ForeScout

CounterACT® Wireless Plugin

Integration with Cisco Wireless Management

Configuration Guide

Version 1.5.1

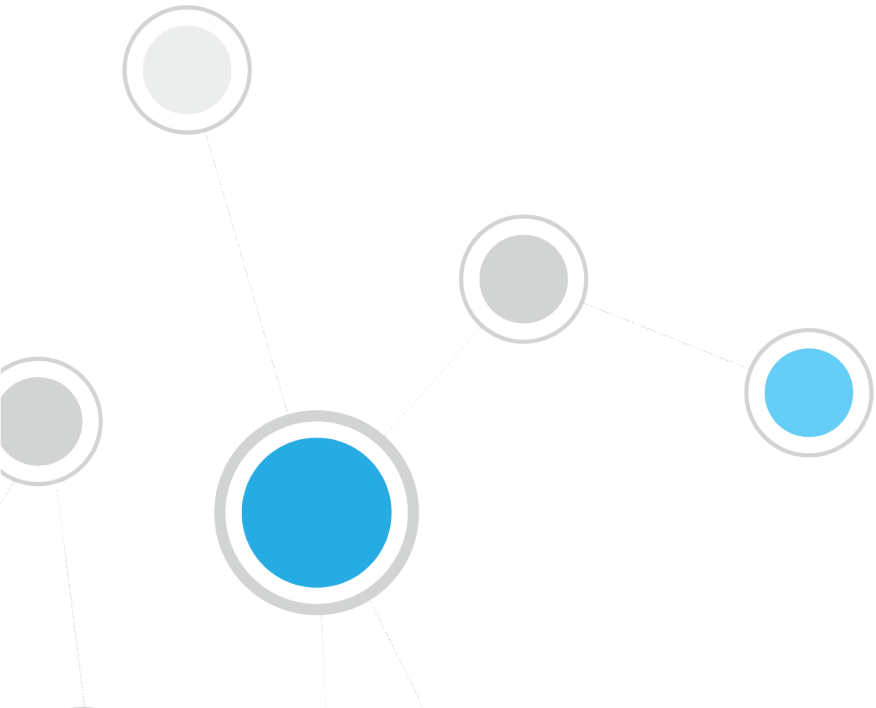


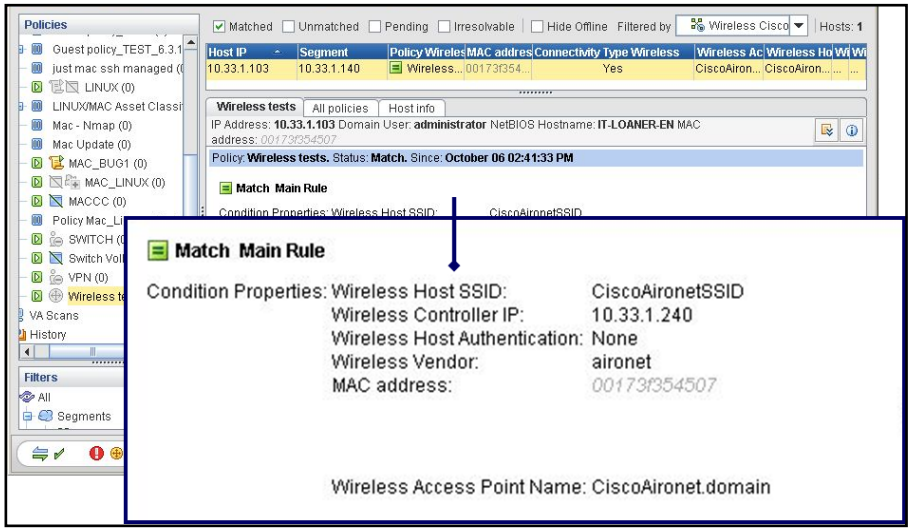
Table of Contents

About the Plugin and Cisco Configuration

This document describes how to configure Cisco wireless controllers and access points (wireless management devices) for integration with the CounterACT Wireless Plugin.

The CounterACT Wireless Plugin is designed to provide NAC capabilities to 802.11 wireless network controllers and access points for the purpose of:

- Viewing information about wireless endpoints connected to your network
- Blocking wireless endpoints from the organizational network



For detailed information about the CounterACT Wireless Plugin refer to http://updates.forescout.com/support/files/plugins/wireless/1.3.2/1.3.2-142/help.pdf

Requirements

- Cisco controller with software 5.0.148.0 or higher
- Cisco Aironet access point with software version 12.4(10b) or higher
- Network Module version 1.0 or above with the following components running:
  - Wireless Plugin,
  - Switch Plugin (To work with notification traps).
- CounterACT version 8.0

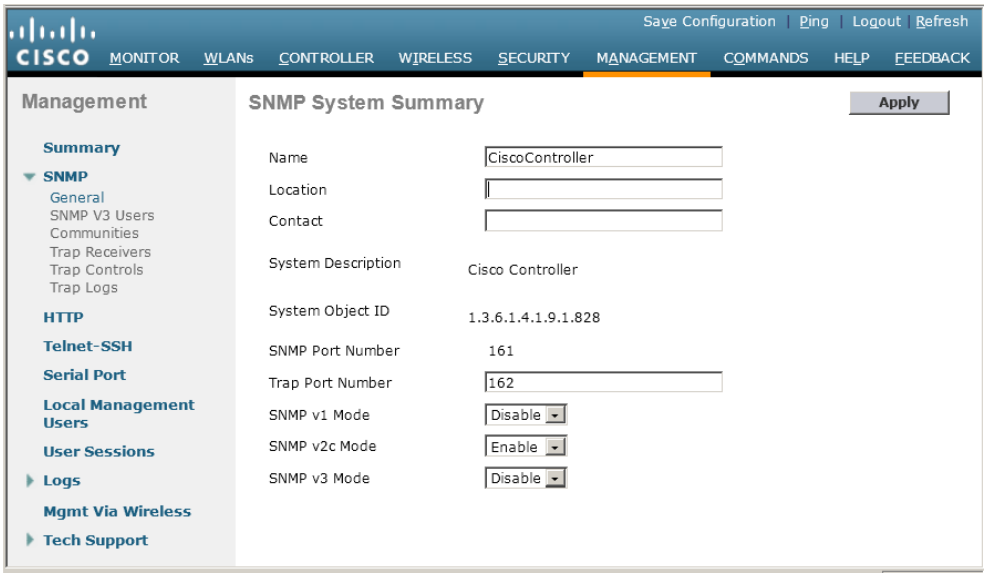
Configuration

Cisco Controller Configuration

You should perform the following Cisco controller configuration steps in order to work with the Wireless Plugin. SNMP Configuration can be used for both read and write access.

To configure a Cisco controller:

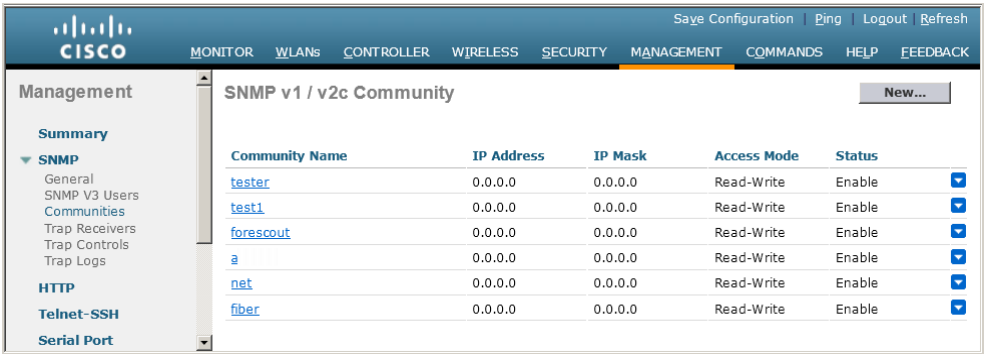
1. Log into the Cisco controller.
2. Select **Management**>**SNMP**>**General**.



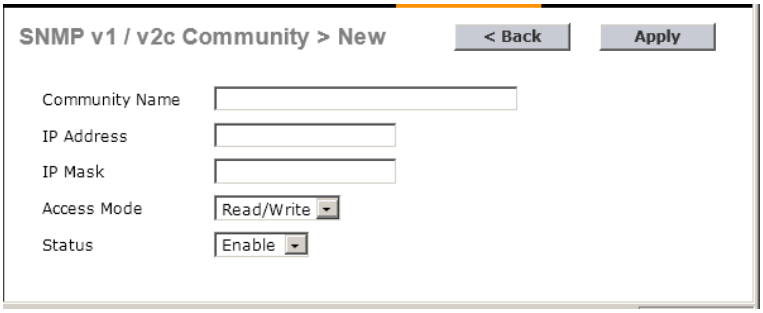
3. Enable the SNMP version that you want to use and select **Apply**.

If you are using notification traps, you must use SNMPv1 or SNMPv2c—the same SNMP parameters are used for the traps and the plugin does not yet support SNMPv3 in this case.

4. (SNMPv1 or SNMPv2c) Select **Management**>**SNMP**>**Communities**.



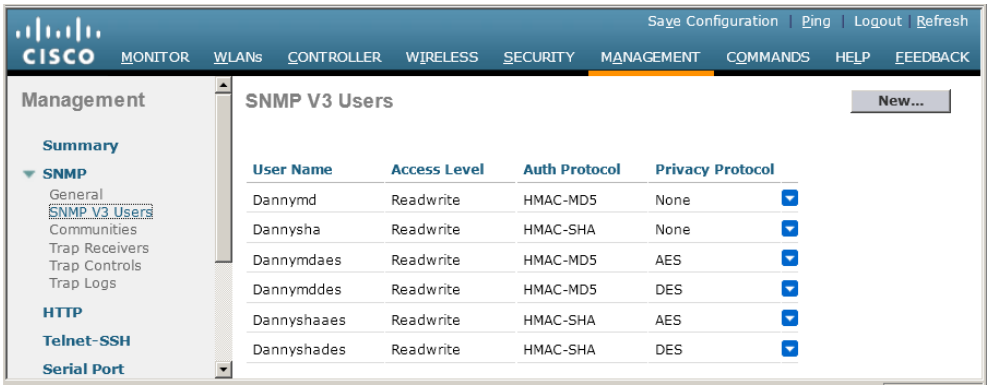
– Select **New**. The SNMP v1 / v2c Community > New pane opens.



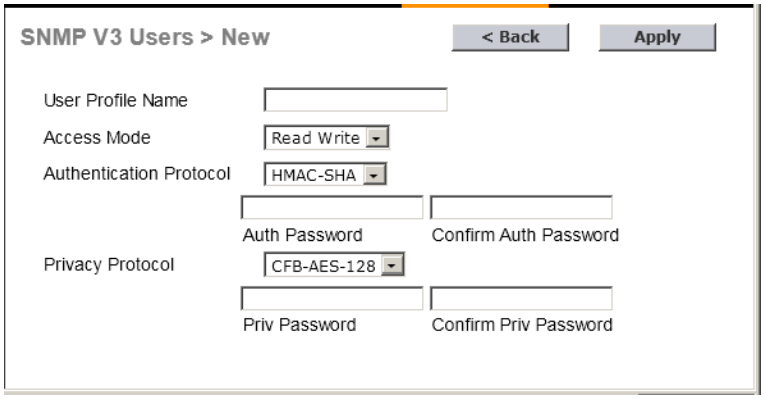
– Enter Community parameters. Verify that **Access Mode** is set to **Read/Write** and that **Status** is **Enabled**. The values for **IP Address** and **IP Mask** should enable access from the CounterACT device.

– Select **Apply**.

5. (SNMPv3) Select **Management**>**SNMP**>**SNMP V3 Users**.



– Select **New**. The SNMP V3 Users > New pane opens.



– Enter SNMPv3 parameters and select **Read Write** from the **Access Mode** dropdown list.
– Select **Apply**.

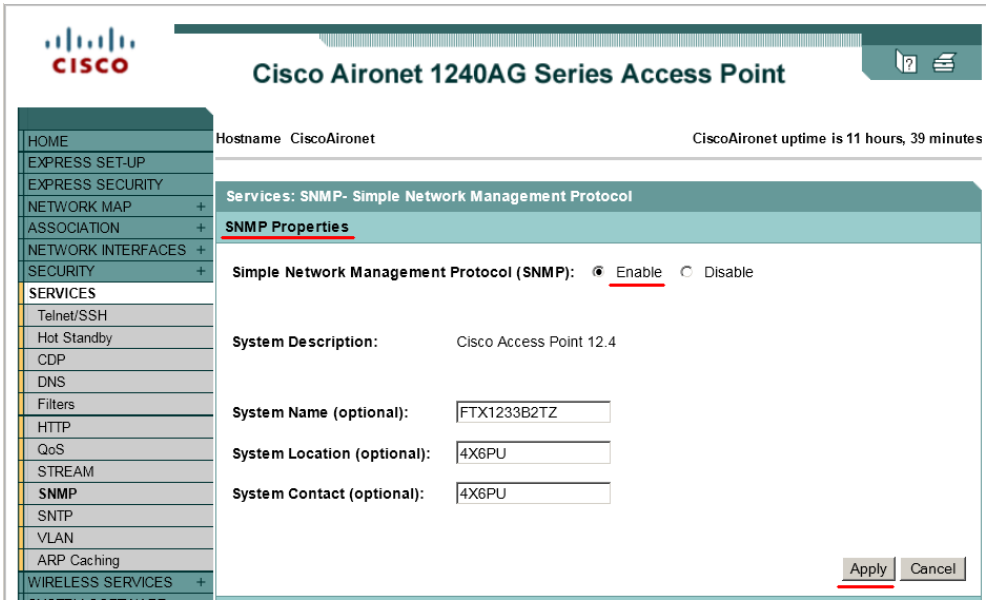
Cisco Aironet Access Point Configuration

You should perform the following Cisco access point configuration steps in order to work with the plugin.

To configure a Cisco access point:

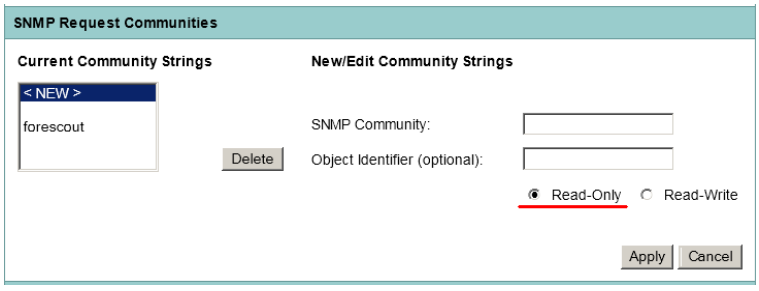
1. Log into the Cisco Aironet access point.
2. Configure read parameters: Select **Services**>**SNMP**.

– Select **Enable** from the SNMP Properties section.



– Select **Apply**.

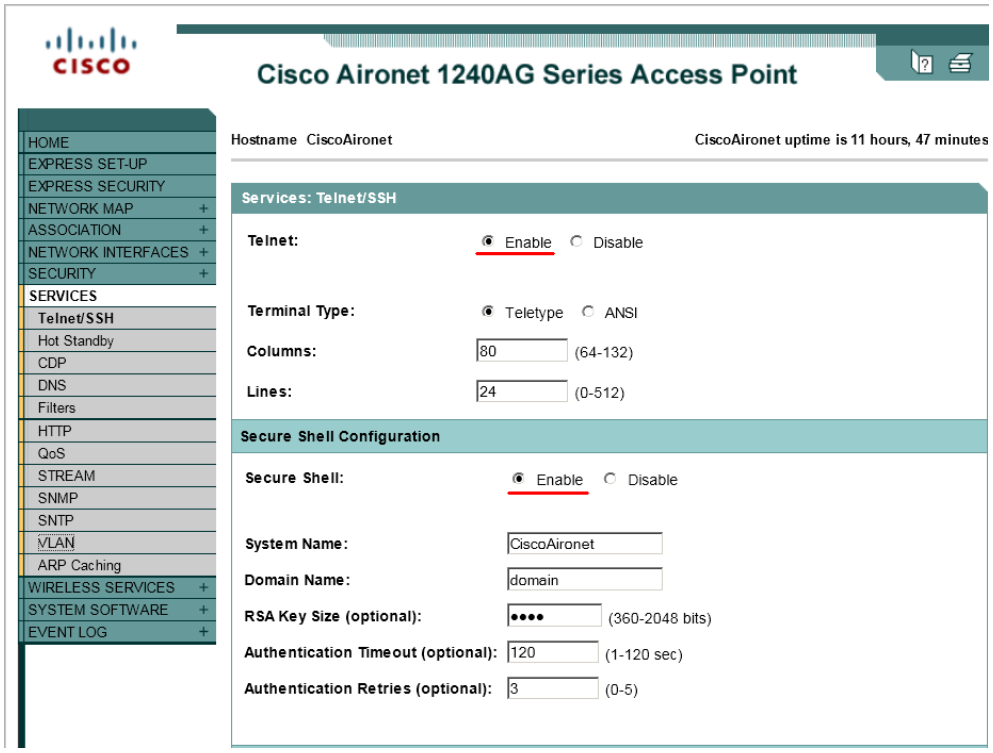
– In the **SNMP Request Communities** section, enter a community string and select **Read-Only**.



– Select **Apply**.

6. Configure write parameters: Select **Services**>**Telnet/SSH**.

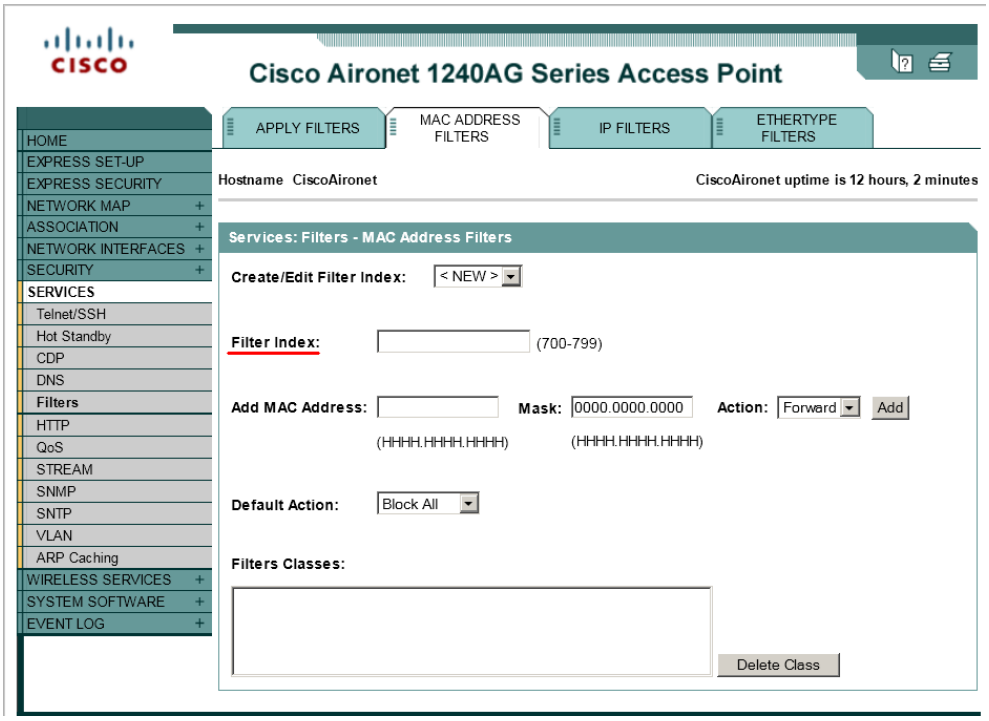
– Verify that **Telnet** or **SSH** is enabled.



– Select **Apply.**

7. View blocked host: Select **Filters**>**MAC Addresses Filters**.

– Verify that **Filter Index** is *not* 770. If you define the filter index using this number you will block the CounterACT access list.



MIBs Used by the Wireless Plugin

The following (read-only) MIBs are used by the Wireless Plugin for Cisco controllers and Cisco Aironet access points:

- OID_SYSTEM_UPTIME: 1.3.6.1.2.1.1.3.0 (system.sysUpTime.0)
- CISCO_OID_MOBILE_CLIENT_SSID_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.7 (bsnMobileStationSsid)
- CISCO_OID_MOBILE_CLIENT_IP_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.2 (bsnMobileStationIpAddress)
- CISCO_OID_MOBILE_CLIENT_AP_MAC_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.4 (bsnMobileStationAPMacAddr)
- CISCO_OID_MOBILE_CLIENT_MAC_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.1 (bsnMobileStationMacAddress)
- CISCO_OID_MOBILE_CLIENT_AUTH_TYPE_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.30 (bsnMobileStationPolicyType)
- CISCO_OID_MOBILE_RSS_AP_MAC_ENTRY: 1.3.6.1.4.1.14179.2.1.11.1.1 (bsnMobileStationRssiDataEntry)
- CISCO_OID_MOBILE_RSS_AP_NAME_ENTRY: 1.3.6.1.4.1.14179.2.1.11.1.4 (bsnMobileStationRssiDataEntry)

Cisco Controller MIBs

To block endpoints, the Wireless Plugin must have read permissions for the following two MIBs:

- CISCO_OID_BLACKLIST_CLIENT_ROW_STATUS: 1.3.6.1.4.1.14179.2.5.6.1.22.12 (bsnBlackListClientRowStatus)
- CISCO_OID_BLACKLIST_CLIENT_MESSAGE: 1.3.6.1.4.1.14179.2.5.6.1.2.12 (bsnBlackListClient)

Cisco Aironet Access Point MIBs

The Cisco Aironet access point uses another three (read-only) MIBs:

- AIRONET_OID_ARP: 1.3.6.1.2.1.4.22.1.2
- AIRONET_OID_CLIENTS_TABLE: 1.3.6.1.4.1.9.9.273.1.2.1.1
- AIRONET_AP_NAME: 1.3.6.1.2.1.1.5.0

Notification Trap MIBs Received by the Plugin

The following MIBs may be received from a Cisco controller when

- 1.3.6.1.4.1.9.9.599.1.3.1.1.1.0: The endpoint IP address
- 1.3.6.1.4.1.9.9.599.1.3.1.1.10.0: The endpoint MAC address
- 1.3.6.1.4.1.9.9.513.1.1.1.1.5.0: The AP name
- 1.3.6.1.4.1.14179.2.2.1.1.3.0: The AP name
- 1.3.6.1.4.1.9.9.599.1.2.2.0: The SSID
- 1.3.6.1.4.1.14179.2.6.2.34.0: The endpoint IP address
- 1.3.6.1.4.1.14179.2.6.2.43.0: The endpoint IP address
- 1.3.6.1.4.1.9.9.599.0.4: Indicates that the client is connected
- 1.3.6.1.4.1.14179.2.6.3.2: Indicates that the client is disconnected

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

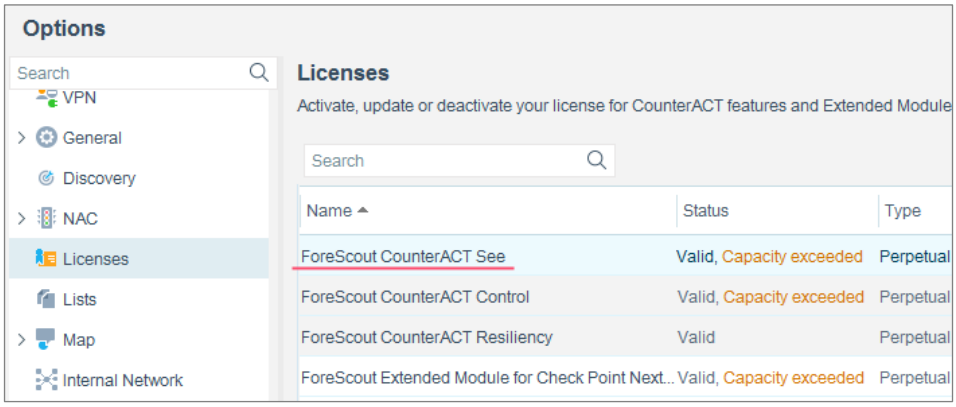
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-15 13:34