



Forescout

Network Module: Centralized Network Controller Plugin

Configuration Guide

Version 1.2.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-07-08 23:35

Table of Contents

About the Centralized Network Controller Integration	5
CNC Plugin Integration: Cisco ACI	5
Use Cases: Data Center Visibility	6
Baseline Deployment Guidelines	6
Supported Vendor Products	7
Requirements	7
Forescout Requirements	7
Network Requirements	7
Third-Party Product Requirements	7
Configuration Prerequisites	8
Configure the Plugin	8
Add a Controller	9
Verify That the Plugin Is Running	16
Test the Plugin Configuration	17
Edit a Controller	18
Remove a Controller	18
Distribute Plugin Processing Load	19
Initiate Plugin Polling	19
Property Resolution	21
Console Information Display	24
Centralized Network Controller Pane	24
Home Tab	26
Asset Inventory Tab	27
CNC Plugin Integrations: Cisco Meraki and Juniper Mist	29
How It Works	30
Baseline Deployment Guidelines	32
Supported Vendor Products	32
Requirements	33
Forescout Requirements	33
Network Requirements	33
Third-Party Product Requirements	34
Configuration Prerequisites	34
For a Cisco Meraki Cloud-Managed Network	34
For a Juniper Mist Cloud-Managed Network	37
Configure the Plugin	38
Add a Controller	38
Edit a Controller	47
Remove a Controller	47
Verify That the Plugin Is Running	48
Test the Plugin Configuration	48
Console Information Display	50
Centralized Network Controller Pane	50
Home Tab	54
Asset Inventory Tab	55

Creating ForeScout Policies.....	56
Property Resolution	56
Action Control	60
Network Module Information	62
Additional Forescout Documentation.....	62
Documentation Downloads	62
Documentation Portal	63
Forescout Help Tools.....	63

About the Centralized Network Controller Integration

The Centralized Network Controller Plugin (CNC Plugin) is a component of the Forescout 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. The Forescout platform integrates with centralized network controller solutions to offer customers full visibility into their networks, including the network devices and the endpoints connected to those devices.

With this plugin version, Forescout integrates its offering with the following centralized network controller solutions:

- [Cisco Application Centric Infrastructure \(ACI\)](#)
- [Cisco Meraki Cloud Management Platform](#)
- [Juniper Mist Wireless LAN Platform](#)

To use the plugin, you should have a solid understanding of

- Cisco ACI software-defined networking architecture, functionality and terminology. For information, refer to <https://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html>
- Cisco Meraki concepts, functionality and terminology, especially the Meraki Dashboard organizational structure – Organization/Network/Device. For information, refer to <https://documentation.meraki.com/>.
- Juniper Mist concepts, functionality and terminology, especially the Mist Dashboard organizational structure – Organization/Site/Device. For information, refer to <https://www.juniper.net/us/en/products-services/wireless/mist/>

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

CNC Plugin Integration: Cisco ACI

The Forescout platform integrates with a wide range of different data center and cloud platforms to enable operational visibility. Cisco ACI software-defined networking architecture is the last addition data center specific integration. By discovery of ACI connected entities and the associated physical connections and logical networking overlays, the CNC Plugin provides enterprise IT greater data center visibility. This includes context, from basic virtual machine operating system properties to the more advanced services notes and ACI VMM properties for VMware.

The CNC Plugin integration with Cisco ACI software-defined networking architecture, together with the Switch Plugin, expand the Forescout platform's ability to recognize endpoints in different ACI network configurations. For example, CNC Plugin

monitoring an ACI fabric for IP address, tenant and endpoint group info, while the Switch Plugin manages downstream L2 switches and obtains their MAC address.

Regarding the ACI networking deployment model (L2 or L3), the Forescout platform gathers a range of operational context directly from the Application Policy Infrastructure Controller (APIC) managing the ACI fabric ESXi hosts. This includes the option to collect context from multiple ACI fabrics.

Use Cases: Data Center Visibility

Visibility use cases include:

- Full data center visibility: CNC Plugin supplies information about all ACI fabric-connected endpoints regardless of networking environment (upstream L3 switch connected to ACI, vSphere integrated with ACI via VMM, ACI endpoints connected to downstream L2 switch)
- Update ServiceNow's CMDB:
 - With new ACI fabric-connected endpoints as they become active
 - With state changes to existing ACI fabric-connected endpoints and the associated tenant, endpoint group and node name, in support of enterprise asset intelligence.
- CNC Plugin supplies information about all ACI fabric-connected endpoints associated with a specific tenant or endpoint group. Then, based on the criticality of these services, run different assessment policies to ensure compliance.

Baseline Deployment Guidelines

Forescout recommends the following baseline deployment guidelines:

- The CNC Plugin communicates with the ACI environment through the APIC, the controller in the Cisco ACI architecture. Regardless of the number of APICs in the deployment, typically 3 or 5, the plugin needs to be configured to know of only one APIC for communication. The CNC Plugin automatically learns the IP addresses of the other APICs. This ensures that if primary APIC stops operating, then CNC Plugin can communicate with one of the other APICs in the cluster.
- Per Connecting CounterACT Device, all its plugin-monitored ACI tenant groups can host a maximum total of 20,000 connected endpoints. This maximum is due to the processing capacity of Forescout's largest Appliance.
- Select a Forescout Appliance, rather than the Enterprise Manager, as the Connecting CounterACT Device.

Supported Vendor Products

In Cisco ACI fabrics that include virtual machine monitors (VMMs) - controller hosts, hypervisor hosts - CNC Plugin only supports retrieval and display of information for the following VMM vendors:

- VMWare

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Requirements

This section describes the requirements for running the Forescout Centralized Network Controller Plugin and configuring it to work with a Cisco ACI software-defined network.

- [Forescout Requirements](#)
- [Network Requirements](#)
- [Third-Party Product Requirements](#)

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Network Module 1.2.1 with the Centralized Network Controller Plugin

Network Requirements

Perform the following enterprise firewall configurations to support communication between Forescout and the Cisco ACI:

- Permit communication from the Connecting CounterACT Device(s) to the ACI Application Policy Infrastructure Controllers (APICs) on TCP/443 for the ACI fabrics that are being monitored by the Centralized Network Controller Plugin
- If a proxy server is required for use between Forescout and the ACI APICs, you must permit the proxy server to connect to the APICs on TCP/443

Third-Party Product Requirements

The CNC Plugin supports Cisco ACI multi-pod and does not support ACI multi-site.

When planning for a single Connecting CounterACT Device to monitor multiple Cisco ACI fabrics, you must make sure to configure each of these fabrics with a unique name.

Authentication

The CNC Plugin requires read-only permissions on an account defined in APIC. This account can be authenticated using any of the following methods:

- Username and password
- TACACS+
- Active Directory

The plugin does not support:

- Username and password authentication with token
- Certificate-based authentication.

Endpoint Requirements

The CNC Plugin supports retrieval and display of information only for endpoints connected directly or indirectly to the ACI fabric and only for endpoints having a 1:1 MAC address-IP address assignment.

The plugin does not support visibility of endpoints that are using the same MAC address for multiple IP Addresses.

Discovery behavior of endpoints having the identical IP address, whether under the same tenant or under different tenants, is not predictable. The last/recent discovered endpoint could overwrite the information/properties of the endpoint having the identical IP address, which was previously discovered.

Configuration Prerequisites

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

- Add ACI endpoint subnets to the Forescout platform segments
- Add ACI node Out-Of-Band Management interface IP address and/or In-Band Management interface IP address to the Forescout platform segments

Configure the Plugin

This section describes how to configure the Centralized Network Controller Plugin (CNC Plugin) so that it can monitor a Cisco ACI software-defined network.

The section presents the following plugin configuration topics:

- [Add a Controller](#)
- [Test the Plugin Configuration](#)
- [Edit a Controller](#)
- [Remove a Controller](#)
- [Distribute Plugin Processing Load](#)

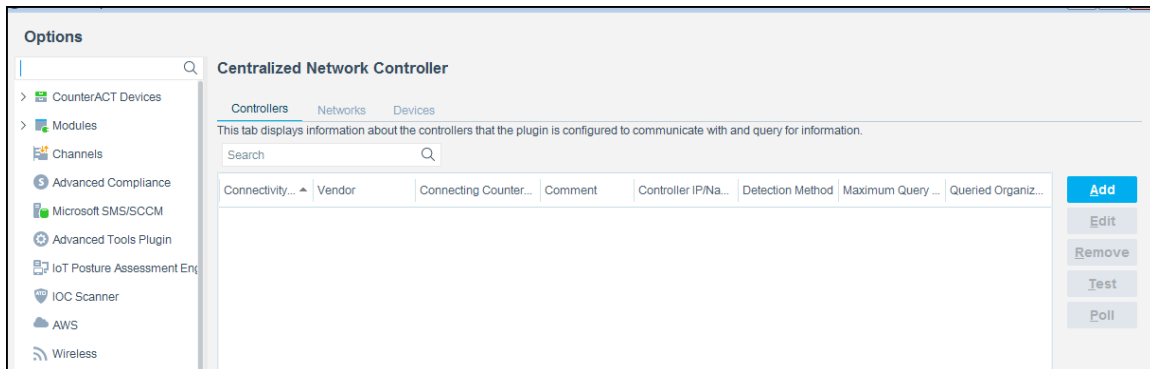
Add a Controller

Configure the Centralized Network Controller Plugin to monitor ACI fabrics of a Cisco ACI software-defined network. Each entry in the Controllers tab configures the plugin to monitor a single ACI fabric. The plugin can monitor multiple ACI fabrics.

Multiple Appliances can monitor a large ACI fabric. This is accomplished by configuring the CNC Plugin running on individual Appliances to monitor different tenants in the large ACI deployment. Moreover, these individual Appliances can each be configured to communicate, by default, with a specific APIC to spread load across the APIC cluster. See [Distribute Plugin Processing Load](#).

To add an ACI fabric:

1. In the Console, 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 *Controllers* tab, select **Add**. The [General](#) pane opens.
5. Configure the plugin to monitor an ACI fabric using the panes of the Add Controller wizard:
 - a. [General](#)
 - b. [Communication](#)
 - c. [Proxy Server](#)
 - d. [Tenants](#)
 - e. [Performance Tuning](#)

General

In the *General* pane, configure basic information needed by the plugin to monitor an ACI fabric of a Cisco ACI software-defined network.

The screenshot shows a window titled "Add Controller - Step 1". Inside, the "General" tab is active, with a sub-header "General" and a description: "Configure the information defining the plugin-controller working relationship." Below this, there are three input fields: "Vendor" with a dropdown menu showing "Cisco ACI", "Connecting CounterACT Device" with a dropdown menu, and "Comment" with a text box. At the bottom, there are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

To configure information for monitoring an ACI fabric:

1. In the *General* pane of the Add Controller wizard, define the following:

Field	Description
Vendor	From the drop-down list, select the <i>Cisco ACI</i> entry.
Connecting CounterACT Device	<p>Enter the name of the Enterprise Manager/Appliance through which all Forescout platform-initiated communication with the ACI fabric is directed. Only this designated Enterprise Manager/Appliance actually communicates with the ACI fabric.</p> <p>An Enterprise Manager/Appliance can only be configured as the Connecting CounterACT Device for a single, plugin-supported vendor, this being either Cisco ACI, Cisco Meraki or Juniper Mist.</p> <p>Forescout recommends choosing an Appliance, rather than the Enterprise Manager, as the Connecting CounterACT Device.</p>
Comment	(<i>optional</i>) Enter comments/descriptive text about the plugin-monitored ACI fabric.

Configure plugin ACI fabric monitoring, using any of the following Connecting CounterACT Device assignments:

- Per Connecting CounterACT Device, a single ACI fabric
- Per Connecting CounterACT Device, multiple ACI fabrics (each fabric is uniquely named)

- Multiple Connecting CounterACT Devices, each assigned the same ACI fabric, where:
 - › The plugin monitors a mutually exclusive set of tenant groups (load balance plugin processing)

2. Select **Next**. The [Communication](#) pane opens.

Communication

In the *Communication* pane, configure the login information that the plugin requires in order to access and retrieve information from the Application Policy Infrastructure Controllers (APICs) that manage the ACI fabric.

The screenshot shows a window titled "Add Controller - Step 2 of 5". On the left, a sidebar lists configuration steps: General (checked), Communication (selected), Proxy Server, Tenants, and Performance Tuning. The main area is titled "Communication" and contains the instruction: "Configure information needed by the plugin to communicate with the Cisco ACI controller." Below this are six input fields: "Controller IP/Name", "Username", "Password", "Verify Password", "Domain (optional)", and "Discovered Controller IPs". At the bottom, there are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

To configure communication with fabric APICs:

1. In the *Communication* pane of the Add Controller wizard, define the following:

Field	Description
Controller IP/Name	<p>Enter either the IPv4 address or the fully qualified domain name (FQDN) of the APICs that the plugin is to monitor. You can enter a maximum of 5 APIC entries.</p> <p>When multiple APICs manage the ACI fabric, it is not necessary to provide the IP address/FQDN of all the APICs managing the ACI fabric. Using the entered APIC IP addresses/FQDNs, the Forescout platform discovers/retrieves the IP address of all the APICs that are managing the plugin-monitored ACI fabric. Per APIC, the plugin retrieves its IP address, in the following, preferential order:</p> <ul style="list-style-type: none"> ▪ IPv4 Out-Of-Band Management interface IP address ▪ IPv4 In-Band Management interface IP address

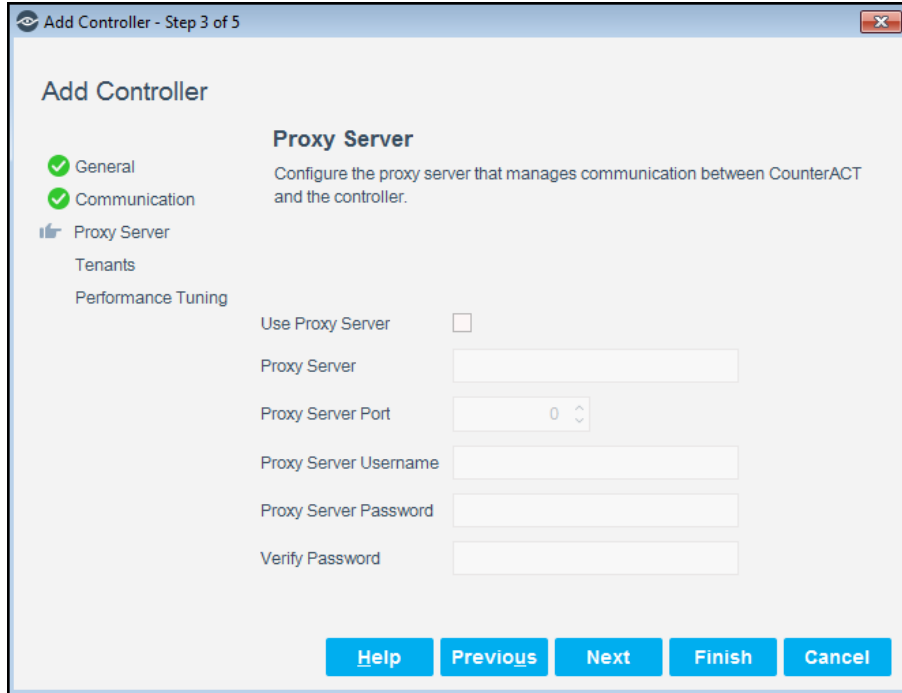
Field	Description
Username	<p>Enter the APIC administrator username that the plugin uses to log in to the APIC. This username must be assigned the following authorization:</p> <ul style="list-style-type: none"> SecurityDomain all Read privilege to use REST API to read/retrieve information from the APICs about the following ACI managed objects: topSystem, fabricNode, l1PhysIf, fvTenant, ethpmPhysIf, compHv, compVm and fvCEp <p>If the administrator username is not assigned the required authorization, plugin information retrieval fails.</p>
Password	<p>Enter the administrator password that the plugin uses to log in to the APIC.</p> <p>Re-enter the provided password in the Verify Password field.</p>
Domain	<p>(<i>optional</i>) If the APIC authenticates usernames by querying an Active Directory server, enter the Active Directory domain name that the plugin must use to log in to the APIC.</p>
Discovered Controller IPs	<p>View only field</p> <p>Displays plugin-discovered IP address of the APICs, in the plugin-monitored ACI fabric, whose IP address you did not define in the Controller IP/Name field.</p>

At any given time, the Forescout platform communicates with only a single APIC managing the ACI fabric. The Forescout platform always attempts to log in to the first APIC IP address provided in the *Controller IP/Name* field. If this APIC is either not accessible or it shuts down, the Forescout platform then attempts to log in to the second APIC IP address provided in the *Controller IP/Name* field. This process continues onward to the next APIC IP address/FQDN entry in the order provided in the *Controller IP/Name* field. When APICs that are defined in the *Controller IP/Name* field are down/not accessible, then, as a fallback, the plugin attempts to access/log in to any discovered APICs, which appear in the *Discovered Controller IPs* field.

2. Select **Next**. The [Proxy Server](#) pane opens.

Proxy Server

Define a proxy server in the *Proxy Server* pane, 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 the Forescout platform and the APICs managing the ACI fabric. The Connecting CounterACT Device was previously configured in the *General* pane.

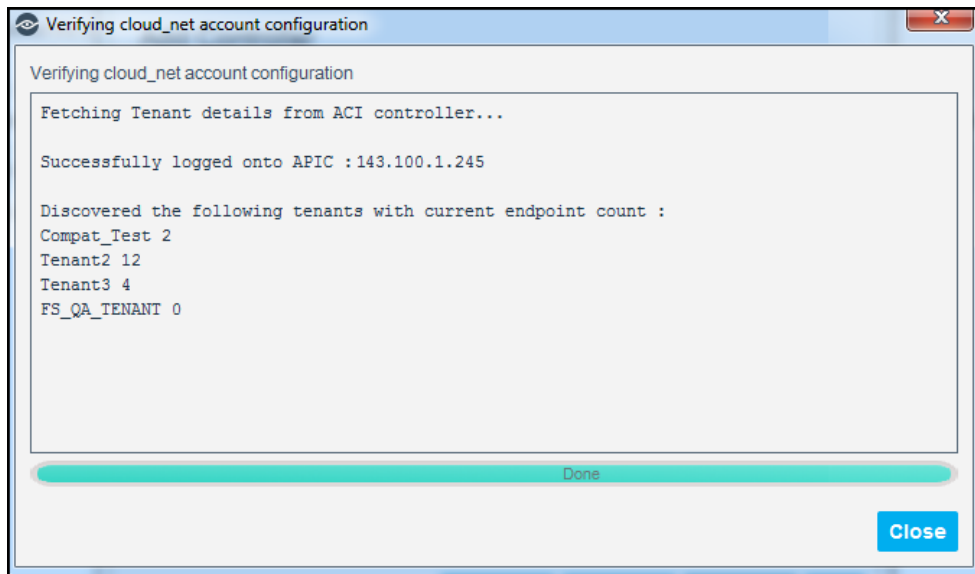


The screenshot shows a window titled "Add Controller - Step 3 of 5". On the left, a sidebar lists configuration steps: "General" (checked), "Communication" (checked), "Proxy Server" (selected with a thumbs-up icon), "Tenants", and "Performance Tuning". The main area is titled "Proxy Server" and contains the instruction: "Configure the proxy server that manages communication between CounterACT and the controller." Below this are several fields: "Use Proxy Server" (checkbox, unchecked), "Proxy Server" (text box), "Proxy Server Port" (spin box with value 0), "Proxy Server Username" (text box), "Proxy Server Password" (text box), and "Verify Password" (text box). At the bottom are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

If communication with fabric APICs does not require a proxy server:

1. Select **Next**.

Selecting **Next** triggers the plugin to retrieve from one of the APICs, specified in the *Controller IP/Name* field of the *Communications* pane, the list of all the tenant groups of the ACI fabric. A progress window opens that displays the list of retrieved tenants.



The screenshot shows a progress window titled "Verifying cloud_net account configuration". The text inside the window reads: "Verifying cloud_net account configuration", "Fetching Tenant details from ACI controller...", "Successfully logged onto APIC : 143.100.1.245", and "Discovered the following tenants with current endpoint count :". Below this is a list of tenants: "Compat_Test 2", "Tenant2 12", "Tenant3 4", and "FS_QA_TENANT 0". At the bottom of the window is a green progress bar labeled "Done" and a "Close" button.

2. Select **Close**. The [Tenants](#) pane opens.

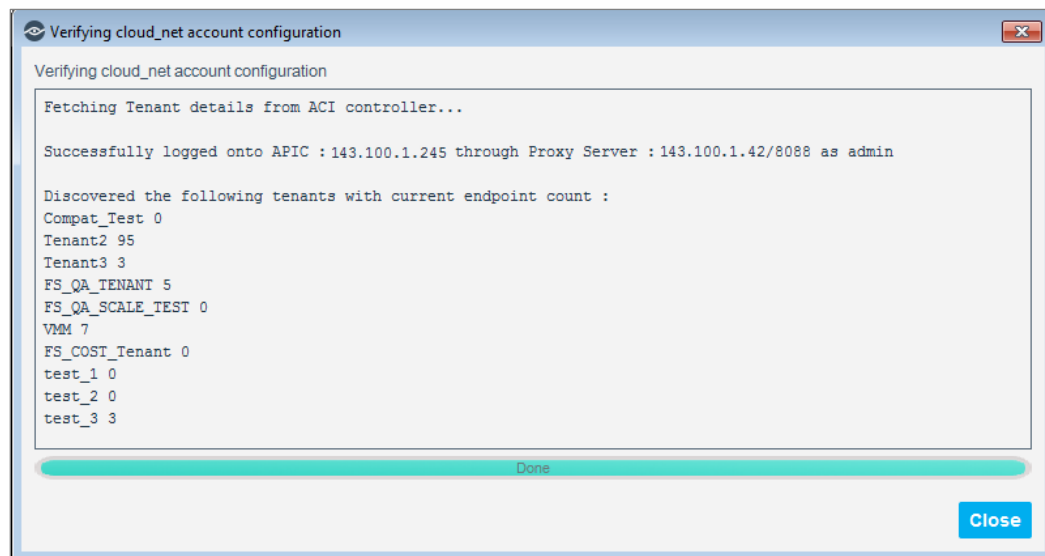
To configure communication with fabric APICs through a proxy server:

1. In the *Proxy Server* pane of the Add Controller wizard, enable (select) the **Use Proxy Server** option. By default, this option is disabled.
2. Define the following information (unless otherwise noted, all information is required):

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**.

Selecting **Next** triggers the plugin to retrieve from one of the APICs, specified in the *Controller IP/Name* field of the *Communications* pane, the list of all the tenant groups of the ACI fabric. A progress window opens that displays the list of retrieved tenants.

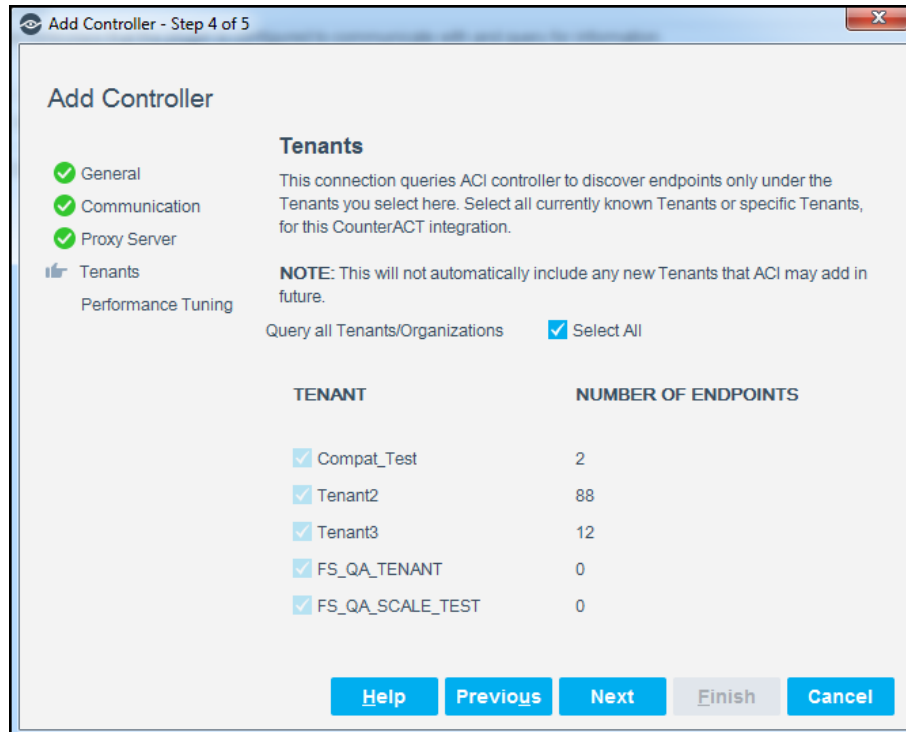


4. Select **Close**. The [Tenants](#) pane opens.

Tenants

In the *Tenants* pane, select the ACI tenant groups that the plugin monitors when querying an APIC managing the ACI fabric. The plugin requests information about connected endpoints that belong to the selected tenant groups. This supports plugin-management of ACI fabrics having a huge number of endpoints, although you may need to use multiple Connecting CounterACT Devices. For example, an ACI fabric has

four tenant groups with each group having 10,000 endpoints. The plugin can manage this ACI using two Connecting CounterACT Devices by assigning two tenants to each Connecting CounterACT Device.

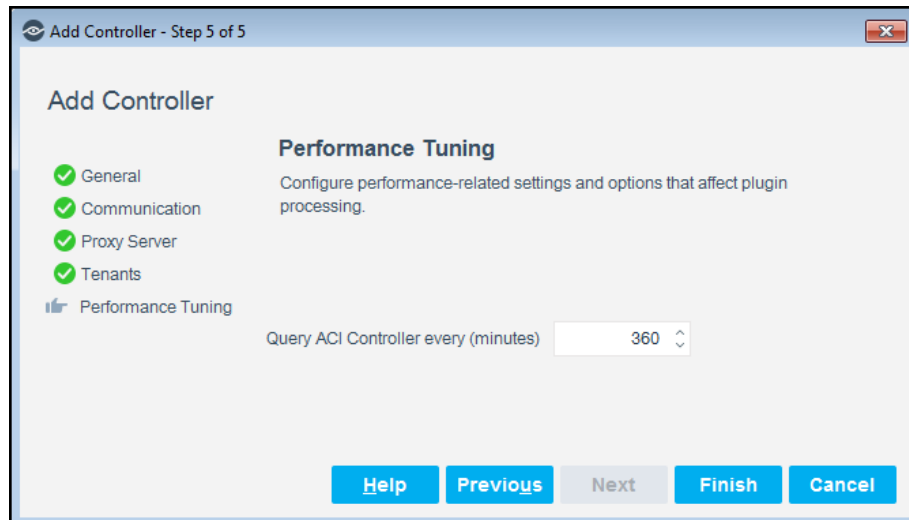


To configure monitoring of fabric tenant groups:

1. In the *Tenants* pane of the Add Controller wizard, do any of the following:
 - a. Select **Query all Tenants/Organizations** – the plugin queries the APIC about **all** ACI tenant groups of the ACI fabric.
 - b. Select individual tenant groups from the tenant list. The plugin queries the APIC about the **selected** ACI tenant groups of the ACI fabric.
2. Select **Next**. The [Performance Tuning](#) pane opens.

Performance Tuning

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



To configure performance-related settings and options:

1. Modify the value of any of the following fields (unless otherwise noted, all information is *optionally* modified):

Field	Description
Query ACI Controller every (minutes)	<p>The plugin uses REST API to periodically poll the APIC and retrieve information about endpoints, tenants, leaf switch ports and fabric nodes. Modify the frequency with which the plugin polls the APIC for ACI fabric information. The default, polling frequency is 360 minutes.</p> <p>See also Initiate Plugin Polling.</p> <p>The plugin also uses the WebSocket notification mechanism to receive information updates about ACI fabric information (endpoint and other APIC-managed object information). The plugin subscribes to the APIC to receive its WebSocket notifications. This method expedites plugin ability to provide updated ACI fabric endpoint visibility (information retrieval).</p>

2. Select **Finish**. The *Add Controller* configuration process is finished.
- The *Controllers* tab lists the new Cisco ACI fabric entry. Continue with [Test the Plugin Configuration](#).

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

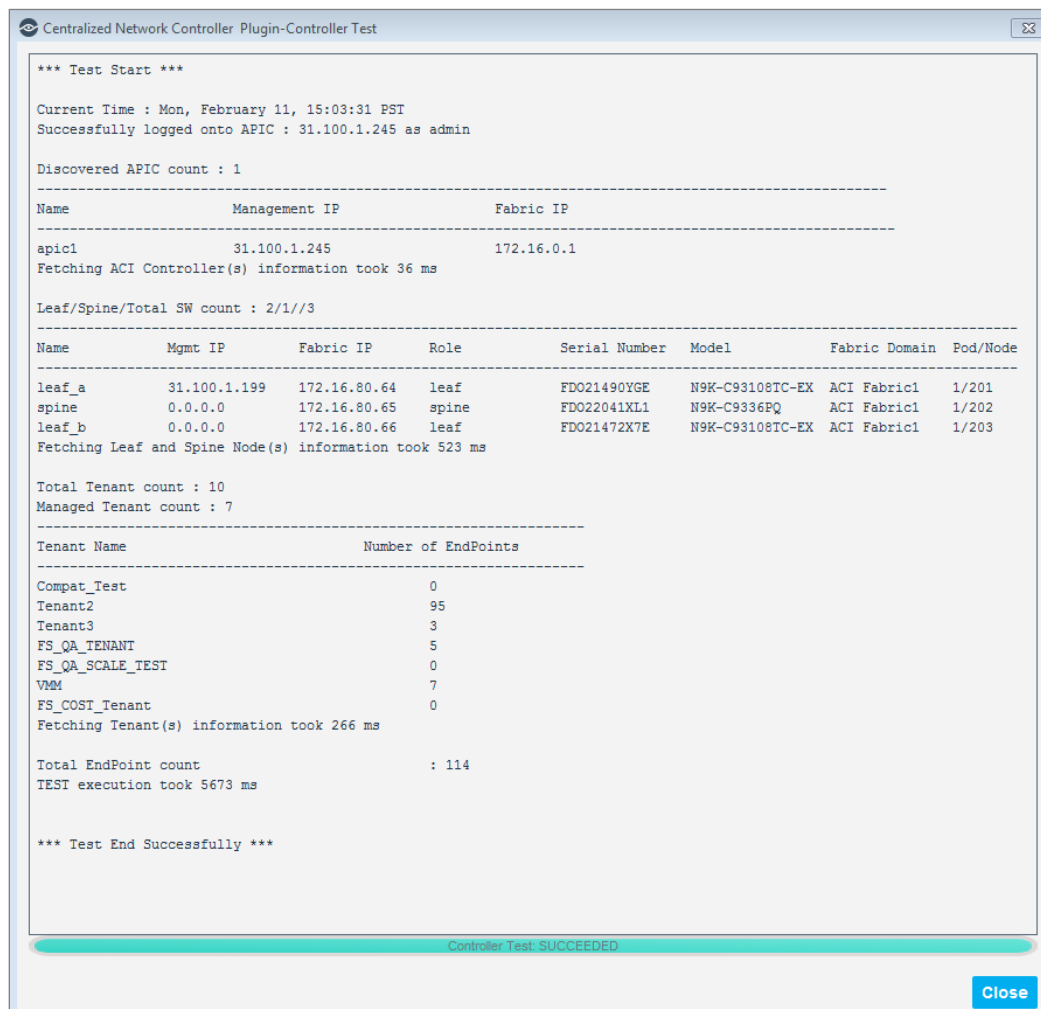
To verify:

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 Cisco ACI fabric entry. At any time, you can test the plugin configuration for an existing Cisco ACI fabric entry in the Controllers tab.

The test verifies plugin configuration validity and checks that the plugin can communicate and work with the selected Cisco ACI fabric/APIC(s)/tenant group(s).



The following conditions are tested:

- The plugin is running on the designated Connecting CounterACT Device.
- The plugin established a communication connection with the APIC:
 - Within the allowed time frame

- Did not encounter any network problem
- Did authenticate
- Used valid API command data
- The plugin queried the APIC and successfully retrieved ACI fabric information

To test the plugin configuration:

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

In the window, the plugin provides test results.

3. Select **Close**.

If the controller test succeeded, using:

- A new ACI fabric entry
- or
- An existing, updated (edited) ACI fabric entry

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

Edit a Controller

You can edit the plugin configuration for a monitored Cisco ACI fabric entry, and enable and disable specific settings.

To edit an ACI fabric:

1. In the *Controllers* tab, select a Cisco ACI fabric entry and then select **Edit**. The *Edit Controller* window opens.
2. Modify the settings and options in the various tabs. For details about these tabs and their content, see [Add a Controller](#) and its subsections.

After editing the plugin configuration for a Cisco ACI fabric entry and before saving the updated plugin configuration, Forescout recommends testing the plugin configuration for the Cisco ACI fabric entry. To do so, continue with [Test the Plugin Configuration](#).

Remove a Controller

Removing the plugin configuration for a monitored Cisco ACI fabric entry stops all plugin interaction with that Cisco ACI fabric.

To remove an ACI fabric:

1. In the *Controllers* tab, select one or more than one Cisco ACI fabric entry and then select **Remove**.
2. When prompted for confirmation, select **Yes**.

3. Select **Apply** to save the updated plugin configuration in the Forescout platform.

Distribute Plugin Processing Load

When an ACI fabric contains a small number of tenants that manage a very large number of endpoints, Forescout recommends distributing the plugin processing load, as follows:

- Configure the plugin to monitor a separate ACI fabric entry for each tenant
- Per ACI fabric entry, distribute the plugin processing load across the fabric's APICs, as follows:
 - In the *Communication* pane, per plugin-monitored ACI fabric, enter a different APIC IPv4 address/FQDN to be the initial APIC with which the plugin communicates (remember that you can enter a maximum of 5 APIC entries in this field). The CNC Plugin preference is to always establish a communication connection with an APIC, in the order in which the APICs were entered in the *Controller IP/Name* field.

For example, you want the plugin to monitor an ACI fabric that includes the following components:

- Tenant-1 and Tenant-2
- APIC-1 and APIC-2

Configure the plugin with two separate ACI fabric entries, one for each tenant, as follows:

- For plugin-monitored ***FabricEntry #1:***
 - In the *Communication* pane, enter the APIC-1 IP address/FQDN as the initial entry in the **Controller IP/Name** field.
 - In the *Tenants* pane, select Tenant-1 from the tenant list
- For plugin-monitored ***FabricEntry #2:***
 - In the *Communication* pane, enter the APIC-2 IP address/FQDN as the initial entry in the **Controller IP/Name** field.
 - In the *Tenants* pane, select Tenant-2 from the tenant list

When configuring the plugin in this manner, the plugin communicates with APIC-1 to obtain information about Tenant-1 endpoints and communicates with APIC-2 to obtain information about Tenant-2 endpoints. You achieve distribution of plugin API polling across different APICs.

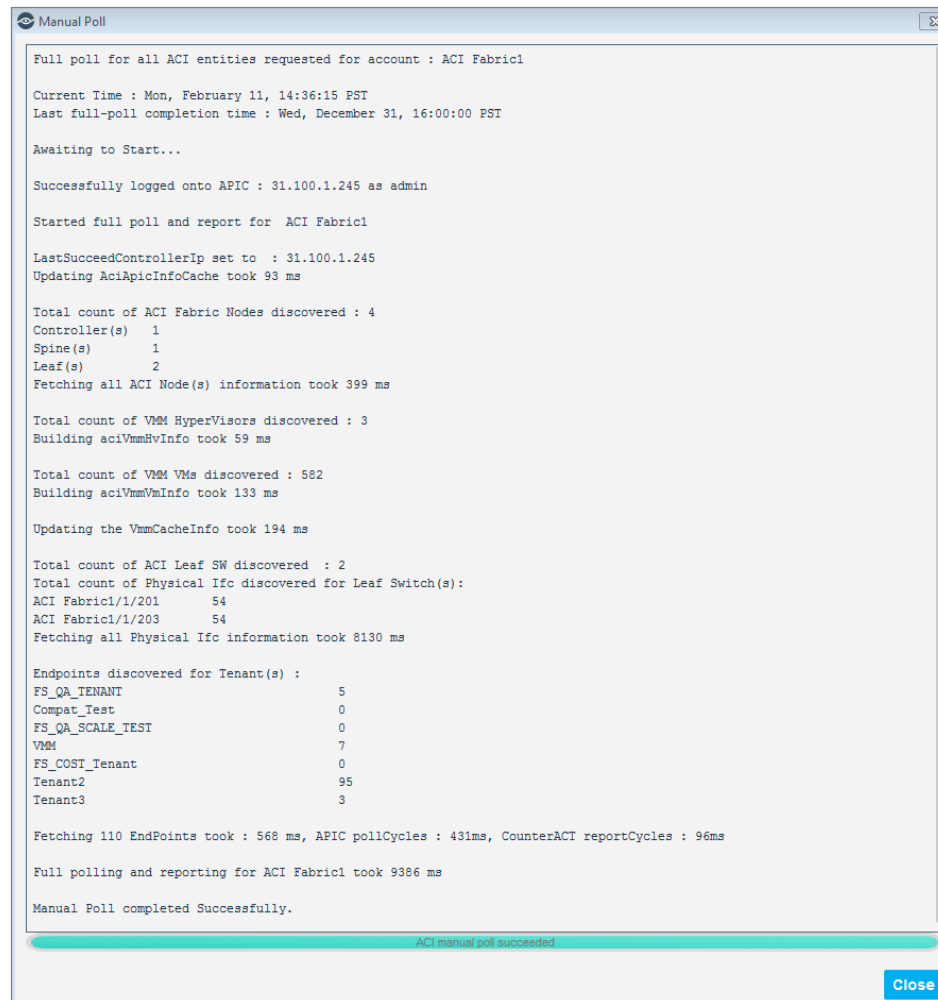
Initiate Plugin Polling

In addition to the plugin's periodic polling, you can initiate the plugin to poll the APIC of a monitored Cisco ACI fabric and retrieve information about endpoints, tenants, leaf switch ports and fabric nodes.

To initiate plugin polling of the APIC:

1. In the *Controllers* tab of the Centralized Network Controller pane, select the Cisco ACI fabric entry you want the plugin to poll.
2. Select **Poll**. The plugin proceeds to poll the APIC and retrieve all information about endpoints, tenants, leaf switch ports and fabric nodes. The *Manual Poll* window opens.

In the window, the plugin provides poll results.



See also [periodic APIC polling](#).

Property Resolution

The Centralized Network Controller Plugin resolves (retrieves) the following properties per plugin-monitored ACI fabric:

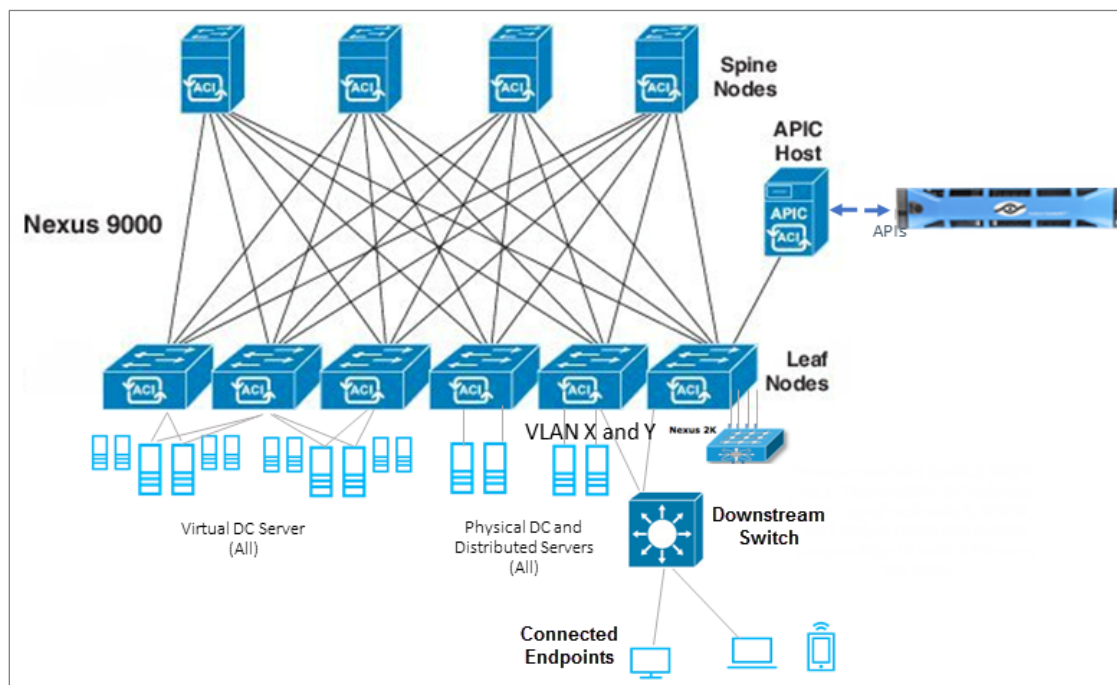
Property	Description
Application Profile	The name of an application profile. An application profile is a logical grouping of multiple endpoint groups (EPG) and is a child object of a single tenant.
Bridge Domain	The name of a bridge domain. A bridge domain defines the L2 forwarding within the ACI fabric and is analogous to a broadcast layer 2 domain in traditional Ethernet networks.
Bridge Domain Description	A description of the bridge domain.
Endpoint Group	The name of an endpoint group (EPG). An EPG is a logical grouping of multiple servers (physical or virtual) and is a child object of a single application profile.
Endpoint Group Description	A description of the endpoint group.
Endpoint VM Name	The VM (virtual machine) name of the endpoint.
Endpoint VMM Controller Name	The name of the VMM (virtual machine monitor) controller host that manages the endpoint.
Endpoint VMM Hypervisor Name	The name of the VMM hypervisor host to which the endpoint belongs.
Fabric Domain	The fabric domain that organizes a set of pods.
Fabric ID	The ID of the fabric domain.
FEX ID	The FEX ID of the leaf switch in the fabric domain to which the endpoint is connected. Note: FEX refers to Cisco Fabric Extender Technology
FEX Port	The FEX port of the leaf switch (the physical Ethernet interface information of the port, for example: eth1/3) to which any of the following are connected: <ul style="list-style-type: none"> An endpoint A downstream switch
IPv4 Address	IPv4 address of the connected endpoint, including the state in which the Forescout platform does not yet know the endpoint's IPv4 address (<i>Host without an IP address</i>)
IPv6 Address	IPv6 addresses, if any, of the connected endpoint. Note: In the Console display, for example, in the Host Details > Profile tab, endpoints having both an IPv4 address and IPv6 address(es), the IPv4 address is always these endpoint's primary IP address, while their IPv6 address(es) are subordinate IP address(es).

Property	Description
Leaf Switch Port VLAN	The leaf switch port VLAN, a number, to which the endpoint is connected.
Leaf Switch Port VXLAN	The leaf switch port VXLAN, a number, to which the endpoint is connected.
Leaf Switch Port	<p>The leaf switch port (the physical Ethernet interface information of the port, for example: eth1/3) to which any of the following are connected:</p> <ul style="list-style-type: none"> An endpoint A downstream switch <p>If an endpoint is connected to either a <i>port-channel</i> or a <i>virtual port-channel</i>, then this property contains the logical name of the <i>port-channel</i> or the <i>virtual port-channel</i> instead of the physical Ethernet interface information of the port</p>
Leaf Switch Port Description	A description of the leaf switch port.
Life Cycle Control	<p>The source from which the ACI learned about the endpoint:</p> <ul style="list-style-type: none"> Network traffic VMM
Node Fabric IP Address	The node's fabric IP address for communicating within the fabric. The address can be either an IPv4 or an IPv6 address.
Node ID	<ul style="list-style-type: none"> For spine switches, leaf switches and controllers: The ID of the node For endpoints: The ID of the leaf switch node in the fabric domain to which the endpoint is connected
Node Name	<ul style="list-style-type: none"> For spine switches, leaf switches and controllers: The name of the node For endpoints: The name of the leaf switch node in the fabric domain to which the endpoint is connected
Node Serial Number	The node's serial number within the fabric.
Node Uptime	The time (in seconds) since the system last booted, which is the result of the system's most recent start.
Node VTEP Address	The IPv4 address of the node's VXLAN tunnel.
Node VTEP IP Pool	The node's VTEP IP address pool used for the node's VXLAN tunnels. This pool contains IPv4 addresses.
Pod ID	The ID of the pod in the fabric domain to which the endpoint is connected.

Property	Description
Role	The role within the fabric of the discovered entity. Fabric roles are: <ul style="list-style-type: none"> ▪ Spine Switch ▪ Leaf Switch ▪ Controller ▪ Service Node ▪ Endpoint
Tenant Group	The ACI tenant group to which the endpoint belongs.
VMM Path Group	The VMM path group to which the endpoint belongs.

Use these properties in policies. In the ForeScout Console, find these properties in the **Cisco ACI** property group.

In network environments in which a Switch Plugin-managed switch is connected, as a downstream L2 switch, to an ACI leaf switch, the Switch Plugin resolves the managed switch properties of the connected endpoint and the CNC Plugin resolves the monitored ACI fabric properties of the connected endpoint.



For example, for the same connected endpoint, the Switch Plugin resolves the property **Switch IP/FQDN and Port Name**, which includes the port name (the physical Ethernet interface information) of the switch port to which the endpoint is connected and the CNC Plugin resolves the property **Leaf Switch Port**, which contains the leaf switch port (the physical Ethernet interface information) of the leaf switch port to which the endpoint is connected.

Conversely, in network environments in which a Switch Plugin-managed switch is connected, as an upstream L3 switch, to an ACI leaf switch, the Switch Plugin

resolves the managed switch properties of the connected endpoint and the CNC Plugin resolves the monitored ACI fabric properties of the connected endpoint.

Console Information Display

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

- [Centralized Network Controller Pane](#)
- [Home Tab](#)
- [Asset Inventory Tab](#)

By default, Cisco ACI retention of connected endpoints is 1 hour; this means that if an ACI fabric does not detect any endpoint activity for 1 hour, the fabric considers that endpoint no longer connected. When this event occurs, the APIC, via WebSocket notification, informs the CNC Plugin about the endpoint's disconnection from the monitored ACI fabric. As a result of this endpoint status update, the CNC Plugin deletes the endpoint from display in the Console. More generally, the CNC Plugin updates an endpoint's status, based solely on notification it receives from the APIC(s) of the monitored ACI fabric and not based on ForeScout platform timers.

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 plugin-monitored Cisco ACI fabrics.

Centralized Network Controller				
<div> Controllers Networks Devices </div>				
This tab displays information about the controllers that the plugin is configured to communicate with and query for information.				
<input type="text"/>				
Connectivity Status ▲	Vendor	Connecting CounterACT Device	Comment	Controller IP/Name
✔	Cisco ACI	45.100.2.231 (Running)	ACI Fabric1	62.100.1.245
✔	Cisco ACI	45.100.3.62 (Running)	ACI Fabric1	62.100.1.245
✔	Cisco ACI	45.100.3.62 (Running)	ACI Fabric2	62.100.3.21

The following Cisco ACI fabric-related information is available:

Column	Description
Connectivity Status	The status of the configured entry or the communication status with the APICs of the monitored ACI fabric. The possible statuses are: <ul style="list-style-type: none"> ▪ New (hourglass icon) – This configured entry is newly added, but has not been saved (select Apply to save). ▪ Up (green icon) – Plugin-APIC communication is successful. ▪ Down (red icon) – Either the plugin is not running on the Connecting CounterACT Device or plugin-APIC communication is not successful.
Vendor	The ACI fabric vendor.
Queried Organizations	<i>Information is not relevant for Cisco ACI fabrics</i>
Connecting CounterACT Device	The Forescout device through which all Forescout platform-initiated communication with the APICs of the monitored ACI fabric is directed.
Comment	User-provided comments/descriptive text.
Controller IP/Name	IPv4 address or fully qualified domain name (FQDN) of a plugin-monitored APIC that manages an ACI fabric.
Detection Method	<i>Information is not relevant for Cisco ACI fabrics</i>
Maximum Query Rate	<i>Information is not relevant for Cisco ACI fabrics</i>

 Not all columns are displayed by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.

Networks Tab

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

Information presented in this tab is not relevant for Cisco ACI fabrics. The information presented in this tab is supplied by CNC Plugin monitoring of a Cisco Meraki cloud management platform.

Devices Tab

The *Devices* tab displays information about the nodes present in plugin-monitored ACI fabric domains

Centralized Network Controller									
<div> Controllers Networks Devices </div>									
This tab displays information about the devices in each network or fabric.									
<div> <input type="text"/> <input type="button" value="Q"/> </div>									
Device Name	Type	Model	IP Address	Total...	Member of Network	Member of Organization/Fa...	MAC Address	Network Vendor	Serial Number
88:15:44:15:84:b0	Wireless	MR34		0	mytest	ForeScout Technologies	88:15:44:15:84:b0	Cisco Meraki	Q2FD-LTNZ-DH6S
apic1	ACI Controller	APIC-SERVER-M2	45.100.1.245	0	N/A	ACI Fabric1	700f6ae81d4c	Cisco ACI	FCH2219V058
e0:55:3d:e9:fb:f0	Security Appliance (M...	Z1	45.33.2.105	0	HKV Floor 3 - Engineering	ForeScout Technologies	e0:55:3d:e9:fb:f0	Cisco Meraki	Q2HN-3T4L-63KH
e0:55:3d:f7:fe:a2	Switch	MS250-24P	45.33.1.237	1	HKV Floor 5 - PM	ForeScout Technologies	e0:55:3d:f7:fe:a2	Cisco Meraki	Q2MW-536N-SWHK
leaf_a	ACI Leaf SW	N9K-C93108TC-EX	45.100.1.199	50	N/A	ACI Fabric1	4c776dc43b60	Cisco ACI	FDO21490YGE
leaf_b	ACI Leaf SW	N9K-C93108TC-EX	0.0.0.0	53	N/A	ACI Fabric1	4c776d24c2b0	Cisco ACI	FDO21472X7E
MATTY_AP	Wireless	MR33	45.33.1.51	0	HKV Floor 3 - Management	ForeScout Technologies	0c8d:db:17:fe:ad	Cisco Meraki	Q2PD-5JTV-RKM3
Meraki01	Wireless	MR34	45.33.1.54	0	HKV Floor 3 - Engineering	ForeScout Technologies	88:15:44:15:e4:40	Cisco Meraki	Q2FD-5K2P-75KQ
QA Meraki-switch	Switch	MS220-24P	45.33.1.226	2	HKV Floor 5 - PM	ForeScout Technologies	88:15:44:7a:f3:ad	Cisco Meraki	Q2KP-83YB-43A2
spine	ACI Spine SW	N9K-C9336PQ	0.0.0.0	0	N/A	ACI Fabric1	28ac9e1a949c	Cisco ACI	FDO22041XL1

The following device-related information is available:

Column	Description
Device Name	Name of the device.
Type	Type of device. The possible types are as follows: <ul style="list-style-type: none"> ACI Controller ACI Leaf Switch ACI Spine Switch
Model	Model of the device.
IP Address	IP address of the device.
Total Connected Endpoints	Total number of endpoints connected to the device
MAC Address	MAC address of the device.
Member of Network	This field is not relevant to Cisco ACI fabric domains
Member of Organization/Fabric	Name of the ACI fabric to which the device belongs.
Network Vendor	The vendor of the network to which the device belongs.
Serial Number	Serial number of the device.

 *Not all columns are displayed by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.*

Home Tab

The nodes and connected endpoints that the Centralized Network Controller Plugin discovers, via its monitoring of an ACI fabric domain, display as entries in the *All Hosts* pane in the Console's *Home* tab. The *All Hosts* pane displays the following

information for node entries [APIC, Leaf Switch, Service Node, Spine Switch] that are discovered by the plugin:

- Columns providing resolved ACI fabric property information. See [Property Resolution](#) for details.

All Hosts														
Search		Online/Offline		Show only unassigned		16 OF 289 HOSTS								
Host	IPv4 Address	Segment	IPv6 Address	MAC Add...	Comment	Display N...	Function	Actions	Node ID	Applicat...	Endpoint...	Pod ID	Leaf Sw...	Tenant...
WORKGROUPEARL	172.16.80.66	ACI_NODES		4c776d24c...			Unknown		203			1		leaf_b
ANDANAWONELS	192.168.88.12	ACI_EPS		005056a8...			Computer		201	Comp_Te...	Compat_T...	1	10	Compat_...
192.168.88.11	192.168.88.11	ACI_EPS		005056a8...			Computer		201	Comp_Te...	Compat_T...	1	10	Compat_...
172.19.1.103	172.19.1.103	ACI_VMM		0050569a...			Computer		201	VMM_AP...	VMM/VMM...	1	135	VMM ACI-VMM...
172.19.1.102	172.19.1.102	ACI_VMM		0050569a...			Computer		201	VMM_AP...	VMM/VMM...	1	135	VMM ACI-VMM...
172.19.1.101	172.19.1.101	ACI_VMM		00505680...			Computer		201	VMM_AP...	VMM/VMM...	1	135	VMM ACI-VMM...
172.18.1.102	172.18.1.102	ACI_VMM		00505680...			Computer		203	VMM_AP...	VMM/VMM...	1	137	VMM ACI-VMM...
172.18.1.101	172.18.1.101	ACI_VMM		00505680...			Computer		203	VMM_AP...	VMM/VMM...	1	137	VMM ACI-VMM...
172.17.0.2	172.17.0.2	ACI_VMM		0050569a...			Computer		201			1	102	VMM Test1-ASAv
172.16.80.65	172.16.80.65	ACI_NODES		28ac9e1a9...			Unknown		202			1		spine
172.16.0.2	172.16.0.2	ACI_VMM		0050569a...			Computer		201			1	103	VMM Test1-ASAv
172.13.1.3	172.13.1.3	ACI_EPS		00d781cf72b			Router or ...		201	FS_QA_A...	FS_QA_TE...	1	73	FS_QA_T...

Asset Inventory Tab

The *Asset Inventory* provides the *Cisco ACI* view. Using this view, you can group the display of detected endpoints based on any the following ACI fabric-related distinctions:

- Application Profile
- Bridge Domain
- Bridge Domain Description
- Endpoint Group
- Endpoint Group Description
- Fabric Domain
- FEX ID
- FEX Port
- Leaf Switch Port
- (Leaf Switch Port) VLAN ID
- (Leaf Switch Port) VxLAN ID
- Node ID
- Node Name
- Pod ID
- Role
- Tenant Group
- VMM Path Group
- VMM vCenter

The following *Asset Inventory* image presents detected endpoints grouped by fabric domain:

Views

Cisco ACI

Application Profile

Bridge Domain

Bridge Domain Description

Endpoint Group

Endpoint Group Description

VMM Controllers

Fabric Domain

FEX ID

FEX Port

Leaf Switch Port

Leaf Switch Port VLAN

Leaf SW Port VLAN

Node ID

Node Name

Pod ID

Role

Tenant Group

VMM Path Groups

Filters

Search

All

Segments (26)

Organizational Units

Default Groups

Groups

Fabric Domain

Search

Fabric Domain

Lists

No. of Hosts

Last Update

Last Host

ACIFabric1

2

6/27/20 2:34:18 PM

10.100.1.245

Field

Fabric Domain: ACIFabric1

Hosts

Fabric Domain

Search

2 OF 26 HOSTS

Host

IPv4 Address

Segment

MAC Address

Comment

Display Name

Switch (PFQDN)

Switch Port Alias

Switch Port Name

Bridge Domain

Bridge Domain

Endpoint Group

Endpoint Group

Function

Actions

192.168.5.6

192.168.5.6

aci

00055a6d693

Tenant2_VRF1_0

this is a descrip...

Tenant2/Tenant2

this is an EPG of ...

10.100.1.245

10.100.1.245

aci

700fae81d4c

The following *Asset Inventory* image presents detected endpoints grouped by node name:

Views

Cisco ACI

Application Profile

Bridge Domain

Bridge Domain Description

Endpoint Group

Endpoint Group Description

VMM Controllers

Fabric Domain

FEX ID

FEX Port

Leaf Switch Port

Leaf Switch Port VLAN

Leaf SW Port VLAN

Node ID

Node Name

Pod ID

Role

Tenant Group

VMM Path Groups

Filters

Search

All

Segments (26)

Organizational Units

Default Groups

Groups

Node Name

Search

Node Name

Lists

No. of Hosts

Last Update

Last Host

apic1

1

6/27/20 2:40:49 PM

10.100.1.245

Field

Node Name: apic1

Hosts

Node Name: Search

1 OF 26 HOSTS

Host

IPv4 Address

Segment

MAC Address

Comment

Display Name

Switch (IP/FQDN)

Switch Port Alias

Switch Port Name

Bridge Domain

Bridge Domain

Endpoint Group

Endpoint Group

Function

Actions

10.100.1.245

10.100.1.245

aci

700fae81d4c

CNC Plugin Integrations: Cisco Meraki and Juniper Mist

The Centralized Network Controller Plugin (CNCP) provides you with the ability to monitor each of the following centralized network controller solutions:

- Cisco Meraki cloud-managed networks
- Juniper Mist Wireless LAN cloud-managed networks

For Cisco Meraki products, the Meraki Dashboard is the centralized cloud management interface.

For Juniper Mist products, the Mist Dashboard is the centralized cloud management interface.

The Centralized Network Controller Plugin integration enables discovery of endpoints connected to the following cloud-managed, network devices:

- Cisco Meraki
 - Security & SD WAN
 - Switch
 - Teleworker Gateway
 - Wireless Access Point
- Juniper Mist
 - Mist Wireless Access Point

Plugin-discovered endpoints receive Forescout classification and assessment processing. In addition to information, which is obtained by the plugin, about discovered (detected) endpoints, plugin resolved properties also provide information about each cloud-managed network being monitored by the plugin. With a Cisco Meraki cloud-managed network, the plugin reports about the organizations, networks, switches, and wireless access points that it discovers. With a Juniper Mist Wireless LAN cloud-managed network, the plugin reports about the organizations, sites, and wireless access points that it discovers. For example, the name of the organization to which the detected endpoint belongs, or the name of the wireless access point to which the wireless client (the endpoint) is connected.

The following cloud-managed entities are analogous to each other:

- The Cisco Meraki **network** and the Juniper Mist **site**

Therefore, in the Forescout Console, plugin-discovered Mist sites display in the *Networks* tab of the *Centralized Network Controller* pane.

How It Works


The following components are required for the Centralized Network Controller Plugin's cloud-managed network integrations:

Cisco Meraki

- **Meraki Dashboard** – The Forescout platform queries the Meraki Cloud Management Service via its Dashboard API to retrieve information about network devices and the endpoints connected to those devices.
- **Meraki cloud-managed, network devices** – The Forescout platform receives syslog events from local Meraki security & SD WANs (MX), switches (MS), teleworker gateways (Z) and wireless access points (MR), which provide endpoint discovery information.

Juniper Mist

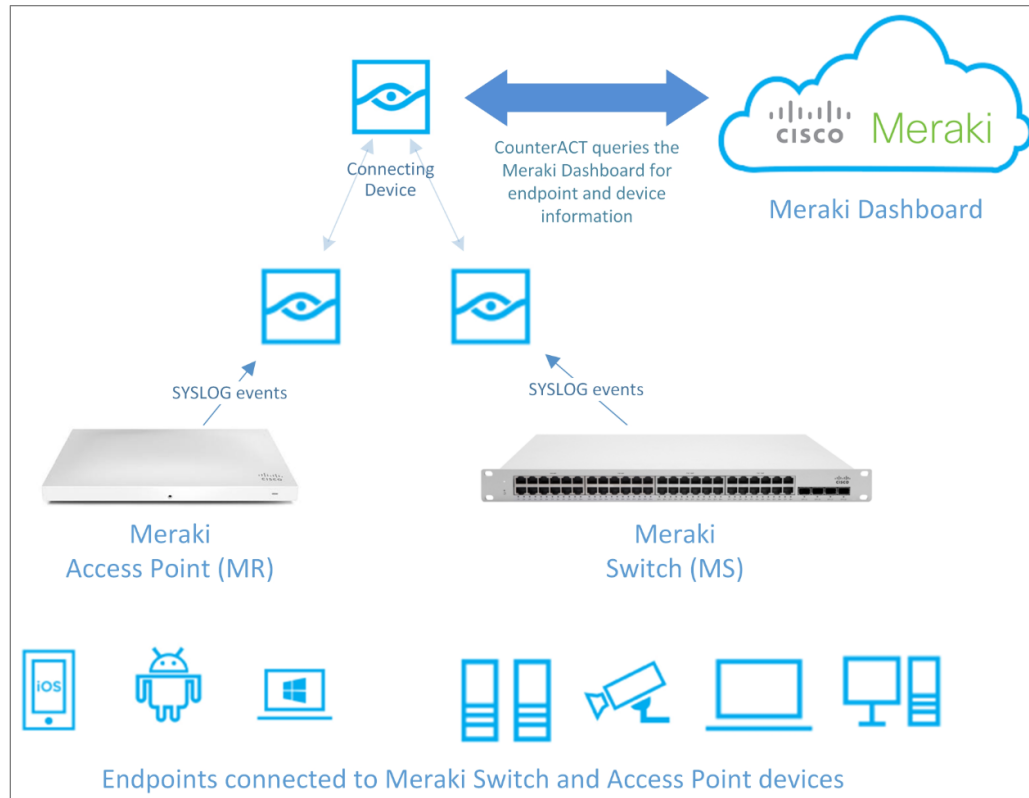
- **Mist Dashboard** – The Forescout platform queries the Mist Cloud Management Service via its Dashboard API to retrieve information about network devices (Mist wireless access points) and the endpoints connected to those devices.

 *Plugin-receipt of syslog events is not available from Juniper Mist network devices.*

Forescout Platform


The following Forescout platform components support these integrations:

- **Centralized Network Controller Plugin** – The Centralized Network Controller Plugin handles communication with both the Meraki Dashboard and the Mist Dashboard, querying each of these dashboards to obtain endpoint and device property information. You define *controllers*, logical entities that represent the third-party solution with which the plugin communicates.
- **Syslog Plugin** – (Cisco Meraki only) The Syslog Plugin receives syslog events from Meraki cloud-managed, network devices. These syslog messages are used to expedite the Centralized Network Controller Plugin's discovery, of endpoint connections and disconnections.



For each cloud-managed network that the plugin monitors:

- In the Forescout Console *Controllers* tab of the Centralized Network Controller, you configure a controller and assign a dedicated Connecting CounterACT Device for that controller.
- A unique Forescout device, either Appliance or the Enterprise Manager, must be defined as the Connecting CounterACT Device to handle communication with the dashboard of the cloud-managed network.
- A configured controller handles one type of cloud-managed network, either Cisco Meraki or Juniper Mist.
- A single controller handles communication with the dashboard of a cloud-managed network that can contain multiple organizations.
- A specific organization can only be queried by a single controller.
- For each controller, the polling rate from the Forescout platform to the dashboard of the cloud-managed network can be configured.
- (Cisco Meraki only) The Forescout platform does not query information directly from the Meraki cloud-managed, network devices. Configure the Forescout platform to receive syslog messages from these devices.

 *Forescout Console does not display endpoint IPv6 addresses reported by Cisco Meraki. The Forescout Console displays the MAC address of IPv6-only endpoints.*

 *Juniper Mist does not support IPv6-related properties.*

Baseline Deployment Guidelines

Forescout recommends the following baseline deployment guidelines:

- Select a Forescout Appliance, and not the Enterprise Manager, as the Connecting CounterACT Device.

Cisco Meraki

The efficiency of the Cisco Meraki integration with the Forescout platform/Centralized Network Controller Plugin has a high degree of dependency on the customer's configuration design. Refer to the guidelines that are provided in the Meraki best practices [documentation](#).

Several key points from Meraki to note:

- The number of Meraki network devices - for example, the MX, MS, MR and MV - per network is a much more variable number that does not have a general recommendation. It will vary from case to case.
- The maximum scale supported in a single organization is 25,000 physical Meraki network devices. If a business intends to have more than 25,000 Meraki network devices in their solution, they are strongly encouraged to work with their Cisco Meraki account team to design a deployment strategy across multiple organizations.
- Network scope general recommendation: one network per physical location or branch
- There is a limit of 1000 devices per network. Networks exceeding this number should be split.

Forescout benchmarked CNCP management of a Cisco Meraki cloud-managed network, using the Meraki Dashboard API. A sample configuration that is validated to work successfully includes, within one organization, over 700 networks, 6,000 devices and 100,000 endpoints. Note that this is not a maximum, as the mix of Meraki devices will vary by customer. There remains a 5 API calls per second maximum for throughput using the API, but this has not been found to be a limiting factor with the benchmarked, sample configuration. Forescout continues to recommend that one organization per Forescout device (Enterprise Manager, Appliance) is the general rule, subject to the environment size.

Juniper Mist

- The Mist Dashboard limit is 5000 API calls per hour. The Centralized Network Controller Plugin makes one API call each time it applies an action, be it the *Assign Mist Label* action or the *Cancel Mist Label Assignment* action, and makes several hundred API calls for its periodic, information queries.

Supported Vendor Products

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Requirements

This section describes the requirements for running the Forescout Centralized Network Controller Plugin and configuring it to work with any one of the integrated cloud-managed networks.

- [Forescout Requirements](#)
- [Network Requirements](#)
- [Third-Party Product Requirements](#)

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Network Module 1.2.1 with the Centralized Network Controller Plugin
- (Cisco Meraki only) 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 1.2.0 with the Syslog Plugin. See [Configure the Syslog Servers](#) and [Syslog Plugin Configuration Prerequisites](#) for details.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

Network Requirements

Configure the following on enterprise firewalls to support communication between the Forescout platform and the dashboard of the cloud-managed network to be monitored by the plugin:


- Allow communication on port 443/TCP
- For the Meraki Dashboard, the URL `api.meraki.com/api/v0/` must be reachable with HTTPS
- For the Mist Dashboard, the URL `api.mist.com/api/v1/` must be reachable with HTTPS

If your organization's network security policy requires that Internet communication traffic be routed through a proxy server, you 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 dashboard of the cloud-managed network.

Third-Party Product Requirements

(Cisco Meraki only) Forescout recommends to configure the Centralized Network Controller Plugin to use syslog events sent to it from local Meraki devices to detect endpoint connections and 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 Forescout device(s) 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 that are specific to the cloud-managed network that you want the plugin to monitor:

- [For a Cisco Meraki Cloud-Managed Network](#)
- [For a Juniper Mist Cloud-Managed Network](#)

For a Cisco Meraki Cloud-Managed Network

Before configuring the Centralized Network Controller Plugin to monitor a Cisco Meraki cloud-managed network, you must complete the following activities, in the order presented:

1. [In the Meraki Dashboard:](#)
 - a. Generate the API Key
 - b. Configure the Syslog Servers
2. [In the Syslog Plugin:](#)
 - a. Configure the Plugin Receiver Port
 - b. Verify the plugin is running

Meraki Dashboard Configuration Prerequisites

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

1. [Generate the Meraki API Key](#)
2. [Configure the Syslog Servers](#)

Generate the Meraki API Key

The Centralized Network Controller Plugin requires the use of an API Key to communicate with the cloud management interface, in this case, the Meraki Dashboard. First, you need to generate the API Key in the Meraki Dashboard. Then,

when adding the controller to the plugin configuration, you must provide the generated API Key.

You must record and save the API Key immediately after generating it, as the API Key is hidden the next time you open the relevant, Meraki Dashboard configuration page.

To generate a Meraki 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 **Enable access to the Cisco Meraki Dashboard API**.
 - 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 opens.
3. In the *API access* section, select **Generate API Key**. The generated API Key displays.
4. Record and save the API Key, before leaving/closing the *Update your account information* page.

You must provide this API Key when adding the controller to the Centralized Network Controller Plugin configuration. See [Add a Controller](#) for details.

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

Configure the Syslog Servers

Before the Centralized Network Controller Plugin can use received syslog events to detect endpoint connections/disconnections, in the Meraki Dashboard, you need to configure the syslog servers. These are the Forescout 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 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 Forescout 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** – Select one or both of the following options:
 - › **Wireless events** – Sends WLAN device (wireless access point) events to the syslog server.
 - › **Switch events** – Sends switch device events to the syslog server.

3. Repeat step 2 for each Forescout device you want to configure as a syslog server.

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

Syslog Plugin Configuration Prerequisites

After completing the Meraki Dashboard configuration prerequisites and before Centralized Network Controller Plugin configuration, complete the following Syslog Plugin-related activities in the Forescout Console:

- [Configure the Plugin Receiver Port](#)
- [Verify the Plugin is Running](#)

Configure the Plugin Receiver Port

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

To configure the port for receiving syslog events:

1. In the Console, select **Tools** > **Options**. The *Options* window opens.
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 box opens.
5. Select a Forescout device and then select **OK**. The *Syslog@<Forescout device> Plugin Configuration* window opens.
6. Select the **Receive From** tab.

The screenshot shows the 'Syslog@10.54.4.13 Plugin Configuration' window with the 'Receive From' tab selected. The window has a blue sidebar on the left. The main content area is divided into sections for configuring syslog sources and ports. The '1st Syslog Source' section includes a 'Source Type' dropdown (set to '<Select Type>') and an 'IP Address' text field. The '2nd Syslog Source' and '3rd Syslog Source' sections have identical fields. The 'Ports for Incoming Syslog Messages' section at the bottom has 'UDP Port' and 'TCP Port' dropdowns, both set to '514'. 'OK' and 'Cancel' buttons are at the bottom right.

7. In the *Ports for Incoming Syslog Messages* section, configure the *UDP Port* field with the identical port number that you 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 Forescout device configured as a syslog server in the Meraki Dashboard.

For more information, refer to the *Forescout Syslog Plugin Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access the guide.

Verify the Plugin is Running

Verify that the Syslog Plugin is running in *all* of the Forescout devices configured as syslog servers in the Meraki Dashboard (Select **Options** > **Modules** and expand the **Core Extensions** module entry).

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

For a Juniper Mist Cloud-Managed Network

Before configuring the Centralized Network Controller Plugin to monitor a Juniper Mist cloud-managed network, you must complete the following activities, in the order presented:

- [Generate the Mist API Token](#)

Generate the Mist API Token

The Centralized Network Controller Plugin requires the use of an API Token to communicate with the cloud management interface, in this case, the Mist Dashboard. First, you need to generate the API Token in the Mist Dashboard. Then, when adding the controller to the plugin configuration, you must provide the generated API Token.

You must record and save the API Token immediately after generating it, as the API Token cannot be re-displayed the next time you open the relevant, Mist API Token generation page.

To generate a Mist API Token:

1. In your browser, access the URL <https://manage.mist.com>. The Mist *Sign In* page opens.
2. Log in to your Mist account by entering your account credentials.
3. While logged in to your Mist account, open another browser tab and access the URL <https://api.mist.com/api/v1/self/apitokens>
4. Select **POST**. The generated API Token displays in the following format:
`key : <randomly generated character string>`
where the character string is the API Token
For example, `key : 342x23XFE...e5`
5. Record and save the API Token, before closing the browser tab.

You must provide this API Token when adding the controller to the Centralized Network Controller Plugin configuration. See [Add a Controller](#) for details.

Note the following about Mist API Tokens:

- An API Token generated for a specific admin has the same privilege as the user

- API Tokens are automatically deleted, if not used within 90 days.

For further information about Mist API Tokens, refer to <https://api.mist.com/api/v1/docs/Auth#api-token>. For information about working with the dashboard, refer to Juniper Mist Wireless LAN cloud management platform documentation.

Configure the Plugin

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

- An organization's networks/sites
- An organization's cloud-managed network devices
- The endpoints connected to these cloud-managed network devices

Plugin *controllers* are logical entities that represent the third-party cloud management interface with which the plugin communicates. A plugin controller is configured to communicate with either of the following, cloud management interfaces:

- A Meraki Dashboard
- A Mist Dashboard

The section describes the following plugin configuration tasks:

- [Add a Controller](#)
- [Edit a Controller](#)
- [Remove a Controller](#)
- [Test the Plugin Configuration](#)

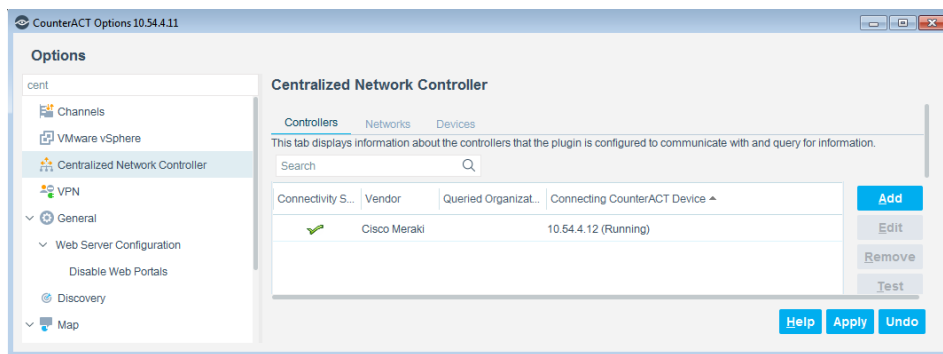
Add a Controller

The section describes how to define controllers in Forescout that communicate with the management interface of the cloud-managed network.

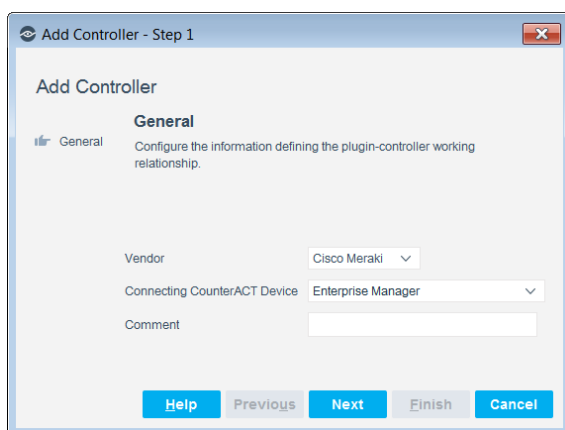
Before adding a controller to the plugin configuration, make sure that you have completed the steps described in [Configuration Prerequisites](#).

To add a controller:

1. In the Console, 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**.



5. Configure the controller using the panes of the Add Controller wizard:

- [General](#)
- [Communication](#)
- [Organizations to Query](#)
- [Detection Method](#) (Cisco Meraki only)
- [Proxy Server](#)
- [Performance Tuning](#)

General

In the *General* pane, configure general information that the plugin requires in order to work with the controller (the management interface/the dashboard) of a cloud-managed network.

To configure general information:

1. In the *General* pane of the Add Controller wizard, define the following:

Field	Description
Vendor	From the drop-down menu, select a cloud-managed network vendor, either <i>Cisco Meraki</i> or <i>Juniper Mist</i> .
Connecting CounterACT Device	<p>Enter the name of the Enterprise Manager/Appliance through which all Forescout platform-initiated communication with the controller is directed. Only this designated Enterprise Manager/Appliance actually communicates with the controller.</p> <p>An Enterprise Manager/Appliance can only be configured as the Connecting CounterACT Device for a single, supported vendor, this being either Cisco ACI, Cisco Meraki or Juniper Mist.</p> <p>Forescout recommends choosing an Appliance, rather than the Enterprise Manager, as the Connecting CounterACT Device.</p>
Comment	(<i>optional</i>) Enter comments/descriptive text about the plugin-monitored controller.

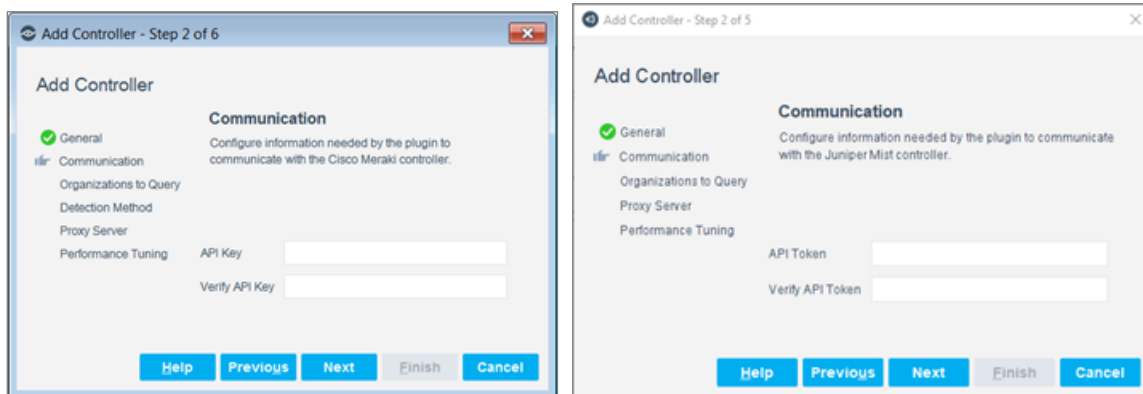
2. Select **Next**. The [Communication](#) pane opens.

Communication

In the *Communication* pane, configure the information that the plugin requires in order to communicate with the controller to obtain information about:

- Organizations associated with the cloud-managed network
- Cloud-managed networks/sites
- The cloud-managed, network devices and the endpoints connected to these devices.

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



To configure communication information:

1. In the *Communication* pane of the Add Controller wizard, define either of the following fields, as available:

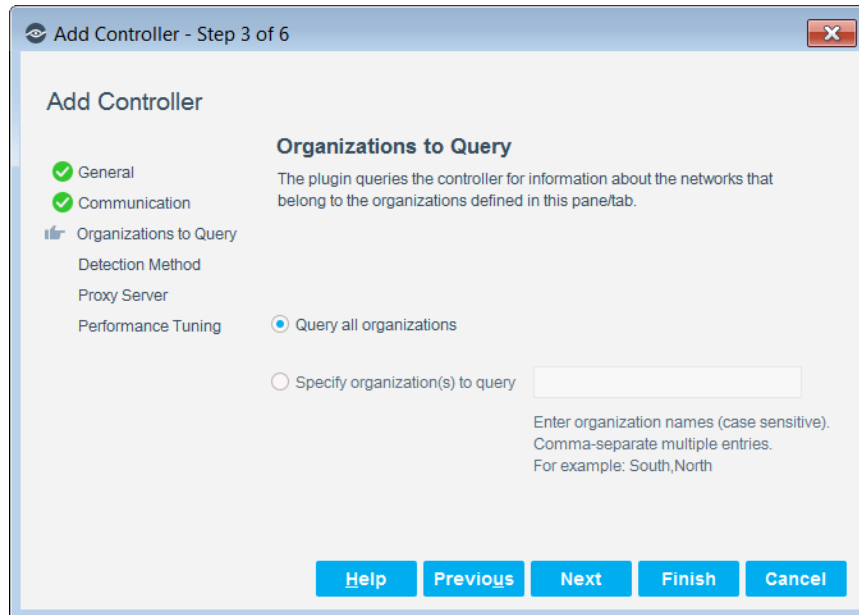
Field	Description
API Key	<p>(Cisco Meraki only) Enter the API Key that the Forescout platform must use to communicate, via API, with the controller and obtain information from the controller.</p> <p>Note: You must have already generated this key in the Meraki Dashboard. See Generate the Meraki API Key for details.</p> <p>Re-enter the API Key in the Verify API Key field.</p>
API Token	<p>(Juniper Mist only) Enter the API Token that the Forescout platform must use to communicate, via API, with the controller and obtain information from the controller.</p> <p>Note: You must have already generated this token in the Mist Dashboard. See Generate the Mist API Token for details.</p> <p>The plugin does not support two factor authentication. Therefore, if access of the account, related to the API Token, requires two factor authentication, the plugin will not be able to authenticate to the Mist Dashboard.</p> <p>Re-enter the API Token in the Verify API Token field.</p>

2. Select **Next**. The [Organizations to Query](#) pane opens.

Organizations to Query

In the *Organizations to Query* pane, specify which organizational networks the plugin should query for information.

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



To configure the organizations to query:

1. In the *Organizations to Query* pane, select one of the following options:
 - **Query all organizations.** The plugin queries the controller about *all* organizational networks
 - **Specify organization(s) to query.** The plugin *only* queries the controller about the networks belonging to those organizations that are specified in this field.
 - › This field is *case-sensitive*, for example, the entries **Finance** and **finance** refer to two **different** organizations.
 - › Comma-separate multiple entries. For example: **South0009, 109zone, RegionABCD**
2. Select **Next**.
 - When configuring the plugin to monitor a Cisco Meraki cloud-managed network, selecting **Next** opens the [Detection Method](#) pane
 - When configuring the plugin to monitor a Juniper Mist cloud-managed network, selecting **Next** opens the [Proxy Server](#) pane

Detection Method

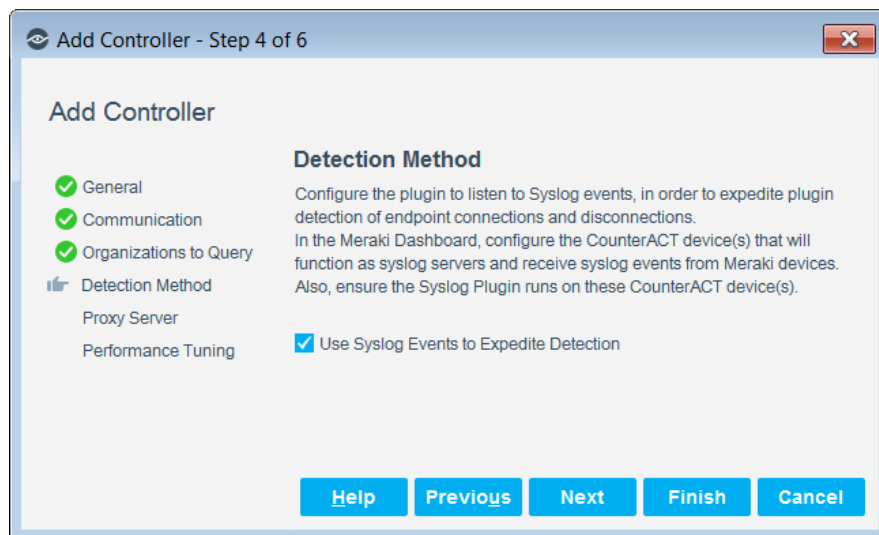
(Cisco Meraki only) In the *Detection Method* pane, instruct the plugin to listen for syslog events that are sent to the Forescout platform from Meraki network devices. When this option is selected, plugin detection of endpoint connections to and disconnections from those devices is *expedited*.

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 through periodic polling of the controller.


The *Use Syslog Events to Expedite Detection* option is enabled by default. To work with this option, you must also configure Meraki Dashboard to send syslog information from the Meraki cloud-managed, network devices.



To expedite detection:

1. In the *Detection Method* pane, verify that **Use Syslog Events to Expedite Detection** is selected. If not, select this option.
2. Configure the Meraki Dashboard to send syslog information from the Meraki cloud-managed, network devices. See [Configuration Prerequisites](#).
3. Select **Next**. The [Proxy Server](#) pane opens.

When the *Use Syslog Events to Expedite Detection* option is disabled (the plugin is not configured to listen for received syslog events about endpoint connections/disconnections), Forescout recommends defining the plugin's purge interval to be 300 seconds (5 minutes). The default purge interval is 5400 seconds (90 minutes).

 *The plugin clears collected information about an endpoint, once the plugin no longer detects the endpoint as connected for the amount of time defined by the purge interval.*

To set the plugin's purge interval on all Appliances:

1. From the Console, stop the CNC Plugin on the Enterprise Manager and all Appliances.

2. Log in to the CLI on the Enterprise Manager
3. Run the following command using an SSH connection:


```
fstool oneach -c fstool cnc set_property config.purge.interval.value 300
```
4. From the Console, start the CNC Plugin on the Enterprise Manager and all Appliances.

Proxy Server

Define a proxy server in the *Proxy Server* pane, 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 the Forescout platform and the management interface (the dashboard) of the cloud-managed network. The Connecting CounterACT Device was previously configured in the *General* pane.

To configure the proxy server:

1. In the *Proxy Server* pane of the Add Controller wizard, enable (select) the **Use Proxy Server** option. By default, this option is disabled.
2. Define the following information (unless otherwise noted, all information is required):

Field	Description
Proxy Server	Enter the IP address of the proxy server.
Proxy Server Port	Select the port to be used to communicate with the proxy server.

Field	Description
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 password in the Verify Password field.

3. Select **Next**. The [Performance Tuning](#) pane opens.

Performance Tuning

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

To configure performance settings for plugin monitoring of a Cisco Meraki cloud-managed network:

1. In the *Performance Tuning* pane, modify the following query properties as required:

Field	Description
Maximum CounterACT Query Rate	Modify the maximum number of plugin queries per second that the Connecting CounterACT Device is allowed to 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 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.
Query for group policies every <n> seconds	Modify the frequency that the plugin queries the controller to retrieve the names of all the group policies defined per network. By default, this query period is 600 seconds. Note: Group policies can be defined for all Cisco Meraki cloud-managed networks except for networks of type <i>Switch</i> .

Add Controller - Step 6 of 6

Add Controller

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

Performance Tuning
Configure performance-related settings and options that affect plugin processing.

Maximum CounterACT Query Rate (per second): 3

Query for connected endpoint information when:

Expedite Detection is enabled, query every (seconds): 600

Expedite Detection is disabled, query every (seconds): 60

Query for device port configuration every (seconds): 600

Query for organization / network information every (seconds): 3600

Query for group policies every (seconds): 600

Buttons: Help, Previous, Next, Finish, Cancel

2. Select **Finish**.

The new controller is listed in the *Controllers* tab. Continue with [Test the Plugin Configuration](#).

To configure performance settings for plugin monitoring of a Juniper Mist cloud-managed network:

1. In the *Performance Tuning* pane, modify the following query properties as required:

Field	Description
Query Mist Controller and Sites every <n> minutes	Modify the frequency of plugin queries for the controller's information: its organizations, its managed sites and the network devices belonging to its managed sites. By default, this query period is 30 minutes.
Query Mist Clients every <n> minutes	Modify the frequency of plugin queries for information about the connected wireless clients (endpoints). By default, this query period is 5 minutes.
Query Mist Labels every <n> minutes	Modify the frequency that the plugin queries the controller to retrieve the names of all the Mist Labels defined per site. By default, this query period is 5 minutes.

Add Controller - Step 5 of 5

Add Controller

- ✓ General
- ✓ Communication
- ✓ Organizations to Query
- ✓ Proxy Server
- Performance Tuning**

Performance Tuning
Configure performance-related settings and options that affect plugin processing.

Query Mist Controller and Sites every (minutes) 30

Query Mist Clients every (minutes) 5

Query Mist Labels every (minutes) 5

Help Previous Next Finish Cancel

2. Select **Finish**.

The new controller is listed in the *Controllers* tab. Continue with [Test the Plugin Configuration](#).

Edit a Controller

You can edit the properties of an existing controller, and enable and disable specific settings.

To edit a controller:

1. In the *Controllers* tab, select a controller entry and then select **Edit**. The *Edit Controller* window opens.
2. Modify the controller properties in the various tabs. For details about these tabs and their content, see [Add a Controller](#) and its subsections.

After editing the plugin configuration for a controller entry and before saving the updated plugin configuration, Forescout recommends testing the plugin configuration for the controller entry. To do so, continue with [Test the Plugin Configuration](#).

Remove a Controller

Removing a controller stops all plugin interaction with that controller.

To remove a controller:

1. In the *Controllers* tab, select one or more than one controller entry and then select **Remove**.
2. When prompted for confirmation, select **Yes**.

3. Select **Apply** to save the updated plugin configuration in the Forescout platform.

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

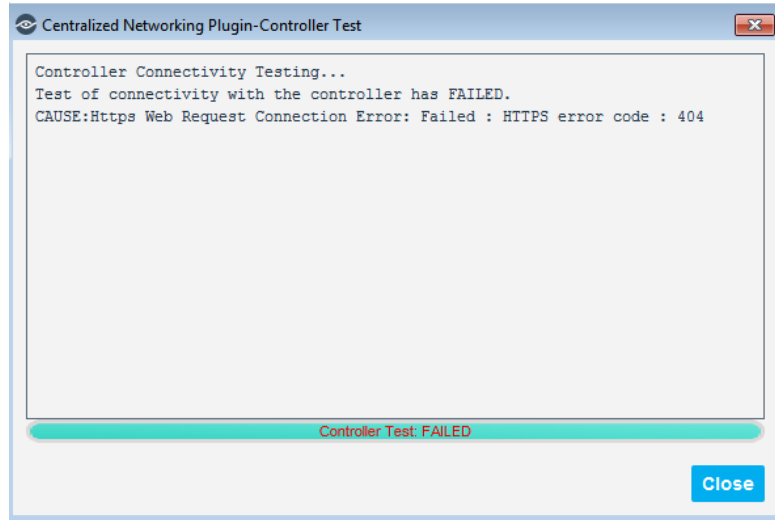
After completing the *Add Controller* configuration process and *before* saving the updated plugin configuration, make sure you test the plugin configuration for the new controller entry. You can test the plugin configuration for an existing controller entry at any time.

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 the plugin test to use.
2. Select **Test**. The *Centralized Network Controller Plugin-Controller Test* window opens. The test automatically runs.



If the test fails, information is provided about the failure.

3. Select **Close**.
4. If the Controller test succeeded, select **Apply** to save the new/updated plugin configuration in the Forescout platform.

After saving the plugin configuration for a new controller entry:

- Select the [Networks Tab](#) to review information 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.

Verify Plugin Processing of Syslog Events

When your Forescout platform deployment is operating, if the Meraki Dashboard, the Syslog Plugin and the CNC Plugin are configured to support plugin receipt of syslog events to detect endpoint connections/disconnections, you can *optionally* verify that the plugin is correctly processing these received events. Create a Forescout policy that evaluates detected endpoints for a match on the **Trap Received** property containing any of the following, resolved information:

- *Link Down Trap* – syslog event received, notifying of endpoint disconnection from a switch
- *Wireless Address Learned* – syslog event received, notifying of endpoint connection to a wireless access point
- *Wireless Address Removed* - syslog event received, notifying of endpoint disconnection from a wireless access point

Console Information Display

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

- [Centralized Network Controller Pane](#)
- [Home Tab](#)
- [Asset Inventory Tab](#)

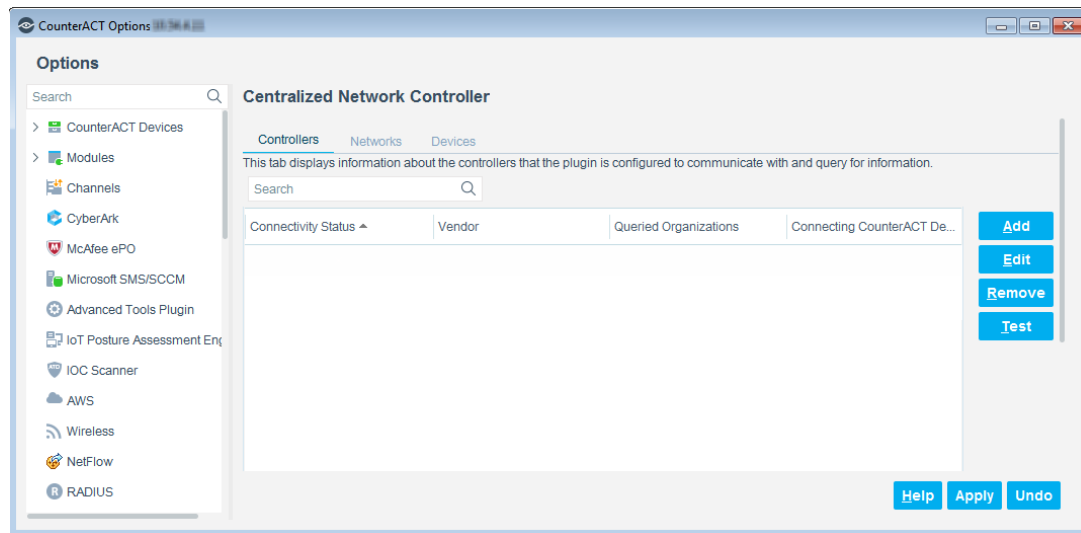
Centralized Network Controller Pane

The Console *Centralized Network Controller* pane comprises the following tabs:

- [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	<p>The status of the configured entry or the communication status with the controller. The possible statuses are:</p> <ul style="list-style-type: none"> ▪ 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 is not successful.

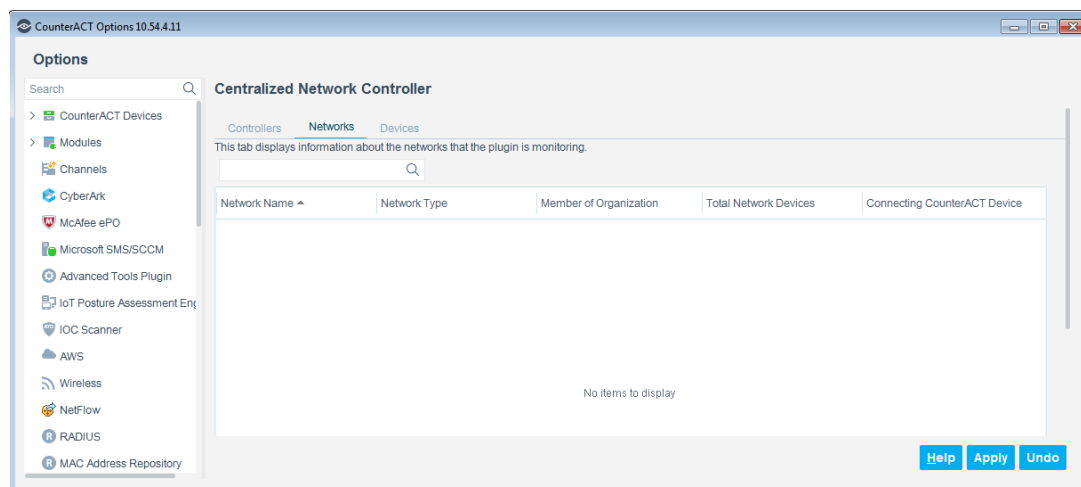
Column	Description
Vendor	The controller's vendor.
Queried Organizations	The organizations whose networks are monitored by the plugin.
Connecting CounterACT Device	The Forescout device through which all Forescout platform-initiated communication with the cloud management interface is directed.
Comment	User-provided comments/descriptive text.
Detection Method	The method used to detect endpoint connections and disconnections. The possible methods are: <ul style="list-style-type: none"> ▪ Polling (only) ▪ Polling and Events
Maximum Query Rate	(Cisco Meraki only) The maximum number of queries per second that the Connecting CounterACT Device is allowed to send to the cloud management interface. The default rate is 3 queries per second.

 *Not all columns are displayed by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.*

Networks Tab

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

 *The Cisco Meraki **network** and the Juniper Mist **site** are analogous cloud-managed entities.*



The following network/site-related information is available:

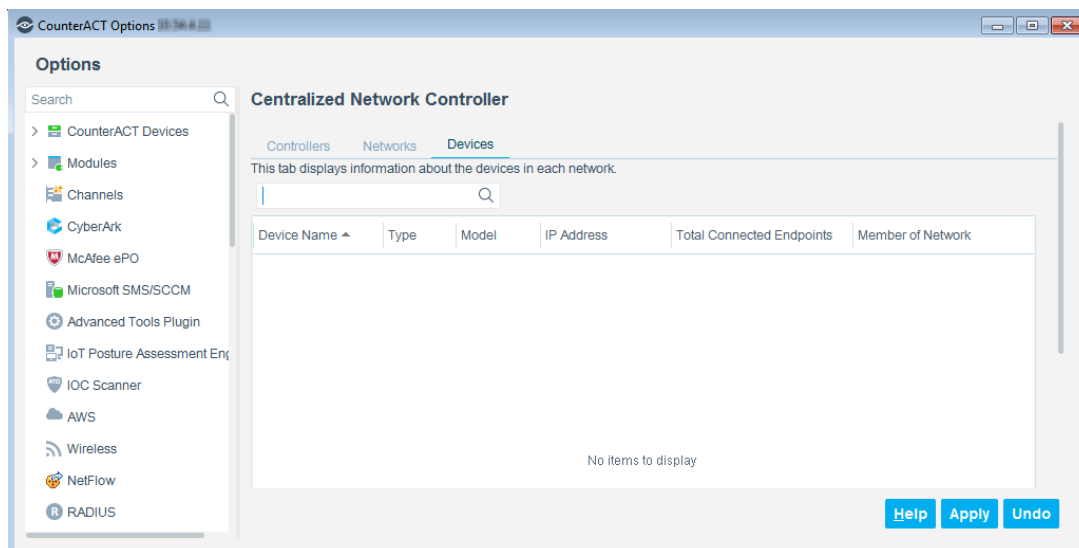
Column	Description
Network Name	The name of the network/site.
Member of Organization	The name of the organization to which the network/site belongs.

Column	Description
Network Type	The type of network/site. The possible types are: <ul style="list-style-type: none"> ▪ Cisco Meraki network: <ul style="list-style-type: none"> - Appliance (security & SD WAN, teleworker gateway) - Combined (security & SD WAN, switch, teleworker gateway, wireless) - Switch - Wireless ▪ Juniper Mist site: <ul style="list-style-type: none"> - Mist Wireless
Vendor	The network/site vendor.
Total Network Devices	The total number of devices detected in the network/site.
Network Time Zone	The time zone in which the network/site is located.
Connecting CounterACT Device	The Forescout device through which all Forescout platform-initiated communication with the cloud management interface, about the network/site, is directed.

 *Not all columns are displayed by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.*

Devices Tab

The *Devices* tab displays information about the devices in each third-party solution network/site.



The following device-related information is available:

Column	Description
Device Name	The name of the device.
Type	The type of device. The possible types are: <ul style="list-style-type: none"> ▪ Cisco Meraki devices: <ul style="list-style-type: none"> - Security & SD WAN - Switch - Teleworker Gateway - Wireless ▪ Juniper Mist devices: <ul style="list-style-type: none"> - Mist Wireless AP
Model	The model of the device.
IP Address	The IP address of the device.
Total Connected Endpoints	Total number of endpoints connected to the device. See about Plugin Connected Endpoint Reporting for Cisco Meraki Devices .
Last Event Received	(Cisco Meraki only) The date of the last syslog event that the plugin received from the device.
MAC Address	The MAC address of the device.
Member of Network	The name of the network/site to which the device belongs.
Member of Organization	The name of the organization to which the device belongs.
Network Vendor	The vendor of the network/site to which the device belongs.
Serial Number	The serial number of the device.

 *Not all columns are displayed by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.*

[Plugin Connected Endpoint Reporting for Cisco Meraki Devices](#)


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 detects and reports 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/site devices and connected endpoints that the Centralized Network Controller Plugin discovers, via its monitoring of cloud-managed networks, appear as entries in the *All Hosts* pane in the Forescout Console's *Home* tab.

 *There can be instances in which the Console cannot report endpoint online/offline in real-time. This issue most typically manifests itself in the following scenario:*

- *Endpoint is displayed as online, but is actually offline.*

The Console displays a revised and current endpoint status immediately following the plugin's next query for endpoint information. See Performance Tuning for information about the setting that controls the frequency of this query.

The Console *All Hosts* pane displays the following information about the network/site devices that the plugin discovers:

Security & SD WAN

- Vendor
- Network ID
- Network Name
- Organization ID
- Organization Name

Switch

- Vendor
- Switch Hostname
- Network ID
- Network Name
- Organization ID
- Organization Name

Teleworker Gateway

- Vendor
- Network ID
- Network Name
- Organization ID
- Organization Name

Wireless Access Point

The following information is reported for both Cisco Meraki and Juniper Mist wireless access points (APs):

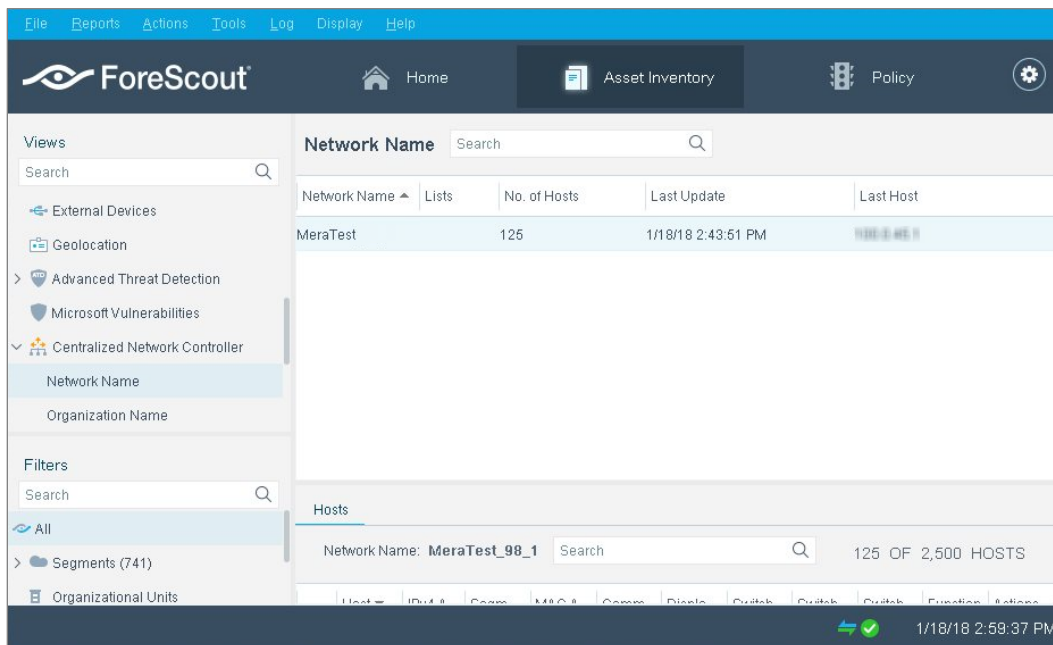
- Vendor
- WLAN AP Name

- Network Function – Lightweight AP (Access Point)
- Network ID (Site ID)
- Network Name (Site Name)
- Organization ID
- Organization Name

Asset Inventory Tab

ForeScout *Asset Inventory* views show the distribution of wired and wireless endpoints across the organizations and networks/sites of cloud managed networks being monitored by the plugin. This eliminates the need to go to the dashboard of a cloud managed network to see how many endpoints are connected to each access point. You can also:

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



The following *Centralized Network Controller* information views are available:

Information	Description
Assigned Meraki Policy	(Cisco Meraki only) The list of endpoints to which the <i>Assign Meraki Policy</i> action is currently applied, due to either Forescout platform policy evaluation or manual application.
Assigned Mist Label	(Juniper Mist only) The list of endpoints to which the <i>Assign Mist Label</i> action is currently applied, due to either Forescout platform policy evaluation or manual application.
Network Name	Current information about the networks/sites to which detected endpoints are connected.

Information	Description
Organization Name	Current information about the organizations to which detected endpoints belong.

Creating ForeScout Policies

Create Forescout policies to:

- Evaluate endpoints connected to your organizations' networks/sites, using criteria that are meaningful/informative to your network security administrators
- Resolve property information for endpoints connected to your organizations' networks/sites, which are entities in plugin-monitored, cloud managed networks
- Apply an eyeControl action on endpoints that match policy conditions (evaluation criteria)

Property Resolution

The Centralized Network Controller Plugin stores obtained information in properties that belong to following property groups:

- [Cisco Meraki/Juniper Mist](#)
- [Switch](#)
- [Wireless](#)
- [Track Changes](#)

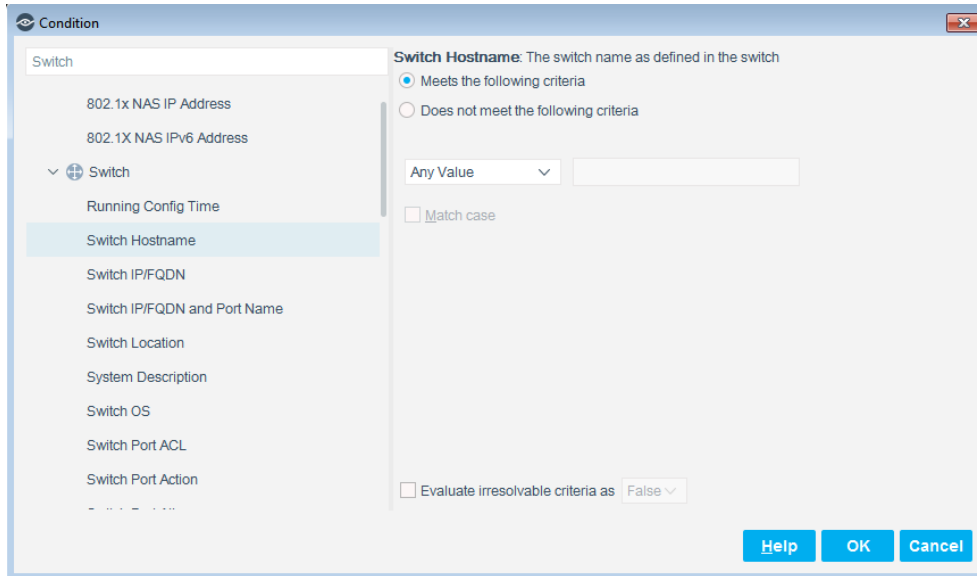
Cisco Meraki/Juniper Mist Properties

The plugin resolves the following properties about detected endpoints that are connected to a plugin-monitored, cloud-managed network:

Property	Description
Assigned Meraki Policy	(Cisco Meraki only) The Meraki policy currently assigned to the detected endpoint by the <i>Assign Meraki Policy</i> action.
Assigned Mist Label	(Juniper Mist only) The Mist label currently assigned to the detected endpoint by the <i>Assign Mist Label</i> action.
Network ID	ID of the network/site to which the detected endpoint is connected.
Network Name	Name of the network/site to which the detected endpoint is connected.
Organization ID	ID of the organization to which the detected endpoint belongs.
Organization Name	Name of the organization to which the detected endpoint belongs.

Switch Properties

The plugin resolves the following properties about detected endpoints that are connected to plugin-monitored, cloud-managed Meraki switches:

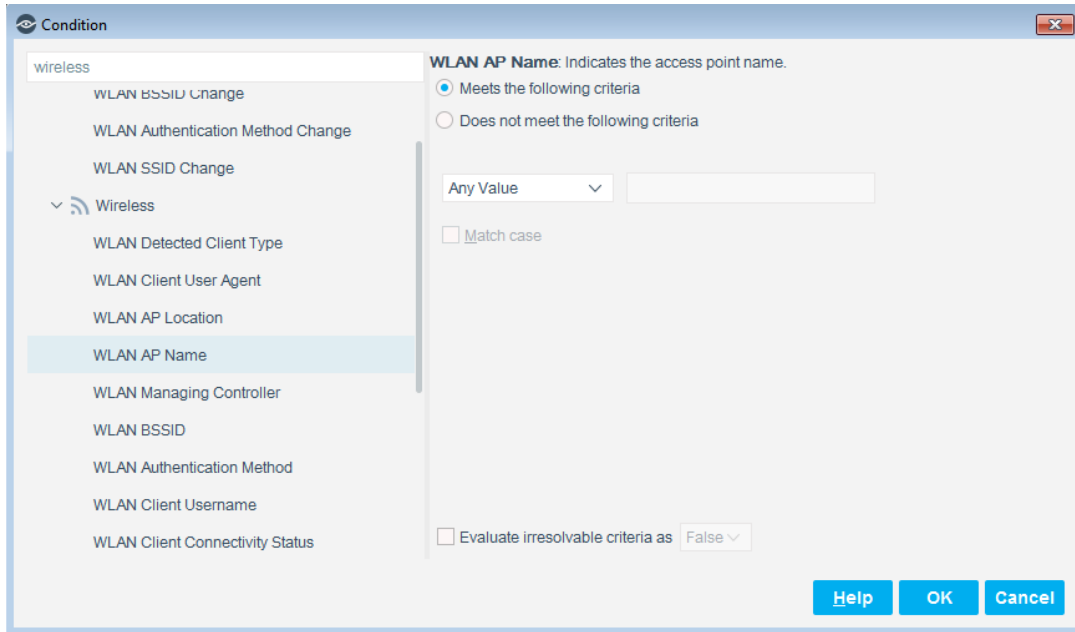


Property	Description
Switch Hostname	The switch name as defined in the switch.
Switch IP/FQDN	The IP address or the fully qualified domain name (FQDN) of the switch.
Switch IP/FQDN and Port Name	The IP address or the fully qualified domain name (FQDN) name of the switch and the port name (the physical Ethernet interface information of the port). The format is <i><IP address/FQDN>: <port></i> .
Switch Port Alias	The 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	The switch port VLAN to which the VoIP endpoint is connected.
Switch Vendor	The Switch vendor name.
Switch VoIP Port	Identifies whether the switch port is a VoIP port.

Other Forescout switch properties are not resolved by this plugin.

Wireless Properties

The plugin resolves the following properties about detected endpoints (wireless clients) that are connected to plugin-monitored, cloud-managed wireless APs:



Property	Description
WLAN AP Name	The 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	The DNS name used by the wireless client to authenticate with the access point.
WLAN Device IP/FQDN	The IP address or the fully qualified domain name (FQDN) of the WLAN device that manages the wireless client.
WLAN Device Vendor	The vendor of the WLAN device that manages the wireless client.
WLAN SSID	(Cisco Meraki only) Identifies the SSID (service set identifier) to which the wireless client is connected.

Other Forescout wireless 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](#)
- [Switch Track Changes Properties](#)
- [Wireless Track Changes Properties](#)

Centralized Network Controller Track Changes Properties

Property	Description
Assigned Meraki Policy Change	Identifies that a change in value occurred in the Assigned Meraki Policy property.
Assigned Mist Label Change	Identifies that a change in value occurred in the Assigned Mist Label property.
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.

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.
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.

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.

Property	Description
WLAN Device IP/FQDN Change	Identifies that a change in value occurred in the WLAN Device IP/FQDN property.
WLAN SSID Change	(Cisco Meraki only) Identifies that a change in value occurred in the WLAN SSID property.

Action Control

The Centralized Network Controller Plugin provides the following eyeControl actions to apply on endpoints that are connected to plugin-monitored, cloud-managed networks:

- *Assign Meraki Policy* – assigns the selected Meraki policy to endpoints connected to a Cisco Meraki cloud-managed network. The plugin only supports applying the *Assign Meraki Policy* action on endpoints that are connected to any of the following Cisco Meraki network devices:
 - Security & SD WAN
 - Teleworker Gateway
 - Wireless Access Point
- *Assign Mist Label* – assigns the selected Mist label to endpoints connected to Mist wireless access points. This action only supports the assignment of *WiFi Client* type labels at the *site* level. The action does not support the assignment of Mist labels of any other label type or label level.

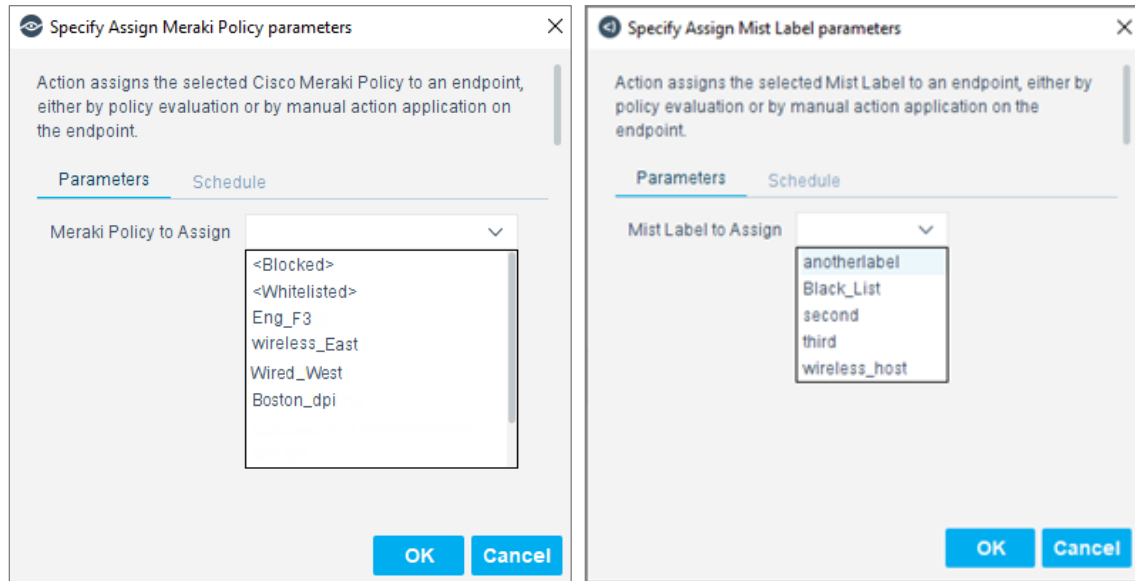
In the Forescout Console, find both these actions in the *Restrict* action group. Use these actions in policies and manually apply them on detected endpoints.

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

To configure the action:

1. In the action's *Parameters* tab, define either of the following fields, as available:

Field	Description
Meraki Policy to Assign	<p>From the drop-down menu, select a Meraki policy option:</p> <ul style="list-style-type: none"> ▪ <i><Blocked></i> - the Meraki-provided policy that prevents assigned endpoints from connecting to cloud-managed network devices. ▪ <i><Whitelisted></i> - the Meraki-provided policy that allows assigned endpoints to connect to cloud-managed network devices without any access restrictions. ▪ Group policy_{1-n} – user-defined, group policies that the plugin obtains from the Meraki Dashboard.
Mist Label to Assign	<p>From the drop-down menu, select a Mist label option:</p> <ul style="list-style-type: none"> ▪ Mist label_{1-n} – user-defined labels that the plugin obtains from the Mist Dashboard.



Cancel Actions

Policy re-evaluation may cancel the applied action; you can also manually cancel the action. The Centralized Network Controller Plugin provides the following eyeControl cancel actions:

- *Cancel Meraki Policy Assignment* – removes the Meraki policy currently assigned to the connected endpoint
 - At action cancelation, the targeted endpoint is then automatically assigned the *Normal* Meraki policy, even if prior to applying the *Assign Meraki Policy* action on the endpoint, the endpoint had no assigned Meraki policy.
- *Cancel Mist Label Assignment* – removes the Mist label currently assigned to the connected endpoint

In the Forescout Console, find both these actions in the *Restrict* action group.

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

Network Module Information

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

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

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

The Network Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation of Forescout.

The plugins listed above are installed and rolled back with the Network Module.

Additional Forescout Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 *Software downloads are also available from these portals.*

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

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