ForeScout

ForeScout CounterACT®

Network Module: Centralized Network Controller Plugin

Configuration Guide

Version 1.0

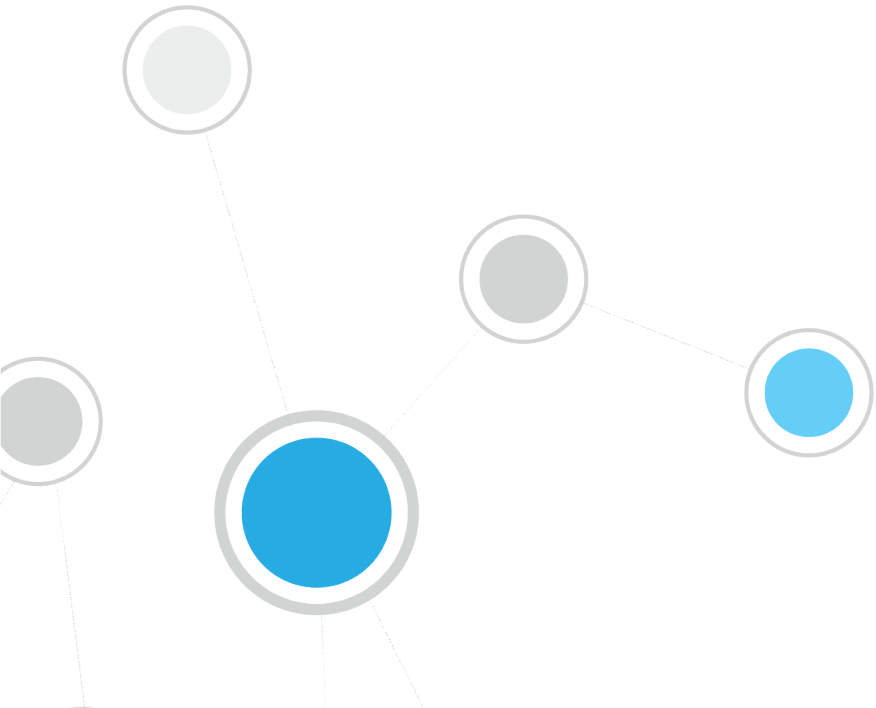


Table of Contents

About the Centralized Network Controller Integration

The Centralized Network Controller Plugin is a component of the ForeScout CounterACT® Network Module. See Network Module Information for details about the module.

Network Controllers provide a centralized interface for management, monitoring and configuration of network infrastructures. CounterACT integrates with Centralized Network Controller solutions to offer customers full visibility into their networks, including the network devices and the endpoints connected to these devices.

For this initial integration, CounterACT has integrated its offering with the Cisco Meraki cloud management platform.

The Meraki Dashboard is the centralized cloud management interface for all Cisco Meraki products.

About This Plugin

The Centralized Network Controller Plugin lets you monitor Cisco Meraki, cloud-managed networks. The integration enables real time discovery of endpoints connected to Meraki Switches (MS) and Wireless Access Points (MR).

In order to communicate with the third-party solution, you will define a *controller: a* logical entity that represents the third-party management interface with which the plugin communicates. In the context of this integration, the CounterACT controller communicates with the Cisco Meraki cloud Dashboard.

Once discovered, endpoints go through CounterACT classification and assessment processes.

You can use plugin properties to resolve information about the Meraki organizations, networks, switches and wireless access points discovered. For example, the name of the organization to which the detected endpoint belongs, or the name of the access point to which the wireless client is connected.

To use the plugin, you should have a solid understanding of Cisco Meraki concepts, functionality and terminology (mainly the Dashboard organizational structure – Organization/Network/Device). For more information refer to https://documentation.meraki.com/

You should also have a solid understanding of CounterACT policies and other basic CounterACT features.

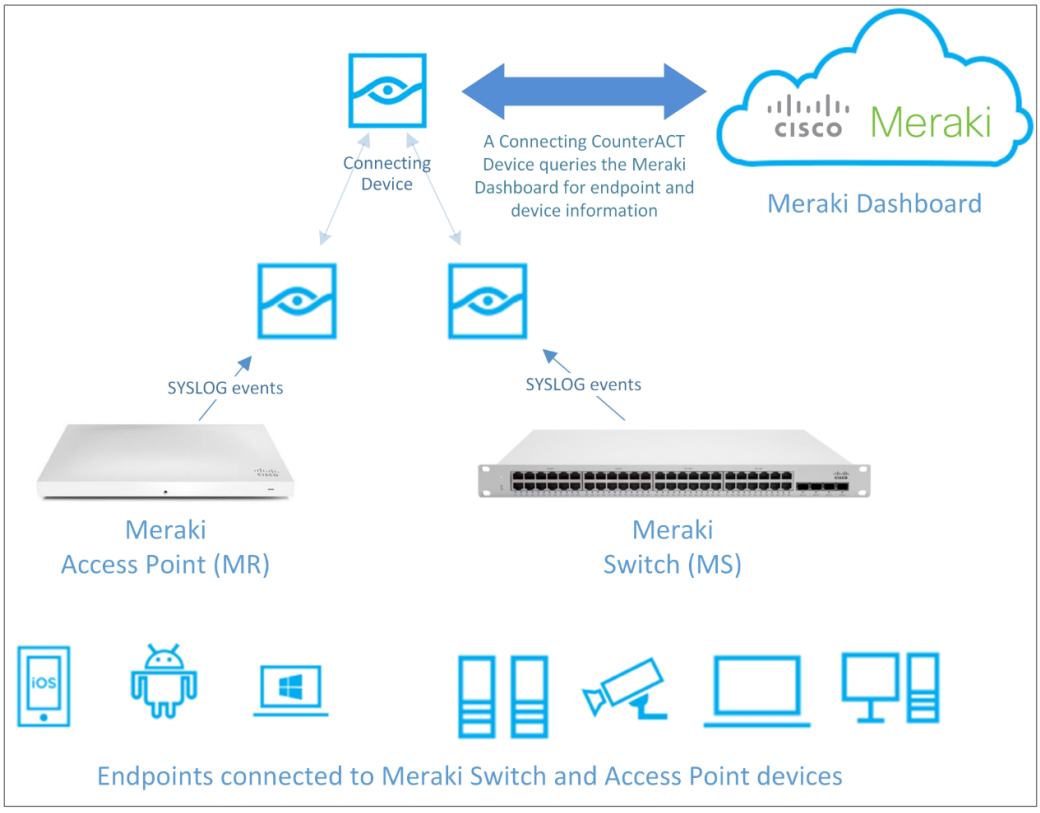
How It Works

The following Meraki components are required for this integrated solution:

- ***Meraki Dashboard*** - CounterACT queries the Meraki Cloud Management Service via its Dashboard API to retrieve information about network devices and the endpoints that are connected to these devices
- ***Meraki Switches and Access Points*** - CounterACT receives syslog events from local Meraki switches (MS) and access points (MR) which provide endpoint discovery information.

The following CounterACT components support this integration:

- ***Centralized Network Controller Plugin*** - This plugin handles communication with the Meraki Dashboard and provides endpoint and device properties. Use the plugin to define *controllers,* logical entities that represent the third-party solution with which the plugin communicates.
- ***CounterACT Syslog Plugin*** – This Plugin enables the receipt of syslog events from Meraki devices. These syslog messages are used to expedite the discovery of endpoints connections and disconnections.



A CounterACT Appliance or Enterprise Manager must be defined as the Connecting CounterACT Device, which handles the communication with the Meraki Cloud Management Service (Dashboard).

Depending on the Meraki customer deployment, a single or multiple plugin controllers are configured within CounterACT, each with a dedicated Connecting CounterACT device.

- A single plugin controller can handle communication with the Meraki Dashboard for more than one Meraki Organization.
- A specific organization can only be queried by a single controller.
- For each plugin controller, the polling rate from CounterACT to the Meraki Dashboard can be configured.
- CounterACT does not query information directly from the Meraki devices - switches and Access Points. It can be configured to receive syslog messages from these devices.

CounterACT Console does not display endpoint IPv6 addresses reported by Meraki. For IPv6 only endpoints, their MAC address is displayed in the Console.

Baseline Deployment Guidelines

- It is recommended to choose the Enterprise Manager as the Connecting CounterACT Device.
- A Connecting CounterACT Device can poll information from multiple Meraki Organizations. It is recommended that a single Connecting CounterACT Device poll information from up to 1000 network devices across single or multiple Organizations.
- For deployments with more than 1000 network devices it is recommended to assign a dedicated Connecting CounterACT Device to poll information from each Organization (each with no more than 1000 devices).

Requirements

This section describes the requirements for running the CounterACT Network Controller Plugin and configuring it to work with third party solutions.

CounterACT Requirements

The plugin requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.
- ForeScout recommends that the Centralized Network Controller Plugin use received syslog events to detect endpoint connections/disconnections. For this plugin processing to take place, the following is required:
  - Core Extensions Module version 1.0 with the Syslog Plugin running. See Configure Syslog Servers and Syslog Plugin Configuration Prerequisites for details.
- An active Maintenance Contract for CounterACT devices is required.

Network Requirements

The following must be configured on enterprise firewalls to support communication between CounterACT and the Meraki Cloud Dashboard:

- Allow communication on port 443/TCP
- The URL **`api.meraki.com/api/v0/`** must be reachable with HTTPS

If your organization's network security policy requires that Internet communication traffic must be routed through a proxy server, you will need to configure the connection parameters for accessing the proxy server that handles communication between the Connecting CounterACT Device, which you configure for use by the Centralized Network Controller Plugin, and the Meraki Cloud Dashboard.

Third-Party Product Requirements

The following Meraki products and software versions are verified for interoperation with CounterACT Centralized Network Controller Plugin:

Vendor	Network Device Type	Network Device Model	Software Version
Cisco Meraki	Access Point	MR-33/34	MR 24.12
	Switch	MS-220/250	MS 9.32

It is recommended that the Centralized Network Controller Plugin is configured to use syslog events sent to it from local Meraki devices to detect endpoint connections/disconnections. For this plugin processing to take place, configure the following in the Meraki Dashboard:

- Configure the syslog servers (receivers of network device events) to be the CounterACT device(s) that are responsible for receiving syslog events sent from the local network devices.

- Configure the syslog server port to be the identical port number as the UDP port for receiving syslog events that is configured in the Syslog Plugin. The default port for this purpose is 514.

  Cisco Meraki only supports use of the UDP protocol to send syslog events.

Configuration Prerequisites

Before proceeding with Centralized Network Controller Plugin configuration, you must complete the following activities, in the order presented:

1. In the Meraki Dashboard:
   a. Generate API Key
   b. Configure Syslog Servers
2. In the Syslog Plugin:
   a. Configure Plugin Receiver Port
   b. Verify Running Plugin

Meraki Dashboard Configuration Prerequisites

Before Centralized Network Controller Plugin configuration, complete the following Meraki Dashboard activities, in the order presented:

1. Generate API Key
2. Configure Syslog Servers

Generate API Key

The Centralized Network Controller Plugin requires the use of an API Key to communicate with the cloud management interface, which is the Meraki Dashboard. In the Meraki Dashboard, generate the API Key. Then, when adding the controller to the plugin configuration, you must provide the generated API Key.

The API key is hidden the next time you enter this configuration page on the Dashboard. Record the API Key immediately after generating it and save.

To generate an API Key:

1. In the Meraki Dashboard, select **Organization** > **Settings**.
2. In the **Dashboard API access** section of the Settings page, do the following:
   a. Select the **Enable access to the Cisco Meraki Dashboard API** checkbox.
   b. Select the **profile** link in the statement **After enabling the API here, go to your profile to generate an API key.** The Update your account information page displays.

3. In the page's **API access** section, select **Generate API Key**. The generated API Key displays.

   Provide this API Key when adding the controller to the Centralized Network Controller Plugin configuration. See section Configure the Plugin, Add Controller.

For details about working with the dashboard, reference the documentation for the Cisco Meraki cloud management platform.

Configure Syslog Servers

In order for the Centralized Network Controller Plugin to use received syslog events to detect endpoint connections/disconnections, in the Meraki Dashboard, configure the syslog servers; these are the CounterACT device(s) responsible for receiving syslog events (wireless events and/or switch events) sent from cloud-managed network devices.

Syslog server configuration is defined per a Meraki network.

To configure a syslog server:

1. In the Meraki Dashboard, per Meraki network, select **Network-wide** > **CONFIGURE** > **General**.
2. In the **Logging** section of the General page, define the following information for each syslog server entry:
   a. **Server IP** - the IP address of a CounterACT device to function as a syslog server (receives syslog events from Meraki network devices).
   b. **Port** - the port that network devices use to send syslog events to the syslog server. The default port for this purpose is 514.
   Cisco Meraki only supports use of the UDP protocol to send syslog events.
   c. Event Type field - make any of the following selections:
      > Select **Wireless events**. Instructs to send WLAN device (wireless access point) events to the syslog server.
      > Select **Switch events**. Instructs to send switch device events to the syslog server.
      > Select both **Wireless events** and **Switch events**. Instructs to send both WLAN device events and switch device events to the syslog server.
3. Repeat step 2 for each CounterACT device you want to configure as a syslog server.

For details about working with the dashboard, refer to the documentation for the Cisco Meraki cloud management platform.

Syslog Plugin Configuration Prerequisites

In order for the Centralized Network Controller Plugin to use received syslog events to detect endpoint connections/disconnections, then after completing the Meraki Dashboard configuration prerequisites and before Centralized Network Controller

Plugin configuration, complete the following Syslog Plugin-related activities in the CounterACT Console:

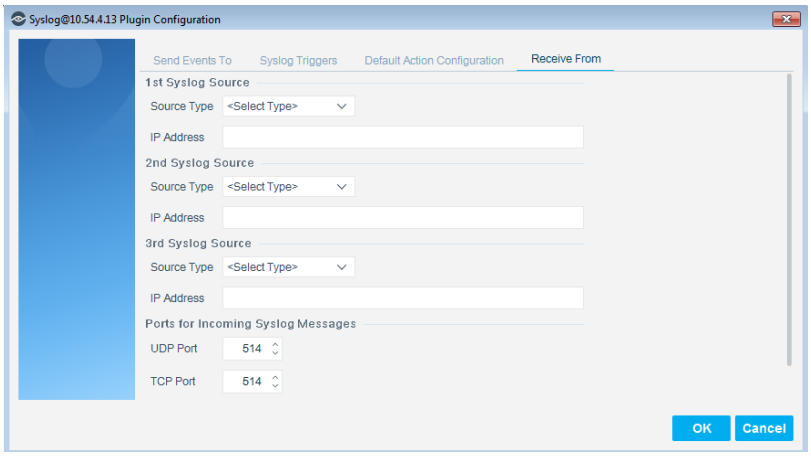
- Configure Plugin Receiver Port
- Verify Plugin is Running

Configure Plugin Receiver Port

Configure the Syslog Plugin port for receiving syslog events for each CounterACT device configured as a syslog server (receiver of wireless events and/or switch events) in the Meraki Dashboard. Each such CounterACT device receives syslog events sent from cloud-managed, local network devices.

To configure the port for receiving syslog events:

1. In the Console toolbar, select **Tools** > **Options**. The Options window displays.
2. In the navigation tree, select **Modules**. The Modules pane opens.
3. In the Modules pane, double-click **Core Extensions**.
4. Select **Syslog** and then select **Configure**. The **Select Appliances** dialog opens.
5. Select a CounterACT device and then select **OK**. The **Syslog@**<CounterACT device> **Plugin Configuration** window opens.
6. Select the **Receive From** tab.



7. In the **Ports for Incoming Syslog Messages** section, configure the **UDP Port** field with the identical port number that is configured for the syslog server port in the Meraki Dashboard. The default UDP port for this purpose is 514.
8. Select **OK** and then select **Yes** to save the plugin configuration update.
9. Repeat steps 4 - 8 for each CounterACT device configured as a syslog server in the Meraki Dashboard.

For details about Syslog Plugin configuration, refer to the *CounterACT® Syslog Plugin Configuration Guide*. See Additional CounterACT Documentation for information on how to access the guide.

Verify Plugin is Running

Verify that the Syslog Plugin is running in *all* of the CounterACT devices configured as a syslog server in the Meraki Dashboard (**Options** window > **Modules** pane and expand the **Core Extensions** module entry).

- If the plugin is not running in *all* of these CounterACT devices, select Syslog and select **Start**.

Configure the Plugin

This section describes how to configure the Centralized Network Controller Plugin so it monitors:

- An organization's networks, whether wireless, switch or a network that includes both types of network devices (combined)
- An organizations network devices (wireless access points and/or switches)
- The endpoints connected to these network devices

Plugin *controllers* are logical entities that represent the third-party cloud management interface with which the plugin communicates. In this integration a controller will communicate with Cisco Meraki cloud based dashboard.

The section presents the following plugin configuration topics:

- Add Controller
- Update Controller
- Test the Plugin Configuration

Add Controller

The section describes how to define controllers in CounterACT that communicate with the management interface.

Before adding a controller to the plugin configuration, make sure that you have completed the steps described in Configuration Prerequisites.

The following configuration information is presented:

- General
- Organizations to Query
- Detection Method
- Proxy Server
- Performance Tuning

General

In the General pane (Step 1), configure the information needed by the plugin to communicate with the specified controller, in order to obtain information about:

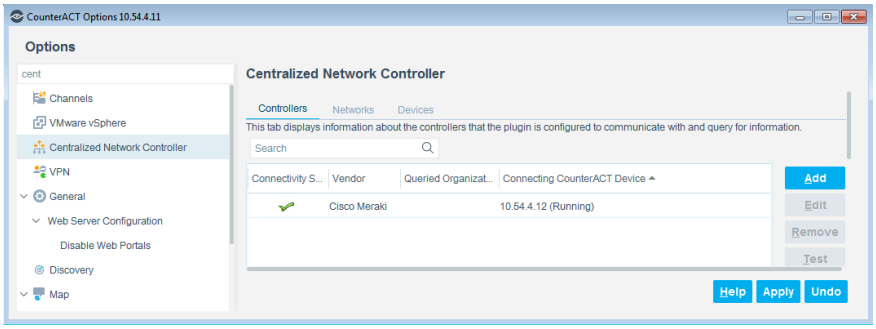
- Meraki Organizations
- Meraki Networks
- The Meraki Networks' Devices (wireless access points and/or switches) and the endpoints connected to these devices.

Multiple Controller Configuration

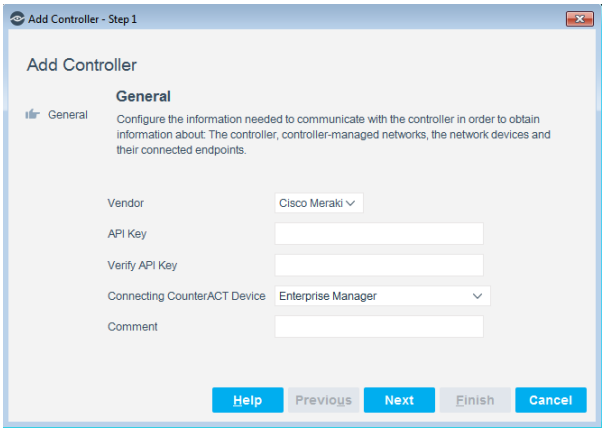
Multiple controllers can be configured based on the Meraki enterprise deployment and its topology. Each controller handles/queries different Meraki organizations. A specific organization can only be queried by a single controller.

To configure general information:

1. In the Console toolbar, select **Tools** > **Options**. The Options window opens.
2. Select **Modules** and then double-click **Network**.
3. Select Centralized **Network Controller** and then select **Configure**. The Centralized Network Controller pane opens.



4. In the Controller tab, select **Add**. The **General** pane opens.



5. Define the following:

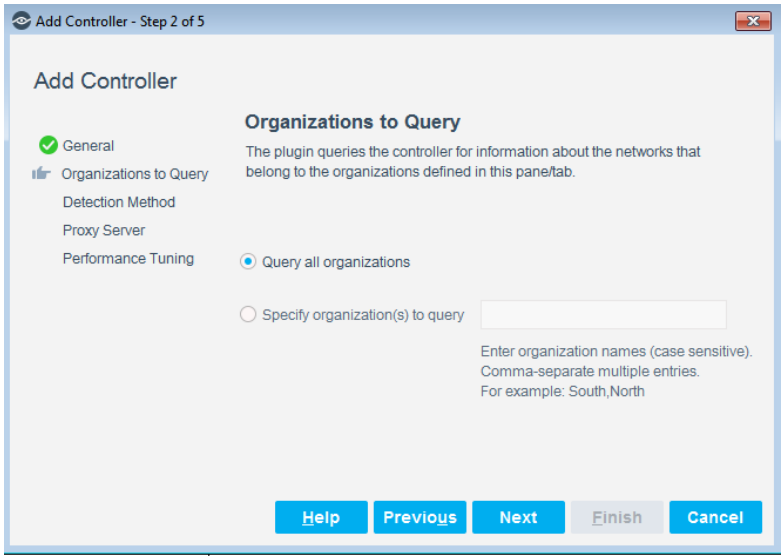
Field	Description
Vendor	From the drop-down list, select the vendor of the controller.
API Key	Enter the API Key that CounterACT must use to communicate, via API, with the controller and obtain information from the controller. ▪ You previously generated this API Key in Meraki Dashboard Configuration Prerequisites, Generate API Key. Re-enter the API Key in the **Verify API Key** field.
Connecting CounterACT Device	Enter the name of the CounterACT device through which all CounterACT-initiated communication with the controller is directed. Only this designated CounterACT device actually communicates with the specified controller. A CounterACT device can only be configured as the Connecting CounterACT Device for one controller.
Comment	(*optional*) Enter comments/descriptive text.

6. Select **Next**. The **Organizations to Query** pane of the Add Controller wizard opens.

Organizations to Query

In the Organizations to Query pane (Step 2), specify which organizational networks the plugin should query for information.

A specific organization can only be queried by a single controller.



To configure the Meraki Organizations to query:

1. In the **Organizations to Query** pane, select one of the following options:
   a. **Query all organizations** - plugin queries the controller about ***all*** organizational networks
   b. **Specify organization(s) to query** - *case sensitive* field. The plugin *only* queries the controller about the networks belonging to those organizations that are specified in this field.

      Case sensitive means, for example, that the entries ***F****inance* and ***f****inance* refer to two ***different*** organizations.

      > Comma-separate multiple entries. For example: **`South0009, 109zone, RegionABCD`**
2. Select **Next**. The **Detection Method** pane opens.

Detection Method

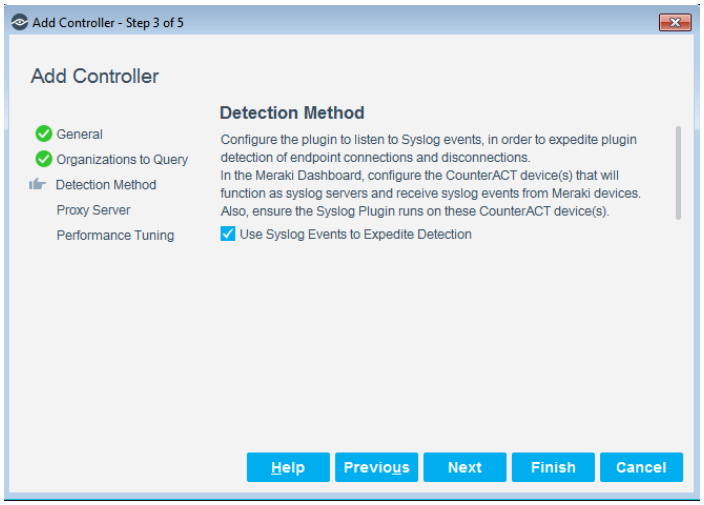
In the Detection Method pane (Step 3), instruct the plugin to listen for syslog events that are sent to CounterACT from Meraki network devices. When this option is selected, plugin detection of endpoint connections to and disconnections from those devices is *expedited*.

With expedited plugin detection, the plugin is configured to listen for syslog events and uses both of the following methods to detect endpoint connections and disconnections:

- Received syslog events
- Periodic polling of the Meraki Dashboard

When the plugin is not configured to listen for syslog events, the plugin detects endpoint connections and disconnections only by its periodic polling of the controller.

This option is enabled by default. To work with the option you must also configure Meraki Dashboard to send syslog information from Switch and Access Point devices.

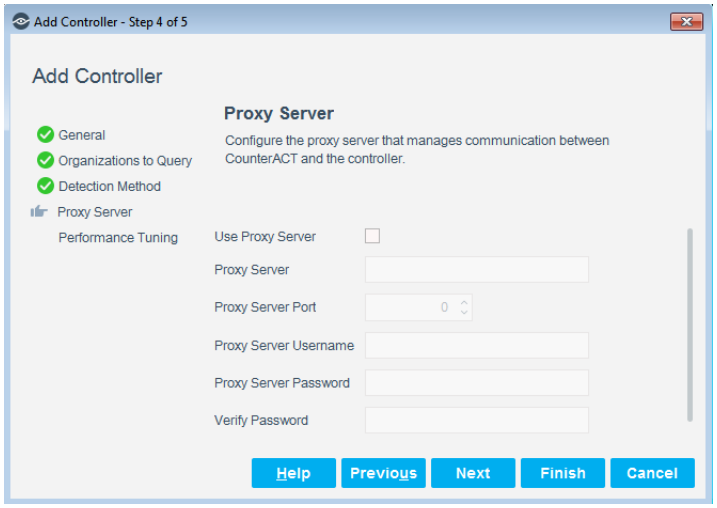


To expedited plugin detection:

1. Verify that the **Use Events to Expedite Detection** option is enabled.
2. Configure Meraki Dashboard to send syslog information from Switch and Access Point devices.
3. Select **Next**. The **Proxy Server** pane opens.

Proxy Server

Define a proxy server in the **Proxy Server** pane (Step 4) if your organization's network security policy *requires* that Internet communication traffic is routed through a proxy server. If this is the case, configure the connection parameters for use by the Connecting CounterACT Device to access the proxy server. The proxy server handles the communication between CounterACT and the Meraki Cloud Dashboard. The Connecting CounterACT Device was previously configured in the General pane.



To configure the proxy server:

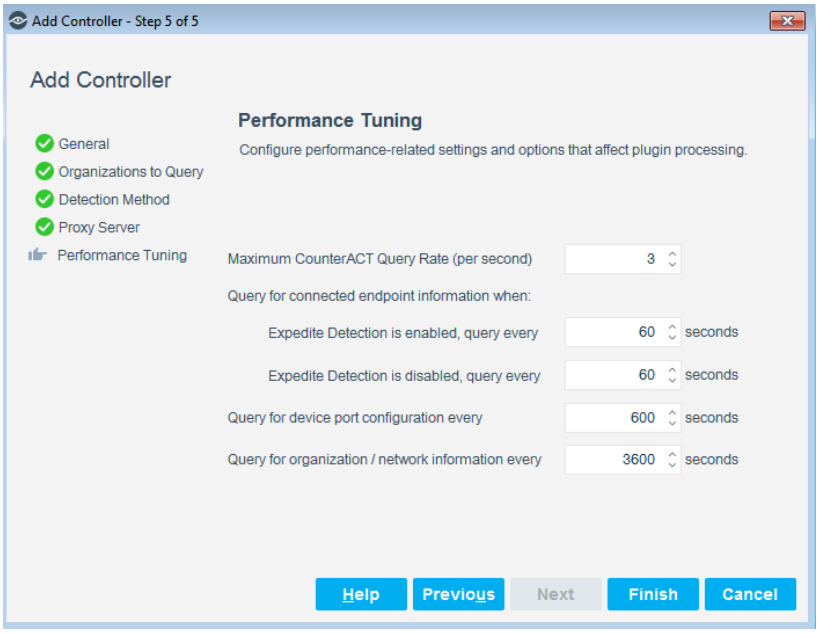
1. In the Proxy Server pane, enable (select) the **Use Proxy Server** option. By default, this option is disabled.
2. In the pane, define the following information (unless otherwise noted, all information is *required* to be defined):

Field	Description
Proxy Server	Enter the IP address of the proxy server.
Proxy Server Port	Select the port that must be used to communicate with the proxy server.
Proxy Server Username	Enter the username for log in access by an authorized account to the proxy server.
Proxy Server Password	Enter the password for log in access by an authorized account to the proxy server. Re-enter the provided password in the **Verify Password** field.

3. Select **Next**. The **Performance Tuning** pane opens.

Performance Tuning

In the **Performance Tuning** pane (Step 5), configure performance-related settings and options that affect plugin processing.



To configure performance-related settings and options:

1. Define or modify the value of any of the following fields (unless otherwise noted, all fields are *optional*ly defined/modified):

Field	Description
Maximum CounterACT Query Rate	Modify the maximum number of plugin queries per second that the Connecting CounterACT Device is allowed send to the cloud management interface. By default, the maximum query rate is 3. The query rate range is 1 - 5.
Expedite Detection is enabled, query every <n> seconds	Modify the frequency of plugin queries for connected endpoint information, when the plugin is configured to use syslog events to expedite detection. By default, this query period is 60 seconds.
Expedite Detection is disabled, query every <n> seconds	Modify the frequency of plugin queries for connected endpoint information, when the plugin is ***not*** configured to use syslog events to expedite detection. By default, this query period is 60 seconds.
Query for device port configuration every <n> seconds	Modify the frequency of plugin queries for switch device port configuration information. By default, this query period is 600 seconds.
Query for organization / network information every <n> seconds	Modify the frequency of plugin queries for all of the controller's information: its organizations, its managed networks and the network devices belonging to its managed networks. By default, this query period is 3600 seconds.

2. Select **Finish**. The *Add Controller* configuration process is finished.

   The Controllers tab displays the new configuration entry. Continue with Test the Plugin Configuration.

Update Controller

The Controllers tab provides the following update plugin configuration functions:

- Edit
- Remove

Edit

Select a controller entry and then select **Edit**. The Edit Controller window opens. Define or modify information fields, enable/disable settings and options that are available in any of the following tabs:

- General
- Organizations to Query
- Detection Method

- Proxy Server
- Performance Tuning

For details about these tabs and their content, see Add Controller.

After editing the plugin configuration for a controller entry and *before* saving the updated plugin configuration, it is recommended to test the plugin configuration for the controller entry. To do so, continue with Test the Plugin Configuration.

Remove

Select one or more than one controller entry and then select **Remove**. Prior to the Console executing the remove request, the following confirmation message is presented:

> *Request to remove the selected controller(s) from the plugin configuration.*
>
> *All plugin interaction with the selected controller(s) will be stopped.*
>
> *Continue?*

- Select **Yes** to execute the removal and then select **Apply** to save the updated plugin configuration in CounterACT.
- Select **No** to cancel the remove request.

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Test the Plugin Configuration

After completing the *Add Controller* configuration process and *before* saving the updated plugin configuration, make sure you test the plugin configuration for the new controller entry. You can test the plugin configuration for an existing controller entry at any time.

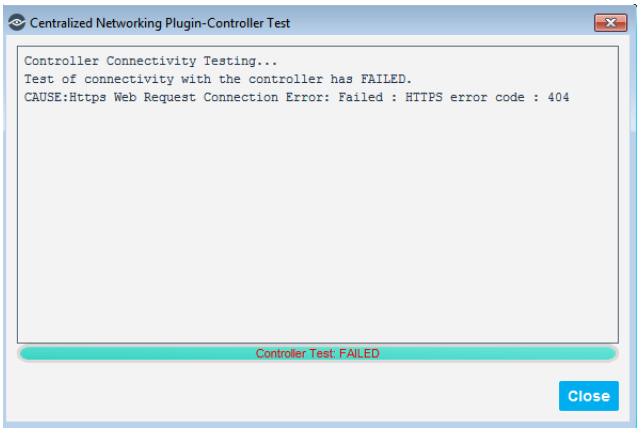
The test verifies plugin configuration validity and checks that the plugin can communicate and work with the selected controller. The following conditions are tested:

- The plugin is running on the designated Connecting CounterACT Device.
- The plugin established a communication connection with the controller:
  - Within the allowed time frame
  - Did not encounter any network problem
  - Did authenticate
  - Used valid API command data

– A match exists between (a) the organizations to query, as specified in the plugin configuration and (b) the controller-provided list of organizations

To test the plugin configuration:

1. In the Controllers tab of the Centralized Network Controller pane, select the controller entry you want to the plugin test to use.
2. Select **Test**. The Centralized Network Controller Plugin-Controller Test window opens. The test automatically runs.



3. If the test fails, information will be provided about the failure:
4. Select **Close**.

If the Controller test succeeded, using:

- A new controller entry

  or

- An existing, updated (edited) controller entry

Then, in the Controllers tab, select **Apply** to save the new/updated plugin configuration in CounterACT.

After saving the plugin configuration for a new controller entry:

- Select the Networks Tab to review about the third party solution networks that the plugin is monitoring.
- Select the Devices Tab to review information about the devices in each third party solution network.

Console Information Display

This section describes the following information displays provided in the Console:

- The Centralized Network Controller Pane
- The Home Tab
- The Asset Inventory Tab

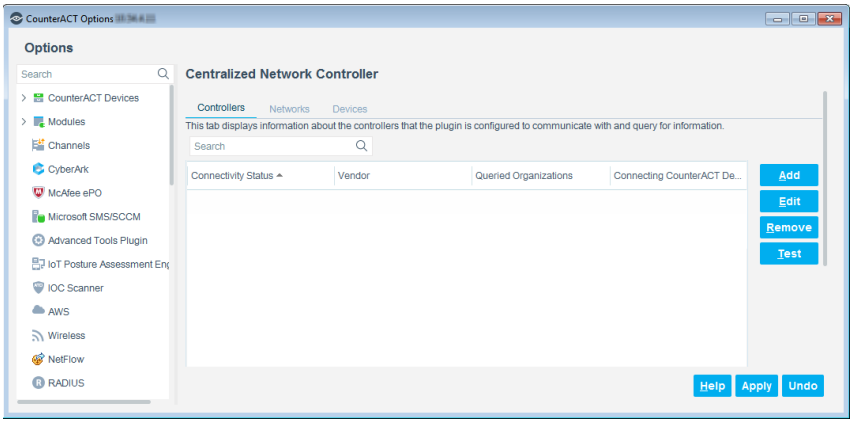
Centralized Network Controller Pane

The Console Centralized Network Controller pane provides the following plugin information displays:

- Controllers Tab
- Networks Tab
- Devices Tab

Controllers Tab

The Controllers tab displays information about the controllers that represent the third party solution the plugin is configured to communicate with and query.



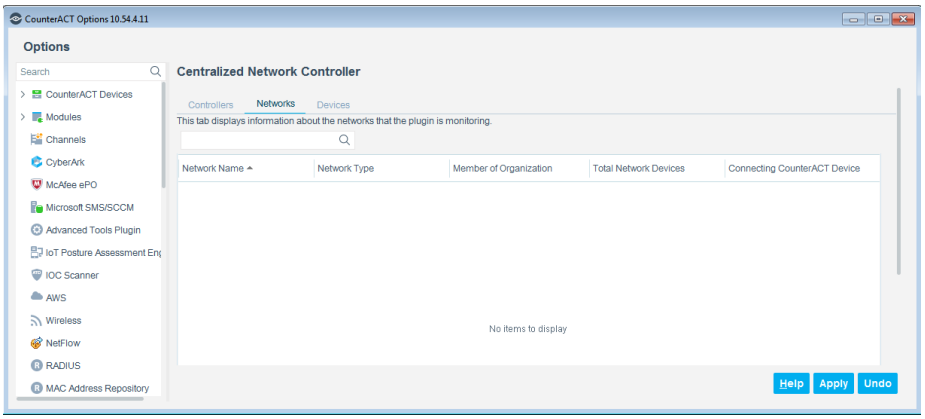
The following controller-related information is available:

Column	Description
Connectivity Status	Identifies the status of the configured entry or the communication status with the controller. The possible statuses are as follows: ▪ **New** (hourglass icon) - This configured entry is newly added, but has not been saved (select **Apply** to save). ▪ **Up** (green icon) - Plugin-controller communication is successful. ▪ **Down** (red icon) - Either the plugin is NOT running on the Connecting CounterACT Device or plugin-controller communication NOT successful. *This column appears by default*.
Vendor	The controller's vendor. *This column appears by default*.
Queried Organizations	The organizations whose networks are being monitored by the plugin. *This column appears by default*.
Connecting CounterACT Device	The CounterACT device through which all CounterACT-initiated communication with the cloud management interface is directed. *This column appears by default*.
Comment	User-provided comments/descriptive text. *This column appears by default*.

Column	Description
Detection Method	The methods used to detect endpoint connections and disconnections. The possible methods are as follows: ▪ Polling (*only*) ▪ Polling and Events
Maximum Query Rate	Maximum queries per second that the Connecting CounterACT Device is allowed to send to the cloud management interface. The default, Connecting CounterACT Device maximum query rate is 3 queries per second.

Networks Tab

The Networks tab displays information about the third party solution networks that the plugin is monitoring.



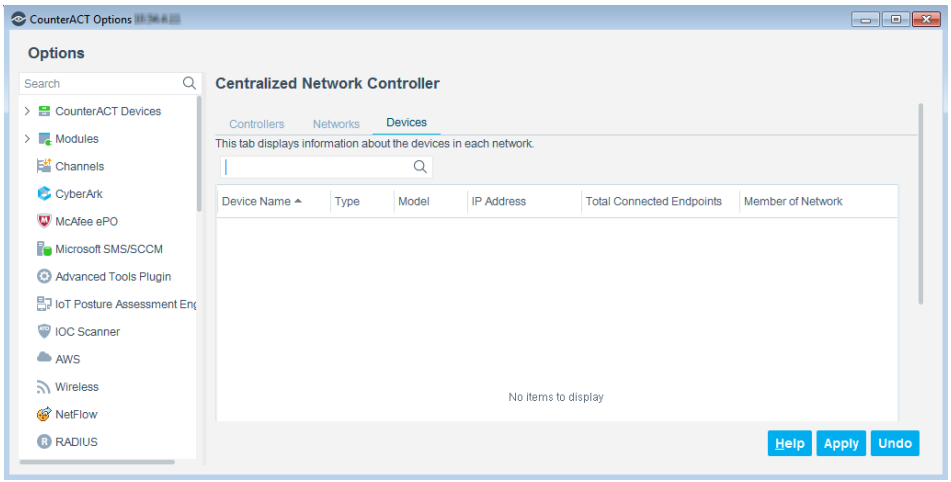
The following network-related information is available:

Column	Description
Network Name	Name of the network. *This column appears by default*.
Member of Organization	Name of the organization to which the network belongs. *This column appears by default*.
Network Type	Type of network. The possible types are as follows: ▪ Wireless ▪ Switch ▪ Combined (both wireless and switch) *This column appears by default*.
Vendor	The network's vendor. *This column appears by default*.
Total Network Devices	Total number of devices detected in the network. *This column appears by default*.
Network Time Zone	The time zone in which the network is located.

Column	Description
Connecting CounterACT Device	The CounterACT device through which all CounterACT-initiated communication with the cloud management interface, about the network, is directed. *This column appears by default*.

Devices Tab

The Devices tab displays information about the devices in each third party solution network.



The following device-related information is available:

Column	Description
Device Name	Name of the device. *This column appears by default*.
Type	Type of device. The possible types are as follows: ▪ Wireless ▪ Switch *This column appears by default*.
Model	Model of the device. *This column appears by default*.
IP Address	IP address of the device. *This column appears by default*.
Total Connected Endpoints	Total number of endpoints connected to the device. *This column appears by default*. See about Plugin Connected Endpoint Reporting.
Last Event Received	The date of the last syslog event that the plugin received from the device.
MAC Address	MAC address of the device.
Member of Network	Name of the network to which the device belongs. *This column appears by default*.
Member of Organization	Name of the organization to which the device belongs.

Column	Description
Network Vendor	The vendor of the network to which the device belongs.
Serial Number	Serial number of the device.

Plugin Connected Endpoint Reporting

1. For Meraki MS switches, the plugin supports VoIP detection for phones connected to either access ports or trunk ports. All potential switch ports (access and trunk) must have configured voice VLANs.

   This means that the plugin does detect and report about both a VoIP phone and, if present, the endpoint that is connected, through the VoIP phone, to the switch.

2. The plugin *does not* detect and report about endpoints that are connected to Meraki switch trunk ports that do not have configured voice VLANS.

Home Tab

The network devices and connected endpoints that the Centralized Network Controller Plugin discovers, via its monitoring of cloud-managed networks, display as entries in the **All Hosts** pane in the Console's **Home** tab. The following information is displayed in the **All Hosts** pane for network device entries that are discovered by the plugin:

Wireless Access Points:

- Vendor
- WLAN AP Name
- Network Function - Lightweight AP (lightweight access point)
- Network Name
- Organization Name

Switches:

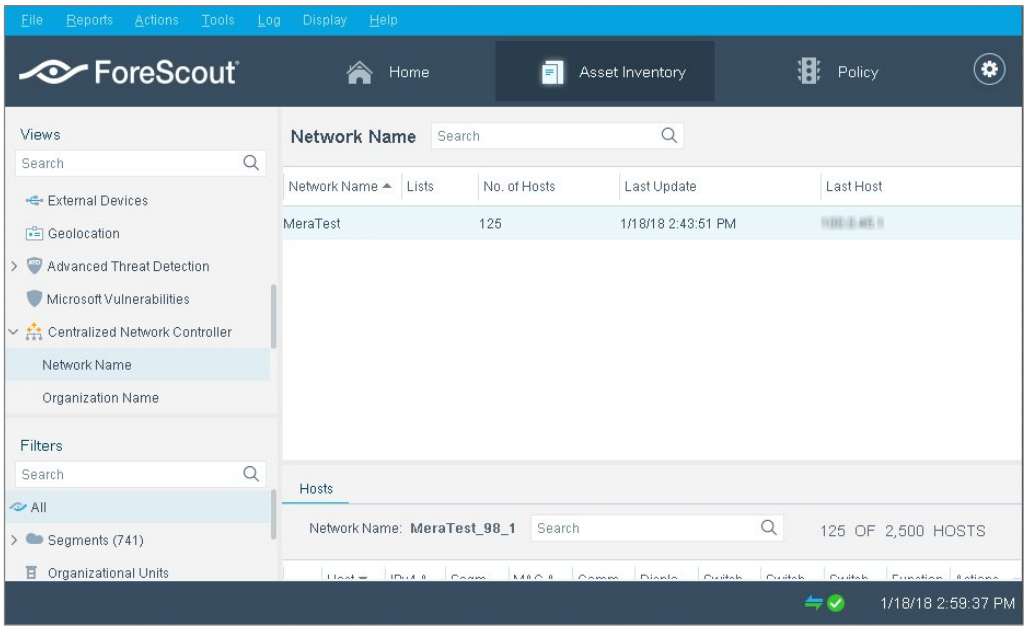
- Vendor
- Switch Hostname
- Network Name
- Organization Name

Asset Inventory Tab

The Asset Inventory view displays how wired and wireless endpoints are distributed across the Meraki organizations and networks.

This means you do not need to go to Meraki dashboard to see how many endpoints are connected to each access point. You can also:

- View network and organizational information reported by the plugin.
- Incorporate inventory detections into policies.



The following information is available:

Information	Description
Network Name	Current information about the networks to which detected endpoints are connected.
Organization Name	Current information about the organizations to which detected endpoints belong.

Creating CounterACT Policies

Create CounterACT policies to resolve endpoint-based properties. For example create a policy that detects all endpoints connected to a specific network.

Policy Properties

The Centralized Network Controller plugin resolves properties from the following property groups:

- Centralized Network Controller Properties
- Wireless
- Switch
- Track Changes

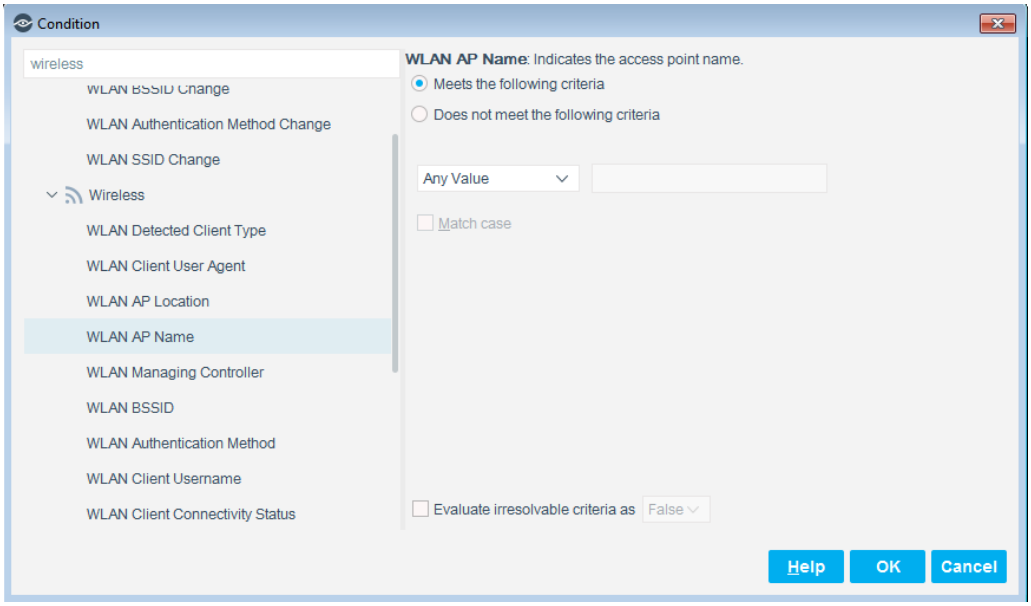
Centralized Network Controller Properties

The plugin resolves the following network-related properties:

Property	Description
Network Name	Name of the network to which the detected endpoint is connected.
Organization Name	Name of the organization to which the detected endpoint belongs.

Wireless Properties

The plugin resolves various properties related to detected Meraki wireless access points.

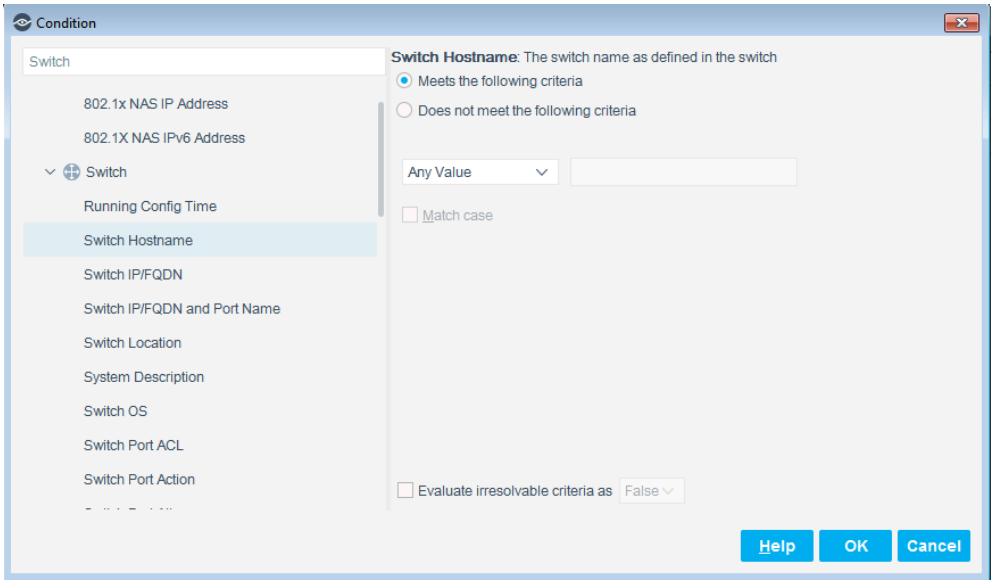


Property	Description
WLAN AP Name	Name of the access point to which the wireless client is connected.
WLAN Client Connectivity Status	Identifies whether the wireless client is connected to an access point.
WLAN Client Username	DNS name employed by the wireless client to authenticate with the access point.
WLAN Client VLAN	VLAN to which the wireless client is connected.
WLAN Device IP/FQDN	Either the IP address or the fully qualified domain name (FQDN) of the WLAN device that is managing the wireless client.
WLAN Device Vendor	Vendor of the WLAN device that manages the wireless client.

Other CounterACT wireless properties are not resolved by this plugin.

Switch Properties

The plugin resolves various properties related to detected Meraki switches.



Property	Description
Switch Hostname	Switch name as defined in the switch.
Switch IP/FQDN	Either the IP address or the fully qualified domain name (FQDN) of the switch.
Switch IP/FQDN and Port Name	Either the IP address or the fully qualified domain name (FQDN) name of the switch and the port name (the physical Ethernet interface information of the port). The format is *<IP address/FQDN>:<port>*.
Switch Port Alias	Description of the port as defined in the switch configuration.
Switch Port Connect	The physical connectivity between the connected endpoint and the switch port.
Switch Port Name	The hard-coded port name.
Switch Port VLAN	The VLAN associated with the switch port.
Switch Port Voice Device	Identifies whether the endpoint connected to the switch port is a VoIP device.
Switch Port Voice VLAN	Switch port VLAN to which the VoIP endpoint is connected.
Switch Vendor	Switch vendor name.
Switch VoIP Port	Identifies whether the switch port is a VoIP port.

Other CounterACT switch properties are not resolved by this plugin.

Track Changes Properties

The plugin resolves the information of the following Track Changes properties.

Centralized Network Controller Track Changes Properties

Property	Description
Centralized Network Controller Network Name Change	Identifies that a change in value occurred in the **Network Name** property.
Centralized Network Controller Organization Name Change	Identifies that a change in value occurred in the **Organization Name** property.

Wireless Track Changes Properties

Property	Description
WLAN AP Name Change	Identifies that a change in value occurred in the **WLAN AP Name** property.
WLAN Client Connectivity Status Change	Identifies that a change in value occurred in the **WLAN Client Connectivity Status** property.
WLAN Client Username Change	Identifies that a change in value occurred in the **WLAN Client Username** property.
WLAN Client VLAN Change	Identifies that a change in value occurred in the **WLAN Client VLAN** property.
WLAN Device IP/FQDN Change	Identifies that a change in value occurred in the **WLAN Device IP/FQDN** property.

Switch Track Changes Properties

Property	Description
Switch Hostname Change	Identifies that a change in value occurred in the **Switch Hostname** property.
Switch IP/FQDN Change	Identifies that a change in value occurred in the **Switch IP/FQDN** property.
Switch IP/FQDN and Port Name Change	Identifies that a change in value occurred in the **Switch IP/FQDN and Port Name** property.
Switch Port Alias Change	Identifies that a change in value occurred in the **Switch Port Alias** property.
Switch Port Connectivity Change	Identifies that a change in value occurred in the **Switch Port Connect** property.
Switch Port Name Change	Identifies that a change in value occurred in the **Switch Port Name** property.

Property	Description
Switch Port VLAN Change	Identifies that a change in value occurred in the **Switch Port VLAN** property.
Switch Port Voice Device Change	Identifies that a change in value occurred in the **Switch Port Voice Device** property.
Switch Port Voice VLAN Change	Identifies that a change in value occurred in the **Switch Port Voice VLAN** property.

Policy Actions

The Centralized Network Controller Plugin does not provide CounterACT control actions. You can however incorporate CounterACT RADIUS Plugin actions to control detected wireless endpoints. For more information refer to the *Enable CounterACT RADIUS-based Management of Wireless Clients* section in the Wireless Plugin Configuration Guide. See Additional CounterACT Documentation for information about how to access this document.

Network Module Information

The Centralized Network Controller Plugin is installed with the CounterACT Network Module.

The Network Module provides network connectivity, visibility and control through the following plugin integrations:

- Centralized Network Controller Plugin
- Switch Plugin
- VPN Concentrator Plugin
- Wireless Plugin

The Network Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Plugins listed above are released and rolled back with the Network Module.

Refer to the *CounterACT Network Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See *Additional CounterACT Documentation* for information about how to access the module guide.

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**.

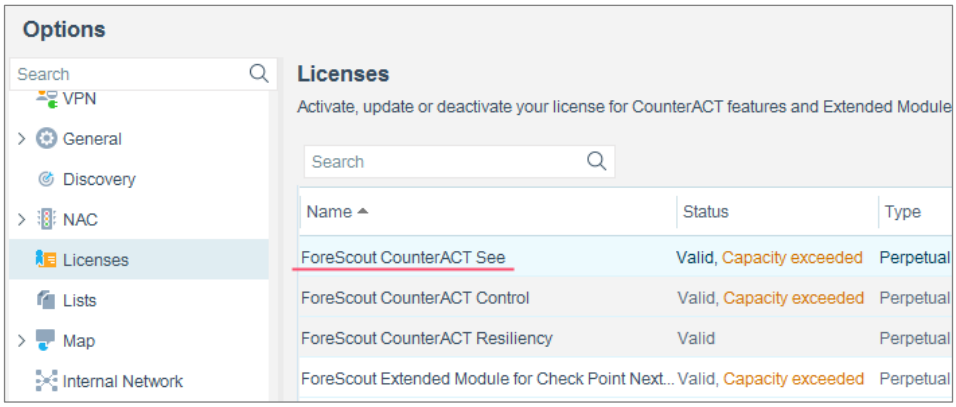
Documentation Portal

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

2018-04-10 09:21