Configuring Controller and AP Settings

The following related topics explain how to configure Cisco Prime Infrastructure to trace switch ports and detect rogue access points.

Related Topics

- Configuring SNMP Credentials for Rogue AP Tracing
- Configuring Protocols for CLI Sessions
- Refreshing Controllers After an Upgrade
- Tracking Switch Ports to Rogue APs
- Configuring Switch Port Tracing
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

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 Cisco Prime Infrastructure, you can use SNMP credentials on this page to connect to the switch.

Step 1 Choose **Administration > Settings > System Settings** > **Network and Device > Switch Port Trace (SPT) > Manual SPT**. The Manual SPT page appears.

Step 2 View or edit the details for a current SNMP credential entry by clicking the **Network Address** link for that entry.

For details on this task, see “Configuring Global SNMP Settings” and “Viewing SNMP Credential Details” in related topics.

Note that the default entry is for network 0.0.0.0, which indicates the entire network. SNMP credentials are defined per network, so only network addresses are allowed. The SNMP credentials defined for network 0.0.0.0 is the SNMP credential default. It is used when no specific SNMP credential is defined. You should update the pre-populated SNMP credential with your own SNMP information.

Step 3 To add a new SNMP entry, choose **Select a command > Add SNMP Entries > Go** (see “Adding SNMP Credentials”).

Related Topics

- Configuring Global SNMP Settings
- Viewing SNMP Credential Details
- Adding SNMP Credentials

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.

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.

Step 1 Choose **Administration > Settings > System Settings > Network and Device > CLI Session**.

Step 2 Select the **Controller Session Protocol** (you can choose SSH or Telnet; SSH is the default).

Step 3 Select the **Autonomous AP Session Protocol** (you can choose SSH or Telnet; SSH is the default).

Step 4 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

Step 5 Click **Save**.

Refreshing Controllers After an Upgrade

The Controller Upgrade 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.

Step 1 Choose **Administration > Settings > System Settings > Network and Device > Controller Upgrade**.

Step 2 Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.

Step 3 Select the **Process Save Config Trap Enable** check box to determine the action Prime Infrastructure takes when a save config trap is received. When this check box is selected, you can choose either to:

- **Retain the configuration in the Prime Infrastructure database**

  or

- **Use the configuration on the controller currently**

Step 4 Click **Save**.

Tracking Switch Ports to Rogue APs

Prime Infrastructure can automatically identify the network switch port to which each rogue access point is connected. Note that this feature relies on Automatic Switch Port Tracing, which requires a full Prime Infrastructure license to work.

Step 1 Choose **Administration > Settings > System Settings** > **Network and Device > Switch Port Trace (SPT) > Auto SPT**. The Auto SPT page appears.

Step 2 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 3 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 4 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.

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 must have 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. Network addresses using /32 subnet masks are not supported in global SNMP credentials configuration. For more guidance, see “Frequently Asked Questions on Rogues and Switch Port Tracing” in Related Topics.
- Switch port configuration—Trunking switch ports must be correctly configured. Switch port security must be disabled.
- Switch Port Tracing is supported only on Cisco Ethernet switches and the following Catalyst switches: 2960, 3560, 3560-E, 3750-E, 3850, 4500 series.
- Switch VLAN settings must be configured accurately. Prime Infrastructure gets switch IP addresses using Cisco Discovery Protocol neighbor information. It then uses VLAN information in the switch to read the switch CAM table entries. If the VLAN information in the switch is not configured properly, Prime Infrastructure will not be able to read the CAM table entries, which results in not being able to trace rogue APs in the switch.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- There must be traffic between the rogue access point and the Ethernet switch, for reliable detection of rogue Ethernet Switch Port information, when the difference in the Ethernet mac address is more or less than two.
- The rogue access point must be connected to a switch within the max hop limit.
- 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).

Note For effective use of Vendor OUI match to eliminate false positive matches, the switch ports must have their location information configured. The switch ports that are not configured will remain for OUI match after elimination by location.

To view the switch port trace details, follow these steps:

Step 1 Add switches with full licenses using the **Configuration > Network > Network Devices** page.

Step 2 Enable **Auto switch port tracing** in **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT** page.

Step 3 Schedule to run wired client status Major Polling background task in **Administration > Dashboards > Job Dashboard** page.

Step 4 Click the Trace switch port icon in Rogue AP detail page. New pop up will show details of switch port traced. Click the detail status to check trace status such as started/Found, and so on.

Note

- Manual SPT will work, even if you do not add any switch to Prime Infrastructure. But you should configure the SNMP credentials correctly in **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT** page.“Private” is the default credential, and will be used during manual Switch Port Tracing if you do not configure it.

- If a switch is added to Prime Infrastructure by selecting **Configuration > Network > Network Devices**, the SNMP credentials entered for the switch will override any switch SNMP credentials entered here, and will be used for switch port tracing. You can change the switch SNMP credentials in the **Configuration > Network > Network Devices** page. Prime Infrastructure will not require any license for adding switch with SPT and will not display wired clients connected to the switches. The **Monitor > Managed Elements > Network Devices > Device Groups > Device Type > Switches and Hubs** page will not display the switch details added with SPT.
- Prime Infrastructure requires full license for adding switch. The **Monitor > Managed Elements > Network Devices > Device Groups > Device Type > Switches and Hubs** page will display the switch details added with full license. Prime Infrastructure will also display wired clients connected to switches. Location of switches is tracked with MSE.

Step 1 Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > SPT Configuration**.

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.

  Note This hop count value is not applicable for Auto SPT.
- 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.

  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.

  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

Step 1 Choose **Dashboard > Wireless > Security**.

Step 2 In the **Malicious Rogue APs**, **Unclassified Rogue APs**, **Friendly Rogue APs**, **Custom Rogue APs**, and **Adhoc Rogues** dashlets: Click the number links showing how many rogues have been identified in the Last Hour, last 24 Hours, or Total Active. The Alarms window opens, showing alarms for the suspected rogues.

Step 3 Choose the rogue for which you want to set up switch port tracking by selecting the check box next to it.

Step 4 Expand the applicable alarm and manually select the **Trace Switch Port** button under the Switch Port Tracing subsection of the alarm details.

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 “Switch Port Tracing Details” for additional information on the Switch Port Tracing Details dialog box.

Related Topics

- Switch Port Tracing Details

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 related topics:

- "Configuring Switch Port Tracing"
- "Configuring SNMP Credentials for Rogue AP Tracing"

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**.

Related Topics

- Configuring Switch Port Tracing
- Configuring SNMP Credentials for Rogue AP Tracing

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.
- Switch Port Tracing is supported only on Cisco Ethernet switches and the following Catalyst switches: 2960, 3560, 3560-E, 3750-E, 3850, 4500 series.
- 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).

Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

The following related topics answer a variety of questions about Prime Infrastructure rogue AP detection and switch port tracing (SPT).

Related Topics

- How Do You Configure Auto SPT?
- How Does Auto SPT Differ From Manual SPT?
- Where Can I See SPT Results (Manual and Auto)?
- How Can I Ensure Auto SPT Runs Smoothly?
- Why Does Auto SPT Take Longer to Find Wired Rogues?
- How Can I Detect Wired Rogues on Trunk Ports?
- How Can I Use the Auto SPT "Eliminate By Location" Feature?
- What is the Difference Between "Major Polling" and "Minor Polling"?

How Do You Configure Auto SPT?

Follow the steps below to configure automatic SPT:

Step 1 Use **Configuration > Network > Network Devices > Add Device** to add switches with a **License Level** of **Full**.

Step 2 Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT** and select **Enable Auto Switch Port Tracing**. Click **OK**.

Step 3 Select **Administration > Settings > Background Tasks > Wired Client Status**. Make sure this task is enabled and that it is scheduled to run at least twice a day.

Related Topics

- Where Can I See SPT Results (Manual and Auto)?
- How Can I Ensure Auto SPT Runs Smoothly?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

How Does Auto SPT Differ From Manual SPT?

Manual SPT runs against individual rogue AP alarms. You must trigger it by clicking on the **Trace Switch Port** icon on the details page for a rogue AP alarm.

Auto SPT runs on batches of alarms, automatically, on the schedule defined for the Wired Client Status background task.

Note that manual SPT triggering depends on CDP being enabled on the access points and switches with appropriate SNMP community strings. For more information on manual SPT and how it works, see the WCS Switch Port Trace Demonstration link in related topics.

Auto and manual SPT also differ in the way they handle licensing and the switch "license level", which can be set to either "Full" or "Switch Port Trace Only" when adding the switch. These three cases demonstrate the differences:

- **Adding switches with "Full" license level**: Prime Infrastructure consumes a license for every added switch with a full license level. All the wired clients connected to switches can be seen by selecting **Monitor > Managed Elements > Network Devices > Device Type > Switches and Hubs**. You can also use MSE to track switch locations. A "Full" license level is mandatory for Auto SPT to be functional.
- **Adding no Switches**: Manual SPT will still work even without adding any switches. But you must remember to configure SNMP credentials appropriately for all switches, using **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- **Adding switches with "Switch Port Trace Only" license level**: If you add a switch to Prime Infrastructure using **Configuration > Network > Network Devices > Add Device**, but select a **Switch Port Trace Only** license level, the SNMP credentials you enter when adding the switch will override the SNMP credentials entered using **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**. The entered credentials will be used for switch port tracing. This is the main difference between not adding switches and adding switches with a license level of "Switch Port Tracing Only". Prime Infrastructure will not consume any licenses for switches with an SPT-only license level, will not show these switches under **Monitor > Managed Elements > Network Devices > Device Type > Switches and Hubs**, and will not show wired clients connected to these switches.

Related Topics

- WCS Switch Port Trace Demonstration
- What is the Difference Between "Major Polling" and "Minor Polling"?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

Where Can I See SPT Results (Manual and Auto)?

Step 1 Display details for the Rogue AP alarm in which you are interested. For example:

a. Click the **Alarm Summary** icon at the top of any Prime Infrastructure page. A list of alarm categories appears.

b. Click the **Rogue AP** link in the list. Prime Infrastructure displays the list of rogue AP alarms.

c. Expand the rogue AP alarm you want. The details page for that alarm appears.

Step 2 In the **Switch Port Tracing** pane, click the **Trace Switch Port** icon. The Switch Port Trace window shows the details of the traced switch port.

If no SPT has been performed, click **Trace Switch Port(s)** to start tracing. Click the **Show Detail Status** button to get details on the status of the trace as it progresses.

Related Topics

- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

How Can I Ensure Auto SPT Runs Smoothly?

The following are recommended best practices for auto SPT:

1. Ensure that Prime Infrastructure manages all switches with a **Full** license level.
2. Ensure all the switches are managed by and synchronized with Prime Infrastructure, so that wired client discovery is successful.
3. For best results, use the choices available under **Administration > Dashboards > Job Dashboard > System Jobs to** check that the following background tasks are running:
   a. **Inventory And Discovery Jobs > Switch Inventory:** Must run periodically.
   b. **Status > Wired Client Status**: Must be running periodically.
   c. **Infrastructure > Data Cleanup**: Is not disabled and is running periodically.

   For Rogue AP tasks, use **Administration > Dashboards > Job Dashboard > System Jobs > Wireless Monitoring > Rogue AP**.
4. Ensure that rogue AP alarms are kept only for the required number of days. Cisco recommends that you keep them for no more than 8 days unless you have special retention requirements. You can configure this by selecting **Administration > Settings > System Settings > Alarms and Events > Alarms and Events** and setting the desired time period in the **Delete cleared security alarms after** field.

5. For immediate wired- client detection, use a trap receiver configuration on the switch, which can trigger Prime Infrastructure's client discovery and rogue detection processes. You can enable this by following these steps:

   a. Use **Administration > System Settings > Client and User > Client** page to enable the **Poll clients on client traps** option. This is strongly recommended only for a smaller environment (around 50 switches) or for some sensitive ports.

   b. Execute the following commands in the CLI for each switch (these commands may vary slightly for each switch platform):

      <switchname># conf t

      <switchname>(config)# Snmp-server enable traps mac-notification change move threshold

      <switchname>(config)# Snmp-server host *PrIinfraIPAddress* version 2c *comstring* mac-notification

      <switchname>(config)# Mac address-table notification change interval 5

      <switchname>(config)# Mac address-table notification change history-size 10

      <switchname>(config)# Mac address-table notification change

   Where:

   – ***PrIinfraIPAddress*** is the IP Address of the Prime Infrastructure server.

   – ***comstring*** is the community string for the switch

   c. Execute the following commands on the interfaces for each switch (these commands may vary slightly for each switch platform):

      <switchname>(config)# Interface *Intname*

      <switchname>(config-if)# description non-identity clients

      <switchname>(config-if)# switchport access vlan *ID*

      <switchname>(config-if)# switchport mode access

      <switchname>(config-if)# snmp trap mac-notification change added

      <switchname>(config-if)# snmp trap mac-notification change removed

   Where:

   – ***Intname*** is the interface name

   – ***ID*** is the VLAN ID

Related Topics

- How Do You Configure Auto SPT?
- What is the Difference Between "Major Polling" and "Minor Polling"?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

Why Does Auto SPT Take Longer to Find Wired Rogues?

Auto SPT takes relatively longer to find wired rogues than does manual SPT for the following reasons:

1. Auto SPT depends on the wired client discovery process, which happens only when the Wired Client Status major polling background task runs. By default, the major poll for this background task is scheduled to run only after every two minor polls, or once every four hours.
2. Even though the wired rogue AP is connected to a switch, Prime Infrastructure will discover a wired port only when the wired rogue AP is in the “associated” state. Prime Infrastructure always checks whether a wired client’s status is associated or disassociated. If the wired client status is disassociated, Prime Infrastructure shows this as no port connected.
3. Rogue tracing is done in batches. The time taken to find a particular wired rogue depends on the batch in which Prime Infrastructure processes it. If a particular rogue was processed in the previous batch, it takes more time to trace it.
4. The time taken to discover any wired rogue depends upon the number of rogue alarms present in Prime Infrastructure and the interval between Wired Client Status major polls.

Related Topics

- What is the Difference Between “Major Polling” and “Minor Polling”?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

How Can I Detect Wired Rogues on Trunk Ports?

You can detect wired rogues on trunk ports by following the steps below.

Note that if you are trying to detect rogues on trunk ports for Cisco 2950 switches, you must first install the updated 2950 support in Prime Infrastructure Device Pack 5.0.

Step 1 Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > SPT Configuration**.

Step 2 Uncheck the **Exclude switch trunk ports** check box, then click **Save**.

Step 3 Choose **Administration > Settings > System Settings > Client and User > Client**.

Step 4 Check the **Discover wired clients on trunk ports** check box, then click **Save**.

Switches will start detecting wired clients on trunk ports starting with the next execution of a major poll by the Wired Client Status background task.

Related Topics

- How Do You Configure Auto SPT?
- What is the Difference Between “Major Polling” and “Minor Polling”?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

How Do You Configure Switch Port Location?

Follow the steps below to configure Switch Port Location:

Step 1 Use **Configuration > Network > Network Devices > Switches and Hubs.**

Step 2 Click a **Device Name**. By default, Configuration tab opens.

Step 3 Click **Switch Port Location** in the top right corner.

Step 4 Select the check box(es) of one or more ports to configure location, and from choose **Configure Location** from the drop-down list, then click **Go**.

Step 5 In the Map Location group, you can configure the following:

- From the Campus/Site drop-down list, choose the campus map for the switch or switch port.
- From the Building drop-down list, choose the building map location for the switch or switch port.
- From the Floor drop-down list, choose the floor map.
- If you have already saved a file with the Campus/Site, Building, and Floor details, click **Import Civic**. This imports civic information for the MSE using Prime Infrastructure . Enter the name of the text file or browse for the filename, and click **Import**.

Step 6 In the ELIN and Civic Location group box, you can configure the following:

- Enter the Emergency Location Identifier Number (ELIN) in the ELIN text box. ELIN is a number that can be used by the local public safety answering point (PSAP) to look up the geographic location of the caller in a master database known as the automatic location information (ALI) database. The ELIN also allows the PSAP to contact the emergency caller directly in the event the phone call is disconnected.
- Complete the required fields on the Civic Address and Advanced tabs.
- If you have the ELIN and Civic location information saved in a file, you can import it by clicking **Import Switch Location**.

Step 7 Click **Save**.

Related Topics

- How Can I Use the Auto SPT “Eliminate By Location” Feature?
- How Do You Configure Switch Port Location?
- How Do You Configure Auto SPT?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

How Can I Use the Auto SPT "Eliminate By Location" Feature?

"Eliminate by location" is one of the algorithms Prime Infrastructure uses to detect wired rogues. It uses the rogue AP location information to search for the associated switch ports. It helps to reduce false positives during Auto SPT processing, using the floor ID of the detecting APs, and increases accuracy in tracking wired rogues.

When "Eliminate by location" is enabled, the Wired Client Status background task discovers all the wired clients from managed switches. The next time auto SPT runs, switch ports will be filtered based on the "eliminate by location" algorithm.

Follow these steps to enable "eliminate by location":

Step 1 Integrate Cisco Mobility Service Engine (MSE) with Prime Infrastructure.

Step 2 Ensure that MSE is in sync with the defined floor area where the detecting APs are placed. MSE should be able to track the rogues.

Step 3 Add all switches to Prime Infrastructure.

Step 4 After all switches are added to Prime Infrastructure and are in the managed state, all switch ports need to be configured for the algorithm to work. If all switches are not configured with switch ports, then the false positive results occur. You can configure from the **Configuration** > **Network** > **Network Devices** > **Switches and Hubs** > click on a **Device Name** > click **Switch Port Location** in the top right corner.

Step 5 Place the detecting access points on the map and make sure that the Cisco MSE is synchronized and rogues APs are detected on the floor.

Eliminate By Location algorithm takes the floor ID of detecting APs and eliminates all others. If some switch ports are not configured, then the value of those ports will be set to Zero and will be considered. Hence the results may contain false positives, which contains the exact floor ID and floor ID which has the value zero.

Step 6 Configure switch port locations to ensure that all ports are assigned to the correct floor area.

Related Topics

- How Do You Configure Switch Port Location?
- How Do You Configure Auto SPT?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)

What is the Difference Between “Major Polling” and “Minor Polling”?

The Wired Client Status background task that triggers auto SPT Definitions are as follows:

Major Polling: During a major poll, Prime Infrastructure triggers client discovery on all wired device ports by syncing all of the essential client information with the database. In Prime Infrastructure 2.2, the frequency of this poll was reduced from twice a day. It is now fully configurable.

Minor Polling: During a minor poll, Prime Infrastructure triggers client discovery only on device interfaces and ports which became active recently. Prime Infrastructure uses interface uptime data to detect when a port or interface is recently added or removed by any client.

Related Topics

- How Does Auto SPT Differ From Manual SPT?
- Why Does Auto SPT Take Longer to Find Wired Rogues?
- Frequently Asked Questions on Rogues and Switch Port Tracing (SPT)