Report By: AP By Controller

Reporting Period: Last 1 hours

Aggregation Frequency: N/A

The specified criteria did not match any data for the report. Please modify the criteria.

Alarm Summary

Rogue AP	0		139
Coverage Hole			0
Security	1	0	0
Controllers	0	1	0
Access Points	1	0	2
Mesh Links	0	0	0
Location	0	0	0

A History Tab appears after some scheduled executions have occurred.

Enabling or Disabling a Schedule

To enable a defined report, check the check box next to the report and select **Enable Schedule** from the Select a command menu. Click **GO**. If the scheduled time period for the report has passed, then *Expired* appears in the Schedule column. To remedy, click the report title and enter new time parameters in the window that appears.

To disable a defined report, check the check box next to the report and select **Disable Schedule** from the Select a command menu. Click **GO**. The disabled state appears in the Schedule column.

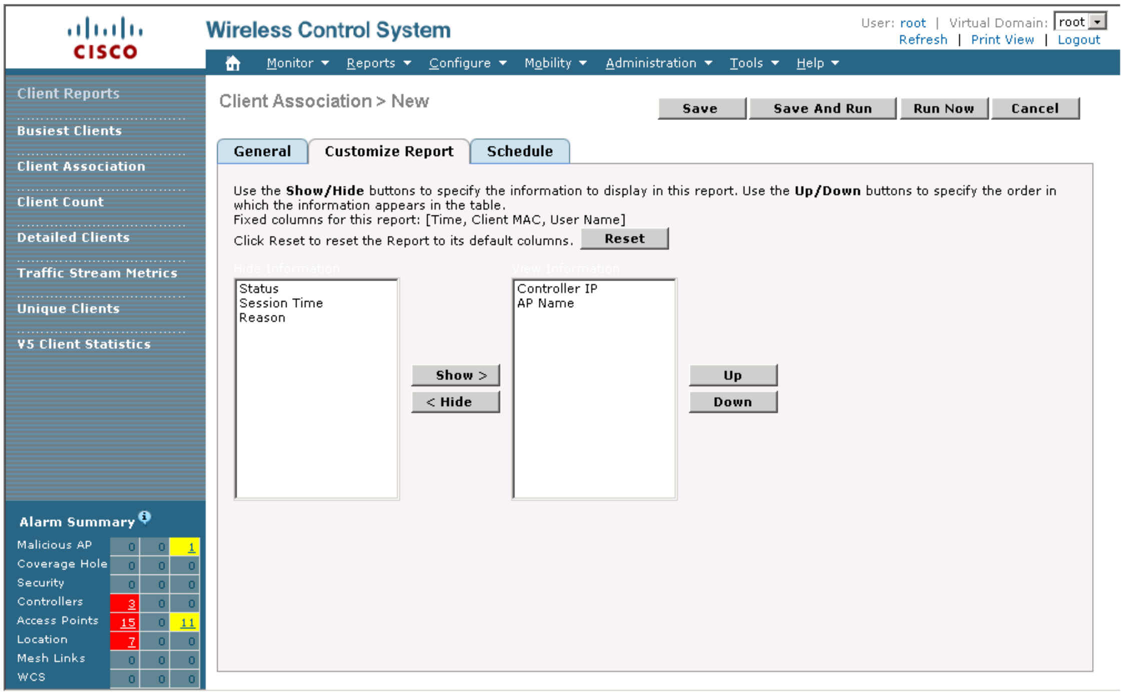
Deleting a Report

To delete a defined report, check the check box next to the report and select **Delete** from the Select a command menu and click **GO**. The report is deleted from the listing.

Customizing a Report

Several reports have a Customize Report tab (see Figure 15-2). Within this tab, you can use the Show and Hide buttons to specify which information you want displayed in the report. After you have column headings appearing in the Show window, you can use the Up and Down buttons to specify the order that you want the information to appear. Some columns may be fixed and vary per report.

Figure 15-2 Customize Report Tab



Client Association > New

Use the **Show/Hide** buttons to specify the information to display in this report. Use the **Up/Down** buttons to specify the order in which the information appears in the table.
Fixed columns for this report: [Time, Client MAC, User Name]
Click Reset to reset the Report to its default columns.

Hide Information:
Status
Session Time
Reason

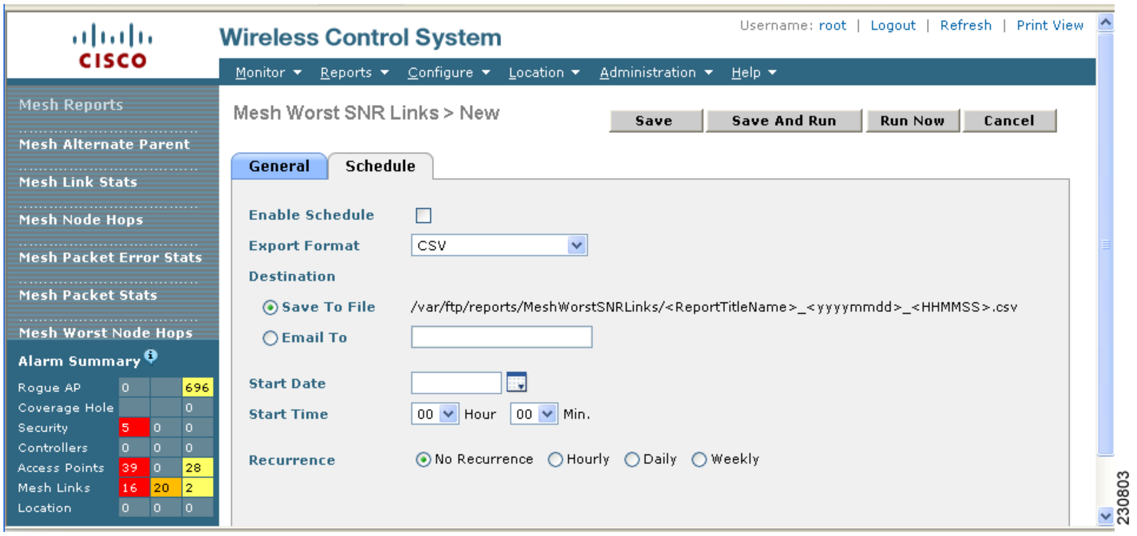
View Information:
Controller IP
AP Name

Alarm Summary			
Malicious AP	0	0	1
Coverage Hole	0	0	0
Security	0	0	0
Controllers	3	0	0
Access Points	15	0	11
Location	7	0	0
Mesh Links	0	0	0
WCS	0	0	0

Accessing the Schedule Panel

The schedule panel is the same for any report. After choosing the Schedule tab, the Schedule window appears (see Figure 15-3).

Figure 15-3 Schedule Tab



Alarm Summary

Rogue AP	0		696
Coverage Hole			0
Security	5	0	0
Controllers	0	0	0
Access Points	39	0	28
Mesh Links	16	20	2
Location	0	0	0

Enable Schedule □

Export Format CSV

Destination

● Save To File /var/ftp/reports/MeshWorstSNRLinks/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

○ Email To

Start Date

Start Time 00 Hour 00 Min.

Recurrence ● No Recurrence ○ Hourly ○ Daily ○ Weekly

Follow these steps after choosing the **Schedule** tab within any report type.

Step 1 Check the **Enable Schedule** check box.

Step 2 Specify if you want the export format to be .csv (a file containing the MAC addresses of access points) or .pdf from the Export Format drop-down menu.

Step 3 Choose either the **Save to File** or **E-mail To** option as the destination type.

- If you select the Save to File option, a destination path must first be defined at the **Administration > Settings** > *Report* page. Enter the destination path for the files in the Repository Path field.
- If you select the E-mail to option, an SMTP Mail Server must be defined prior to entry of the target e-mail address. Choose **Administrator > Settings** > *Mail Server* to enter the appropriate information.

Step 4 Enter a start date (MM:DD:YYYY format) in the provided field or click the calendar icon to select a date. The report begins running on this date.

Step 5 Specify a start time using the hour and minute drop-down menus.

Step 6 Click on one of the recurrence buttons to select how often the report is run.

Step 7 When entry is complete, do one of the following:

- Click **Save** to save the entry.
- Click **Save and Run** to save the changes and run the report now. The report is run, and the results are either e-mailed or saved to a designated file as defined in the Schedule tab. The report runs again at the scheduled time.

- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any scheduled time associated with the report.

Note You can use the Run command to check a report scenario before saving it or to run ad hoc reports as necessary.

802.11n Scaling Reports

The 802.11n Scaling reports can help you to find out the client mix in your network and respective utilization of the infrastructure. These reports can also help you discover how the current controller deployment scales up to the given client mix and how you can scale to add more controllers and access points.

802.11n Scaling reports include:

- Client Count
- Throughput

Note The 802.11n Scaling reports do not include clients connected to Autonomous IOS access points.

Client Count

The Client Count is a graph report which displays the associated clients and authenticated clients. The clients can be filtered by controller, floor area, SSID, access point, and client protocol.

Note The Client Count report does not include clients connected to Autonomous IOS access points.

To access this report, follow these steps:

Step 1 Choose **Reports > 802.11n Scaling**.

Step 2 From the left sidebar menu, click **Client Count**.

In the report window, saved reports are displayed in a table.

Creating a New Client Count Report

To create a new Client Count report, follow these steps:

Step 1 From the Reports > 802,11n Scaling > Client Count report page, choose *New* from the Select a command drop-down menu.

Step 2 Click **GO**.

Step 3 Enter applicable report parameters.

- Report Title

- Report By:

  Note The parameters change depending upon the Report By selection.

  - Controller—Choose the controller from the drop-down menu.
  - Floor Area—Choose the campus, building, and floor from the drop-down menus.
  - Outdoor Area—Choose the campus and outdoor area from the drop-down menus.
  - AP by Floor Area—Choose the campus, building, floor, and access point from the drop-down menus.
  - AP by Outdoor Area—Choose Campus, Outdoor Area, and Access Point from the drop-down menus.
  - SSID —Choose All SSIDs or other applicable SSID from the drop-down menu.
- Protocol—All Clients, 802.11a/n, 802.11b/g/n, 802.11a. 802.11b, 802.11g, 802.11n_5GHz, and 802.11n_2.4GHz.
- Reporting Period.

Step 4 Configure the report schedule. See the "Enabling or Disabling a Schedule" section on page 15-2.

Step 5 Click **Save**, **Save and Run**, **Run Now**, or **Cancel**.

You can manage saved reports using the Select a command drop-down list.

Throughput

The 802.11n Throughput report is a graph report which displays the total throughput of a selected device or service domain along with the selected clients below it. These selected clients are differentiated by protocol types.

Note The Throughput report does not include clients connected to Autonomous IOS access points.

To access this report, follow these steps:

Step 1 Choose **Reports > 802.11n Scaling**.

Step 2 From the left sidebar menu, click **Throughput**.

Step 3 In the report window, saved reports are displayed in a table.

Creating a New Throughput Report

To create a new Throughput report, follow these steps:

Step 1 From the Reports > 802.11n Scaling > Throughput report page, choose **New** from the Select a command drop-down menu.

Step 2 Click **GO**.

Step 3 Enter applicable report parameters.

- Report Title
- Report By:

  Note The parameters change depending upon the Report By selection.

  - Controller—Choose the controller from the drop-down menu.
  - Floor Area—Choose the campus, building, and floor from the drop-down menus.
  - Outdoor Area—Choose the campus and outdoor area from the drop-down menus.
  - AP by Controller—Choose the controller and access point from the drop-down menus.
  - AP by Floor Area—Choose the campus, building, floor, and access point from the drop-down menus.
  - AP by Outdoor Area—Choose campus, outdoor area, and access point from the drop-down menus.
- Protocol—All clients, 802.11a/n, 802.11b/g/n, 802.11a, 802.11b, 802.11g, 802.11n_5GHz, 802.11n_2.4GHz.
- Reporting Period

Step 4 Configure the report schedule. See the "Accessing the Schedule Panel" section on page 15-4 for more information.

Step 5 Click **Save**, **Save and Run**, **Run Now**, or **Cancel**.

You can manage saved reports using the Select a command drop-down list.

Access Point Reports

In the left sidebar menu, all of the access point report options are listed.

Note The access point reports do not show the status of autonomous access points.

The choices are as follows:

- AP List by Location and SSID Report—Displays information on access points located in specific physical areas and specific SSIDs.
- AP Profile Status Report—Displays information on access points located in specific physical areas and with specific SSIDs.
- AP Up Times—This report displays information related to the uptime of various devices on your network. You can choose between AP up time, LWAPP up time, and LWAPP join time and then sort the report from lowest-to-highest up times or from highest-to-lowest up times. The graphical trending identifies the availability of services to the client with a quick summary of overall network availability over a given period of time. The report also displays the access point and map location if applicable.

- Busiest APs Report—Allows you to view information on the busiest access points in terms of total utilization. The total utilization is the sum of transmitting, receiving, and channel utilization.
- Traffic Stream Metrics Report—Shows voice traffic stream metrics and high density related reports. This report is useful in determing the current and historical quality of service (QoS) for given client(s) at the radio level. The controller keeps multiple records of the voice metrics data for each client. The access points update the controller with traffic stream metric information every 90 seconds, and 10 minutes of data is stored at one time to generate an on-demand report. WCS polls the data from the controllers and aggregates it as hourly, daily, and weekly. The generated data that is returned includes but is not limited to the following: uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
- Graphical Traffic Stream Metrics Report—The Traffic Streams Metrics (Graphs) report is equivalent to the Traffic Streams Report, but the information is displayed in graph form.

Viewing or Modifying Access Point Reports

Follow these steps to view or modify existing access point reports.

Step 1 Choose **Reports > Access Point Reports**. The Access Point Report page appears.

Step 2 Choose the Access Point Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Access Point Report

Follow these steps to create a new access point report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Access Point Reports**. The Access Point Reports page appears.

Step 2 Click on one of the report types summarized under Access Points Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**.

Step 4 Specify a report title.

Step 5 Use the Report By drop-down menu to choose of which physical area to report. The following options are available:

- AP By Outdoor Area—Generates the report of the outdoor area on a per-access point basis.
- AP by Floor Area—Generates the report of the floor area on a per-access point basis.

Step 6 Perform one of the following:

If you chose outdoor, you need to specify in which campus and outdoor area it is located.
If you chose floor area, you need to choose in which campus, building, and floor the area is located.

Step 7 Determine which access points you want to include in the report.

Step 8 Specify if you want to include 802.11a/n or 802.11b/g/n radios in the report.

Step 9 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Audit Reports

Network configuration audit reports give configuration differences between WCS and the controllers managed by it. Such audits can be performed based on the controllers' current configuration or the templates that have been applied to them. Data for this report is collected by the Network Audit Configuration task which is enabled by default on a newly installed WCS system and is scheduled to run once every 7 days. To change the frequency of the background task, refer to the "Running Background Tasks" section on page 16-1. The report shows the audit status for each controller and shows the attribute differences in the configurations. Even controllers which are not reachable during the network audit configuration task are listed. The authorization for the audit reports is tied into the security framework so that only certain users can have access. By default, the admin, configManagers, system monitoring, superusers, and root users have access.

Note The Audit Reports do not show the status of autonomous access points.

Viewing or Modifying Audit Reports

Follow these steps to view or modify existing audit reports.

Step 1 Choose **Reports > Audit Reports**. The Audit Report page appears.

Step 2 Choose the Audit Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Note Even controllers that are not audited or not reachable are listed on the report.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Network Configuration Audit Report

Follow these steps to create a new audit report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Audit Reports**. The Audit Reports page appears.

Step 2 Click on one of the report types summarized under Audit Reports (left-side). Currently only one network configuration audit report is available.

Note With a clean install, Background Tasks > Network Audit is enabled.

Step 3 Select **New** from the Select a command menu. Click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report to include all controllers or a selected controller.

Step 6 From the Audit Time drop-down menu, determine if you want to view the latest report or choose from a network audit time. Audit time is the time when the network audit background task was excluded. *Latest* is the default selection.

Step 7 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Note You can also choose Run Now to run the report. The report shows the data collected by the network audit task. You must set the network audit schedule appropriately.

Client Reports

You can run reports of all unique clients that have accessed the network for a specified duration. For example, you may want to show all clients that were on a certain floor in the last three days and see detailed information network activity.

Note The Client Count report is the only client reports that shows the status of autonomous access points.

The client report options are as follows:

Busiest Clients Report—Displays information on the busiest clients in terms of total throughput of clients during a given period of time. WCS polls Tx and Rx bytes from controllers and reports them on a per client basis. Within a 15 minute minute polling cycle (the default), the number of actual Tx and Rx bytes between this and previous polling cycles is calculated.The throughput is the Kb/s between this cycle and previous polling cycles. Utilization is the percentage of bandwidth used during the polling cycle (the throughput multiplied by 1000, divided by the bandwidth based on the radio, and then multiplied by 100). The bandwidth is the maximum speed for the radio (54 Mb/s for 802.11a/g, 11 Mb/s for 802.11b, 100 Mb/s for wired guest clients, and 200 Mb/s for 802.11n).

- Client Association Report—Shows a detailed association history of the clients as collected from the controller. The generated data that is returned includes but is not limited to the following: the username and MAC address of the client, which access point it is associated with, and a status.

  Note The client association history only goes back 7 days. You cannot retrieve any history prior to that.

- Client Count Report—Displays data on the numbers of clients that connected to the network through a specific device, in a specific geographical region, or through a specific SSID.
- Detailed Clients Report—Consolidates client-related information currently present in other client reports in WCS. It includes network information (such as access point name, MAC and IP addresses, the controller name and IP address, and SSID information), client information (such as client name, MAC and IP addresses, brief configuration information such as client OUI, CCX rev, and client type voice/data/location), client statistics (such as RSSI, SNR, throughput, and session length), client location, and ACS information (whether the authentication succeeded or failed). The report can be generated multiple ways.
- Traffic Stream Metrics Report—Shows voice traffic stream metrics and high density related reports for clients. The controller keeps multiple records of the voice metrics data for each client. The traffic stream metrics report is used to determine the current and history quality of service (QoS) for given client(s) at the radio level. The generated data that is returned includes but is not limited to the following: uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
- Unique Client Report—Shows which unique clients have accessed the network within a specified duration. For example, you could show all clients on a particular floor in the last three days and view detailed information about their network activity. The generated data that is returned includes but is not limited to the following: the vendor and MAC address of the client, which access point it is associated to, and the Cisco Compatible Extensions version supported by the client.
- V5 Client Statistics Report—Collects client statistics for V5 clients and above that are in an associated and authenticated state. The report contains counters for a Dot11 statistics measurement and a security statistics measurement. If V5 clients exist, a request is initiated for Dot11 measurement; and if the request is successful, the database is populated with the Dot11 response for the client. Then the security request is initiated and if successful, the database is populated with the security response for the client.

Viewing or Modifying Client Reports

Follow these steps to view or modify existing client reports.

Step 1 Choose **Reports > Client Reports**. The Client Report page appears.

Step 2 Choose the Client Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Client Report

Follow these steps to create a new client report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Client Reports**. The Client Reports page appears.

Step 2 Click on one of the report types summarized under Client Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Enter the number of clients you want displayed in the report.

Step 6 Choose ALL SSIDs or choose a specific SSID to restrict the report to access points using that SSID.

Step 7 Enter a specific client MAC address. If no MAC address is specified, then all the clients per specified SSID would be reviewed.

Step 8 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 9 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 10 Determine which access points you want to include in the report.

Step 11 Specify if you want to include 802.11a/n or 802.11b/g/n radios in the report.

Step 12 In the Reporting Period section, choose **Last** to determine the timeframe the report should encompass or choose **Between** and use the calendar icon to choose a date and set the hour and minutes.

Step 13 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Compliance Reports

The PCI DSS Compliance report provides a summary of your Wireless LAN Security components with reference to the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. PCI DSS compliance is required for all merchants and service providers that store, process, or transmit cardholder data. PCI DSS standards can be located at https://www.pcisecuritystandards.org.

To see the information a PCI Compliance Report provides, see the "Compliance Reports Results" section on page 15-13.

Viewing or Modifying Compliance Reports

This report identifies the device and network configuration in light of PCI requirements and provides PCI auditors with information about the level of compliance on your network. With the PCI requirements, the contents of this detailed report can serve as guidance to the auditors while they perform PCI audit of the network. To access this report, follow these steps:

Step 1 Choose **Reports > Compliance Reports**.

Step 2 From the left sidebar menu, click **PCI Compliance Reports**.

In the report window, saved reports are displayed in a table.

Creating a New Compliance Report

To create a new PCI Compliance report, follow these steps:

Step 1 From the Reports > Compliance Reports > PCI Compliance report page, choose **New** from the Select a command drop-down menu.

Step 2 Click **GO**.

Step 3 Enter the applicable report parameters:

- Report Title
- Reporting Period

Step 4 Configure the report schedule. Refer to the "Enabling or Disabling a Schedule" section on page 15-2 for more information.

Step 5 Click **Save**, **Save and Run**, **Run Now**, or **Cancel**.

Compliance Reports Results

Note Do not consider this report as a replacement for a formal PCI compliance audit. This report only addresses various aspects of the PCI standards as applicable to Cisco Unified Wireless Network (CUWN).

This report addresses the following PCI requirements and resulting issues:

- Install and maintain a firewall configuration to protect cardholder data—Includes the following information:
  - New rogue access points (most recent alarms for rogue access points) and rogue adhocs (rogue adhoc alarms) detected on your wireless LAN network—Lists all threats associated with rogue access points and rogue adhocs.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

  - Lists all devices with default configuration scuh as default username/password, default SNMP community string, and SSID broadcast.

    Note A configuration sync background task must be run at least once to get appropriate results.

- Encrypt transmission of cardholder data across open, public networks.
  - Lists all encryption and authentication violations.
- Track and monitor all access to network resources and cardholder data.
  - Lists detailed association history for clients that connect to your wireless LAN network.

    Note A configuration sync background task must be run at least once to get appropriate results.

- Annually test security controls, limitations, network connections, and restrictions to assure the ability to adequately identify and to stop any unauthorized access attempts. User a wireless analyzer at least quarterly to identify all wireless devices in use.
  - Lists all wireless devices in the network (controllers, access points, and location servers).
  - Lists all intrusion attempts including signature attacks, MFP attacks, access point threats and attacks, client security events, and Cisco wired IPS events (only criticial and major alarms are included).

Inventory Reports

In the left sidebar menu, all of the inventory report options are listed. These reports generate inventory-related information of controllers, access points, and mobility service engines managed by WCS. The information provided can be grouped and includes but is not limited to the following: hardware type and distribution, software distribution, CDP information, and so on. These reports are generated based on the data already stored in the WCS database. Because inventory reports are not on-demand reports, some configuration changes may have occurred since the storage and may not duplicate the attributes of the controller that are reflected in the stored data.

Note The inventory reports do not show the status of autonomous access points.

The choices are as follows:

- Access Point Inventory Report—Provides data on deployed access points. The data that is returned includes but is not limited to the following: the access points' MAC address, base radio MAC, 802.11a/n or b/g/n radio MAC, model, location, and radio status.
- Combined Inventory Report—Provides data on all deployed controllers, access points, and location appliances. The data that is returned includes but is not limited to the following: base radio MAC and 802.11a/n or b/g/n radio MAC.
- Controller Report—Provides data on deployed controllers. The data that is returned includes but is not limited to the following: the model, IP address, and serial number of the controller, what software version it is running, and where it is located.

- Mobility Service Engines Report—Provides data on deployed location appliances. The data that is returned includes but is not limited to the following: the IP address and version of the location appliance, which port is being used, and the time the appliance starts up.

Viewing or Modifying Inventory Reports

Follow these steps to view or modify existing inventory reports.

Step 1 Choose **Reports > Inventory Reports**. The Inventory Reports page appears.

Step 2 Choose the Inventory Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Inventory Report

Follow these steps to create a new inventory report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Inventory Reports**. The Inventory Reports page appears.

Step 2 Click on one of the report types summarized under Inventory Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Mesh Reports

Mesh reports are used to analyze and diagnose mesh networks. In the left sidebar menu, all of the mesh report options are listed.

Note The mesh reports do not show the status of autonomous access points.

The following reports can be generated for 1510 mesh access points.

- Mesh Alternate Parent–Lists the number of alternate parents available for a mesh access point. A value of zero (0) indicates the mesh access point has no alternate parents.

- Mesh Link Stats–Lists link statistics for a mesh access point such as packets transmitted, packet error rate, parent changes, SNR, and hops from the root access point.
- Mesh Node Hops–Lists the number of hops between a mesh access point and its root access point.
- Mesh Packet Error Statistics–Notes the percentage of packet errors for packets transmitted by the neighbor mesh access point. Packet error rate percentage = 1- (number of successfully transmitted packets/number of total packets transmitted).
- Mesh Packet Queue Statistics–Generates a graph of packet queue statistics for each access point selected and for each report type selected. The report types are Packet Queue Average, Packets Dropped Per Minute, and Packet Dropped Count. The Packet Queue Average report shows the average number of packets for each queue when the MIB was polled. The Packets Dropped Per Minute report shows the number of packets dropped since the last sample divided by the number of minutes since the sample. The Packet Dropped Count contains the counter for the number of packets dropped.
- Mesh Packet Statistics—Generates a graph of the total number of packets transmitted and the total number of packets successfully transmitted by the neighbor mesh access point.
- Mesh Stranded APs—Displays any potentially stranded access points. A stranded access point is one listed as a mesh neighbor but not currently joined with a controller or one joined with a controller known by WCS but no longer seen by a mesh neighbor. The report displays all current access points believed to be stranded and lists the current detecting access points (the last set of access points detecting the device when the access point is not seen by any mesh neighbor). The report also displays the state of the stranded access point. As determined by WCS, the three states are:
  - Detected and Never Associated: An access point which has never joined a controller and is being detected as a neighbor.
  - Not Detected and Previously Associated: An access point which has associated to a controller at one time but is no longer associated. No mesh access points are detecting this access point as a neighbor.
  - Detected and Not Associated: An access point which has associated to a controller at one time but is no longer associated. A neighbor access point is detecting this access point.
- Mesh Worst Node Hops–Lists mesh access points by name and MAC address and notes those that are 10 hops (default) away from the root access point. Number of hops can be modified.
- Mesh Worst SNR Links–Lists the10 (default) mesh access point-to-neighbor links that exhibit the worst signal-to-noise ratio (SNR). You can change the number of links to display.

Viewing or Modifying Mesh Reports

Follow these steps to view or modify existing inventory reports.

Step 1 Choose **Reports > Mesh Reports**. The Mesh Reports page appears.

Step 2 Choose the Mesh Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Creating a New Mesh Report

Follow these steps to create a new mesh report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Mesh Reports**. The Mesh Reports page appears.

Step 2 Click on one of the report types summarized under Mesh Reports (left-side).

Step 3 Select **New** from the Select a command menu. Click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 If you want to report more items than the default setting, enter a new value. For example, you could enter a new value at the Mesh Worst SNR Links field which is currently configured by default to report the 10 worst links.

Step 6 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 7 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 8 If necessary, enter which access points to include in the report.

Step 9 Select the neighbor type and display option (table or graph).

Step 10 At the Graph Type parameter, choose either packet count or packets per minute.

Step 11 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or select a specific date and time range for reporting.

Note Hours are defined on a 24-hour basis rather than a 12-hour basis with AM and PM. For example, select hour 13 for 1 PM.

Step 12 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Performance Reports

In the left sidebar menu, all of the performance report options are listed.

Note Performance reports do not show the status of autonomous access points.

The choices are as follows:

- 802.11 Counters Report—Shows counters for the access points at the MAC layer such as error frames, fragment counts, RTS/CTS frame count, and retried frames which can help interpret performance at the MAC layer.

- Controller Utilization Report— Shows utilization based on metrics such as but not limited to CPU usage, memory usage, link utilization, radio utilization, and overall network utilization of the devices (controllers, access points, mobility service engines) on your network based upon filtering criteria selected at the time of report generation. These statistics help identify current network performance and assist with capacity planning for scalability needs.
- Coverage Hole Summary Report—Identifies where the potential coverage holes occur in your network. If a certain spot recurs more than others, you can tweak the RRM settings or place additional access points. The data that is returned includes but is not limited to the following: the base radio MAC address of the alarming access point, the radio type, and the coverage threshold.
- Location Server Utilization—Shows utilization based on metrics such as but not limited to CPU usage, memory usage, link utilization, radio utilization, and overall network utilization of the devices (controllers, access points, mobility service engines) on your network based upon filtering criteria selected at the time of report generation. These statistics help identify current network performance and assist with capacity planning for scalability needs..
- Radio Utilization Report—Shows utilization based on metrics such as but not limited to CPU usage, memory usage, link utilization, radio utilization, and overall network utilization of the devices (controllers, access points, mobility service engines) on your network based upon filtering criteria selected at the time of report generation. These statistics help identify current network performance and assist with capacity planning for scalability needs.
- Tx Power Level and Channel Report—Shows the channel plan assignment and transmit power level trends of the devices based on the filtering criteria used at the time of report generation. The trending of power levels and channel plan assignments help identify abnormal behavior and provide an outlook into how the wireless network has been performing. The data that is returned includes but is not limited to the following: the transmit power level for 802.11a/n and 802.11b/g/n interfaces, the channel number used for 802.11a/n and 802.11b/g/n interfaces, and the grouping types.
- Voice Statistics Report—Helps analyze the wireless network usage from a voice perspective. It presents details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls per radio on the network. Voice client need CAC support to gather useful data from this report.

Viewing or Modifying Performance Reports

Follow these steps to view or modify existing performance reports.

Step 1 Choose **Reports > Performance Reports**. The Performance Reports page appears.

Step 2 Choose the Performance Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Performance Report

Follow these steps to create a new performance report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Performance Reports**. The Performance Reports page appears.

Step 2 Click on one of the report types summarized under Performance Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 6 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 7 If necessary, enter which access points or location server to include in the report.

Step 8 Specify if you want to include 802.11a/n or 802.11b/g/n radios.

Step 9 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or choose a specific date and time range for reporting.

Step 10 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.

Security Reports

In the left sidebar menu, all of the security report options are listed. The security reports display information about the security of the wireless network.

Note Security reports do not show the status of autonomous access points.

The choices are as follows:

- New Rogue APs—Displays, in tabular form, all rogues detected in a selected timeframe. It provides which new rogues were detected within a selected time. The created time indicates the time at which the rogue was first detected.
- New Rogue AP Count—Displays, in graphical form, all rogues detected in a selected timeframe.
- Rogue APs—Displays all rogues that are active in your network and have been updated in the selected timeframe. WCS receives updated events for rogues that are detected
- Rogue APs Event—Displays all the events received by WCS. The controller sends updates of detected rogues if any of the attributes change or new rogues are detected.

Note This report was formally called the Rogue Detected by AP.

- Rogue Adhocs—Displays all adhocs that have been updated in the selected timeframe.
- Rogue Adhocs Event—Displays all adhoc events that WCS has received in the selected timeframe.
- Security Summary Report— Shows the number of association failures, rogues access points, ad hocs, and access point connections or disconnections over one month.

Viewing or Modifying Security Reports

Follow these steps to view or modify existing security reports.

Step 1 Choose **Reports > Security Reports**. The Security Reports page appears.

Step 2 Choose the Security Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel.

Step 4 Refer to the "Accessing the Schedule Panel" section on page 15-4 to complete the scheduling process.

Step 5 Click the **History** tab if you want to review details of the current and past runs of the report.

Creating a New Security Report

Follow these steps to create a new security report.

Note Some of these steps or options are not required for every report.

Step 1 Choose **Reports > Security Reports**. The Security Reports page appears.

Step 2 Click on one of the report types summarized under Security Reports (left-side).

Step 3 Choose **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 6 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 7 If necessary, enter which access points or location server to include in the report.

Step 8 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or choose a specific date and time range for reporting.

Step 9 Click the **Schedule** tab to complete the scheduling process. Refer to the "Accessing the Schedule Panel" section on page 15-4.