Configuring Controller and AP Settings

This chapter contains the following topics:

Configuring SNMP Credentials for Rogue AP Tracing

The SNMP Credentials page allows you to specify credentials to use for tracing rogue access points. Use this option when you cannot find a specific entry using a number-based entry. When a switch credential is not added to Prime Infrastructure, you can use SNMP credentials on this page to connect to the switch.

To configure SNMP credentials:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **SNMP Credentials**. The SNMP Credentials page appears.

Step 3 To view or edit details about a current SNMP entry, click the **Network Address** link. See the "Configuring Global SNMP Settings" section on page 2-6 for more information.

Note The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. The default community string is *private* for both read and write. You should update the prepopulated SNMP credential with your own SNMP information.

Step 4 To add a new SNMP entry, choose **Add SNMP Entries** from the **Select a command** drop-down list, then click **Go**. See the "Adding a New SNMP Credential Entry" section on page 2-9 for more information.

Configuring Protocols for CLI Sessions

Many Prime Infrastructure wireless features, such as autonomous access point and controller command-line interface (CLI) templates and migration templates, require executing CLI commands on the autonomous access point or controller. These CLI commands can be entered by establishing Telnet or SSH sessions. The CLI session page allows you to select the session protocol. SSH is the default.

Note In CLI templates, you are not required to answer the question responses (such as *Yes* or *No* answer to a command, *Press enter to continue*, and so on.). This is automatically performed by Prime Infrastructure.

To configure the protocols for CLI sessions:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **CLI Session**.

Step 3 The default controller session protocol SSH is selected. To choose Telnet, select that radio button.

Step 4 The default autonomous access point session protocol SSH is selected. To choose Telnet, select the radio button.

Step 5 The **Run Autonomous AP Migration Analysis on discovery** radio button is set to **No** by default. Choose **Yes** if you want to discover the autonomous APs as well as perform migration analysis, then click **Save**.

Refreshing Controllers After an Upgrade

The Controller Upgrade Settings page allows you to auto-refresh after a controller upgrade so that it automatically restores the configuration whenever there is a change in the controller image. To perform an auto-refresh:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Controller Upgrade Settings**.

Step 3 Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.

Step 4 Determine the action Prime Infrastructure takes when a save config trap is received. When this check box is enabled, you can choose to retain or delete the extra configurations present on the device but not on Prime Infrastructure. The setting is applied to all controllers managed by Prime Infrastructure.

If you select the Auto Refresh on Save Config Trap check box in the Configure > Controllers > Properties > Settings page, it overrides this global setting.

It might take up to three minutes for the automatic refresh to occur.

Step 5 Click **Save**.

Whenever a save config trap is received by Prime Infrastructure, this check box is selected. When this check box is enabled, it determines the action taken by Prime Infrastructure.

When this check box is enabled, the user can choose to retain or delete the extra configurations present on the device and not on Prime Infrastructure.

This setting is applied to all of the controllers managed by Prime Infrastructure. The setting in the Controllers > Properties page for processing the save config trap overrides this global setting.

When there is a change in the controller image, the configuration from the controller is automatically restored.

Tracking Switch Ports to Rogue APs

The **Administration > System Settings > Rogue AP Settings** page allows you to enable Prime Infrastructure to automatically identify the network switch port to which each rogue access point is connected.

To configure rogue AP auto trace:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Rogue AP Settings**. The Rogue AP Settings page appears.

Step 3 Select the **Enable Auto Switch Port Tracing** check box to allow Prime Infrastructure to automatically trace the switch ports to which rogue access points are connected. Then specify the parameters for auto port tracing, including:

- How long to wait between rogue AP-to-port traces (in minutes)
- Whether to trace Found On Wire rogue APs
- Which severities to include (Critical, Major, or Minor).

Step 4 Select the **Enable Auto Containment** check box to allow Prime Infrastructure to automatically contain rogue APs by severity. Then specify the parameters for auto containment, including:

- Whether to exclude Found On Wire rogue APs detected by port tracing
- Which severities to include in the containment (Critical, Major).
- The containment level (up to 4 APs).

Step 5 Click **OK**

Configuring Switch Port Tracing

Currently, Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, Prime Infrastructure gathers the information received from the controllers. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in Prime Infrastructure log and only for rogue access points, not rogue clients.

A rogue client connected to the rogue access point information is used to track the switch port to which the rogue access point is connected in the network.

If you try to set tracing for a friendly or deleted rogue, a warning message appears.

For Switch Port Tracing to successfully trace the switch ports using v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

See the "Configuring Switch Port Tracing" section on page 7-4 for information on configuring Switch Port Tracing settings.

The Switch Port Trace page allows you to run a trace on detected rogue access points on the wire.

To correctly trace and contain rogue access points, you must correctly provide the following information:

- Reporting APs—A rogue access point has to be reported by one or more managed access points.
- AP CDP Neighbor—Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials—All switches to be traced must have a management IP address and SNMP management enabled. You can add network address based entries instead of only adding individual switches. The correct write community string must be specified to enable/disable switch ports. For tracing, read community strings are sufficient.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be disabled.
- Only Cisco Ethernet switches are supported.
- Switch VLAN settings must be properly configured.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- You should have some traffic between rogue access points and the Ethernet switch.
- The rogue access point must be connected to a switch within the max hop limit. The default hop count is 2, and the maximum is 10.
- If SNMPv3 is chosen, use the context option and create one for each VLAN, in addition to the one for the main group (which is required for non-VLAN-based MIBs).

Step 1 Choose **Administration > System Settings > Switch Port Trace**.

Step 2 Configure the following basic settings:

- MAC address +1/-1 search—Select the check box to enable.

  This search involves the MAC address +1/-1 convention where the wired-side MAC address of the rogue access point is obtained by adding or subtracting the radio MAC address by one.

- Rogue client MAC address search—Select the check box to enable.

  When a rogue access point client exists, the MAC address of the client is added to the searchable MAC address list.

- Vendor (OUI) search—Select the check box to enable. OUI refers to Organizational Unique Identifier search which searches the first three bytes in a MAC address.
- Exclude switch trunk ports—Select the check box to exclude switch trunk ports from the switch port trace.

  Note When more than one port is traced for a given MAC address, additional checks are performed to improve accuracy. These checks include the: trunk port, non-AP CDP neighbors present on the port, and whether or not the MAC address is the only one on this port.

- Exclude device list—Select the check box to exclude additional devices from the trace. Enter into the device list text box each device that you want to exclude from the switch port trace. Separate device names with a comma.
- Max hop count—Enter the maximum number of hops for this trace. Keep in mind that the greater the hop count, the longer the switch port trace takes to perform.
- Exclude vendor list—Enter in the vendor list text box any vendors that you want to exclude from the switch port trace. Separate vendor names with commas. The vendor list is not case sensitive.

Step 3 Configure the following advanced settings:

- TraceRogueAP task max thread—Switch port tracing uses multiple threads to trace rogue access points. This field indicates the maximum number of rogue access points that can be traced on parallel threads.
- TraceRogueAP max queue size—Switch port tracing maintains a queue to trace rogue access points. Whenever you select a rogue access point for tracing, it is queued for processing. This field indicates the maximum number of entries that you can store in the queue.
- SwitchTask max thread—Switch port tracing uses multiple threads to query switch devices. This field indicates the maximum number of switch devices that you can query on parallel threads.

Note The default value for these parameters should be good for normal operations. These parameters directly impact the performance of switch port tracing and Prime Infrastructure. Unless required, We do not recommend that you alter these parameters.

- Select CDP device capabilities—Select the check box to enable.

  Note Prime Infrastructure uses CDP to discover neighbors during tracing. When the neighbors are verified, Prime Infrastructure uses the CDP capabilities field to determine whether or not the neighbor device is a valid switch. If the neighbor device is not a valid switch, it is not traced.

Step 4 Click **Save** to confirm changes made. Click **Reset** to return the page to the original settings. Click **Factory Reset** to return settings to the factory defaults.

Establishing Switch Port Tracing

To establish switch port tracing:

Step 1 In Prime Infrastructure home page, click the **Security** dashboard.

Step 2 In the Rogue APs and Adhoc Rogues dashlet, click the number URL, which specifies the number of rogues in the last hour, last 24 hours, or total active. The Alarms window opens.

Step 3 Choose the rogue you are setting switch port tracking by checking the checkbox.

Step 4 From the **Troubleshoot** drop-down list, choose **Traceroute**. The Traceroute window opens, and Prime Infrastructure runs a switch port trace.

When one or more searchable MAC addresses are available, Prime Infrastructure uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue switch port.

See the "Switch Port Tracing Details" section on page 7-6 for additional information on the Switch Port Tracing Details dialog box.

Switch Port Tracing Details

In the Switch Port Tracing Details dialog box, you can enable or disable switch ports, trace switch ports, and view detail status of the access point switch trace. For more information on Switch Port Tracing, see the following topics:

- Configuring Switch Port Tracing—Provides information on configuring switch port trace settings.
- Configuring SNMP Credentials for Rogue AP Tracing—Provides information on configuring SNMP switch credentials.

In the Switch Port tracing Details dialog box, do one of the following:

- Click **Enable/Disable Switch Port(s)**—Enables or disables any selected ports.
- Click **Trace Switch Port(s)**—Runs another switch port trace.
- Click **Show Detail Status**—Displays details regarding the switch port traces for this access point.
- Click **Close**.

Switch Port Tracing Troubleshooting

Switch Port Tracing (SPT) works on a best-effort basis. SPT depends on the following information to correctly trace and contain rogue APs:

- Reporting access points—A rogue access point must be reported by one or more managed access points.
- Access point CDP neighbor—Access point Cisco Discovery Protocol (CDP) neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials
  - All the switches that need to be traced should have a management IP address and SNMP management enabled.
  - With the new SNMP credential changes, instead of adding the individual switches to Prime Infrastructure, network address based entries can be added.
  - The new SNMP credential feature has a default entry 0.0.0.0 with default community string as private for both read/write.
  - The correct write community string has to be specified to enable/disable switch ports. For tracing, a read community string should be sufficient.
- Switch port configuration
  - Switch ports that are trunking should be correctly configured as trunk ports.
  - Switch port security should be disabled.
- Only Cisco Ethernet switches are supported.

Note The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

- Switch VLAN settings should be properly configured.
- CDP protocol should be enabled for all the switches.
- An Ethernet connection should exist between the rogue access point and the Cisco switch.
- There should be some traffic between the rogue access point and the Ethernet switch.
- The rogue access point should be connected to a switch within the max hop limit. Default hop is 2. Max hop is 10.
- If SNMPv3 is used, then make sure you use the context option and create one for each VLAN in addition to the one for the main group (which is required for non-VLAN based MIBs).