Forescout

Network Module: Network Controller Plugin

Configuration Guide

Version 1.0.1

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

2020-07-21 19:41

Table of Contents

About the Network Controller Integration

The Network Controller Plugin (NC Plugin) is a component of the Forescout Network Module. See Network Module Information for details about the module.

Centrally-managed network solutions provide a central component, for example, a network controller, that interfaces with multiple networks for the purposes of configuring, monitoring, managing and reporting about their varied network devices. Also, centrally-managed network solutions have their central component, reside either on premise or in the product solution cloud.

The Forescout platform integrates with centrally-managed network solutions to offer Forescout customers:

- Full visibility into their networks, including the network devices and the endpoints connected to those devices.
- Ability to control the network access of detected endpoints.

With this version of the NC Plugin, the Forescout platform integrates its offering with the following centrally-managed network solutions:

- Arista CloudVision Wired
- Arista CloudVision WiFi
- Cisco Meraki
- Ruckus SmartZone

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

- The Cisco Meraki centrally-managed network solution - concepts, topology, functionality and terminology. For information, refer to https://documentation.meraki.com/.
- The Ruckus SmartZone centrally-managed network solution - concepts, topology, functionality and terminology. For information, refer to https://support.ruckuswireless.com/documents.
- The Arista CloudVision WiFi centrally-managed network solution - concepts, topology, functionality and terminology. For information, refer to https://www.arista.com/en/support/product-documentation.
- The Arista CloudVision Wired centrally-managed network solution - concepts, topology, functionality and terminology. For information, refer to https://www.arista.com/en/support/product-documentation.

You should also have a solid understanding of the basics about Forescout platform feature functionality and Forescout policies.

Network Controller Plugin Integrations: Arista CloudVision WiFi and Wired, Cisco Meraki, and Ruckus SmartZone

The Network Controller Plugin provides you with the ability to monitor the following, centrally-managed network solutions:

- Arista Cloudvision WiFi centrally-managed networks (cloud based)
- Arista CloudVision Wired centrally-managed networks (premise based)
- Cisco Meraki centrally-managed networks (cloud based)
- Ruckus SmartZone centrally-managed networks (premise based)

The Network Controller Plugin enables the discovery of centrally-managed, network devices and the discovery of the endpoints connected to these centrally-managed, network devices. Control features vary by product.

- Cisco Meraki network devices:
  - Security & SD WAN
  - Switch
  - Teleworker Gateway
  - Wireless Access Point
- Ruckus SmartZone network device:
  - AP
- Arista CloudVision Wired network device:
  - Switch
- Arista CloudVision WiFi network device:
  - Wireless Access Point

In order to execute *eyeSight* and *eyeControl* activities in a centrally-managed network, the NC Plugin communicates with the following management interfaces:

- The ***Meraki Dashboard*** for Cisco Meraki managed networks
- The ***SmartZone Public API*** for Ruckus SmartZone managed networks
- The **CloudVision Portal API** for Arista CloudVision Wired managed networks
- The **Arista Cloud Services API** for Arista CloudVision WiFi managed networks

Plugin-discovered (detected) endpoints receive Forescout classification and assessment processing. In addition to information obtained by the plugin about detected endpoints, plugin resolved properties also provide information about the managed networks and their network devices.

Terms in Use

The following table lists terms used in this document and their equivalent, product solution terms:

Document Terms	Cisco Meraki	Ruckus SmartZone	Arista CloudVision WiFi	Arista CloudVision Wired
Entity, Entities	**Organization(s)** – logical, enterprise entities that contain the elements in the row entries below	**Zone(s)** – logical, enterprise entities that contain the elements in the row entries below	**Location(s)** – logical, enterprise entities that contain the elements in the row entries below	**Organization(s)** – logical, enterprise entities that contain the elements in the row entries below. See Entities Note
Network(s)	**Network(s)**	**AP Group(s)**	**Network(s)**	**Network(s)** See Entities Note
Network Device(s)	**Device(s)** - Security & SD WANs, Switches, Teleworker Gateways and Wireless Access Points	**Device(s)** – APs	**Device(s)** - Wireless Access Points	**Device(s)** – Switches
Endpoint(s)	Endpoints connected to/disconnected from any of the network devices listed in the row above	Endpoints connected to/disconnected from any of the network devices listed in the row above	Endpoints connected to/disconnected from any of the network devices listed in the row above	Endpoints connected to/disconnected from any of the network devices listed in the row above

Arista CloudVision Wired itself does not have a concrete concept of **entities**. Therefore, the Network Controller Plugin queries the entire deployment since it cannot programmatically break it down into smaller entities. Because of this, the plugin implements the following definitions:

- ***Organization(s)*** – All network devices and endpoints discovered by Arista CloudVision Wired have *CloudVision Wired Organization* as their Organization Name
- ***Network(s)*** – All network devices and endpoints discovered by Arista CloudVision Wired have *CloudVision Wired Network* as their Network Name

How It Works

The following components are required for the Network Controller Plugin integration with supported, centrally-managed network solutions:

- Arista CloudVision WiFi components
- Arista CloudVision Wired components
- Cisco Meraki components
- Ruckus SmartZone components

- Forescout Platform components

Arista CloudVision WiFi

The following Arista CloudVision WiFi components are required for this integrated solution:

- ***Arista Cloud Services*** – The Network Controller Plugin queries the Arista Cloud Services REST API to retrieve information about wireless access points and the endpoints connected to those devices. Validation is done through a Key Validation Service (KVS) in the Arista Cloud.
- ***Arista centrally-managed, network devices*** – The Forescout platform receives syslog events from individual Arista wireless access points, which provide endpoint discovery information.

Arista CloudVision Wired

The following Arista CloudVision Wired components are required for this integrated solution:

- ***CloudVision Portal API*** – The Network Controller Plugin queries Arista CloudVision Wired via its Portal API to retrieve information about switches and the endpoints connected to those devices.

Deployment Considerations

Before deploying and enabling the Arista CloudVision Wired integration, consider the following:

- The CloudVision Portal detects connected endpoints based on DHCP requests and displays that information in the *Connected Endpoints* section of the CloudVision Web GUI.
- Since DCHP cannot supply real-time information about when an endpoint has gone offline, use the Switch Plugin integration to get near real-time information about endpoints connected to an Arista based wired network, and eyeControl capabilities such as Assign to VLAN.
- Enabling the Network Controller plugin alongside the Switch plugin in this scenario is not recommended since the Network Controller plugin overrides the Switch Plugin gathered properties.
- Arista CloudVision Wired integrations in conjunction with the Switch plugin may see alerts in the CloudVision Portal if changes are made directly to the Arista switches. Management through the CloudVision Portal is recommended in this case.
- The Arista CloudVision Wired integration does not offer any control action at this time. Configuration of RADIUS-based controls should be considered.

Cisco Meraki

The following Meraki components are required for this integrated solution:

- ***Meraki Dashboard*** – The Network Controller Plugin queries the Meraki Cloud Management Service via its Dashboard API to retrieve information about network devices and the endpoints connected to those devices.
- ***Meraki centrally-managed, network devices*** – The Forescout platform receives syslog events from individual Meraki security & SD WANs, switches, teleworker gateways and wireless access points, which provide endpoint discovery information.

Ruckus SmartZone

The following Ruckus SmartZone components are required for this integrated solution:

- ***Ruckus SmartZone Public API*** – The Network Controller Plugin queries SmartZone via its Public API to retrieve information about wireless access points and the endpoints connected to those devices.
- ***Ruckus SmartZone centrally-managed, network devices*** – The Forescout platform receives syslog events from individual Ruckus wireless APs, which provide endpoint discovery information.

Forescout Platform

The following Forescout platform components support this integration:

- ***Network Controller Plugin*** – In the Forescout Console, you configure the plugin by defining *controllers*; these represent the centrally-managed network that the plugin is configured to communicate with, via the product solution's management interface, for the purposes of executing *eyeSight* and *eyeControl* activities.

  The plugin communicates with the product solution management interface to:

  - Query the management interface to obtain information about the centrally managed networks. The plugin stores (resolves) the information it obtains from the management interface in various properties for presentation in the Forescout Console.
    - For a Cisco Meraki network, the plugin obtains and reports information about the organizations, networks, and the network devices that it discovers.
    - For a Ruckus SmartZone network, the plugin obtains and reports information about the zones, AP groups, and the network devices that it discovers.
    - For Arista CloudVision WiFi, the plugin obtains and reports information about network locations, and the network devices that it manages.
    - For an Arista CloudVision Wired network, the plugin obtains and reports information about the network devices that it discovers.
    - For all centrally-managed networks, plugin-discovered (detected) endpoints, connected to the network devices, receive Forescout classification processing and property resolution.
  - Submit requests to the management interface to apply (execute) plugin actions on targeted endpoints, as directed by the Forescout platform.
- ***Network Controller Content Plugin*** – Provides the Network Controller Plugin with vendor specific component information that enables the Network Controller Plugin to work with each supported vendor's centrally-managed network solution.
- ***Syslog Plugin*** – Receives syslog events from centrally-managed network devices. These syslog messages are used to expedite the Network Controller Plugin's discovery of endpoint connections and disconnections.

For each centrally-managed network that the plugin monitors:

- In the Forescout Console *Network Controller* pane/tab of the Network Controller Plugin, you configure a controller and assign a dedicated Connecting CounterACT Device for that controller.

- A configured controller handles one centrally-managed network product solution, for example, Cisco Meraki.
- A single controller handles communication with the management interface of a centrally-managed network that can contain multiple entities.
- For each controller, the polling rates from the Forescout platform to the management interface of the centrally-managed network can be configured.
- The Forescout platform does not query information directly from centrally-managed network devices. Configure the Forescout platform to receive syslog messages from these devices.

The Forescout Console does not display endpoint IPv6 addresses reported by Arista CloudVision WiFi, Arista CloudVision Wired, Cisco Meraki, and Ruckus SmartZone. For IPv6-only endpoints, their MAC address is displayed in the Console.

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 Network Controller Plugin has a high degree of dependency on the customer’s configuration design. Refer to the guidelines that are provided in the Cisco 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 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 continues to recommend that one organization per Forescout device (Enterprise Manager, Appliance) is the general rule, subject to the environment size.

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 Network Controller Plugin and configuring it to work with any of the integrated centrally-managed network solutions.

- Forescout Requirements
- Network Requirements
- Vendor Product Integration 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 Network Controller Plugin
- Network Controller Content Plugin 1.0.1, installed. For information about this component, refer to the *Forescout Network Controller Content Plugin Configuration Guide*.
- Forescout recommends that the 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 1.2.1 with the Syslog Plugin running. 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 management interface of the centrally-managed network that the NC Plugin queries for information:

- Arista CloudVision WiFi
  - The URL https://launchpad.wifi.arista.com and the Wireless Manager service must be reachable with HTTPS. The Wireless Manager service is launched from Launchpad by clicking on **Wireless Manager**.

    The Wireless Manager URL must be appended with **/new/webservice** as in **https://awm15004.srv.wifi.arista.com/new/webservice/**. See Add a Controller for more details.
- Arista CloudVision Wired
  - Allow communication on port 443/TCP
  - For the CloudVision Portal API, the URL **<FQDN/IP address>/** must be reachable with HTTPS.

    Examples using FQDN and using IP address:
    - **https://cvp.lab.company/**
    - **https://158.1.1.2/**

See Add a Controller for more details.

- Cisco Meraki
  - Allow communication on port 443/TCP
  - For the Meraki Dashboard, the URL **`api.meraki.com/api/v0/`** must be reachable with HTTPS as in **`https://api.meraki.com/api.v0/.`**

    See Add a Controller for more details.
- Ruckus SmartZone
  - Allow communication on port 8443/TCP
  - For the SmartZone Public API, the URL **`<FQDN/IP address>:8443/wsg/api/public/v8_1/`** must be reachable with HTTPS.

    Examples using FQDN and using IP address:
    - › **`https://ruckussmartzone.lab.company.com:8443/wsg/api/public/v8_1/`**
    - › **`https://158.1.1.1:8443/wsg/api/public/v8_1/`**

    See Add a Controller for more details.

If your organization's network security policy requires that Internet or specific 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 Network Controller Plugin, and the management interface of the centrally-managed network.

Vendor Product Integration Requirements

Forescout recommends configuring the Network Controller Plugin to use syslog events sent to it from individual network devices to detect endpoint connections and disconnections. For this plugin processing to take place, configure the following in the management interface of the centrally-managed network:

- Configure the syslog servers (receivers of network device events) to be the Forescout device(s) responsible for receiving syslog events sent from individual 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.
- Arista CloudVision WiFi only supports use of 514/UDP to send syslog events.
- Arista CloudVision Wired does not support syslog.

Configuration Prerequisites

Before configuring the Network Controller Plugin, you must complete the following activities that are specific to the centrally-managed network that you want the plugin to monitor:

- Configuration Prerequisites for Arista CloudVision WiFi

- Configuration Prerequisites for Arista CloudVision Wired
- Configuration Prerequisites for Cisco Meraki
- Configuration Prerequisites for Ruckus SmartZone

Configuration Prerequisites for Arista CloudVision WiFi

To monitor an Arista CloudVision WiFi Network:

1. In the Arista Launchpad:
   a. Generate an Arista key pair in Launchpad for API access.
   b. Configure the Syslog Servers.
2. In the Syslog Plugin:
   a. Configure the Plugin Receiver Port.
   b. Verify that the plugin is running.

Arista Launchpad Configuration Prerequisites

The Network Controller Plugin communicates to the REST API using a key value pair generated on the Arista Launchpad. Appropriate service privileges can be assigned to this key-value pair. The key-value pair can only be used to log in and access the services through the API.

Generate an Arista Key

Record and save the Key ID and Key Value. The key value is obfuscated with asterisks, click on the entry to see the plain text

To generate an Arista Key:

1. In the Arista Launchpad at https://launchpad.wifi.arista.com, select the **Admin tab**.
2. Select **Keys > New Key**.
3. Type a **Key Name** and press the Enter key.
4. Record and save the Key ID and Key Value. The key value is obfuscated with asterisks, click on the entry to see the plain text
5. Select **Service Privileges** from the new key’s ellipsis menu.
6. Under **Select Profile** select **Admin** or **Custom** from the drop-down list.

   If Admin was selected no further steps are needed. If Custom was selected continue with the remaining steps.
7. For Custom, set the Wireless Manager to **ON**.
8. Select the Role of **Superuser** from the **Select Role** drop-down list.
9. Enable both **Wi-Fi Access Management** and **WIPS Management**.
10. Enable all locations.
11. Click **Save**.

For information about working with the launchpad, refer to the Arista Launchpad documentation.

Configure Syslog Servers

Before the Network Controller Plugin can use received syslog events to detect endpoint connections/disconnections, you need to configure the syslog servers in the CloudVision WiFi web portal. These are the Forescout device(s) responsible for receiving syslog events (wireless events) sent from managed, CloudVision WiFi network devices.

Syslog server configuration can be defined per CloudVision location.

To Configure Syslog Servers:

1. In the Arista Launchpad at https://launchpad.wifi.arista.com, select **CloudVision WiFi** from the **Dashboard tab**.
2. Select **Configure > WiFi** from the left menu.
3. Select the **Device Settings** from the top menu.
4. Scroll down and select **Device Access Logs**.
5. Enter the **Syslog Server IP/Hostname** of the Forescout device serving as a syslog server responsible for receiving syslog events (wireless events and/or switch events) sent from managed, Arista CloudVision WiFi network devices.

Configuration Prerequisites for Arista CloudVision Wired

Before configuring the Network Controller Plugin to monitor an Arista CloudVision network, you must complete the following activities, in the order presented.

To monitor an Arista CloudVision Wired Network:

1. In the CloudVision Web Interface:
   a. Create a CloudVision user
   b. Enable the *Connected Endpoints* feature.
   c. Configure Arista EOS devices
      › Enable DHCP Snooping
      › Enable injection of DHCP Options 82.
      Refer to the Arista Networks documentation for more information.

CloudVision Portal API Configuration Prerequisites

Before configuring the Network Controller Plugin, create the CloudVision Wired User using the CloudVision Web GUI.

Create the CloudVision Wired User

- In the Arista CloudVision Web GUI (*Settings (cog icon) > Access Control > Users*), create a new administrator account that is assigned the appropriate access permissions.
- Alternatively, use an existing administrator account that is assigned the appropriate access permissions. For its access of the management interface, the Network Controller Plugin requires the use of an administrator account that authenticates with the management interface. These administrator account credentials must be provided when adding the controller to the Network Controller Plugin configuration. See Add a Controller for details.

For information about working with the CloudVision Portal API, refer to the CloudVision Portal management platform documentation.

Configuration Prerequisites for Cisco Meraki

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

To monitor a Cisco Meraki network:

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 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 Network Controller Plugin requires the use of an API Key to communicate with the 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 is displayed.

    Record and save the API Key. You must provide this API Key when adding the controller to the Network Controller Plugin configuration. See Add a Controller for details.

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

Configure the Syslog Servers

Before the Network Controller Plugin can use received syslog events to detect endpoint connections/disconnections, you need to configure the syslog servers in the Meraki Dashboard. These are the Forescout device(s) responsible for receiving syslog events (wireless events and/or switch events) sent from managed, Cisco Meraki 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.

Configuration Prerequisites for Ruckus SmartZone

Before configuring the Network Controller Plugin to monitor a Ruckus SmartZone network, you must complete the following activities, in the order presented:

1. In the Ruckus SmartZone Public API:
   a. Create the Ruckus SmartZone User
   b. Configure the Syslog Servers
2. In the Syslog Plugin:
   a. Configure the Plugin Receiver Port
   b. Verify the Plugin is Running

Ruckus SmartZone Public API Configuration Prerequisites

Before Network Controller Plugin configuration, complete the following Ruckus SmartZone Public API activities, in the order presented:

- Create the Ruckus SmartZone User
- Configure the Syslog Servers

Create the Ruckus SmartZone User

In the Ruckus SmartZone Web GUI (*Administration* > *Admins and Roles*), create a new administrator account that is assigned the appropriate access permissions.

Alternatively, use an existing administrator account that is assigned the appropriate access permissions. For its access of the management interface, the NC Plugin requires the use of an administrator account that can authenticate with the management interface. You must provide these administrator account credentials when adding the controller to the Network Controller Plugin configuration. See Add a Controller for details.

For information about working with the SmartZone Public API, refer to the Ruckus Wireless SmartZone management platform documentation.

Configure the Syslog Servers

Before the Network Controller Plugin can use received syslog events to detect endpoint connections/disconnections, you need to configure the syslog servers in the Ruckus SmartZone Public API. These are the Forescout device(s) responsible for receiving syslog events (wireless events) sent from managed, Ruckus network devices.

There are several approaches to configuring syslog servers in the Ruckus SmartZone Public API. The following procedure provides one possible configuration approach, a per Zone configuration.

To configure a syslog server:

1. In the Ruckus SmartZone Web GUI, select **Access Points**. In the leftmost panel, the *Zones/AP Groups* navigation tree opens.
2. Select the zone to edit and then select the **pencil** (edit icon). The *Configure Group* window opens.
3. Select **Syslog Options** and define the following information for each syslog server entry:
   a. *Primary Server Address* - the IP address of a Forescout device to function as a syslog server (receives syslog events from Ruckus 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.
   c. *Protocol* - the protocol that network devices use to send syslog events to the syslog server. Ruckus SmartZone supports use of either UDP protocol or TCP protocol to send syslog events.
   d. *Priority* – Select **Info**
   e. *Send Logs* – Select **All Logs**

      This option may generate a large number of syslog events, however, it is necessary in order to ensure that endpoint connection and disconnection events are sent to the Forescout platform/NC Plugin.
4. Repeat step 3 for each Forescout device you want to configure as a syslog server.

For information about working with the SmartZone Public API, refer to the Ruckus Wireless SmartZone management platform documentation.

Syslog Plugin Configuration Prerequisites

Syslog is not supported for Arista CloudVision Wired

After completing the management interface (Meraki Dashboard, Ruckus SmartZone Public API) configuration prerequisites and before Network Controller

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

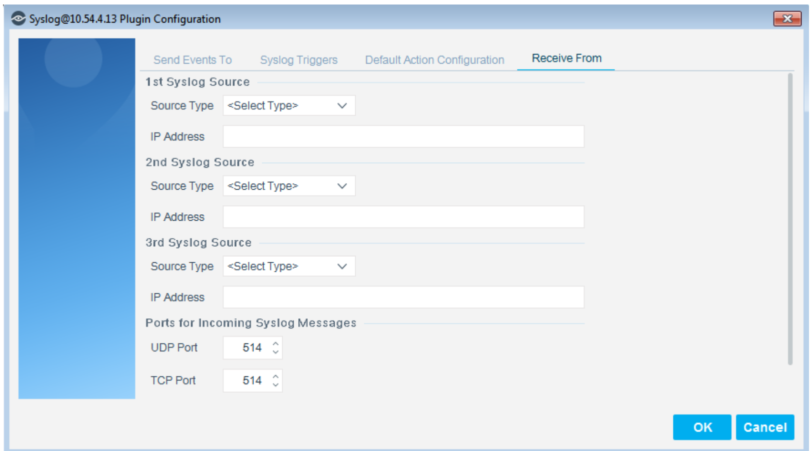
- Configure the Plugin Receiver Port
- Verify the Plugin is Running

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 management interface. Each such Forescout device receives syslog events sent from managed, individual 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.


Syslog@10.54.4.13 Plugin Configuration
Send Events To
Syslog Triggers
Default Action Configuration
Receive From
OK
Cancel

1st Syslog Source
Source Type <Select Type>
IP Address

2nd Syslog Source
Source Type <Select Type>
IP Address

3rd Syslog Source
Source Type <Select Type>
IP Address

Ports for Incoming Syslog Messages
UDP Port 514
TCP Port 514

7. In the *Ports for Incoming Syslog Messages* section, do any of the following:
   a. For Cisco Meraki network devices, configure the *UDP Port* field with the identical port number that you configured for the syslog server port in the Meraki Dashboard.
   b. For Ruckus SmartZone network devices, configure either the *UDP Port* field or the *TCP Port* field with the identical port number that you configured for the syslog server port and protocol in the Ruckus SmartZone Web GUI.

   The default, syslog server port is 514, regardless of protocol.
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 management interface.

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 that are configured in the management interface as syslog servers (In the Console, 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**.

Configure the Plugin

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

- An entity's networks
- An entity's centrally-managed network devices
- The endpoints connected to these centrally-managed network devices

Plugin *controllers* are logical entities that represent the management interface of the centrally-managed network with which the plugin communicates. Each controller that you configure for the plugin communicates with one of the following management interfaces:

- Arista CloudVision Portal API (CloudVision Wired)
- Arista CloudVision WiFi
- Cisco Meraki Dashboard
- Ruckus SmartZone Public API

The section describes the following plugin configuration tasks:

- Add a Controller
- Edit a Controller
- Remove a Controller
- Test the Plugin Configuration

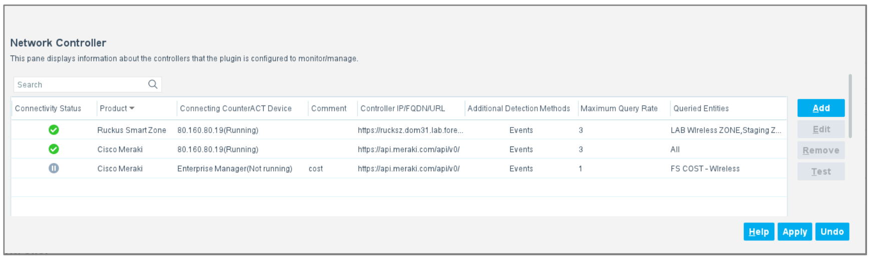
Add a Controller

The section describes how to define controllers in Forescout that communicate with the management interface of a centrally-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 **Network Controller** and then select **Configure**. The *Network Controller* pane opens.

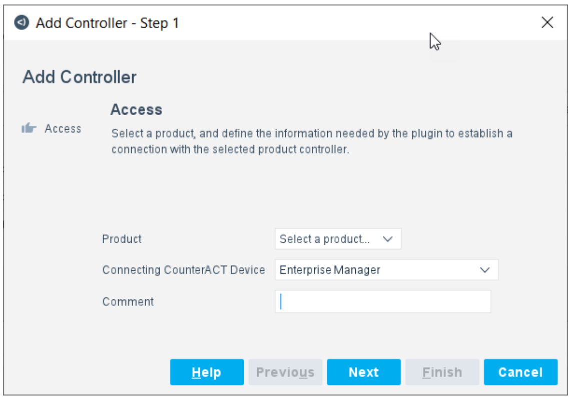


Network Controller

This pane displays information about the controllers that the plugin is configured to monitor/manage.

Connectivity Status	Product	Connecting CounterACT Device	Comment	Controller IP/FQDN/URL	Additional Detection Methods	Maximum Query Rate	Queried Entities
✓	Ruckus Smart Zone	80.160.80.19(Running)		https://rucksz.dom31.lab.fore...	Events	3	LAB WIreless ZONE,Staging Z...
✓	Cisco Meraki	80.160.80.19(Running)		https://api.meraki.com/api/v0/	Events	3	All
⏸	Cisco Meraki	Enterprise Manager(Not running)	cost	https://api.meraki.com/api/v0/	Events	1	FS COST - WIreless

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



Add Controller - Step 1

Add Controller

Access

Select a product, and define the information needed by the plugin to establish a connection with the selected product controller.

Product: Select a product...

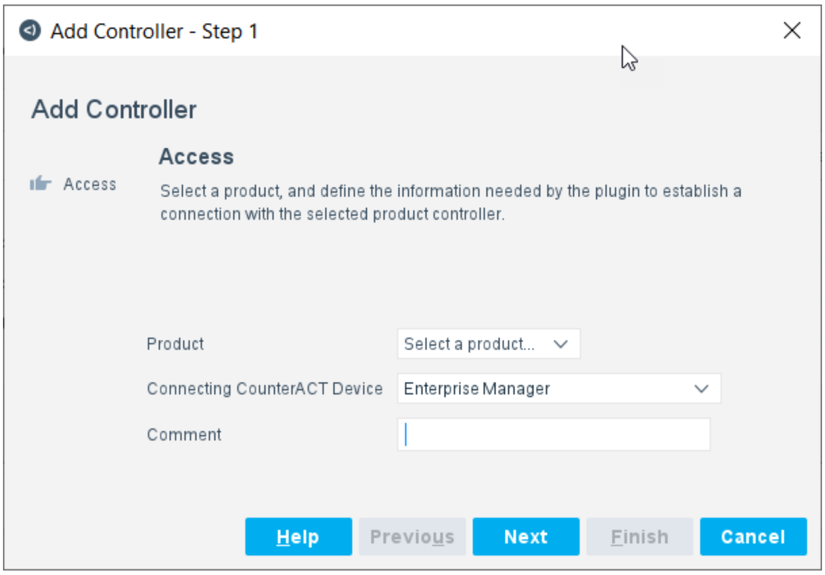
Connecting CounterACT Device: Enterprise Manager

Comment:

5. Configure the controller using the panes of the Add Controller wizard:
   - Access
   - Communication
   - Proxy Server
   - Organizations/Zones
   - Additional Detection Methods
   - Performance Tuning

Access

In the *Access* pane, configure basic information that the plugin requires in order to work with the controller of a centrally-managed network, via its management interface.



Add Controller - Step 1

Add Controller

Access

Select a product, and define the information needed by the plugin to establish a connection with the selected product controller.

Product: Select a product...

Connecting CounterACT Device: Enterprise Manager

Comment:

To configure Access pane information:

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

Field	Description
Product	From the drop-down menu, select the *Cisco Meraki* entry.
Connecting CounterACT Device	Enter the name of either the Enterprise Manager or an Appliance through which all Forescout platform-initiated communication with the management interface is directed.
Comment	(*optional*) Enter comments/descriptive text about the plugin-monitored controller.

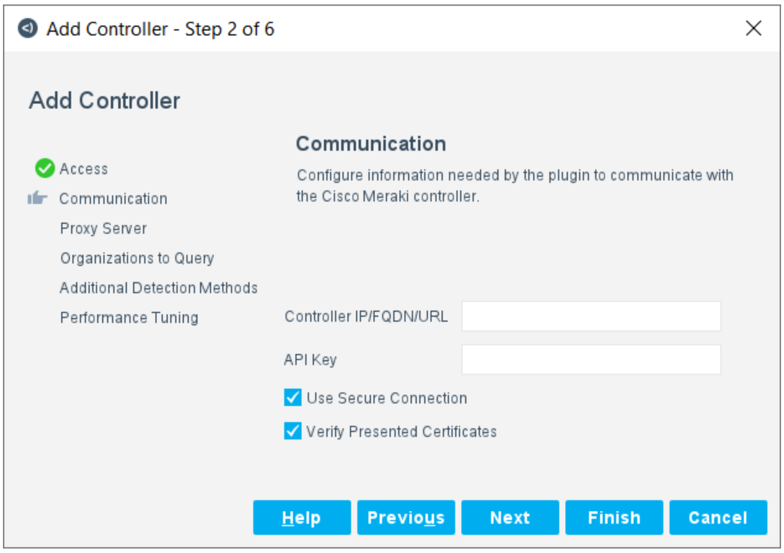
2. Select **Next**. The Communication pane opens.

Communication

In the *Communication* pane, configure the information that the plugin requires in order to communicate with the controller to obtain the following entity-associated information:

- Centrally-managed networks
- Managed networks' devices
- The endpoints connected to these devices.

Multiple controllers can be configured based on the product solution enterprise deployment and its topology.


Add Controller - Step 2 of 6

Add Controller

Communication

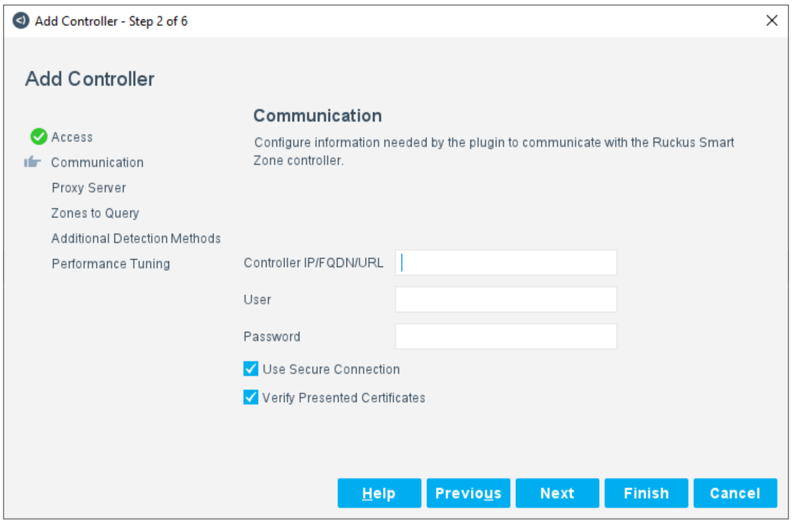
Configure information needed by the plugin to communicate with the Cisco Meraki controller.

Controller IP/FQDN/URL

API Key

☑ Use Secure Connection

☑ Verify Presented Certificates



Add Controller - Step 2 of 6

Add Controller

Communication

Configure information needed by the plugin to communicate with the Ruckus Smart Zone controller.

Controller IP/FQDN/URL

User

Password

☑ Use Secure Connection

☑ Verify Presented Certificates

To configure communication information:

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

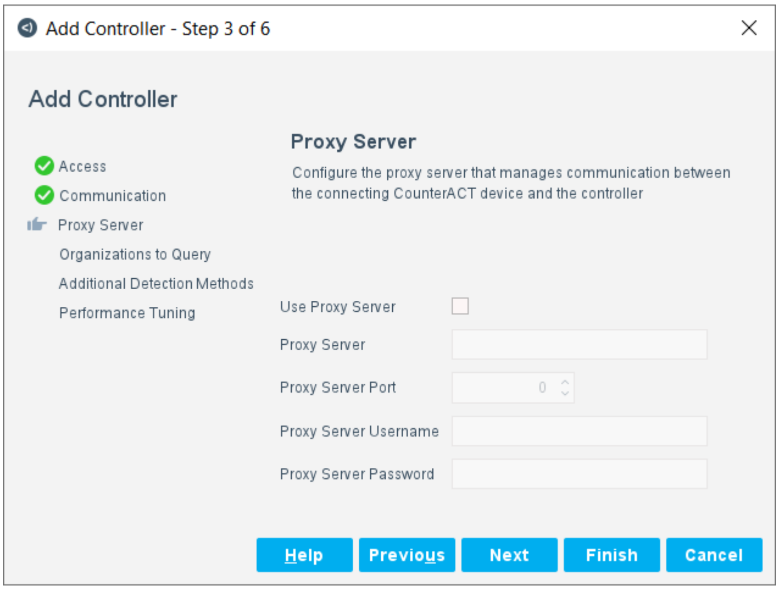
Field	Description
Controller IP/FQDN/URL	Enter one of the following controller identifiers: ▪ An IPv4 address ▪ An IPv6 address ▪ A fully qualified domain name (FQDN) ▪ A URL - URL examples per Vendor › Meraki: **`https://api.meraki.com/api/v0/`** › Ruckus SZ: **`https://RuckSZ.dom31.lab.forescout.com:8443/wsw/api/public/v8_1/`** › CloudVision WiFi: **`https://awm15004.srv.wifi.arista.com/new/webservice/`** › CloudVision Wired: **`https://10.100.146.130/`** ***Note:*** (Arista CloudVision WiFi only) Enter the URL of the Arista Wireless Manager service followed by **`/new/webservice`**
API Key	(Cisco Meraki only) Enter the API Key that the Forescout platform must use to communicate, via API, with the management interface and obtain information about the centrally-managed network. ***Note***: You must have already generated this key in the Meraki Dashboard. See Generate the Meraki API Key for details.
Key ID	(Arista CloudVision WiFi only) Enter the Key ID that the Forescout platform must use to communicate, via API, with the management interface and obtain information about the centrally-managed network. ***Note***: You must have already generated this key-value pair in Arista Launchpad See *Arista Launchpad Configuration Prerequisites.*

Field	Description
Key Value	(Arista CloudVision WiFi only) Enter the Key Value that the Forescout platform must use to communicate, via API, with the management interface and obtain information about the centrally-managed network. ***Note***: You must have already generated this key-value pair in Arista Launchpad See *Arista Launchpad Configuration Prerequisites.*
User	(Ruckus SmartZone and Arista CloudVision Wired) Enter the username that the Forescout platform must use to authenticate, via API, with the management interface and obtain information about the centrally-managed network. ***Note***: Administrator account credentials must already exist in the Ruckus SmartZone Public API. See Create the Ruckus SmartZone User for details. See Create the CloudVision Wired User for details.
Password	(Ruckus SmartZone and CloudVision Wired) Enter the password that the Forescout platform must use to authenticate, via API, with the management interface and obtain information about the centrally-managed network. ***Note***: Administrator account credentials must already exist in the Ruckus SmartZone Public API. See Create the Ruckus SmartZone User for details. See Create the CloudVision Wired User for details.
Use Secure Connection	Select this option to instruct the plugin to establish TLS-secured communication with the management interface. If this option is not selected, the plugin establishes unsecured communication with the controller.
Verify Presented Certificates	Select this option to instruct the plugin to require the management interface to present its certificate that the plugin then verifies (authenticates) as part of establishing TLS-secured communication. Use of this option requires that the management interface's trusted certificate chain is defined in the Console's certificate interface.

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 or specific 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 Connecting CounterACT Device and the management interface.


Add Controller - Step 3 of 6

Add Controller

Proxy Server

Configure the proxy server that manages communication between the connecting CounterACT device and the controller

Use Proxy Server □

Proxy Server

Proxy Server Port 0

Proxy Server Username

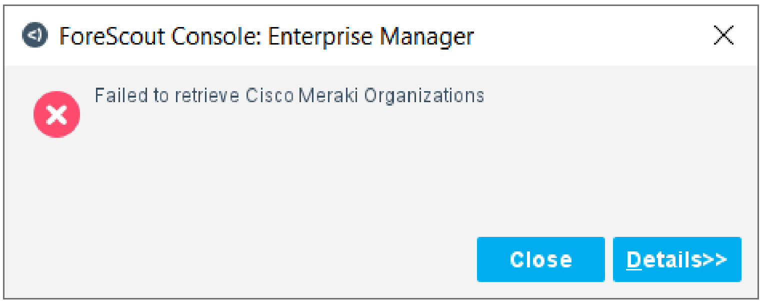
Proxy Server Password

To configure the proxy server:

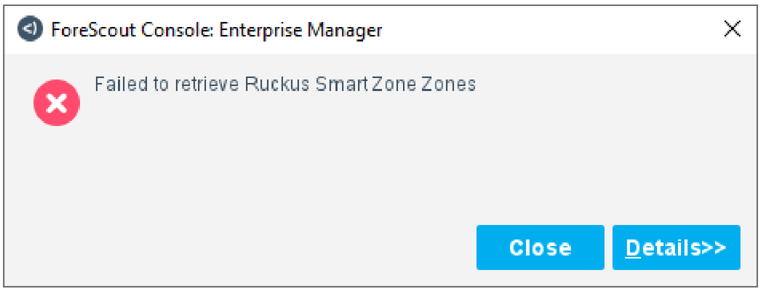
1. In the *Proxy Server* pane of the Add Controller wizard, enable (select) the **Use Proxy Server** option. By default, this option is disabled.
2. Define the following information (unless otherwise noted, all information is required):

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.
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.

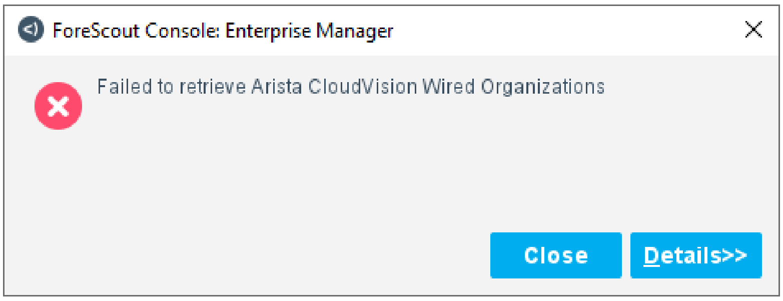
3. Select **Next**. Before opening the next pane, the plugin attempts to communicate with the controller and obtain the list of entities whose networks the plugin can query.
   a. If the plugin is unsuccessful, the following message displays, per controller of the centrally-managed network:


ForeScout Console: Enterprise Manager

Failed to retrieve Cisco Meraki Organizations



Failed to retrieve Ruckus Smart Zone Zones



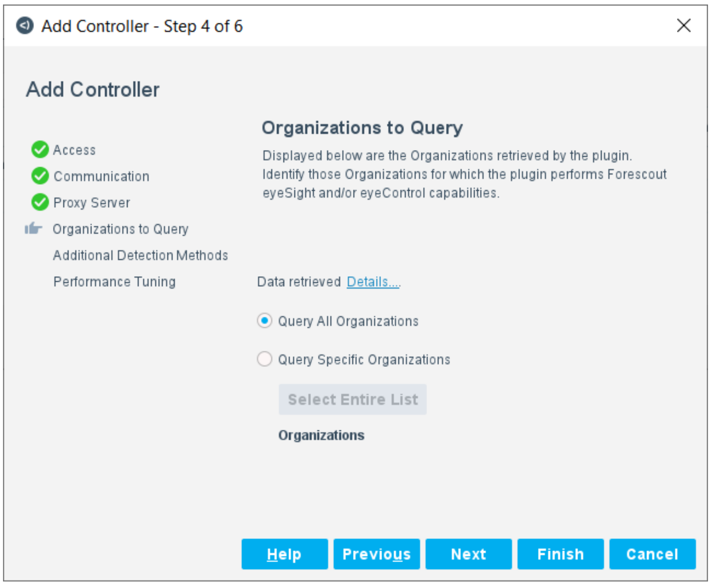
Failed to retrieve Arista CloudVision Wired Organizations

Select **Close**. The Organizations/Zones pane opens.

b. If the plugin is successful, the Organizations/Zones pane opens and displays the entities (either organizations or zones) it obtained from the controller.

Organizations/Zones/Locations to Query

In the *Organizations/Zones/Locations to Query* pane, specify which entities (either organizations, zones, or locations) the plugin is to query for information about their networks.



Organizations to Query

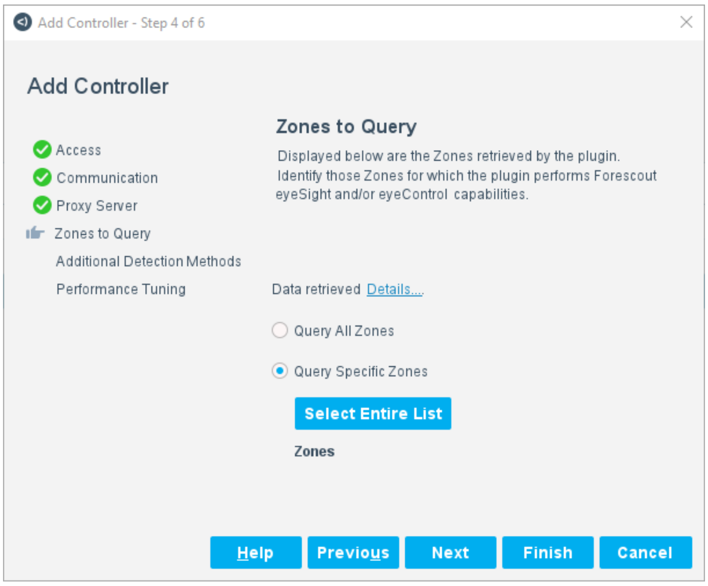
Displayed below are the Organizations retrieved by the plugin. Identify those Organizations for which the plugin performs Forescout eyeSight and/or eyeControl capabilities.

Data retrieved Details...

● Query All Organizations

○ Query Specific Organizations

Organizations



Zones to Query

Displayed below are the Zones retrieved by the plugin. Identify those Zones for which the plugin performs Forescout eyeSight and/or eyeControl capabilities.

Data retrieved Details...

○ Query All Zones

● Query Specific Zones

To configure the entities to query:

1. In the *Organizations/Zones/Locations to Query* pane, select one of the following options:
   - **Query All Organizations/Zones/Locations**. The plugin always queries the controller about the networks of ***all*** entities, including entities that are defined at a later date, after selection of this option.
   - **Query Specific Organizations/Zones/Locations**. The plugin queries the controller *only* about those specific networks whose entity is selected in the **Organizations/Zones/Locations** list. Entities defined at a later date that have not been explicitly selected in the list do not have their network(s) included in plugin queries.
     - (Arista CloudVision WiFi Only) There is a limit of 1,000 network devices per location.
     - (Arista CloudVision WiFi only) There is a limit of 10,000 endpoints per location. This limitation can come into effect when a selected location has one or more child locations where the total number of endpoints for the selected location tree totals >10,000 endpoints.
     - (Arista CloudVision WiFi only) The exact locations to query must be selected. The Network Controller plugin parses the endpoints exactly at the selected level. It does not parse any devices/endpoints that are located at child locations if they are not explicitly selected.
     - (Arista CloudVision Wired only) The plugin always returns a hardcoded, preset, Organization called *CloudVision Wired Organization*. See Terms in Use for more information.

     This option includes is a button that toggles between **Select Entire List**/**Clear Selections**.
2. Select **Next**. The Additional Detection Methods pane opens.

Additional Detection Methods

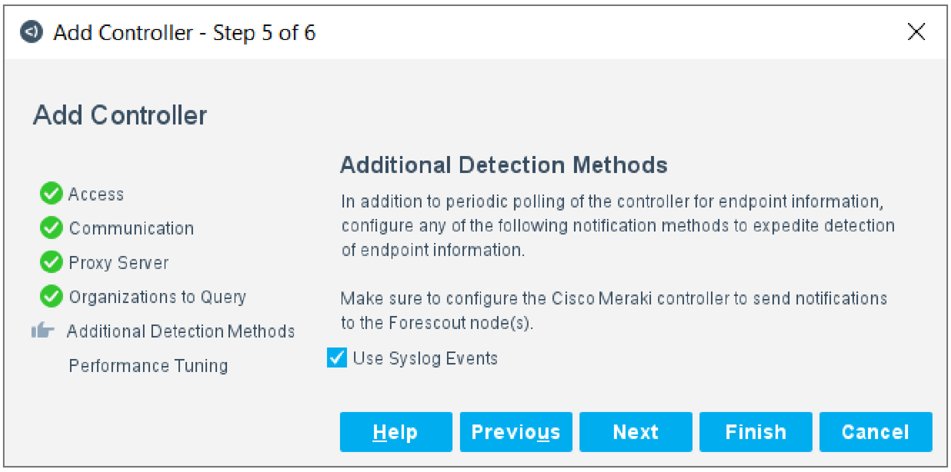
This pane is not displayed for Arista CloudVision Wired since syslog is not supported.

In the *Additional Detection Methods* pane, instruct the plugin to listen for syslog events that are sent to the Forescout platform from centrally-managed network devices. When this option is selected, plugin detection of endpoint connections to/disconnections from those devices is *expedited*.

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

- Periodic polling of the controller, via its management interface (standard plugin method)
- Received syslog events (additional detection method)

When the plugin is not configured to listen for syslog events, the plugin relies on its periodic polling of the controller to detect endpoint connections and disconnections.



Add Controller - Step 5 of 6

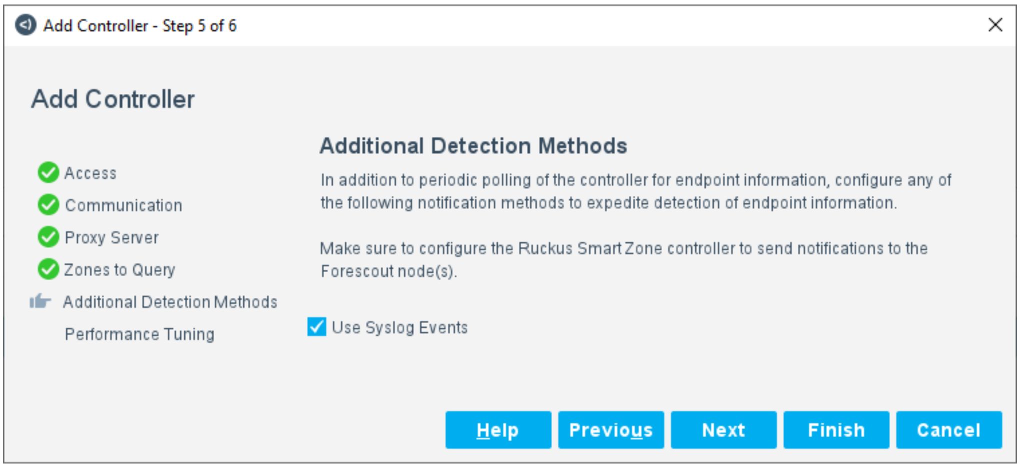
Add Controller

Additional Detection Methods

In addition to periodic polling of the controller for endpoint information, configure any of the following notification methods to expedite detection of endpoint information.

Make sure to configure the Cisco Meraki controller to send notifications to the Forescout node(s).

☑ Use Syslog Events



Add Controller - Step 5 of 6

Add Controller

Additional Detection Methods

In addition to periodic polling of the controller for endpoint information, configure any of the following notification methods to expedite detection of endpoint information.

Make sure to configure the Ruckus SmartZone controller to send notifications to the Forescout node(s).

☑ Use Syslog Events

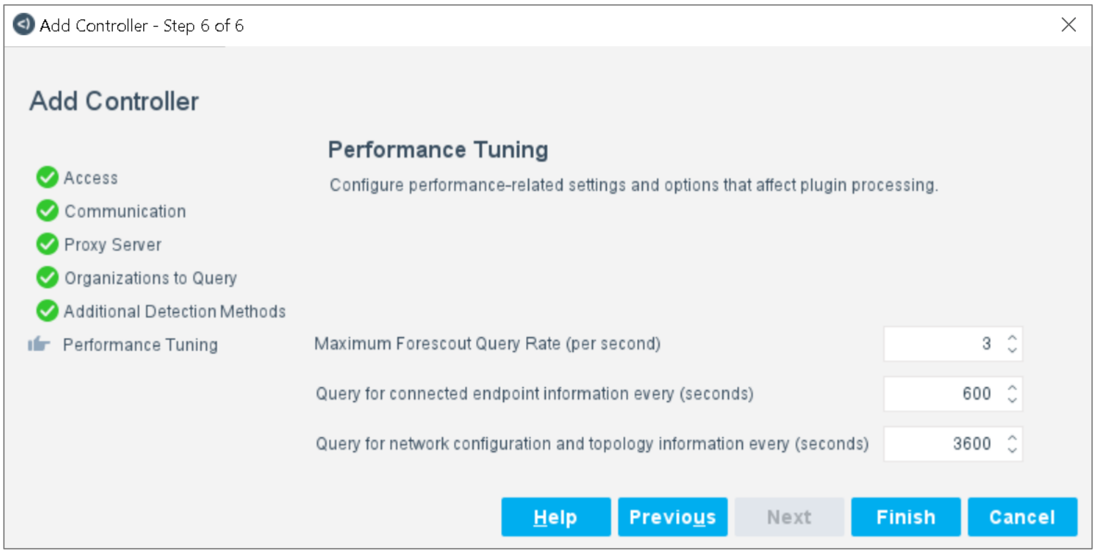
To expedite detection of endpoint connections/disconnections:

1. In the *Additional Detection Methods* pane, verify that **Use Syslog Events** is selected (this option is enabled by default) or select it.
2. Select **Next**. The Performance Tuning pane opens.

Also, remember that working with this option requires both management interface configuration and Syslog Plugin configuration. See Configuration Prerequisites.

Performance Tuning

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



Performance Tuning

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

Maximum Forescout Query Rate (per second) 3

Query for connected endpoint information every (seconds) 600

Query for network configuration and topology information every (seconds) 3600

To configure performance settings for plugin monitoring of a centrally-managed network:

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

Field	Description
Maximum Forescout Query Rate (per second)	Modify the maximum number of queries per second that the plugin per controller is allowed to send to the management interface. ▪ For Cisco Meraki, the query rate range is 1–5 ▪ For Ruckus SmartZone, Arista CloudVison WiFi and Wired, the query rate range is 1–10 The default, maximum query rate is 3.

Field	Description
Query for connected endpoint information every (seconds)	Modify the frequency, in seconds, of queries for connected endpoint information. ▪ When *Use Syslog Events* is enabled (see the *Additional Detection Methods* pane), the default query period is 600 seconds (10 minutes). ▪ When *Use Syslog Events* is disabled: > For Arista CloudVision WiFi, the recommended query period is 180 seconds (3 minutes) > For Cisco Meraki, the recommended query period is 180 seconds (3 minutes) > For Ruckus SmartZone, the recommended query period is 60 seconds (1 minute) ***Note***: (Cisco Meraki only) This query requests the Cisco Meraki dashboard to supply the plugin with the previous 5 minutes worth of endpoint information. When this setting's query rate is less than every 300 seconds (5 minutes), the supplied Cisco Meraki data may include endpoints that are currently disconnected (offline) yet report them as being connected (online). ***Note***: (Arista CloudVision Wired only) The “Connected Endpoints” feature in Arista CloudVision Wired is dependent on DHCP requests. To avoid reporting offline hosts as online, the plugin only considers hosts that were “Last Seen” one hour ago or sooner, as online.
Query for network configuration and topology information every (seconds)	Modify the frequency, in seconds, of queries for the following centrally-managed network information: ▪ Arista CloudVision WiFi - Locations - Managed network devices ▪ Arista CloudVision Wired: Topology information – The network devices being managed by Arista CloudVision Wired. ▪ Cisco Meraki: - Switch device port configuration information - Topology information - organizations, managed networks and the network devices belonging to managed networks - The names of all the group policies defined per network. ***Note***: Group policies can be defined for all Cisco Meraki centrally-managed networks except for networks of type *Switch*. ▪ Ruckus SmartZone: - Topology information - zones, managed AP groups and the network devices belonging to managed AP groups By default, this query period is 3600 seconds.

2. Select **Finish**.

   The new controller is listed in the *Network Controller* 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 *Network Controller* 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 *Network Controller* 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 or *after* editing the plugin configuration for a controller entry but *before* saving the updated plugin configuration, make sure you test the plugin configuration for the new/updated 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:

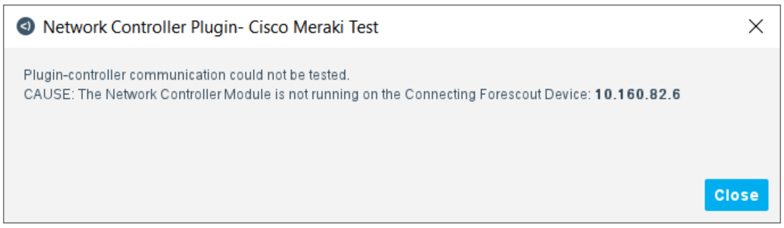
- The plugin is running on the designated Connecting CounterACT Device.
- The plugin established a communication connection with the management interface/controller:
  - Within the allowed time frame
  - Did not encounter any network problem

  - Used valid API command data (Cisco Meraki)
  - Used valid user/password credentials (Ruckus SmartZone and Arista CloudVision Wired)
  - Did authenticate

- The plugin retrieves information about the entities selected to be queried (see the Organizations/Zones pane).

To test the plugin configuration:

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



Network Controller Plugin- Cisco Meraki Test

Plugin-controller communication could not be tested.
CAUSE: The Network Controller Module is not running on the Connecting Forescout Device: **10.160.82.6**

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

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

Verify Plugin Processing of Syslog Events

Not supported by Arista CloudVison Wired

When your Forescout platform deployment is operating, if the management interface, the Syslog Plugin and the NC 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 Up Trap* – (Cisco Meraki only) syslog event received, notifying of endpoint connection to a switch
- *Link Down Trap* – (Cisco Meraki only) 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

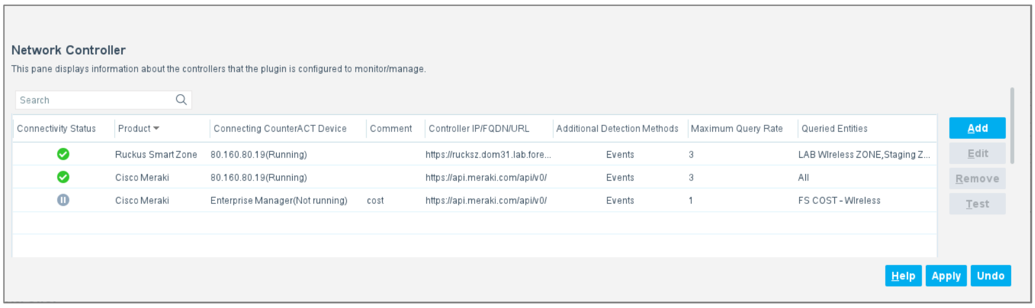
This section describes the following information displays provided in the Forescout Console:

- Network Controller Pane
- Home Tab

- Asset Inventory Tab

Network Controller Pane

The *Network Controller* pane displays information about the controllers that represent the centrally-managed network that the plugin is configured to communicate with, via the product solution's management interface, for the purposes of executing *eyeSight* and *eyeControl* activities. Access the *Network Controller* pane via the following Console selections: **Tools** > **Options** > **Modules** > **Network** > **Network Controller** > **Configure**.



Network Controller

This pane displays information about the controllers that the plugin is configured to monitor/manage.

Connectivity Status	Product	Connecting CounterACT Device	Comment	Controller IP/FQDN/URL	Additional Detection Methods	Maximum Query Rate	Queried Entities
✓	Ruckus Smart Zone	80.160.80.19(Running)		https://rucksz.dom31.lab.fore...	Events	3	LAB WIreless ZONE,Staging Z...
✓	Cisco Meraki	80.160.80.19(Running)		https://api.meraki.com/api/v0/	Events	3	All
⏸	Cisco Meraki	Enterprise Manager(Not running)	cost	https://api.meraki.com/api/v0/	Events	1	FS COST - WIreless

The following controller-related information is available:

Column	Description
Connectivity Status	The status of the configured entry or the communication status with the controller. The possible statuses are: ▪ **New** (hourglass icon) – Plugin is starting to run on the Connecting CounterACT Device ▪ **Up** (green icon) – Plugin-controller communication is successfully established. ▪ **Pause** (pause icon) – Plugin cannot determine plugin-controller communication status, due to any of the following causes: - Plugin may not be running on the Connecting CounterACT Device - The configured entry is newly added but has not been saved (select **Apply** to save). ▪ **Down** (red icon) – Plugin-controller communication is down/failed.
Product	The centrally-managed network product.
Connecting CounterACT Device	The designated Enterprise Manager or Appliance through which all Forescout-platform-initiated communication with the management interface of the centrally-managed network is directed.
Comment	User-provided comments/descriptive text.
Controller IP/FQDN/URL	The controller identifier configured for plugin use, which can be any of the following: ▪ An IPv4 address ▪ An IPv6 address ▪ An FQDN ▪ A URL

Column	Description
Additional Detection Methods	The methods, in addition to polling, that the plugin uses to detect endpoint connections and disconnections. The available, additional methods are: ▪ Events
Maximum Query Rate	The maximum number of plugin queries per second that the controller is allowed to send to the cloud management interface.
Queried Entities	The entities, either selected organizations or selected zones, whose networks are being monitored by plugin queries to the controller of the centrally-managed network.

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

Home Tab

The network devices and connected endpoints that the Network Controller Plugin discovers, via its monitoring of centrally-managed networks, appear as entries in the *All Hosts* pane in the Forescout Console's *Home* tab.

The Console *All Hosts* pane displays the following information about the network 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/AP

- Vendor

- WLAN AP Name
- Network Function – Lightweight AP (Access Point)
- Network ID#
- Network Name#
- Organization ID&
- Organization Name&

For plugin-discovered wireless network devices, entries tagged with a hash (#) display information about network/AP group and entries tagged with an ampersand (&) display information about organization/zone. See the Terms in Use. For Arista CloudVision WiFi, the *Network Name* property corresponds to the *Location*.

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

Plugin Reporting of Endpoints Connected to Cisco Meraki Network

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.

3. When detected endpoints disconnect from a Cisco Meraki network, there is a delay in the Console update/display of their current, disconnected (offline) status. The delay period is two iterations of the NC Plugin query for connected endpoint information. See the *Performance Tuning* tab for the defined value of the setting *Query for connected endpoint information every (seconds)*.

Plugin Reporting of Endpoints Connected to Ruckus SmartZone Network

When detected endpoints disconnect from a Ruckus SmartZone network, there is a delay in the Console update/display of their current, disconnected (offline) status. The delay period is 120 seconds (2 minutes).

Plugin Reporting of Endpoints Connected to Arista CloudVision WiFi Network

When detected endpoints disconnect from Arista CloudVision WiFi, there is a delay in the Console update/display of their current, disconnected (offline) status. The delay period for the API call to update is 120 seconds for a disconnection. The next endpoint query that the network controller makes reflects this change.

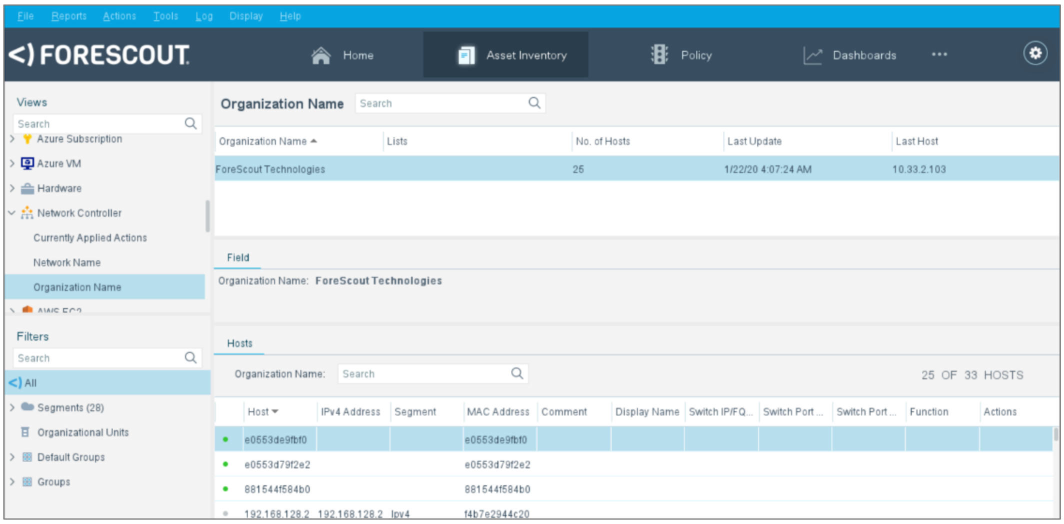
Plugin Reporting of Endpoints Connected to Arista CloudVision Wired Network

The “Connected Endpoints” feature in Arista CloudVision Wired is dependent on DHCP requests. Due to the nature of DHCP, there is no real-time reporting of when hosts go offline since endpoints only make DHCP requests when they go online. To avoid reporting offline hosts as online, the plugin only considers hosts that were “Last Seen” one hour ago or sooner, as online.

Asset Inventory Tab

Forescout *Asset Inventory* views show the distribution of wired and wireless endpoints across the entities and networks of centrally-managed networks being monitored by the plugin. This eliminates the need to go to the management interface of a centrally-managed network to see how many endpoints are connected to each network device. You can also:

- View plugin-reported entity and network information.
- View endpoints that are currently applied with a Network Controller Plugin action.
- Incorporate inventory detections into policies.



Organization Name

Organization Name	Lists	No. of Hosts	Last Update	Last Host
ForeScout Technologies		25	1/22/20 4:07:24 AM	10.33.2.103

Organization Name: **ForeScout Technologies**

	Host	IPv4 Address	Segment	MAC Address	Comment	Display Name	Switch IP/FQ...	Switch Port ...	Switch Port ...	Function	Actions
●	e0553de9fbf0			e0553de9fbf0							
●	e0553d79f2e2			e0553d79f2e2							
●	881544f584b0			881544f584b0							
●	192.168.128.2	192.168.128.2	Ipv4	f4b7e2944c20							

The following *Network Controller* information views are available:

Information	Description
Currently Applied Actions	The list of endpoints to which one or more than one Network Controller Plugin action is currently applied, due to either Forescout platform policy evaluation or manual application.
Network Name	Current information about the networks/AP groups to which detected endpoints are connected.
Organization Name	Current information about the entities, either organizations or zones, to which detected endpoints belong.

Property Resolution

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

- Network Controller
- Switch
- Wireless
- Track Changes

Network Controller Properties

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

Property	Sub-Fields	Description
Currently Applied Actions	▪ **Action Name** ▪ **Action Parameters**	Identifies all Network Controller Plugin actions that are currently applied on the detected endpoint. For each currently applied action, the property lists its name and any associated parameters; multiple parameters are comma-separated.
Network ID		ID of the network/AP group to which the detected endpoint is connected.
Network Name		Name of the network/AP group to which the detected endpoint is connected.
Organization ID		ID of the entity, either organization or zone, to which the detected endpoint belongs.
Organization Name		Name of the entity, either organization or zone, to which the detected endpoint belongs.

Switch Properties

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

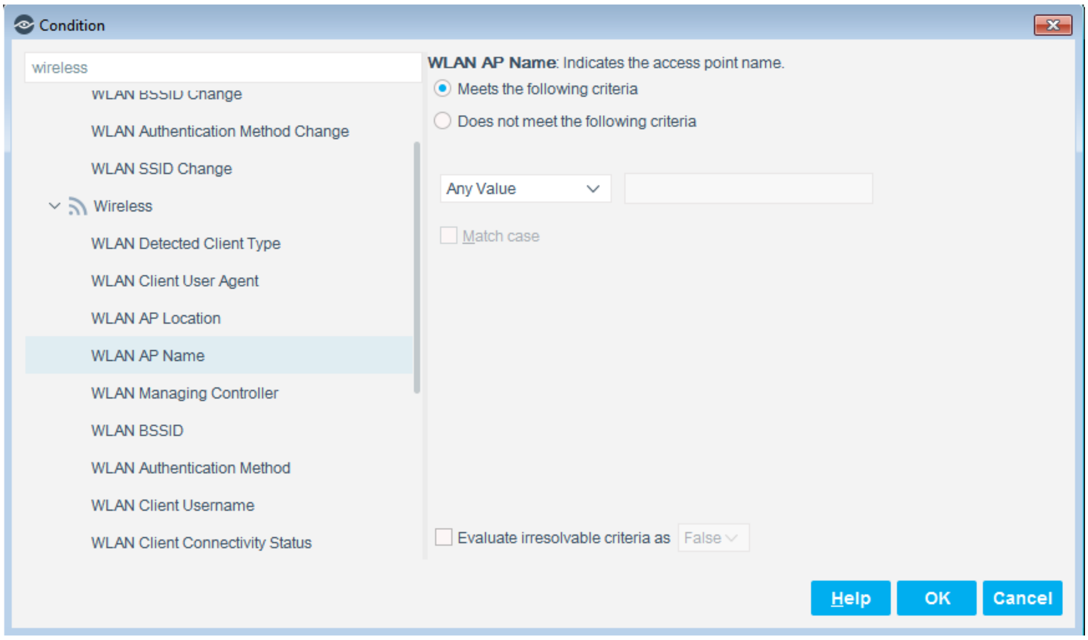
🗎 *Currently, the Network Controller plugin does not discover switches in Arista CloudVision WiFi and Ruckus SmartZone networks.*

Property	Description
Switch Hostname	The switch name as defined in the switch.
Switch IP/FQDN	The IP address or the FQDN of the switch.
Switch IP/FQDN and Port Name	The IP address or the FQDN of the switch and the port name (the physical Ethernet interface information of the port). The format is *<IP address/FQDN>:<port>*.
Switch Port Alias	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.

The Network Controller Plugin does not resolve any other Forescout switch properties.

Wireless Properties

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



WLAN AP Name: Indicates the access point name.

● Meets the following criteria

○ Does not meet the following criteria

Any Value

□ Match case

□ Evaluate irresolvable criteria as False

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 Client VLAN	Identifies the VLAN to which the wireless client is connected.
WLAN Device IP/FQDN	The IP address or the FQDN of the access point to which the wireless client is connected.
WLAN Device Vendor	The vendor of the managing controller of the centrally-managed network.
WLAN Network Function	The plugin resolves this property with any of the following values: ▪ **Lightweight AP** - the device is determined to be a lightweight access point that is managed by the controller of the centrally-managed network ▪ **Other** - the device is determined to be a connected wireless client (an endpoint).
WLAN SSID	Identifies the SSID (service set identifier) to which the wireless client is connected.

The Network Controller Plugin does not resolve any other Forescout wireless properties.

Track Changes Properties

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

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

Network Controller Track Changes Properties

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

Switch Track Changes Properties

🗎 *Currently, plugin does not discover switches in Ruckus SmartZone networks*

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.

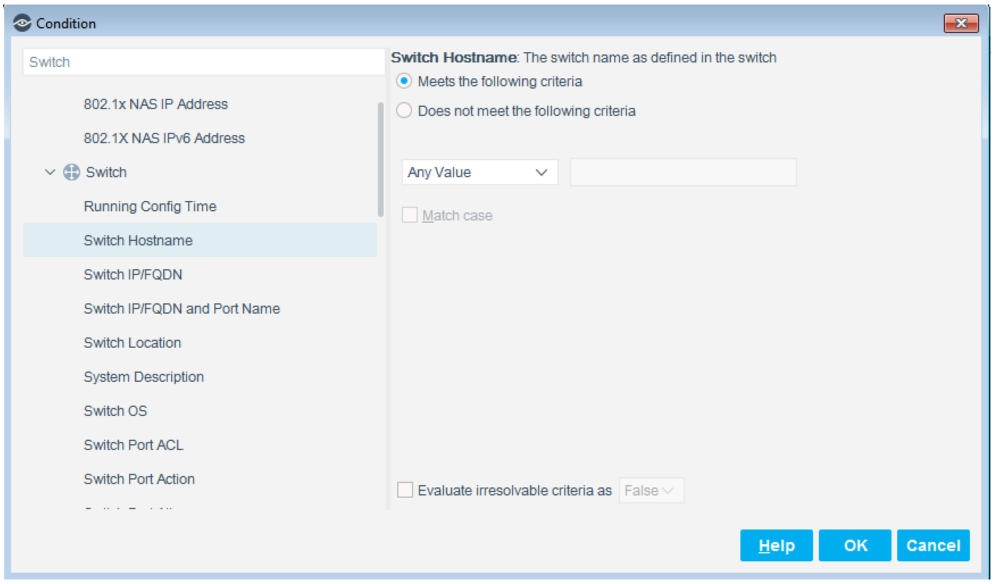
Property	Description
WLAN Client Connectivity Status Change	Identifies that a change in value occurred in the **WLAN Client Connectivity Status** property.
WLAN Client Username Change	Identifies that a change in value occurred in the **WLAN Client Username** property.
WLAN Client VLAN Change	Identifies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

Creating ForeScout Policies

Create Forescout policies to:

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

For example, create a policy that evaluates endpoint properties and identify those endpoints that are connected to a specific, centrally-managed switch or those endpoints that are connected to a specific centrally-managed wireless AP.



Switch Hostname: The switch name as defined in the switch

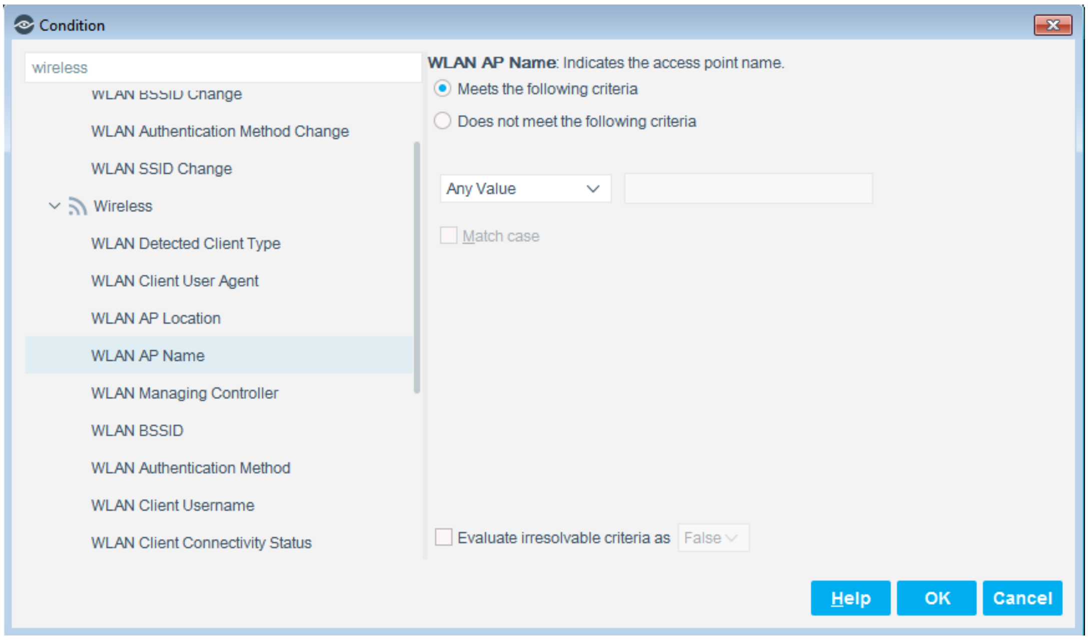
● Meets the following criteria

○ Does not meet the following criteria

Any Value

□ Match case

□ Evaluate irresolvable criteria as False



WLAN AP Name: Indicates the access point name.

● Meets the following criteria

○ Does not meet the following criteria

Any Value

□ Match case

□ Evaluate irresolvable criteria as False

Action Control

The Network Controller Plugin provides Forescout eyeControl actions that apply control on endpoints. You can incorporate these actions in policies, and you can also manually apply these actions on detected endpoints that you select. In the Forescout Console, find these actions in the *Restrict* action group. See also Forescout eyeControl Cancel Actions.

No actions are supported for Arista CloudVision Wired.

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.

The Network Controller Plugin provides the following Forescout eyeControl actions:

- Assign to VLAN-Network Controller
- Block Network Access
- Restrict Network Access
- Whitelist Network Access

Assign to VLAN-Network Controller

Use the *Assign to VLAN-Network Controller* action to assign connected endpoints to a specific VLAN on a network device port. The plugin applies the *Assign to VLAN-Network Controller* action only on endpoints that are connected to the following network device type:

- Switch

When the plugin applies this action on a targeted endpoint that is connected to a Cisco Meraki switch, there is always some delay in the Console update/display of the endpoint's newly assigned IP address, which results from action processing. This delay has the following, two contributing factors:

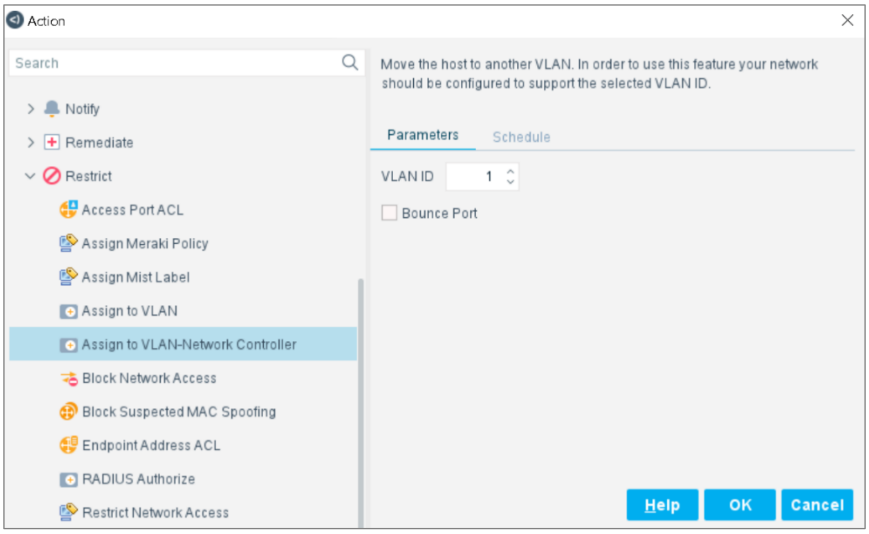
1. The amount of time it takes the Meraki controller to be updated about the connected endpoint's newly assigned IP address

2. Then, only after #1 occurs, the amount of time until the next NC Plugin query for connected endpoint information

To configure the action:

1. In the action's **Parameters** tab, define the following fields:

Field	Description
VLAN ID	Enter the ID of the VLAN that the plugin assigns, via the network controller, to endpoints that are connected to a switch port and targeted by the action.
Bounce Port	Enable (select) this option to have the plugin, via the network controller, bounce the port to which endpoints, targeted by the action, are connected. By default, this option is disabled. Bouncing a port - shutting port and re-opening it - causes the switch to assign the affected endpoint a new IP address. Do *not* enable this option for Cisco Meraki switches, as it is *not* necessary.



Move the host to another VLAN. In order to use this feature your network should be configured to support the selected VLAN ID.

VLAN ID 1

□ Bounce Port

Block Network Access

The *Block Network Access* action completely restricts targeted endpoints from connecting to all centrally-managed network devices.

Ruckus SmartZone Networks

Currently, this is the only eyeControl action that the plugin supports for use in Ruckus SmartZone networks.

Arista CloudVision WiFi

This action adds clients to the *Banned Clients* list. By default, Arista CloudVision WiFi does not block the network access of clients in the *Banned Clients* list.

To block access of banned clients:

1. In the Arista Launchpad at https://launchpad.wifi.arista.com, select the **Wireless Manager** from the *Dashboard* tab.
2. Select **Configuration > WIPS > Intrusion Prevention**.

3. Under *Banned Clients*, enable:
   a. **Banned Client connection to Authorized and Guest Aps**
   b. **Banned Client connection to Uncategorized Indeterminate Aps**

Restrict Network Access

The *Restrict Network Access* action assigns the selected policy to targeted endpoints. The policies from which to choose are user-defined that the plugin obtains from the management interface of the controller.

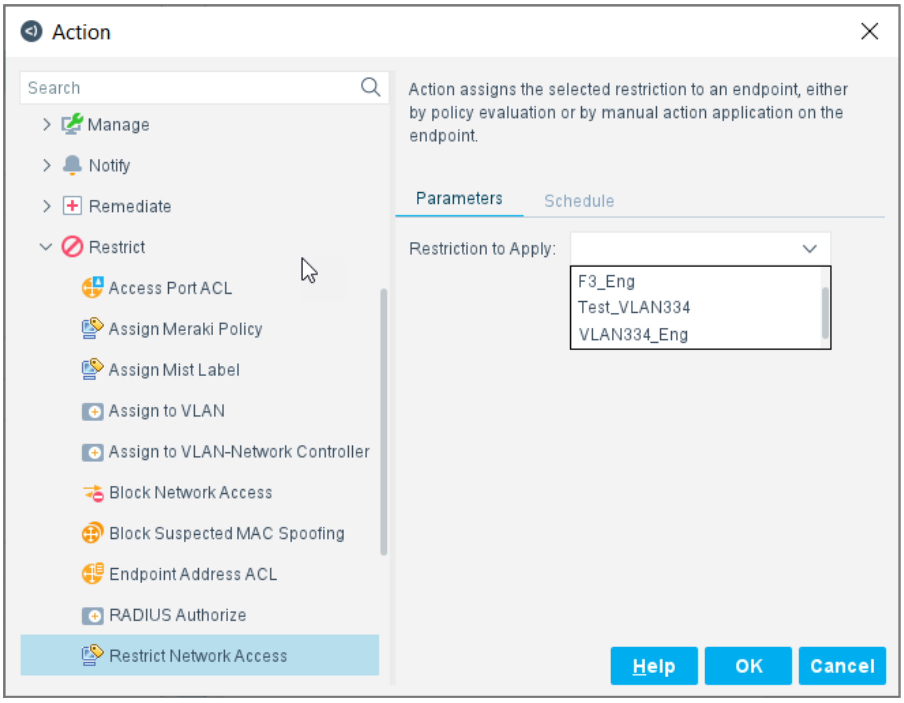
(Cisco Meraki only) The plugin applies the *Restrict Network Access* action only on endpoints that are connected to any of the following Meraki network device types:

- Security & SD WAN
- Teleworker Gateway
- Wireless Access Point

To configure the action:

1. In the action's **Parameters** tab, define the following field:

Field	Description
Restriction to Apply	From the drop-down menu, select a policy option that the plugin assigns, via the network controller, to connected endpoints that are targeted by the action.


Action assigns the selected restriction to an endpoint, either by policy evaluation or by manual action application on the endpoint.

Restriction to Apply: F3_Eng, Test_VLAN334, VLAN334_Eng

Whitelist Network Access

The *Whitelist Network Access* action permits targeted endpoints to connect, without restriction or limitation, to any centrally-managed network device.

Cancel Actions

Periodic policy re-evaluation, by the Forescout platform, may cancel actions that are currently applied on connected endpoints; you can also manually cancel actions that are currently applied on connected endpoints. In the Forescout Console, find these actions in the *Restrict* action group. The Network Controller Plugin provides the following Forescout eyeControl cancel actions:

- Cancel Block Network Access
- Cancel Restrict Network Access
- Cancel VLAN Assignment-Network Controller
- Cancel Whitelist Network Access

Cancel Block Network Access

Cancels the Block Network Access action, which is currently applied on the targeted endpoints.

> 🗎 *Currently, this is the only eyeControl cancel action that the plugin supports for use in Arista CloudVision WiFi and Ruckus SmartZone networks.*

(Cisco Meraki only) At action cancelation, targeted endpoints are automatically assigned the Normal Meraki policy.

Cancel Restrict Network Access

Cancels the policy currently assigned to the connected endpoints that are targeted by this action.

(Cisco Meraki only) At action cancelation, targeted endpoints are automatically assigned the *Normal* Meraki policy.

Cancel VLAN Assignment-Network Controller

Cancels the applied VLAN assignment for the connected endpoints that are targeted by this action. The targeted endpoints are also re-assigned to their original VLAN; the VLAN that was in effect for them prior to the *Assign to VLAN-Network Controller* action being applied.

If the *Assign to VLAN-Network Controller* action was applied with the *Bounce Port* option, then cancel action processing also bounces the port.

Cancel Whitelist Network Access

Cancels the *Whitelist Network Access* action, which is currently applied on the targeted endpoints.

(Cisco Meraki only) At action cancelation, targeted endpoints are automatically assigned the *Normal* Meraki policy.

Network Module Information

The 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 from 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 Forescout 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.