C H A P T E R **10**

Managing Clients

A client is a device that is connected to an access point or a switch. NCS supports both wired and wireless clients. After you add controllers and switches to NCS, the client discovery process starts. Wireless clients are discovered from managed controllers or autonomous access points. The wireless client count includes autonomous clients as well. Only in the case of switches, NCS polls for clients immediately after the device is added. In the case of controllers, these are polled during regular client status poll. NCS gets the client information from the switch and updates this information in the database. For wired clients, the client status polling to discover client associations occurs in every two hours (by default). A complete polling happens twice every day to poll complete information of all wired clients connected to all switches.

NCS uses background tasks to perform the data polling operations. There are three tasks associated with clients:

1. Autonomous AP Client Status

2. Lighweight Client Status

3. Wired Client Status

> **Note** You can refresh the data collection tasks (such as polling interval) from the Administration > Background Tasks page. For details, see the "Performing Background Tasks" section on page 15-15.

> **Note** NCS enables you to track clients and be notified when these clients connect to the network. For details, see the "Tracking Clients" section on page 10-30.

> **Note** For more information about enabling traps and syslogs on switches for wired client discovery, see the "Tracking Clients" section on page 10-30.

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administer can assign a username to a device. For details, see the "Configuring Unknown Devices" section on page 9-199.

If a client device is authenticated to the network through web auth, NCS may not have username information for the client.

client status is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.

- Disconnected clients—Clients that are disconnected from the wired switch.

- Unknown clients—Clients that are marked as unknown when the SNMP connection to the wired switch is lost.

Note   See the "Configuring Unknown Devices" section on page 9-199for more information about tracking clients.

NCS supports both Identity and non-identity wired clients. The support for wired clients is based on the Identity service. The identity service provides secure network access to users and devices and it also enables the network administrators to provision services and resources to the users based on their job functions.

This chapter describes the following sections:

- Client Dashlets on the General Dashboard, page 10-3
- Client Dashboard, page 10-3
- Monitoring Clients and Users, page 10-10
- Client Troubleshooting, page 10-20
- Tracking Clients, page 10-30
- Enabling Automatic Client Troubleshooting, page 10-32
- Client Details from Access Point Page, page 10-33
- Viewing Currently Associated Clients, page 10-33
- Running Client Reports, page 10-33
- Running ISE Reports, page 10-33
- Specifying Client Settings, page 10-33
- Receiving Radio Measurements for a Client, page 10-33
- Viewing Client V5 Statistics, page 10-35
- Viewing Client Operational Parameters, page 10-36
- Viewing Client Profiles, page 10-38
- Disabling a Current Client, page 10-38
- Removing a Current Client, page 10-39
- Enabling Mirror Mode, page 10-39
- Viewing a Map (High Resolution) of a Client Recent Location, page 10-39
- Viewing a Map (High Resolution) of a Client Current Location, page 10-39
- Running a Client Sessions Report for the Client, page 10-40
- Viewing a Roam Reason Report for the Client, page 10-40
- Viewing Detecting Access Point Details, page 10-41
- Viewing Client Location History, page 10-41
- Viewing Voice Metrics for a Client, page 10-41

Client Dashlets on the General Dashboard

Note The dashlets that you see on the dashboard are presented in the form of interactive graphs. See the "Interactive Graphs" section on page 9-230 for more information.

When you log into NCS, the General dashboard displays a few client-related dashlets.

- Client Count By Association/Authentication—Displays the total number of clients by Association and authentication in NCS over the selected period of time.
  - Associated client—All clients connected regardless of whether it is authenticated or not.
  - Authenticated client—All clients connected and passed authentication, authorization and other policies, and ready to use the network.
- Client Count By Wireless/Wired—Displays the total number of wired and wireless clients in NCS over the selected period of time.
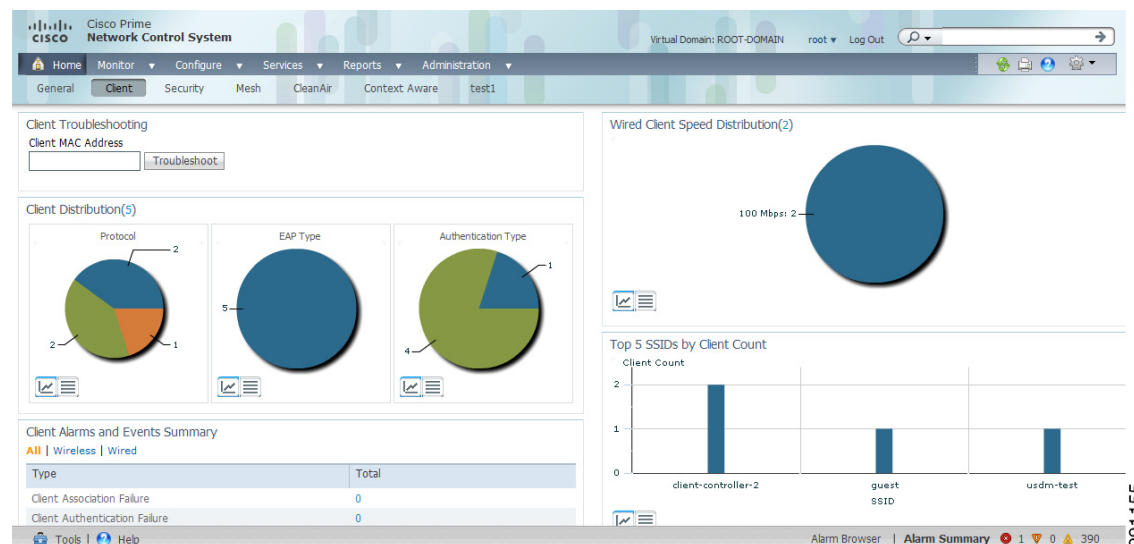
Client Dashboard

Note The dashlets that you see on the dashboard are presented in the form of interactive graphs. See the "Interactive Graphs" section on page 9-230 for more information.

The Client dashboard (see Figure 10-1) on the NCS home page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in the NCS database. On the other hand most of the information in Client Details page are polled directly from the controller/switch.

Figure 10-1   Client Dashboard

Click the **Edit Content** link to choose the dashlets you want to have appear on the Client dashboard. You can choose the dashlet from the Available dashlets list and then click to add it to the left or right column. For more information on using the Edit Content link, see the "Dashboards" section on page 2-13. For example, if you wanted to see the client count in both the General and Client dashboards, you could add the same dashlet to both.

To return to the original client dashboard before customization, click **Edit Tabs** and click **Reset to Factory Default**.

The client dashboard displays the following dashlets:

- Client Troubleshooting Dashlet, page 10-4
- Client Distribution Dashlet, page 10-4
- Client Alarms and Events Summary Dashlet, page 10-6
- Client Traffic Dashlet, page 10-7
- Wired Client Speed Distribution Dashlet, page 10-8
- Top 5 SSIDs by Client Count, page 10-9
- Top 5 Switches by Switch Count, page 10-9
- Client Posture Status Dashlet, page 10-9
- Client Posture Status Dashlet, page 10-9

Client Troubleshooting Dashlet

To troubleshoot a client, enter a client MAC address, and then click the **Troubleshoot** button (see Figure 10-2). The properties information appears.

Figure 10-2   Client Troubleshooting

> **Note**   If the client is not currently associated, most of the information will not appear.

For details about client troubleshooting see "Client Troubleshooting" section on page 10-20.

Client Distribution Dashlet

This dashlet (see Figure 10-3) shows how many clients are on your network presently. You can see how clients are distributed by protocol, EAP type, and authentication type.

- Protocol
    - 802.11—wireless client protocol
   - 802.3—wired client protocol.

Note   You can click a protocol to access the list of users belonging to that protocol. For example, if you click the 802.3 protocol, you can directly access the list of the wired clients and users in the Clients and Users page.

- EAP-Type—Represents Extensible Authentication Protocol (EAP) types such as EAP-FAST, PEAP, and so on

- Authentication Type—Represents types such as WPA (TKIP), WPA2 (AES), open, and so on

You can choose to display this information in table form or in a pie chart. The pie charts are clickable. If you hover your mouse cursor over a particular portion of the pie chart, a heading and percentage appears, and you can then click the pie chart piece to open a filtered list. When you click the number (next to the header 'Client Distribution') represented by Client Distribution, you get a list of clients represented by this number (the same page that you see when you choose Monitor > Clients and Users). You can filter the data that is displayed in client distribution by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

*Figure 10-3   Client Distribution*
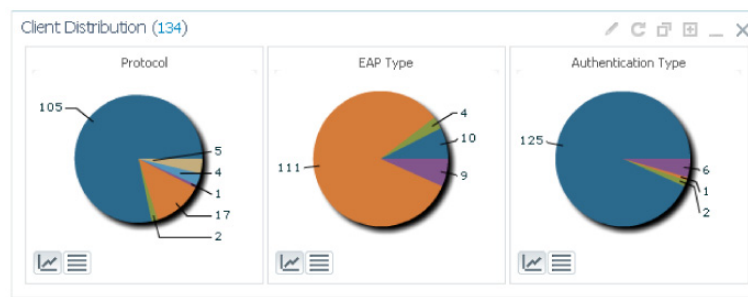
Note   The *Edited* label next to the Client Distribution count indicates that the dashlet has been customized. If you reset to the default page, the *Edited* label is cleared.

Client Authentication Type Distribution

This Client Authentication Type graph shows the number of clients for each authentication type (see Figure 10-4). You can choose to display this information in table form or in a pie chart. When you click the number represented by Total Clients, you get a list of clients represented by this number (the same page that you see when you choose Monitor > Clients and Users). You can filter the data that is displayed in client authentication type distribution by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

Figure 10-4   Client Authentication Type
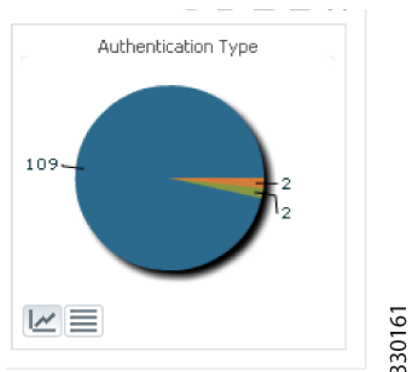
Client Alarms and Events Summary Dashlet

This dashlet (see Figure 10-5) shows the most recent client alarms of both wired and wireless clients.

- Client Association Failure
- Client Authentication Failure
- Client WEP Key Decryption Error
- Client WPA MIC Error Counter Activated
- Client Excluded
- Autonomous AP Client Authentication Failure
- Wired Client Authentication Failure
- Wired Client Authorization Failure
- Wired Client Critical VLAN Assigned
- Wired Client Auth fail VLAN Assigned
- Wired Client Guest VLAN Assigned
- Wired Client Security Violation

Note   For more information about the alarms and events, see the "Alarm and Event Dictionary" section on page 13-1.

Click the number in the Total column to open the Events page (the same page that you see when you choose Monitor > Events).

Figure 10-5   Client Alarms and Events Summary

Client Alarms and Events Summary
All | Wireless | Wired

Type	Total
Client Association Failure	0
Client Authentication Failure	0
Client WEP Key Decryption Error	0
Client WPA MIC Error Counter Activated	0
Client Excluded	0
Autonomous AP Client Authentication Failure	0
Wired Client Authentication Failure	0
Wired Client Authorization Failure	0
Wired Client Critical VLAN Assigned	0
Wired Client Auth fail VLAN Assigned	0
Wired Client Guest VLAN Assigned	0
Wired Client Security Violation	0
Radius Server not reachable	0

Client Traffic Dashlet

Controllers keep counters for the number of bytes transferred and received for each client. NCS reads the number every 15 minutes and then calculates the difference, comparing the prior polling. This client traffic data is then aggregated every hour, every day, and every week (see Figure 10-6). It shows the average and maximum values in megabytes per second for both downstream and upstream traffic. You can display the information in table form or in an area chart. When generating the chart based on the floor, NCS adds up all client traffic on this floor. You can filter the data that is displayed in client traffic by clicking the Dashlet Options icon and choosing either controller IP, SSID, or floor area.

For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes form ISE, and hence you need to enable accounting information and other necessary functions on switches.

Figure 10-6   Client Traffic
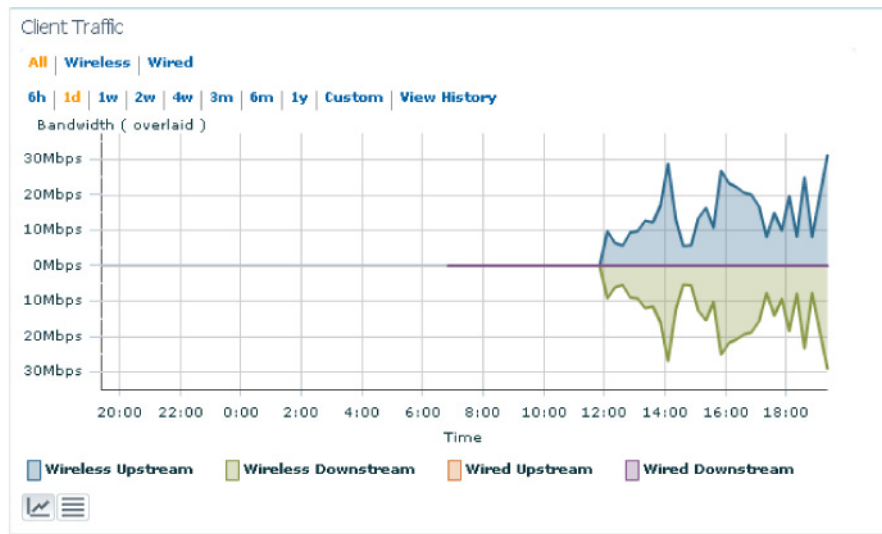
If you click **View History**, the Client Traffic Historical Charts dashlet appears for the various time frames. The Client Traffic Historical Charts dashlet shows the client traffic over the last 6 hours, last day, last week, last month, and last year. The blue line shows the authenticated client count and the orange line shows the associated client count. The upper right-hand corner shows when the chart was last updated.

Wired Client Speed Distribution Dashlet

This dashlet displays the wired client speeds and the client count for each speed. There are three different speeds on which clients run:

- 10 Mbps
- 100 Mbps
- 1 Gbps

Figure 10-7   Wired Client Speed Distribution
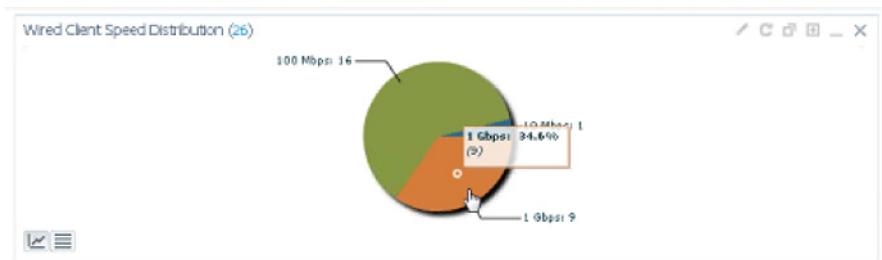
Note   Since ports are in Auto Negotiate mode (by default). For example, you will 100 Mbps speed for a client that runs in 100 Mbps speed.

Top 5 SSIDs by Client Count

This dashlet (see Figure 10-8) shows the count of currently associated and authenticated clients. You can choose to display the information in table form or in an area chart.

*Figure 10-8   Top 5 SSIDs by Client Count*

Note   In NCS 1.0, the WGB, Wired Guest, and OEAP 600 (Office Extended Access Point 600) are tracked as wireless clients.

Top 5 Switches by Switch Count

This dashlet (see Figure 10-9) displays the five switches that have the most clients as well as the number of clients associated to the switch.

*Figure 10-9   Top 5 Switches by Switch Count Dashlet*
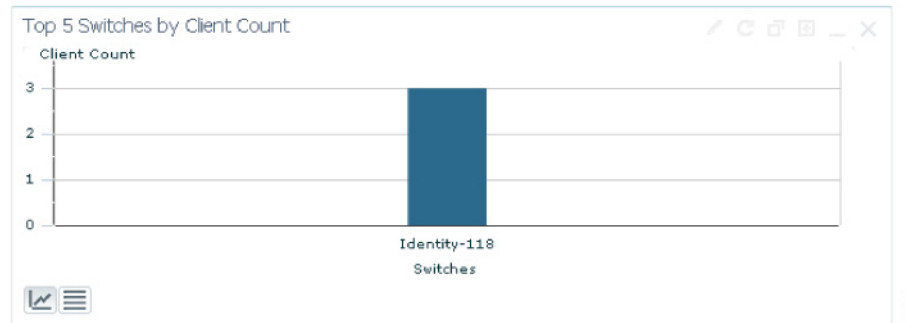
Client Posture Status Dashlet

NCS collects the posture status information from the Identity Services Engine (ISE). You need to add an ISE for authorization and authentication purpose. For information about adding ISE, see "Adding an Identity Services Engine" section on page 16-81. After you enable necessary functions in ISE, NCS shows the data in the Client Posture Status dashlet.

This dashlet (see Figure 10-10) displays the client posture status and the number of clients in each of the following status:

- Compliant

- Non-compliant

- Unknown

- Pending

- Not Applicable

- Error

Figure 10-10   Client Posture Status Dashlet
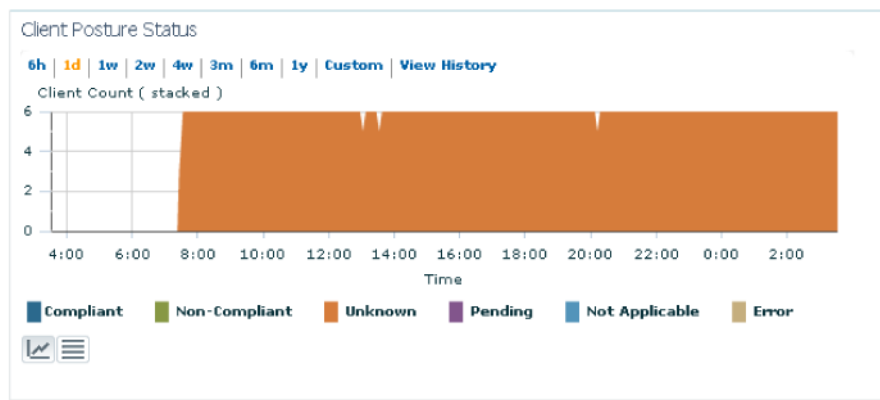
Monitoring Clients and Users

Using the Monitor Clients and Users feature, you can view all the clients in your network—both wired and wireless. In addition, you can view the client association history and statistical information. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information may help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage.

The Client Detail page shows the association history graph to represent the time-based data. The information will help you identify, diagnose, and resolve client issues.

Note   Some of the features mentioned in this chapter are not applicable for wired clients (for example, disabling or removing).

Choose **Monitor > Clients and Users** to view both wired and wireless clients information. The Clients and Users page appears. In the Clients and Users page, you see the clients in tabular format with different tools available at the top of the table.

This section contains the following topics:

Filtering Client and Users

When you navigate to the Clients and Users list page, all Associated Clients are displayed by default. There are 14 preset filters that allow you to view a subset of clients (see Table 10-1).

Note In NCS 1.0, the WGB, Wired Guest, and OEAP 600 (Office Extended Access Point 600) are tracked as wireless clients.

Table 10-1 lists the quick filters that are available on the Clients and Users page. Click the Show drop-down list to select the filter that you want to show.

Table 10-1   Client List Filters

Filter	Results
All	All clients including inactive
2.4GHz Clients	All clients using 2.4 GHz radio band
5GHz Clients	All clients using 5.0 GHz radio band
All Lightweight Clients	All clients connected to lightweight APs
All Autonomous Clients	All clients connected to autonomous APs
All Wired Clients	All clients directly connected to switch managed by NCS
Associated Clients	All clients connected regardless of whether it is authenticated or not
Clients detected by MSE	All clients detected by MSE including wired and wireless
Clients detected in last 24 hours	All clients detected in last 24 hours
Clients Known by ISE	Shows all the clients which are authenticated by ISE.
Clients with Problems	Clients which are associated, but have not completed policy.
Excluded Clients	All lightweight wireless clients being excluded by controller
H-REAP Locally Authenticated	Clients connected to H-REAP APs and authenticated locally
New Clients detected in last 24 hours	New Clients detected in last 24 hours

Table 10-1   Client List Filters

Filter	Results
On Network Clients	Clients which have gone through authentication/authorization and able to send and receive data. This means the clients that have completed all set policies and are on the network. The clients are not Identity clients, are always shown as 'On Network'.
WGB Clients	All WGB clients. **Note** If an access point is bridge capable, and the AP mode was set to Bridge, you can view clients identified as WGBs. WGB clients bridge wireless to wired. Any Cisco IOS access point can take on the role of a WGB, acting as a wireless client with a wired client connected to it. The information about this WGB is propagated to the controller and appears as a client in both NCS and WLC.

In addition, you can use the filter button ( ) to filter the records that match the filter rules. If you want to specify a filter rule, choose All from the Show drop-down list before you click .

Note   When you select a preset filter and click the filter button, the filter criteria is greyed out. You can only see the filter criteria but will not be able to change it. When the All option is selected to view all the entries, clicking the filter button shows the Quick Filter options, where you can filter the data using the filterable fields, there is also a free form text box, where you can enter text and filter the table.

Viewing Clients and Users

Note   You can use the advanced search feature to narrow the client list based on specific categories and filters. See the "Using the Search Feature" section on page 2-33 section or the "Advanced Search" section on page 2-34 for more information.
You can also filter the current list using the Show drop-down list. See the " Filtering Client and Users" section on page 10-11 for more information.

Note   See the "Configuring the Search Results Display" section on page 10-32 for other available client parameters. See the " Filtering Client and Users" section on page 10-11 for information on filtering this client list.

Note   To view complete details in the Monitor > Client and Users page and to perform operations such as Radio Measurement, users in User Defined groups need permission for Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location.

To view clients and users, follow these steps:

Step 1   Choose **Monitor > Clients and Users** to view both wired and wireless clients information. The Clients and Users page appears (see Figure 10-11).

Figure 10-11   Clients and Users

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click ⚙ ▾, and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere on a row, the row will be selected and the client details are shown.

The following are columns that are available to show in the Clients and Users table:

- IP Address—Client IP address.

- MAC Address—Client MAC address.

- User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.

- Type—Indicates the client type.
    - [icon] indicates a lightweight client
    - [icon] indicates a wired client
    - [icon] indicates an autonomous client

- Vendor—Device vendor derived from OUI.

- AP Name—Wireless only

- Device Name—Network authentication device name, for example, WLC, switch.

- Location—Map location of connected device.

- ISE—Yes/No. This column represents whether the client is authenticated using the ISE which is added to NCS.

- Endpoint Type—Endpoint type as reported by ISE, available only when ISE is added (for example, iPhone, iPad, Windows workstation).

- Posture—Latest client posture status

- SSID—Wireless only

- Profile Name—Wireless only

- VLAN——Indicates the access VLAN ID for this client.

- Status—Current client status

  - Idle—Normal operation; no rejections of client association requests.

  - Auth Pending—Completing an AAA transaction.

  - Authenticated—802.11 authentication complete.

  - Associated—802.11 association complete. This is also used by wired clients to represent that a client currently connected to the network.

  - Power Save—Client is in power save mode.

  - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.

  - To Be Deleted—The client will deleted after disassociation.

  - Excluded—Automatically disabled by system due to perceived security threat.

- Interface—Controller interface (wireless) or switch interface (wired) that client is connect to.

- Protocol

  - 802.11—wireless

  - 802.3—wired

- Speed—Ethernet port speed (wired only). Displays "N/A" for wireless

- Association Time—Last association start time (for wireless client). For a wired client, this is the time when client connected to a switch port. This is blank for a client which is associated by has problems being on the network.

- Session Length—Session length

- On Network—Shows Yes for the clients which are associated and successfully finished authentication, if required.

- Authentication Type—WPA, WPA2, 802.1x, MAC Auth Bypass, or Web Auth.

- Authorization Profile Names—Authorization profiles applied to this client by ISE. This contains data only when ISE is added and client is authenticated by ISE.

- Traffic (MB)—Traffic (transmitted/received) in this session in MB

- Average Session Throughput (kbps)—Average session throughput in kbps

- Automated Test Run—Indicates whether client is in auto test mode. This is applicable for wireless clients only.

- AP MAC Address—Wireless only

- AP IP Address—Wireless only

- Anchor Controller—Lightweight wireless only

- CCX—Lightweight wireless only

- Client Host Name—Wired and wireless. Result of DNS reverse lookup.

- Device IP Address—IP address of the connected device (WLC, switch or autonomous AP)

- Port—Switch port on WLC

- E2E—Lightweight wireless only

- Encryption Cipher—Wireless only
- MSE—MSE server managing this client
- RSSI—Wireless only
- SNR—Wireless only
- Session ID—Audit-session-ID used in ISE and switch
- Session Time—For active session, current time - session start time
- Vender Name—Vender name derived from OUI

Step 2 Select a client or user. The following information appears:

- Client Attributes
- Client Statistics

> **Note** Client Statistics shows the statistics information after the client details are shown.

- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCXv5 Information

The following attributes are populated only when ISE is added to NCS:

- ISE
- Endpoint Type
- Posture
- Authorization Profile Names

> **Note** NCS queries ISE for client authentication records for the last 24 hours to populate this data. If the client is connected to the network 24 hours before it is discovered in NCS, you may not see the ISE-related data in the table. You may see the data in client details page. To workaround this, reconnect the client to network. The ISE information is shown in the table after the next client background task run.

Client Attributes

When you select a client from the Clients and Users list, the client attributes appear under the Clients and Users list. Clients are identified using the MAC address.

> **Note** The details that appear in the client attribute group box are from the device, whereas the details that appear in the Clients and Users list are from the database. Therefore, there can some discrepancy on the details that appear on the Clients and Users list and the Client Attributes group box.

Note   For wired clients, the information comes from switch. Also, the data that appears in the details page is live data collected on demand from the controller/switch/ISE.

These details include the following client details:

- General—Lists the generation information such as User Name, MAC address, and so on.

    Note   Click the ⊕ icon next to the username to access the correlated users of a user.

- Session —Lists the client session information.
- Security (wireless and Identity wired clients only)—Lists Security policy, authentication information, and EAP type.

    Note   The identity clients are the clients whose authentication type will be 802.1x, MAC Auth Bypass or Web Auth. For non-identity clients, the authentication type will be N/A.

    Note   The data that appears under the client attributes differs based on identity and non-identity clients. For identity clients, you can see the security information such as Authentication status, Audit Session ID, and so on.

- Statistics (wireless only)
- Traffic—Shows the client traffic information.

    Note   For wireless clients, client traffic information comes from controller. For wired clients, the client traffic information comes form ISE, and hence you need to enable accounting information and other necessary functions on switches.

Client Statistics

The Statistics includes the following information for the selected client:

- Client AP Association History
- Client RSSI History (dBm)—History of RSSI (Received Signal Strength Indicator) as detected by the access point with which the client is associated.
- Client SNR History—History of SNR (signal-to-noise Ratio of the client RF session) as detected by the access point with which the client is associated
- Bytes Sent and Received (Kbps)—Bytes sent and received with the associated access point.
- Packets Sent and Received (per second)—Packets sent and received with the associated access point.
- Data rate over time

    Note   Hover your mouse cursor over points on the graph for additional statistical information.

> **Note** This information is presented in interactive graphs. See the "Interactive Graphs" section on page 9-230 for more information.

Client Association History

The Association History section displays information regarding the last ten association times for the selected client. This information can help in troubleshooting the client.

- Client Association History (for wireless clients) includes the following information:
  - Date and time of association
  - Duration of association
  - Username
  - IP address
  - Access point name
  - Controller name
  - SSID
  - Protocol
  - Amount of traffic (MB)
  - Hostname
  - Roam reason (such as *No longer seen from controller* or *New association detected*)
- Client Association History (for wired clients) includes the following information:
  - Date and time of association
  - Duration of association
  - Username
  - IP address
  - Access point and controller name
  - Map location
  - SSID
  - Protocol
  - Amount of traffic (MB)
  - Hostname
  - Roam reason (such as *No longer seen from controller* or *New association detected*)

> **Note** Click the **Edit View** link to add, remove or reorder columns in the Current Associated Clients table. See the "Configuring the List of Access Points Display" section on page 5-45 for adding a new parameters than can be added through Edit View.

Client Event Information

The Event section of the Client Details page displays all events for this client including the event type as well as the date and time of the event.

Click an event type to view its details. See the "Monitoring Failure Objects" section on page 5-144 for more information.

Client Location Information

The following location parameters appear (if available) for the selected client:

- Map Area—The map area in which the client was last located.
- ELIN—The Emergency Location Identification Number. This is applicable only to the wired clients that are located by MSE.
- Civic Address—The fields under the Civic Address tab is populated if a civic address is imported for a client. This is applicable only to the wired clients that are located by MSE.
- Advanced—Detailed information about the client. The fields under this tab is populated if a civic address is imported for a client.

For more information on the importing Civic information for the client, see "Configuring a Switch Location" section on page 9-196.

Wired Location History

You can view the Location History for wired clients.

📝

Note   The wired clients have to be located by MSE and the history for wired clients should be enabled on the MSE.

The following Location History information is displayed for a client:

- Timestamp
- State
- Port Type
- Slot
- Module
- Port
- User Name
- IP Address
- Switch IP
- Server Name
- Map Location
- Civic Location

Wireless Location History

You can view the Location History for wireless clients.

Note   The wireless clients have to be located by MSE and the history for wired clients should be enabled on the MSE.

Client CCXv5 Information

CCXv5 clients are client devices that support Cisco Compatible Extensions version 5 (CCXv5). Reports specific to CCXv5 clients provide client details that enhance client diagnostics and troubleshooting.

Note   The CCXv5 manufacturing information is displayed for CCXv5 clients only.

To view specific client details, perform a client search using the applicable search parameters. For more information on performing a client search, see the "Client CCXv5 Information" section on page 10-19 or the "Advanced Search" section on page 2-34.

CCXv5 information displays in the **Monitor Clients** > **Client Details** page. CCXv5 information includes the following:

CCXv5 Manufacturing Information:

- Organizationally Unique Identifier—The IEEE assigned organizational unique identifier, for example the first 3 bytes of the MAC address of the wireless network connected device.
- ID—The manufacturer identifier of the wireless network adapter.
- Model—Model of the wireless network adapter.
- Serial Number—Serial number of the wireless network adapter.
- Radio—Radio type of the client.
- MAC Address—MAC address assigned to the client.
- Antenna Type—Type of antenna connected to the wireless network adapter.
- Antenna Gain—The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

Note   Click **More** to view the following additional CCXv5 parameters.

Automated Troubleshooting Report—If the automated test runs, this report displays the location of automated troubleshooting log AUTO_TS_LOG<ClientMac>.txt. If no automated test runs, Not Exists appears.

- Click **Export** to save the .zip file. The file contains three logs: automated troubleshoot report, frame log, and watch list log.

Note   The **Settings** > **Client** page allows you to enable automatic client troubleshooting on a diagnostic channel. This feature is only available for Cisco Compatible Extension clients version 5. See the "Processing Diagnostic Trap" section on page 15-77 for more information.

Radio Receiver Sensitivity—Displays receiver sensitivity of the wireless network adapter including:

- Radio
- Data Rate
- Minimum and Maximum RSSI

CCXV5 Capability Information—Displays the Capability Information parameters for CCXv5 clients only.

- Radio
- Client Status—Success or failure.
- Service Capability—Service capabilities such as voice, streaming (uni-directional) video, interactive (bi-directional) video.

Radio Channels—Identifies the channels for each applicable radio.

Transmit Data Rates—Identifies the transmission data rates (Mbps) for each radio.

Transmit Power Values—Identifies the transmission power values including:

- Power mode
- Radio
- Power (dBm)

Client Troubleshooting

You can begin troubleshooting several ways: by entering a MAC address in the Client dashboard, by using the search function, or by selecting a row in the Monitor > Clients and Users page. Any method provides all the information necessary to troubleshoot historical client issues. You can monitor the status of the connection, verify the user's current and past locations, and troubleshoot client connectivity problems. You may want to use the client troubleshooting option if a user experiences repeated connectivity issues. The Client Details page shows SNR over time, RSSI over time, client reassociations, client reauthentications, and any RRM events. An administrator can correlate reassociations and reauthentications and determine if the problem was with the network or client.

> **Note** You can troubleshoot current client issues only. You cannot troubleshoot the historic client issues. However, for location assisted clients, you can find the location history.

> **Note** The client troubleshooting feature is available for identity wired clients only. This feature is not available for non-identity wired clients.

NCS 1.0 provides integrated management for wired and wireless devices or clients. You can monitor and troubleshoot both wired and wireless clients. SNMP is used to discover clients and collect client data. ISE is polled periodically to collect client statistics and other attributes to populate related dashboard dashlets and reports. If ISE is added to the systems and devices are authenticating to it, the Client Details page displays security information.

To launch the Client Troubleshooting tool, select a client, and then click the ![icon] icon indicated above the IP address that you want to troubleshoot. The Troubleshooting Client page appears.
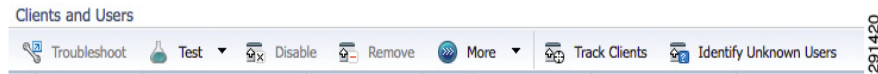
The troubleshooting page displays the following states for wired clients:

- Link Connectivity
- 802.1X Authentication
- MAC Authentication
- Web Authentication
- IP Connectivity
- Authorization
- Successful Connection

Note   The exact states displayed depends on the security used by the client.

The following are the security mechanisms used by clients:

- 802.1X
- MAC Authentication
- Web Authentication

Table 10-2 summarizes the validity of states against the security types. The states are arranged in the order the client goes through.

Table 10-2   Security Mechanisms

Security/Client State	Link Connectivity	802.1X Authentication	MAC Authentication	Web Authentication	IP Connectivity	Authorization
802.1X	X	X			X	X
MAC Authentication	X		X		X	X
Web Authentication	X			X	X	X

Table 10-3 provides the list of problems and suggested actions depending on the state in which a client failed:

Table 10-3   Client State, Problem, and Suggested Action

Client State	Problem	Suggested Action
Link Connectivity	Cannot find the client in network	• Check whether the client cable is plugged into the network • Check whether the client is using proper cable to connect to the network • Make sure that the port to which client is connected is not disabled administratively. • Make sure that the port to which client is connected is not error disabled. • Check whether the speed and duplex are set to Auto on the port to which client is connected.

	Authentication in progress	• Wait for some time and check the status again.
		• If the client is in this state from a long time, check the following:
		  – Check whether the supplicant on the client is configured properly as required.
		  – Modify the timers related to authentication method and try.
		  – If you are not sure which authentication method will work with the client, use the fall back authentication feature.
		  – Try disconnecting and reconnecting.

802.1X Authentication	802.1X Authentication Failure	• Check whether Radius Server(s) is reachable from the switch. • Check whether client choice of EAP is supported by Radius Server(s). • Check client's username/password/certificate is valid. • See whether the certificates used by Radius server are accepted by the client.
MAC Authentication	MAC Authentication Failure	• Check whether Radius Server(s) is reachable from the switch. • Check whether the client's MAC address is in known client's list on the Radius Server. • Check whether the client's MAC address is not in excluded client's list.

Table 10-3   Client State, Problem, and Suggested Action (continued)

Client State	Problem	Suggested Action

Web Authentication	Client could not be authenticated through web/guest interface	• Check that the guest credentials are valid and not expired
		• Check whether client is able to get redirected to login page
		• Check whether radius server is reachable.
		• Check whether pop-ups are not blocked.
		• If not getting redirected then
		   – Check DNS resolution on client is working.
		   – Check that client is not using any proxy settings.
		   – Check whether the client can access https://<virtual-ip>/login.html
		• Check whether client's browser accepts the self signed certificate offered by controller

IP Connectivity	Client could not complete DHCP interaction	• Check whether the DHCP server is reachable. • Check whether DHCP server is configured to serve the WLAN. • Check whether DHCP scope is exhausted. • Check whether multiple DHCP servers are configured with overlapping scopes. • Check local DHCP server is present if DHCP bridging mode enabled (move it to second) client is configured to get address from DHCP server • Check if client has static IP configured and ensure client generates IP traffic
Authorization	Authorization Failure	• Check that the VLAN defined for authorization is available on the switch • Check that default port ACL is configured for ACL authorization
Successful Connection	None	None

Using the Search Feature to Troubleshoot Clients

Client search is the primary method for you to locate clients. For a detailed description of the search feature, see to the "Using the Search Feature" section on page 2-33.

To troubleshoot a client using the search feature, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2 Type the full or partial client MAC address in the advanced search field, and click **Search**. The Search Results page appears.

Step 3 Click **View List** to see the clients that matched the search criteria in the Clients page. The Monitor > Clients and Users page appears (see Figure 10-12).

Figure 10-12 *Client and Users*
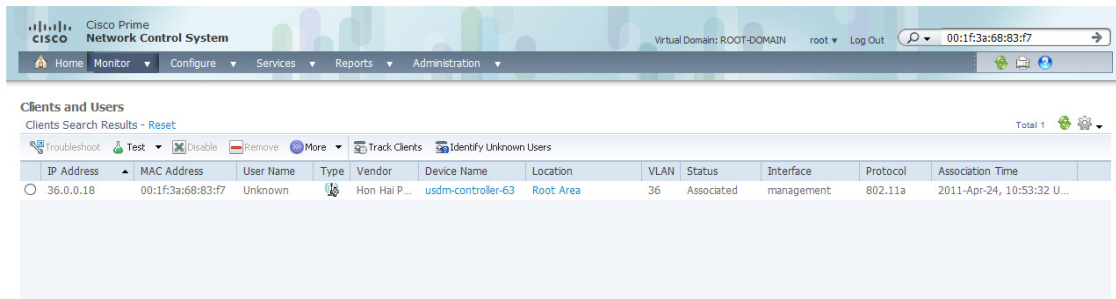
Note You can click the Reset link to set the table to the default display so that the search criteria is no longer applied.

Step 4 Select a client, and then click the icon indicated above the IP address that you want to troubleshoot. The Troubleshooting Client page appears (see Figure 10-13). If you are troubleshooting a Cisco Compatible Extension v5 client (wireless), your Troubleshooting Client page has additional tabs.
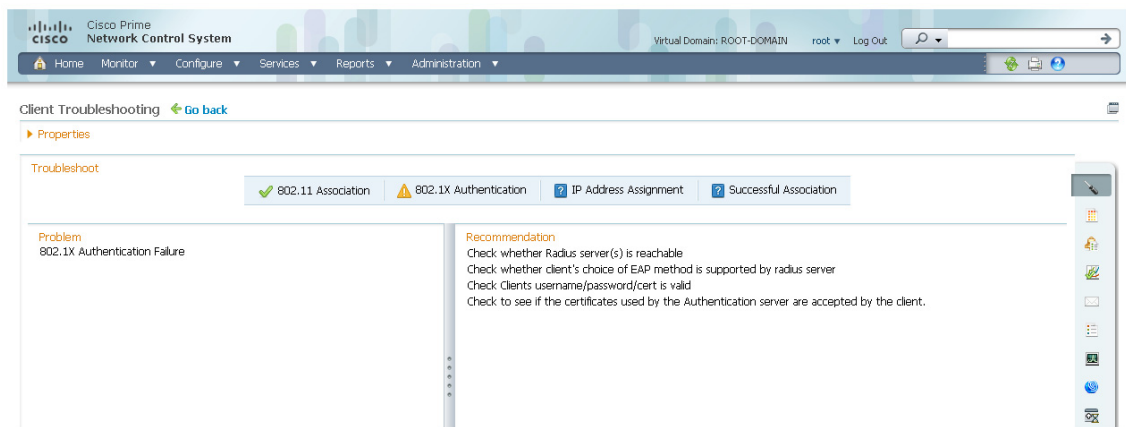
Note If you receive a message that the client does not seem to be connected to any access point, you must reconnect the client and click **Refresh**.

Note You can use the detach/clone icon located in the top right corner of the page to detach the current page into a new window/tab.

Figure 10-13 *Troubleshooting Client Page*

> **Note** Click **Go back** to return to the page from where you launched client troubleshooting. For example, if you have launched client troubleshooting from the list page, you can return to the list page.

The summary page briefly describes the problem and recommends a course of action.

> **Note** Some Cisco Compatible Extension features do not function properly when you use a web browser other than Mozilla Firefox 3.6 or later or Internet Explorer 7.0 or later on a Windows workstation.

Step 5 To view log messages logged against the client, click the **Log Analysis** tab (see Figure 10-14).

Step 6 To begin capturing log messages about the client from the controller, click **Start**. To stop log message capture, click **Stop**. To clear all log messages, click **Clear**.

> **Note** Log messages are captured for ten minutes and then stopped automatically. You must click **Start** to continue.

Step 7 To select log messages to display, click one of the links under Select Log Messages (the number between parentheses indicates the number of messages). The messages appear in the box. The message includes the following information:

- A status message
- The controller time
- A severity level of info or error (errors are displayed in red)
- The controller to which the client is connected

Figure 10-14   Log Analysis

**Step 8** To display a summary of the client's event history, click the **Event History** tab (see Figure 10-15).

Event History provides messages related to connectivity events for this client. In this example (see Figure 10-15), the client failed to successfully authenticate. Date/time is provided to assist the network administrator in troubleshooting this client.

Figure 10-15   Event History Tab

Step 9   To view the event log, click the **Event Log** tab (see Figure 10-16). Click **Start** to begin capturing log messages from the Client. When a sufficient number of messages have been collected, click **Stop**.

Figure 10-16   Event Log
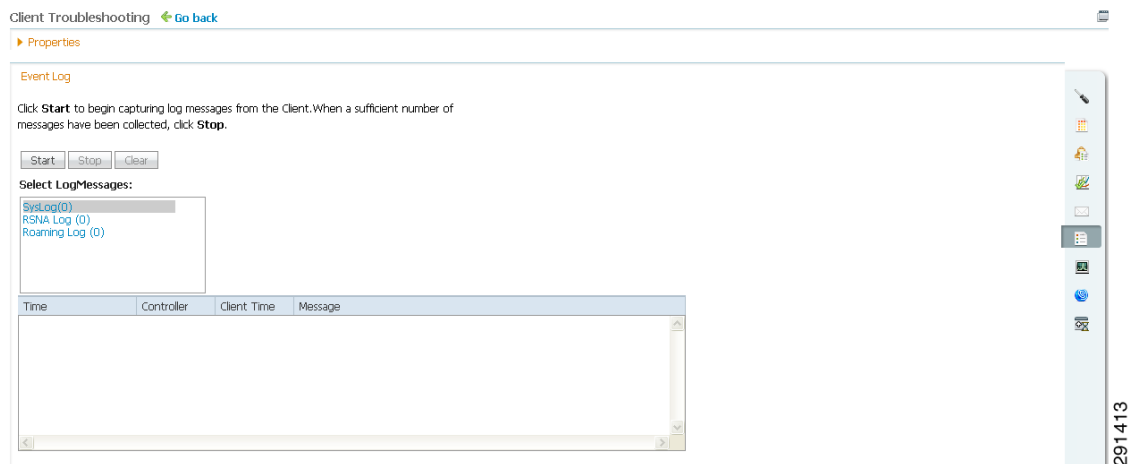
Step 10   If you click the ACS View Server tab, you can interact with the Cisco Access Control (ACS) System View Server. This tab displays the latest authentication records received either from ACS View server or Identity Services Engine (ISE), whichever is configured in NCS. You must have View Server credentials established before you can access this tab. (The tab will show the server list as empty if no view servers are configured.) See the "Configuring ACS View Server Credentials" section on page 9-229 for steps on establishing credentials.

If the ACS View Server is already configured, you can select a time range and click **Submit** to retrieve the authentication records from ACS View Server. NCS uses the ACS View NS API to retrieve the records.

Step 11   You can click the Identity Services Engine tab to view information about the ISE authentication. Enter the date and time ranges to retrieve the historical authentication and authorization information and click **Submit**. The results of the query are displayed in the Authentication Records portion of the page.

Step 12   You can click the CleanAir tab to view information about the air quality parameters and the active interferers for the CleanAir enabled access point. This tab provides the following information about the air quality detected by the CleanAir enabled access point.

- AP Name—Click to view the access point details. See the "Monitoring Access Points Details" section on page 5-56 for more information.

- AP MAC Address

- Radio

- CleanAir Capable—Indicates if the access point is CleanAir Capable.

- CleanAir Enabled—Indicates if CleanAir is enabled on this access point.

- Admin Status—Enabled or disabled.

- Operational Status—Displays the operational status of the Cisco Radios (Up or Down).

- Channel—The channel upon which the Cisco Radio is broadcasting.

- Extension Channel—Indicates the secondary channel on which Cisco radio is broadcasting.

- Channel Width—Indicates the channel bandwidth for this radio interface. See the "Configuring 802.11a/n RRM Dynamic Channel Allocation" section on page 9-121 for more information on configuring channel bandwidth.

- Power Level—Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.

- The power levels and available channels are defined by the Country Code setting, and are regulated on a country by country basis.

- Average AQ Index—Average air quality index.

- Minimum AQ Index—Minimum air quality index.

The following information about the active interferers is displayed:

- Interferer Name—The name of the interfering device.

- Affected Channels—The channel the interfering device is affecting.

- Detected Time—The time at which the interference was detected.

- Severity—The severity index of the interfering device.

- Duty Cycle(%)—The duty cycle (in percentage) of the interfering device.

- RSSI(dBm)—The Received Signal Strength Indicator of the interfering device.

- Click **CleanAir Details** to know more about the air quality index.

Step 13   (Optional) If Cisco Compatible Extension Version 5 clients are available, you can click a Test Analysis tab as shown in Figure 10-17.

Figure 10-17   Test Analysis Tab

The Test Analysis tab allows you to run a variety of diagnostic tests on the client. Select the check box for the applicable diagnostic test, enter any appropriate input information and click **Start**. The following diagnostic tests are available:

- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and the client.

- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to verify that IP connectivity exists on the local subnet.

- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to verify that IP connectivity exists to the DNS server.

- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to verify that name resolution is functioning correctly.

- 802.11 Association—Directs an association to be completed with a specific access point to verify that the client is able to associate properly with a designated WLAN.

- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to verify that the client is able to properly complete an 802.1x authentication.

- Profile Redirect—At any time, the diagnostic system may direct the client to activate one of the client's configured WLAN profiles and to continue operation under that profile.

Note   To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as an input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and to associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired).

Step 14   (Optional) If Cisco Compatible Extension Version 5 clients are available, a Messaging tab as shown in Figure 10-18 appears. Use this tab to send an instant text message to the user of this client. From the Message Category drop-down list, choose a message and click **Send**.

Figure 10-18   Messaging Tab
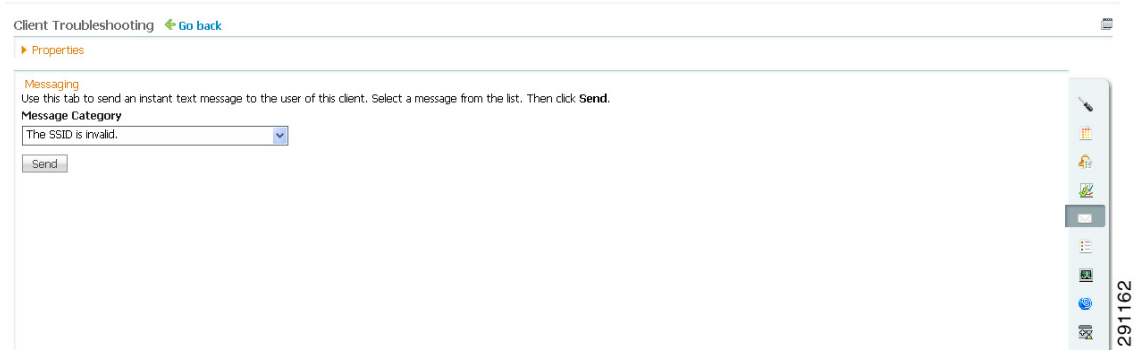
Step 15 You can click the **Identity Services Engine** tab to view information about the identity services parameters. You must have Identity Services Engine (ISE) configured before you can access this tab. (The tab will show the server list as empty if no ISEs are configured.)

> **Note** If ISE is not configured it provides a link to add an ISE to NCS.

ISE provides authentication records to NCS via REST API. Network administrator can choose time period for retrieving authentication records from ISE (see Figure 10-19).

Figure 10-19   Identity Services Engine Tab
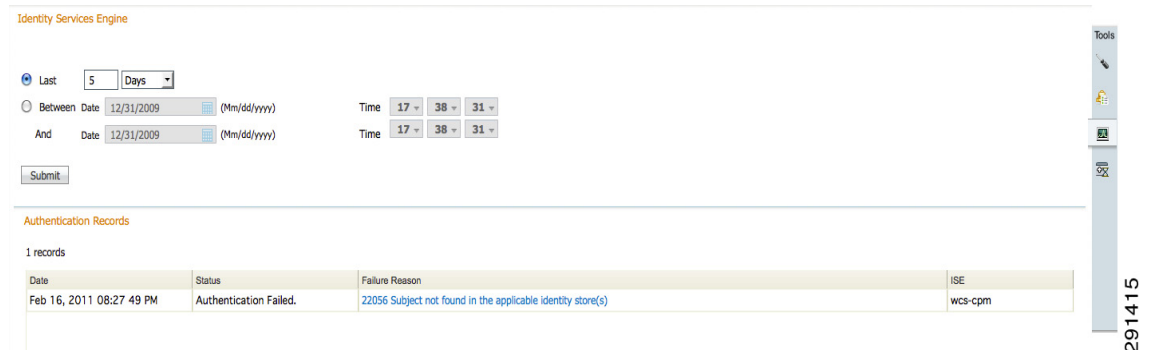
Step 16 To view the client location history, click the **Context Aware History** tab (see Figure 10-20).

Figure 10-20   Identity Services Engine Tab

Step 17   Close the Troubleshooting Client page.

Tracking Clients

This feature enables you to track clients and be notified when these clients connect to the network.

To track clients, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Click **Track Clients**. The Track Clients dialog box appears listing the currently tracked clients.

Tip   This table supports a maximum of 2000 rows. To add or import new rows, you must first remove some older entries.

Step 3   To track a single client, click **Add**, and then enter the following parameters

- Client MAC address
- Expiration—Choose Never or enter a date.

Step 4   To track multiple clients, click **Import**. This allows you to import a client list from a CSV file. Enter MAC Address and username.

A sample csv file can be downloaded that provides data format.

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

Notification Settings

To specify notification settings for the tracked clients, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Click **Track Clients**. The Track Clients dialog box appears listing the currently tracked clients.

Step 3   Select the tracked client(s) for which you want to specify notification settings.

Step 4   Specify the notification settings. There are three options for notifications:

    a. Purged Expired Entries—you can set duration to keep tracked clients in NCS database. Clients can be purged:

- after 1 week
- after 2 weeks
- after 1 month
- after 2 months
- after 6 months
- kept indefinitely

    b. Notification Frequency—you can specify when NCS sends notification of tracked client:

- on first detection
- on every detection

    c. Notification Method—you can specify for tracked client event to generate alarm or send email.

Step 5   Click **Save**.

Identifying Unknown Users

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administer can assign a username to a device.

If a client device is authenticated to the network through web auth, NCS may not have username information for the client.

Clients are marked as unknown when the NMSP connection to the wired switch is lost. A client status is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.

To view the unknown devices, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Click **Identify Unknown Users**.

Step 3   Click **Add** to assign client MAC addresses to username.

Step 4   Enter MAC Address and username.

> ✎
>
> **Note**   Once a client and MAC address has been added, NCS uses this data for client lookup based on matching MAC address.

Step 5   Click **Add**.

Step 6 Repeat Step 3 to Step 5 for each client that you want to enter MAC Address and its corresponding username.

Step 7 Click **Save**.

> **Note** This table supports a maximum of 10000 rows. To add or import new rows, you must first remove some older entries.

Configuring the Search Results Display

The **Edit View** page allows you to add, remove, or reorder columns in the clients table.

To edit the available columns in the clients table, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Click the **Edit View** link.

Step 3 To add an additional column to the clients table, click to highlight the column heading in the left column. Click **Show** to move the heading to the right column. All items in the right column are displayed in the clients table.

Step 4 To remove a column from the clients table, click to highlight the column heading in the right column. Click **Hide** to move the heading to the left column. All items in the left column are not displayed in the clients table.

Step 5 Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

> **Note** Additional client parameters include: AP MAC Address, Anchor Controller, Authenticated, CCX, Client Host Name, Controller IP Address, Controller Port, E2E, Encryption Cipher, MSE, RSSI, SNR, and H-REAP Local Authentication.

Enabling Automatic Client Troubleshooting

In the Settings > Client page, you can enable automatic client troubleshooting on a diagnostic channel. This feature is available only for Cisco Compatible Extension clients version 5.

To enable automatic client troubleshooting, follow these steps:

Step 1 Choose **Administration > Settings**.

Step 2 From the left sidebar menu, choose **Client**.

Step 3 Select the **Automatically troubleshoot client on diagnostic channel** check box.

> **Note**   When the check box is selected, NCS processes the diagnostic association trap. When it is not
> selected, NCS raises the trap, but automated troubleshooting is not initiated.

Step 4   Click **Save**.

Client Details from Access Point Page

You can also view the client information from the access point page. Choose **Monitor > Access Points**.
Click an access point URL from the column to see details about that access point. Click the **Current
Associated Clients** tab.

Viewing Currently Associated Clients

You can also view the currently associated clients (wired) from the switch details page. Choose **Monitor
> Controllers**, select an IP address, and choose **Clients > Current Associated Clients** from the left
sidebar menu. For details see

Running Client Reports

You can run client reports such as busiest clients, client count, client sessions, client summary,
throughput, unique clients and v5 clients statistics from the Report Launch pad. See the "Creating and
Running a New Report" section on page 14-6.

Running ISE Reports

You can also launch ISE reports from the Report Launch pad. See the "Creating and Running a New
Report" section on page 14-6. For more information about running the ISE reports, see the ISE online
help.

Specifying Client Settings

The Administration > Settings > Client page allows you to specify various client settings. For details,
see "Configuring Clients" section on page 15-76.

Receiving Radio Measurements for a Client

In the client page, you can receive radio measurements only if the client is Cisco Compatible Extensions
v2 (or higher) and is in the associated state (with a valid IP address). If the client is busy when asked to
do the measurement, it determines whether to honor the measurement or not. If it declines to make the
measurement, it shows no data from the client.

To receive radio measurements, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

> ✎
>
> **Note**   You can also perform a search for a specific client using the NCS Search feature. See the "Using the Search Feature" section on page 2-33 or the "Advanced Search" section on page 2-34 for more information.

Step 3   From the **Test** drop-down list, choose **Radio Measurement**.

> ✎
>
> **Note**   The Radio Measurement option only appears if the client is Cisco Compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address).

Step 4   Select the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram.

Step 5   Click **Initiate**. The different measurements produce differing results. See the "Radio Measurement Results for a Client" section on page 10-34 for more information.

> ✎
>
> **Note**   The measurements take about 5 milliseconds to perform. A message from NCS indicates the progress. If the client chooses not to perform the measurement, that will also be communicated.

Radio Measurement Results for a Client

Depending on the measurement type requested, the following information may appear:

- Beacon Response
    - Channel—The channel number for this measurement
    - BSSID—6-byte BSSID of the station that sent the beacon or probe response
    - PHY—Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP)
    - Received Signal Power—The strength of the beacon or probe response frame in dBm
    - Parent TSF—The lower 4 bytes of serving access point TSF value
    - Target TSF—The 8-byte TSF value contained in the beacon or probe response
    - Beacon Interval—The 2-byte beacon interval in the received beacon or probe response
    - Capability information—As found in the beacon or probe response
- Frame Measurement
    - Channel—Channel number for this measurement
    - BSSID—BSSID contained in the MAC header of the data frames received
    - Number of frames—Number of frames received from the transmit address
    - Received Signal Power—The signal strength of 802.11 frames in dBm

- Channel Load
    - Channel—The channel number for this measurement
    - CCA busy fraction—The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration)
- Noise Histogram
    - Channel—The channel number for this measurement
    - RPI density in each of the eight power ranges

Viewing Client V5 Statistics

To access the Statistics request page, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the **Test** drop-down list, choose **V5 Statistics**.

> ✎
> **Note**   This menu will be shown only for CCX v5 and later clients.

Step 4   Click **Go**.

Step 5   Select the desired type of stats (Dot11 Measurement or Security Measurement).

Step 6   Click **Initiate** to initiate the measurements.

> ✎
> **Note**   The duration of measurement is five seconds.

Step 7   Depending on the V5 Statistics request type, the following counters are displayed in the results page:

- Dot11 Measurement
    - Transmitted Fragment Count
    - Multicast Transmitted Frame Count
    - Failed Count
    - Retry Count
    - Multiple Retry Count
    - Frame Duplicate Count
    - Rts Success Count
    - Rts Failure Count
    - Ack Failure Count
    - Received Fragment Count
    - Multicast Received Frame Count
    - FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.

- – Transmitted Frame Count
- Security
  - – Pairwise Cipher
  - – Tkip ICV Errors
  - – Tkip Local Mic Failures
  - – Tkip Replays
  - – Ccmp Replays
  - – Ccmp Decryp Errors
  - – Mgmt Stats Tkip ICV Errors
  - – Mgmt Stats Tkip Local Mic Failures
  - – Mgmt Stats Tkip Replays
  - – Mgmt Stats Ccmp Replays
  - – Mgmt Stats Ccmp Decrypt Errors
  - – Mgmt Stats Tkip MHDR Errors
  - – Mgmt Stats Ccmp MHDR Errors
  - – Mgmt Stats Broadcast Disassociate Count
  - – Mgmt Stats Broadcast Deauthenticate Count
  - – Mgmt Stats Broadcast Action Frame Count

Viewing Client Operational Parameters

To view specific client operational parameters, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the **Test** drop-down list, choose **Operational Parameters**.

The following information is displayed:

Operational Parameters:

- Device Name—User-defined name for device.
- Client Type—Client type can be any of the following:
  - – laptop(0)
  - – pc(1)
  - – pda(2)
  - – dot11mobilephone(3)
  - – dualmodephone(4)
  - – wgb(5)
  - – scanner(6)

- tabletpc(7)

- printer(8)

- projector(9)

- videoconfsystem(10)

- camera(11)

- gamingsystem(12)

- dot11deskphone(13)

- cashregister(14)

- radiotag(15)

- rfidsensor(16)

- server(17)

- Transmit Power Mode—Power mode of the client.

- Data Rate—Data rates that the client will use for transmissions.

- SSID—SSID being used by the client.

- IP Address—IP address assigned to the client.

- Subnet Mask—The mask for the IP address assigned to the client.

- Default Gateway—The default gateway chosen for the client.

- Operating System—Identifies the operating system that is using the wireless network adaptor.

- Operating System Version—Identifies the version of the operating system that is using the wireless network adaptor.

- WNA Firmware Version—Version of the firmware currently installed on the client.

- Enterprise Phone Number—Enterprise phone number for the client.

- Cell Phone Number—Cell phone number for the client.

- Power Save Mode—Will display any of the following power save modes: awake, normal, or maxPower.

Radio Information:

- Radio Type—The following radio types are available:

    - unused(0)

    - fhss(1)

    - dsss(2)

    - irbaseband(3)

    - ofdm(4)

    - hrdss(5)

    - erp(6)

- Radio Channel—Radio channel in use.

DNS/WNS Information:

- DNS Servers—IP address for DNS server.

- WNS Servers—IP address for WNS server.

Security Information:

- Credential Type—Indicates how the credentials are configured for the client.
- Authentication Method—Method of authentication used by the client.
- EAP Method—Method of Extensible Authentication Protocol (EAP) used by the client.
- Encryption Method—Encryption method used by the client.
- Key Management Method—Key management method used by the client.

Viewing Client Profiles

To view specific client profile information, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the **More** drop-down list, choose **Profiles**.

The following information is displayed:

- Profile Name—List of profile names as hyperlinks. Click to display the profile details.
- SSID—SSID of the WLAN to which the client is associated.

Disabling a Current Client

To disable a current client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client that you want to disable.

Step 3 Click **Disable**. The Disable Client page appears.

Step 4 Enter a description in the Description text box.

Step 5 Click **OK**.

Note Once a client is disabled, it cannot join any network/ssid on controller(s). To re-enable the client, choose Configure > Controllers > *IP Address* > Security > Manually Disabled Clients, and remove the client entry from there.

Removing a Current Client

To remove a current client, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client that you want to remove.

Step 3   Choose **Remove**.

Step 4   Click **Remove** to confirm the deletion.

Enabling Mirror Mode

When enabled, mirror mode enables you to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point.

> **Note**   Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port as any connections to this port become unresponsive.

To enable mirror mode, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the More drop-down list, choose **Enable Mirror Mode**.

Step 4   Click **Go**.

Viewing a Map (High Resolution) of a Client Recent Location

To display a high-resolution map of the client recent location, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the More drop-down list, choose **Recent Map (High Resolution)**.

Step 4   Click **Go**.

Viewing a Map (High Resolution) of a Client Current Location

To display a high-resolution map of the client present location, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Present Map (High Resolution)**.

Step 4 Click **Go**.

Running a Client Sessions Report for the Client

To view the most recent client session report results for this client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Client Sessions Report**.

Step 4 Click **Go**. The Client Session report details display. See the for more information.

Viewing a Roam Reason Report for the Client

To view the most recent roam report for this client, follow these steps:

Step 1 Choose **Monitor > Clients and Users**.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list, choose **Roam Reason**.

Step 4 Click **Go**.

This page displays the most recent roam report for the client. Each roam report has the following information:

- New AP MAC address
- Old (previous) AP MAC address
- Previous AP SSID
- Previous AP channel
- Transition time—Time that it took the client to associate to a new access point.
- Roam reason—Reason for the client roam.

Viewing Detecting Access Point Details

To display details of access points that can hear the client including at which signal strength/SNR, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the More drop-down list, choose **Detecting APs**.

Step 4   Click **Go**.

Viewing Client Location History

To display the history of the client location based on RF fingerprinting, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the More drop-down list, choose **Location History**.

Step 4   Click **Go**.

Viewing Voice Metrics for a Client

To view traffic stream metrics for this client, follow these steps:

Step 1   Choose **Monitor > Clients and Users**.

Step 2   Choose a client from the Client Username column.

Step 3   From the More drop-down list, choose **Voice Metrics**.

Step 4   Click **Go**.

The following information appears:

- Time—Time that the statistics were gathered from the access point(s).
- QoS
- AP Ethernet MAC
- Radio
- % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.

- Avg Queuing Delay (ms) (Uplink)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.

- % Packets > 40 ms Queuing Delay (Downlink)——Percentage of queuing delay packets greater than 40 ms.

- % Packets 20ms—40ms Queuing Delay (Downlink)—Percentage of queuing delay packets greater than 20 ms.

- Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.