

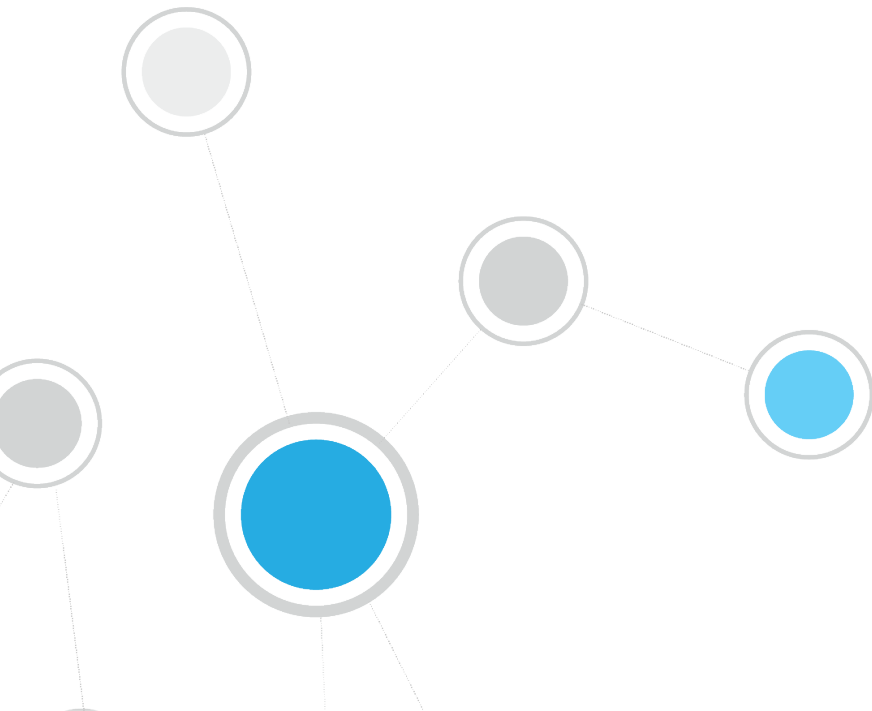


# ForeScout CounterACT<sup>®</sup>

## Network Module: Switch Plugin

### Configuration Guide

**Version 8.12**



## Table of Contents

<b>About the Switch Plugin .....</b>	<b>6</b>
Plugin Architecture .....	6
Communication between the Switch Plugin and Switches.....	7
Multi-Process Switch Plugin Architecture.....	8
Supported Vendors.....	8
Switch Vendors .....	8
Layer 3 Device Vendors.....	9
IPv6 Support .....	9
VoIP Support .....	10
ACL Capabilities .....	11
Failover Clustering Support.....	11
Trunk Port Management .....	12
Endpoint Detection .....	12
VoIP Device Treatment .....	12
Access Control List Treatment .....	12
Requirements .....	13
CounterACT Version Requirements .....	13
SNMP Requirements .....	13
Getting Started .....	13
<b>Configuring Switches in the Switch Plugin .....</b>	<b>14</b>
Manage Switch Configurations .....	15
Switch Tab Toolbar .....	15
Displaying Additional Switch Information.....	17
Switch Tab Information and Failover Clustering.....	17
Plugin Switch Management Using the Generic Vendor Option .....	18
Plugin Management of Layer 3 Devices .....	18
Methods for Adding Managed Switches.....	19
Add Switches to the Switch Plugin .....	20
General Configuration .....	21
CLI Configuration .....	22
SNMP Configuration.....	27
Permissions Configuration .....	29
ACL Configuration – Cisco and Brocade Switches.....	44
ACL Configuration – Enterasys Matrix N-Series Switches .....	52
ACL Configuration – Juniper Switches .....	53
Security Group Tagging Configuration.....	55
802.1X Integration .....	57
The ACL Repository .....	59
Global Configuration Options for the Switch Plugin.....	65
Verify That the Plugin Is Running .....	75
Edit Switch Configurations in the Plugin .....	75
Editing Multiple Switches .....	76

Verify the Plugin Is Running.....	79
Test the Switch Configuration .....	79
Running the Test.....	79
Test Failure Scenarios .....	80
View Managed Switch Information.....	84
Switch Tab Display .....	84
Replicate Switch Configuration.....	89
Duplicate Existing Switch Configuration.....	90
Use Switch Configuration as a Template.....	91
Auto-Discovery – Discover Neighboring Switches.....	92
Notification of Auto-Discovered Switches.....	95
Non-Switch Devices .....	95
Duplicate Switch Restrictions .....	96
<b>Working with Switch Information at the CounterACT Console.....</b>	<b>97</b>
Viewing Switch Information in the All Hosts Pane .....	97
View Information in the Profile Tab.....	99
CounterACT Policies.....	101
Switch Properties .....	101
Restrict Actions.....	107
Remediate Actions.....	118
Detect and Ignore Switch Virtual Interfaces.....	120
Clear ACLs from All Switch Ports .....	122
<b>Switch Setup .....</b>	<b>123</b>
Configuring Cisco Switches for SNMPv3.....	124
Configuring H3C Switches for SNMP.....	125
Configuring Huawei Switches .....	125
Configuring NETCONF on Juniper EX Series Switches .....	126
Configuring MAC Notification Traps on Cisco Switches.....	126
Configuring MAC Notification Traps – Configuration from CounterACT .....	127
Configuring MAC Notification Traps – Configuration from the Switch .....	128
Configuring Switches for ACL Integration.....	129
Layer 3 Switch Support for ACL.....	130
<b>Appendix 1: See and Control Capabilities Summary .....</b>	<b>132</b>
SEE Capabilities .....	132
CONTROL Capabilities .....	135
<b>Appendix 2: Troubleshooting, Workarounds and Feature Functionality Support .....</b>	<b>137</b>
Troubleshooting .....	137
Plugin VoIP Detection for Cisco Trunk Port Configuration Exception.....	137
Configuration Flags for Workarounds .....	138
Disable Reporting of Last Trap Received .....	138
Control the Update Frequency of Number of MACs Found .....	139
Support for Handling Multiple Entries for Same MAC .....	140
Support for VoIP for Enterasys Switches.....	141

Ignore Untagged Ports on Avaya (Nortel) Switches .....	141
Ignore Entity Mapping MIB when Detecting Physical Port .....	142
Pad MAC Addresses Missing Any Leading Zeros .....	142
Ignore Link Down Traps After Assign to VLAN Action.....	144
Configuration Flags Supporting Plugin Functionality .....	145
cli_hybrid_port_bounce_poe .....	145
<b>Appendix 3: Setting Up a VLAN .....</b>	<b>147</b>
<b>Appendix 4: MIBs Used by the Switch Plugin .....</b>	<b>148</b>
<b>Appendix 5: Using Network Device Compliance Policies .....</b>	<b>156</b>
How It Works.....	157
Prerequisites for Network Device Compliance Property Use .....	158
Define User with Privileged Permissions.....	158
Configure the Plugin .....	158
Activate the cdm Configuration Flag.....	161
Tuning .....	163
Filter Resolved Running Config Information .....	163
Adjust the Device Properties Query Rate .....	165
<b>Appendix 6: Working with ACL Capabilities .....</b>	<b>166</b>
Endpoint Address ACL Action .....	166
IP Address Blocking Capability .....	167
MAC Address Blocking Capability .....	167
Access Port ACL Action.....	167
Use Cases .....	168
Reduced Switch Processing Load .....	168
Pre-Connect Mode .....	168
Identifying Supported ACL Blocking .....	169
Switch Vendor ACL Support .....	169
What to Do.....	172
<b>Appendix 7: Improve Switch Management for Large Deployments.....</b>	<b>173</b>
Multi-Process Switch Plugin Architecture.....	173
Number of Sub-Processes to Run .....	173
Deploy Plugin Multi-Process Operation .....	174
Engineer Appliance Management Processing Load.....	174
Enable Multi-Process Operation for the Plugin .....	174
Determining the Number of Sub-Processes to Run.....	174
Plugin Multi-Process Operation Post-Upgrade .....	175
Administer Plugin Multi-Process Operation per Appliance .....	176
Disable Multi-Process Operation of the Switch Plugin for an Appliance.....	176
Force Appliance Use of the Switch Plugin Configured Settings .....	176
<b>Appendix 8: Switch Alerts .....</b>	<b>177</b>
<b>Network Module Information .....</b>	<b>180</b>

<b>Additional CounterACT Documentation.....</b>	<b>180</b>
Documentation Downloads .....	180
Documentation Portal .....	181
CounterACT Help Tools.....	181

## About the Switch Plugin

The Switch Plugin is a component of the ForeScout CounterACT® Network Module. See [Network Module Information](#) for details about the module.

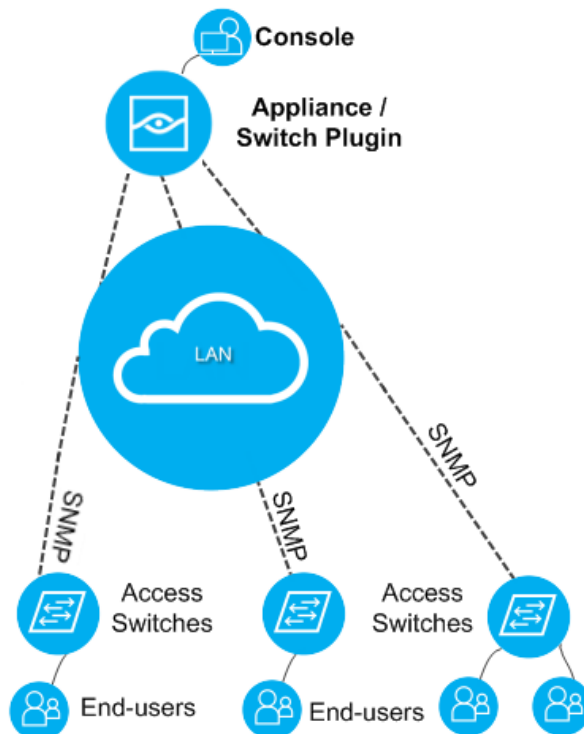
The ForeScout CounterACT® Switch Plugin provides a powerful set of features, letting you:

- Track the location of endpoints connected to network switches and retrieve relevant switch information. For example, you can see the IP address and port of the switch to which an endpoint is connected.
- Quickly detect new endpoints on the network; the Switch Plugin receives notification of port status changes via SNMP traps and alerts the CounterACT Console.
- Assign switch ports to VLANs; you can set up dynamic, role-based VLAN assignment policies and quarantine VLANs.
- Use ACLs to open or close network zones, services or protocols for specific endpoints at a switch and handle scenarios that address broader access control.

## Plugin Architecture

### *Single Appliance Solution*

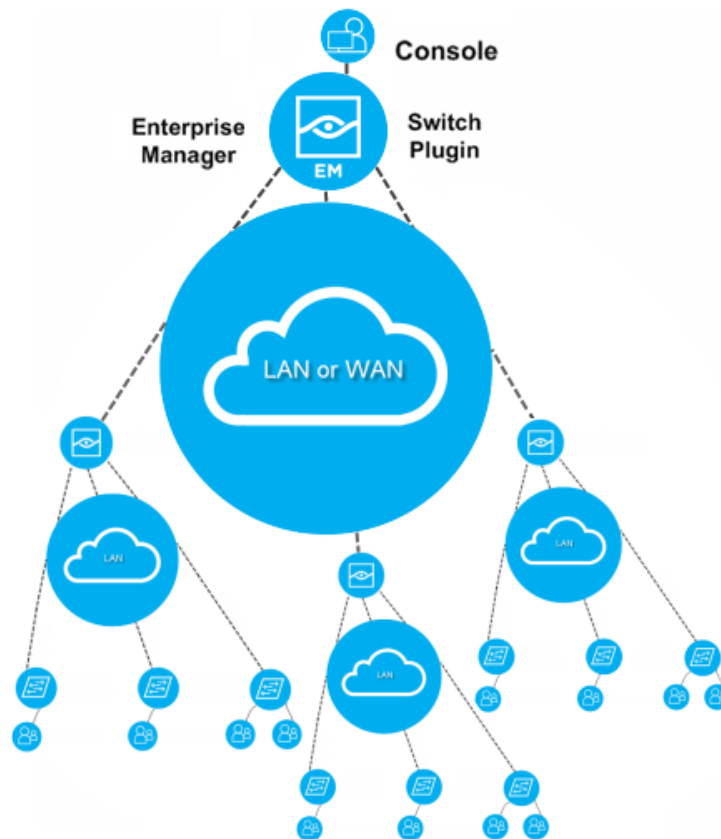
If you are working with a single Appliance, the plugin communicates with switches via the Appliance.



### Multiple Appliance Solutions

If your CounterACT solution includes multiple Appliances connected to an Enterprise Manager, by default, the plugin communicates with switches via the Enterprise Manager.

You can change this setting, on a per-switch basis, to enable an Appliance that is physically closer to the switch to communicate with the switch (recommended).



- 📄 *If an Appliance is removed from CounterACT, all switches managed via this Appliance are reassigned to be managed via the Enterprise Manager. If an Appliance is disconnected, switches must be reassigned manually.*

### Communication between the Switch Plugin and Switches

The Switch Plugin queries each switch for:

- Switch port attributes and information about connected endpoints
- Its ARP table to discover new endpoints connected to the switch

Switch information can be transferred using either SNMP, CLI or both. The transfer method(s) used between the plugin and a managed switch is (are) specific to each switch vendor.

## Multi-Process Switch Plugin Architecture

When CounterACT manages a large switch deployment containing many L2/L3 switches, implementing a multi-process Switch Plugin architecture significantly increases CounterACT's real-time switch management capacity.

In a multi-process architecture, the Switch Plugin initiates and sustains several processes simultaneously. A high-level parent process communicates between individual switch-management child processes and the CounterACT infrastructure. This architecture allows numerous switch management sessions to run concurrently, multiplying the capacity of the Switch Plugin as compared with single-process versions of the Switch Plugin. For details about implementing a multi-process Switch Plugin architecture, see [Appendix 7: Improve Switch Management for Large Deployments](#).

## Supported Vendors

The Switch Plugin manages the network devices of a broad range of vendors. The following network device types can be managed by the plugin:

- [Switch](#)
- [Layer 3](#)

## Switch Vendors

The Switch Plugin manages the switches of the following vendors:

- 3COM
- Alaxala
- Alcatel
- Apresia
- Arista
- Avaya (Nortel)
- Brocade
- Cisco
- Comtec
- D-Link
- DASAN
- Dax
- Dell
- Enterasys
- Extreme
- Force10
- H3C
- Hirschmann
- HPE
- Huawei
- Juniper
- Linksys
- NEC

For detailed information about specific, switch vendor models and operating system versions that are validated for Switch Plugin management, refer to the *WIRED INTEGRATIONS (SWITCHES)* section in the *CounterACT Network Devices Compatibility Matrix*. You can access this matrix in one of the following locations, depending on the licensing mode your deployment is using:

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#), Documentation Page.

See [Additional CounterACT Documentation](#) (*Identifying Your Licensing Mode in the Console*) to learn which licensing mode your deployment is using.



## Layer 3 Device Vendors

The Switch Plugin manages the firewalls of the following vendors:

- Check Point
- Cisco ASA
- Forcepoint Stonesoft
- Fortinet
- Juniper SRX
- Palo Alto Networks

The plugin also manages routers that run the Linux operating system.

For details about the limit of plugin management of Layer 3 devices, see [Plugin Management of Layer 3 Devices](#).

## IPv6 Support

The Switch Plugin provides IPv6-related support for the switches of the following vendors:


- Avaya (Nortel)
- Brocade
- Cisco
- Dell
- HPE-Comware
- Juniper

Plugin provided IPv6-related support is as follows:

- The plugin can **manage both dual-stack switches and IPv6-only switches**, as switch management is accomplished using either a switch IPv4 address or a switch IPv6 address.
- The Switch Plugin performs Neighbor table read operations; Neighbor table write operations are not supported.

 *For Cisco switches, the plugin also reads the Bindings table, as necessary.*

- The plugin reports IPv6 address information [IPv6 addresses and IPv6 link-local address] of connected IPv6 endpoints. This support is provided for both **IPv6-only endpoints** and **dual-stack endpoints**.
- Plugin-provided actions (restrict and remediate actions) can be applied on connected dual-stack endpoints and connected IPv6-only endpoints, with the following exceptions:
  - The Pre-Connect ACL feature is not supported for managed *IPv6-only switches*.
  - The *Access Port ACL* action is not supported for managed *IPv6-only switches*.
  - The *Endpoint Address ACL* action cannot be applied on connected *IPv6-only endpoints*.

 *Plugin application of the Endpoint Address ACL action on connected dual-stack endpoints, using the **IP ACL** option, only restricts the IPv4 traffic of these endpoints.*

For information about overall CounterACT IPv6-related support, refer to the *CounterACT 8.0 Release Notes*. For information about required configurations for CounterACT handling of IPv6 endpoints, refer to the *Work with IPv6 Addressable*

*Endpoints How-to Guide*. See [Additional CounterACT Documentation](#) for information on how to access these guides.

## VoIP Support

The Switch Plugin lets you perform *Assign to VLAN* and *Switch Block* actions in a VoIP environment. VoIP is supported for the following switch devices:

- 3COM switches
- Alcatel switches
  - VoIP detection is supported for phones connected to ports that are each configured with two static VLANs and the phone tags its own traffic with the voice VLAN.
  - VoIP detection is supported for phones connected to mobile ports. Such ports are configured for dynamic VLAN assignment, where VoIP traffic is dynamically moved to the voice VLAN by the switch.
- Avaya (Nortel) switches
- Brocade switches
- Cisco switches and phones
  - For managed Cisco switches, (1) VoIP detection is supported for phones connected to either access ports or trunk ports. (2) All potential switch ports (access and trunk) must have voice VLANs that are configured using `switchport voice vlan <n>`.
  - For managed Cisco Small Business 300 Series switches, (1) VoIP detection is supported for phones connected to either general ports or trunk ports and only when the `Auto Smartport detection` property is enabled on the switch. (2) All potential switch ports (general and trunk) must have voice VLANs that are configured using `switchport voice vlan <n>`.

For the plugin to use a CDP query with managed Cisco switches in order to determine, more frequently and more reliably, the disconnect status of the data endpoint on a VoIP port (voice VLAN, data VLAN), see [verify disconnect of data endpoint](#).

For exceptional situations in which the potential Cisco trunk ports cannot have their voice VLANs configured using `switchport voice vlan <n>`, the Switch Plugin can still provide VoIP detection for these trunk ports, see [Troubleshooting, Plugin VoIP Detection for Cisco Trunk Port Configuration Exception](#).

- Enterasys switches
- Force10 switches
- H3C switches
  - VoIP detection is supported for phones connected to H3C trunk ports and H3C hybrid ports.
- HPE switches
- Juniper EX series switches

The *Switch Port Voice Device* property is used to resolve whether a detected endpoint, connected to a switch port, is a VoIP device.

See [Global Configuration Options for the Switch Plugin](#) for more general information about working with VoIP devices.

## ACL Capabilities

Access Control Lists (ACLs) applied on a switch, perform packet filtering on traffic traveling through the switch and are commonly used to restrict the network usage of connecting endpoints. The Switch Plugin offers CounterACT operators the following ACL capabilities for switch management:

- The *Endpoint Address ACL* action
- The *Access Port ACL* action
- The Pre-Connect Mode

For an overview of Switch Plugin access control list (ACL) capabilities, see [Appendix 6: Working with ACL Capabilities](#). For configuration of the plugin to use ACL capabilities, see any of the following:

- [ACL Configuration – Cisco and Brocade Switches](#)
- [ACL Configuration – Enterasys Matrix N-Series Switches](#)
- [ACL Configuration – Juniper Switches](#)

For working with plugin ACL actions, see [Restrict Actions](#).

## Failover Clustering Support

The Switch Plugin supports CounterACT's *Failover Clustering* functionality. Failover Clustering provides for the continued, operational availability of the CounterACT service, in the event of Appliance failure (one Appliance, many Appliances or an entire data center of Appliances). Both endpoints handled by and switch devices managed by the failed Appliance(s) are automatically transferred to designated Appliances having available capacity. Refer to the *ForeScout CounterACT Resiliency Solutions User Guide* for detailed information about this feature. See [Additional CounterACT Documentation](#) for information on how to access this guide.

In support of CounterACT *Failover Clustering*, the Switch Plugin provides continuity of switch device management, including applied switch restrict actions, in the event of Appliance *failover* to a *recipient* Appliance and subsequent *fallback* to the re connected *original* Appliance.

For details about Switch Plugin processing that is affected due to *Failover Clustering*, see the following sections:

- [Switch Tab Information and Failover Clustering](#)
- [Auto-Discovery – Discover Neighboring Switches](#)
- [Restrict Actions](#)

## Trunk Port Management

Switch Plugin management provides the following handling of switch trunk ports:

- [Endpoint Detection](#)
- [VoIP Device Treatment](#)
- [Access Control List Treatment](#)

### Endpoint Detection

The plugin provides detection of endpoints that are connected to a managed switch's trunk ports, as follows:

- Detect endpoints that are connected to the trunk ports of a managed switch.
- Resolves and display in the Console the switch properties of these connected endpoints.

For details about enabling this handling, see the [Switch Advanced Settings](#) section about the option **Detect endpoints connected to trunk ports**.

### VoIP Device Treatment

The plugin provides the following VoIP device treatment on switch trunk ports of the specific, supported switch vendors:

- VoIP Detection:
  - Cisco - plugin VoIP detection is supported for phones connected to Cisco trunk ports
  - H3C - plugin VoIP detection is supported for phones connected to H3C trunk ports
- Action Application:
  - Cisco - the plugin applies the *Assign to VLAN* action and the *Switch Block* action on detected endpoints located behind a VoIP device that is connected to a Cisco trunk port
  - H3C - the plugin applies the *Assign to VLAN* action and the *Switch Block* action on detected endpoints located behind a VoIP device that is connected to an H3C trunk port

### Access Control List Treatment

The plugin provides the following Access Control List-related treatment for switch trunk ports:

- The plugin can be enabled to block endpoints on the access port or, if not found on the access port, on a trunk port, when applying the *Endpoint Address ACL* action. For details about enabling this treatment, see the plugin configuration for ACL application on Cisco and Brocade Switches, Enterasys Matrix N-Series Switches and Juniper Switches.
- For a detected endpoint, the **Switch Port Host ACL Locations – Candidates** lists any *trunk ports*, if the access port is not known *and* both the

**Enable ACL** and the **Block hosts learned via downstream devices** options are configured for the managed switch. The **Switch Port Host ACL Locations – Candidates** entry displays in the Console Profile tab and lists more than one candidate if there is more than one eligible *trunk port*.

## Requirements

This section describes:

- [CounterACT Version Requirements](#)
- [SNMP Requirements](#)

### CounterACT Version Requirements


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

- CounterACT version 8.0.
- An active Maintenance Contract for CounterACT devices is required.

### SNMP Requirements

SNMP is the primary method used by the plugin to manage switches. The Switch Plugin supports use of the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

 *When the plugin manages Cisco switches running version IOS 12.1 or below, if the plugin is configured to manage these switches using SNMPv3, make sure that the plugin is also configured to use CLI with these switches.*

Plugin receives SNMP traps on port 162. In addition, both standard and vendor-specific switch MIBs might be queried.

For information about enabling plugin handling of SNMP traps and plugin forwarding of SNMP traps, see [Handle SNMP Traps](#).

#### MIB Requirements

[Appendix 4: MIBs Used by the Switch Plugin](#) lists MIBs that must be included on the switch.

## Getting Started

The Switch Plugin is bundled with your CounterACT software.

To work with the Switch Plugin, you will need to perform some or all of the following steps:

1. Start the Switch Plugin.  
This is only necessary if you did not add any switches in the (CounterACT) Initial Setup wizard.
2. Configure switches so that they can work with the Switch Plugin. See [Switch Setup](#).
3. If you need the plugin to manage a switch whose switch vendor is not found in the [Switch Vendors](#) list, see [Plugin Switch Management Using the Generic Vendor Option](#) for details and then continue with step 5.
4. If you need the plugin to manage a Layer 3 device, verify plugin management of that device in the [Layer 3 Device Vendors](#) and see [Plugin Management of Layer 3 Devices](#) and then continue with step 5.
5. Add switches to the Switch Plugin. See [Add Switches to the Switch Plugin](#).
6. Configure switches that were discovered automatically. See [Auto-Discovery – Discover Neighboring Switches](#).
7. Test each switch configuration (**recommended**). See [Test the Switch Configuration](#).
8. Configure the plugin options. See [Global Configuration Options for the Switch Plugin](#).

## Configuring Switches in the Switch Plugin

Configuration tools let you specify which of your switches are managed by the plugin. These tools also let you control specific tasks performed by the plugin, for example, you can enable or disable the option to query switches for connected endpoints and port attributes.

Once a switch is configured, the CounterACT device that is managing the switch retrieves information about endpoints connected to the switch and about the switch. Information about the switch includes, for example, the port at which the endpoint is connected, the switch port status and the switch IP address. You can view this information at the Console when an endpoint connected to the switch is detected by the Switch Plugin. Refer to the *Working at the Console* chapter in the *CounterACT Administration Guide* for information about working with the Console. See [Additional CounterACT Documentation](#) for information on how to access this guide.

By default, the Enterprise Manager is responsible for communicating with all switches. You can change this on a per-switch basis so that, for example, an Appliance that is physically closer to a switch performs this task (recommended).

Advanced tools let you carry out performance tuning—for example, you can:

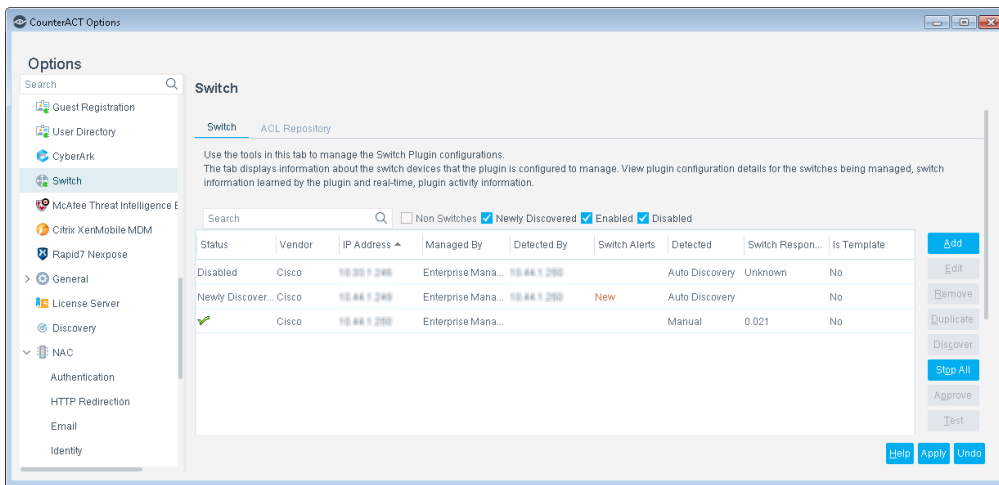
- Define ports that should never be blocked
- Change the default timeout and retry number for SNMP requests sent to the switch
- Change various default query rates

# Manage Switch Configurations

Plugin configuration definitions for the network devices that the plugin manages - switches, firewalls and Linux routers - display in the Console Switch tab. View switch configuration details, switch information learned/discovered by the plugin, real-time information regarding plugin activity and switch status.

### To display the Console Switch tab:







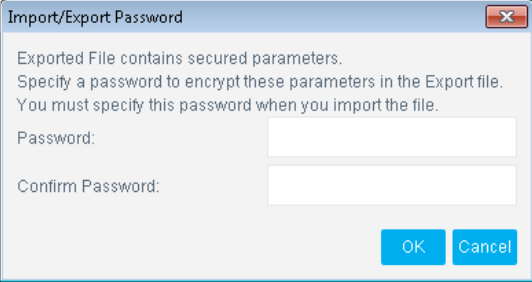

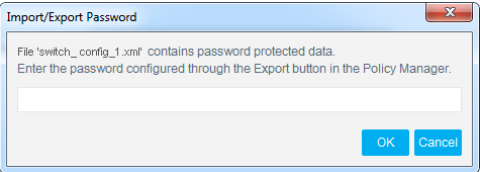

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options window opens.
2. In Options navigation tree, select **Switch**. The Switch tab opens displaying the Switch tab in the foreground and the ACL Repository tab in the background.



Use the tools in the Switch tab to add and manage switches and to review and test their configurations.

## Switch Tab Toolbar

Option	Description
	Add a switch to the plugin.
	Edit a switch configuration. See <a href="#">Edit Switch Configurations in the Plugin</a> for information about this feature. You can edit the configuration of multiple switches, provided that all selected switches are from the same vendor.
	Disconnect selected switches from the Switch Plugin. Actions carried out from this switch remain enabled. Switch discovery and endpoint learning are stopped.
	Duplicate a switch configuration. See <a href="#">Duplicate Existing Switch</a> for information about this feature.

Option	Description
	<p>Run the auto-discovery feature.</p> <p>If the switch vendor does not support auto-discovery or the switch's status is not Enabled, the <b>Discover</b> button is disabled.</p> <p>See <a href="#">Auto-Discovery – Discover Neighboring Switches</a> for information about this feature.</p>
	<p>Halt Switch Plugin functionality on all CounterACT devices. This includes:</p> <ul style="list-style-type: none"> <li>▪ Clear <i>Assign to VLAN</i> action, <i>Switch Block</i> action and any ACL actions. All related information, which the plugin placed on a configured switch in support of any of these actions, is removed.</li> <li>▪ Stop switch discovery capabilities.</li> <li>▪ Stop learning endpoint attributes.</li> </ul>
	<p>Enable auto-discovered switches.</p> <p>The switch status first changes from <b>Newly Discovered</b> to <b>Disabled</b>. The status is updated to  (Enabled) when read and write permissions are successfully assigned.</p>
	<p>Check switch connectivity and read and write access permissions.</p> <p>See <a href="#">Test the Switch Configuration</a> for information about this feature.</p>
	<p>Export the current configuration of selected switches to an XML file. You must encrypt the exported file.</p>  <p>The screenshot shows a dialog box titled "Import/Export Password" with the following text: "Exported File contains secured parameters. Specify a password to encrypt these parameters in the Export file. You must specify this password when you import the file." It includes fields for "Password:" and "Confirm Password:" and "OK" and "Cancel" buttons.</p>
	<p>Import switch configurations from an XML file. Enter the password used when the switch configurations were exported to decrypt the file.</p>  <p>The screenshot shows a dialog box titled "Import/Export Password" with the following text: "File 'switch_config_1.xml' contains password protected data. Enter the password configured through the Export button in the Policy Manager." It includes a password input field and "OK" and "Cancel" buttons.</p>
	<p>Edit Switch Plugin options that apply to all managed switches. See <a href="#">Global Configuration Options for the Switch Plugin</a> for information about these options.</p>

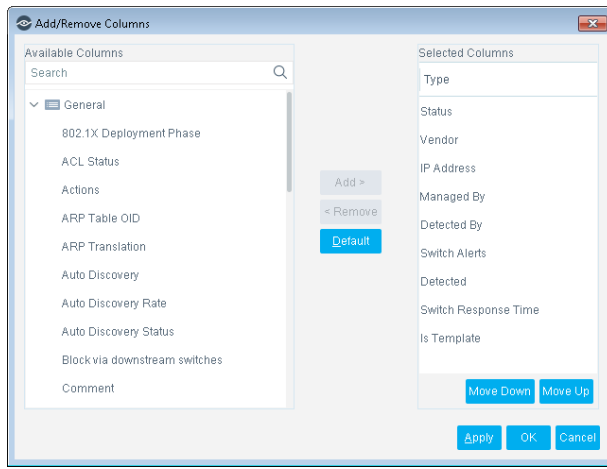


## Displaying Additional Switch Information

Basic information about the configuration of all switches appears automatically in the Switch tab. However, additional information can be displayed by adding columns to the table in the tab.

### To add or remove columns in the Switch tab:

1. Right-click any column header in the Switch tab.
2. Select **Add/Remove Columns** and then select the information that you want to display.



3. Select **OK**.

## Switch Tab Information and Failover Clustering

During a failover scenario, the Switch tab displays the following information in the **Managed By** column for managed switch devices that are currently failed over to a *recipient* Appliance:

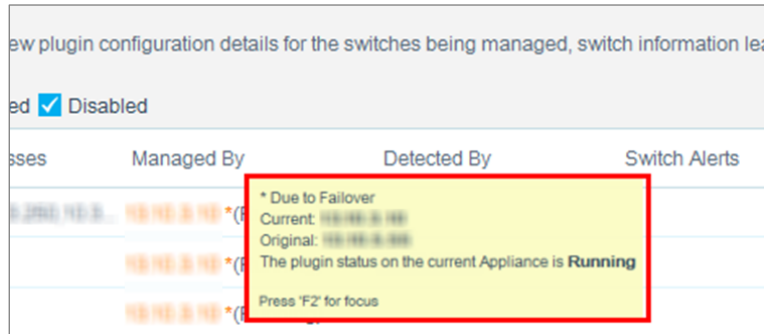
- *<current managing Appliance, after failover> \*(<current managing Appliance status>)*

Status	Vendor	IP Address	IP Interface Addresses	Managed By	Detected By	Switch Alerts	Detected	Comment
✓	Cisco	10.80.1.250	10.80.2.250, 10.80.3.250, 10.1...	13.10.3.10 *(Running)			Manual	
Disabled	Cisco	10.80.1.250		13.10.3.10 *(Running)	10.80.1.250		Auto Discovery	
✓	Cisco	10.84.1.250	10.84.2.250	13.10.3.10 *(Running)			Manual	

A **Managed By** column tooltip is displayed for managed switch devices that are currently failed over to a *recipient* Appliance. The tooltip contains the following information:

- **Current:** Current managing Appliance, after failover.
- **Original:** Original managing Appliance, prior to failover.

- **Plugin status:** *The plugin status on the current Appliance is <plugin status>.*



For information about CounterACT *Failover Clustering* and the Switch Plugin, see [Failover Clustering Support](#).

## Plugin Switch Management Using the Generic Vendor Option

If your switch vendor does not appear in the [Switch Vendors](#) list, try using the vendor option *Generic* to configure the Switch Plugin to manage the relevant switches. In Switch Plugin terminology, when the plugin is configured to manage a switch using the *Generic* vendor option, that switch is called a *generic switch*.

The plugin manages generic switches using either CLI, SNMP or both query methods.

Only the following switch actions are available for use with managed, generic switches:

- *Switch Block* action (restrict action)
- *Expedite IP Discovery* action (remediate action)

When configuring the plugin to manage a generic switch, the necessary information and procedures are provided in section [Add Switches to the Switch Plugin](#).

## Plugin Management of Layer 3 Devices

Configure the Switch Plugin to manage the following Layer 3 devices:

- Firewalls from the following vendors:
  - Check Point
  - Cisco ASA
  - Forcepoint Stonesoft
  - Fortinet
  - Juniper SRX
  - Palo Alto Networks
- Routers that run the Linux operating system (Linux routers)

Plugin management of Layer 3 devices provides the following:

- For all vendor firewalls, the plugin reads their ARP table. For the Check Point firewall and the Fortinet firewall, this includes the plugin working with the Check Point firewall's Virtual System Extension (VSX) configuration and the Fortinet firewall's Virtual Domain (VDM) configuration. ARP table reading is used by the plugin for ARP learning - IP address to MAC address mapping information. Plugin ability to obtain this firewall information is important in order to address the following NAC scenario:

The network infrastructure of the organization uses switches that only provide layer 2 functionality and layer 3 functionality is provided by firewalls.

- For the Juniper SRX firewall, the plugin also writes to its ARP table. ARP table writing is used by the plugin to clear redundant IP addresses to MAC address entries from the firewall's ARP table.
- For Linux routers, the plugin reads their ARP table. ARP table reading is used by the plugin for ARP learning - IP address to MAC address mapping information.

The plugin uses only CLI and an SSH connection to manage Layer 3 devices.

Only the following switch action is available for use with managed Layer 3 devices:

- *Expedite IP Discovery* action (remediate action)

When configuring the plugin to manage a Layer 3 device, the necessary information and procedures are provided in section [Add Switches to the Switch Plugin](#).

## Methods for Adding Managed Switches

There are several, available methods by which to configure the Switch Plugin to manage new/additional switch devices. These methods are as follows:

1. Use the Configuration Wizard - Manually **Add** a new switch device, using the Add Switch wizard. See [Add Switches to the Switch Plugin](#).
2. Approve a *Newly Discovered* Switch - Manually **Approve** newly discovered switches. See [Auto-Discovery – Discover Neighboring Switches](#).
3. Duplicate an Existing Switch - **Duplicate** a currently managed switch to add a single switch or add multiple switches. See [Duplicate Existing Switch Configuration](#).
4. Import Switches - **Import** switches from an XML file; the file's content was previously generated via performing an **Export**.
5. Switch Template Discovery - Use the switch template feature and received SNMP traps to automatically add switches. See [Use Switch Configuration as a Template](#).

Methods 1 - 4 are initiated from the Console Switch tab toolbar.

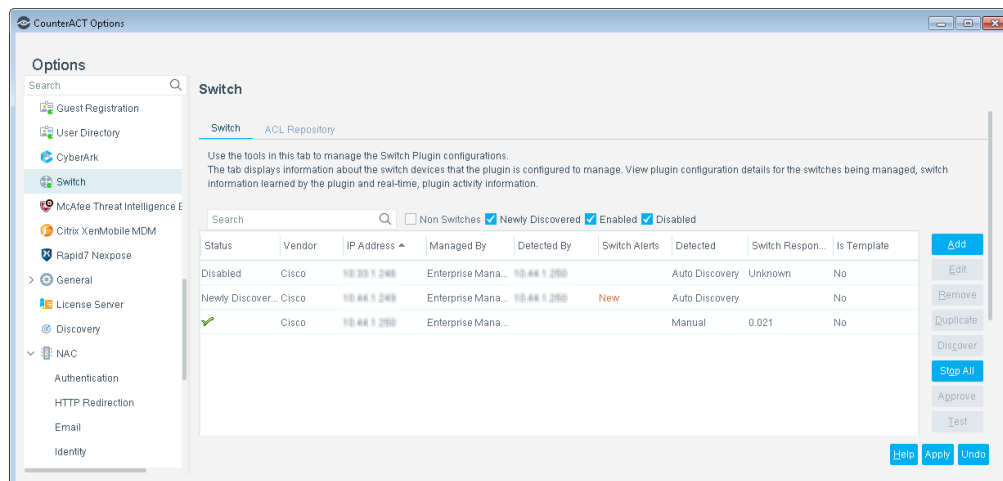
## Add Switches to the Switch Plugin

This section describes how to manually add a plugin configuration for the management of a switch or a Layer 3 device. The section presents the following plugin-configuration topics:

- [General Configuration](#)
- [CLI Configuration](#)
- [SNMP Configuration](#)
- [Permissions Configuration](#)
- ACL Configuration:
  - [ACL Configuration – Cisco and Brocade Switches](#)
  - [ACL Configuration – Enterasys Matrix N-Series Switches](#)
  - [ACL Configuration – Juniper Switches](#)
- [Security Group Tagging Configuration](#)
- [802.1X Integration](#)

### To add a new switch:

1. Select **Options** from the **Tools** menu. The CounterACT Options window opens.
2. Select **Switch**. The Switch tab opens.



3. Select **Add**. The Add Switch wizard opens displaying the General page.
4. In each page of the wizard, enter any required information and then select **Next**.  
The subsequent pages of the wizard depend on the value chosen for **Vendor** in the General page.
5. In the last page of the wizard, select **Finish**. The new switch is added to the list of switches in the Switch tab. The switch has a status of **Disabled**.
6. Select **Apply** to add the switch to the Switch Plugin.

## General Configuration

Use the **General** page of the Add Switch wizard to enter general switch information.

The screenshot shows a window titled "Switch - Wizard - Step 1" with a close button in the top right. The main content area is titled "Add Switch" and has a "General" tab selected. Below the tab, there is a "General" section with the following text: "Enter the switch device information. If the device vendor you are configuring does not appear in the vendor list, select Generic from the list. CounterACT resolves switch information for generic switches but does not carry out Switch block and Assign to VLAN actions. Refer to the online Help if the generic switch does not properly resolve switch information." Below this text are four input fields: "Address" (text box), "Connecting Appliance" (dropdown menu with "Enterprise Manager" selected), "Vendor" (dropdown menu with "Select Vendor..." selected), and "Comment" (text box). At the bottom left of the form area is a checkbox labeled "Use switch configuration as template". At the bottom right are five buttons: "Help" (blue), "Previous" (grey), "Next" (blue), "Finish" (grey), and "Cancel" (blue).

### Address

Enter the IP/FQDN of the switch, which can be any of the following:

- An IPv4 address
- A fully qualified domain name (FQDN)
- An IPv6 address

The value you configure is then used throughout the Console to identify the switch entry.

*Switches often have more than one IP address (for example, Layer 3 switches). When you add a new switch to the plugin, only a single IP address can be configured. The Switch Plugin learns the other IP addresses - IPv4 addresses and/or IPv6 addresses - automatically and reports them to the CounterACT Console which displays them in the **IP Interface Addresses** column of the **Switch** tab.*

### Connecting Appliance

Specify the CounterACT device that will manage this switch. In a multi-Appliance system, you should configure each switch to communicate via the Appliance closest to it.

If you intend to run policies that use the switch properties *Running Config* or *Interface Table* (for determining network device compliance), it is recommended that the **Connecting Appliance** contains the IP address of this switch in its Appliance **IP Assignment** range. Doing this helps ensure consistent compliance validation and saves network utilization. Refer to the *CounterACT Administration Guide* for information about Appliance **IP Assignment**. See [Additional CounterACT Documentation](#) for information on how to access this guide.

## Vendor

From the dropdown menu, select the vendor of the network device you want the plugin to manage.

- Switch management: Either select a specific switch vendor or select the **Generic** option to configure the plugin to manage the switch using the generic vendor option (for switch vendors not appearing in the [Switch Vendors](#) list).
  - For plugin management of an HPE switch running a *ProVision/ProCurve* operating system, select the vendor option **HP**.
  - For plugin management of an HPE switch running a *Comware* operating system, select the vendor option **HPE-Comware**.
- 📖 *If the plugin is currently configured to manage an HPE switch, which runs either Comware operating system version 5.x or version 7.x, as an H3C switch (the **Vendor** field is configured with H3C), it is recommended to delete the existing plugin configuration for managing this switch and configure it anew using the vendor option **HPE-Comware**.*
- Firewall management: Select a specific firewall vendor (listed in the dropdown menu as `<vendor name>-FW`).
- Linux Router management: Select the **Router-Linux** option.

## Comment

Enter comments about the switch configuration.

## Use switch configuration as template

Select this checkbox to instruct the Switch Plugin to copy the plugin configuration for managing this switch to newly detected, unmanaged switches that belong to the same SNMP community. This option is not available for use if **Juniper** is defined in the **Vendor** field.

For more information, see [Use Switch Configuration as a Template](#) in the [Replicate Switch Configuration](#) section.

## CLI Configuration

Use the **CLI** configuration page of the Add Switch wizard to specify whether to enable use of the CLI for communication from the Switch Plugin to the switch. CLI settings are described in this section.

- 📖 *When configuring the Switch Plugin to manage a Cisco Small Business 300 Series switch, do not enable **Use CLI**. The plugin interoperates with these switches using SNMP only.  
The plugin does not support applying ACL actions on the Cisco Small Business 300 series switch, since ACL support requires plugin-switch CLI interoperation.*

CLI parameters **must** be configured for the plugin to manage the following network devices:

- Layer 3 devices - all supported vendor firewalls and Linux routers
- Alaxala switches
- Arista switches
- Avaya (Nortel) - for Switch Plugin performance of Neighbor table read operations. See [IPv6 Support](#).
- Brocade dual-stack switches, in order for the Switch Plugin to perform Neighbor table read operations. See [IPv6 Support](#).
- Cisco switches in order for Switch Plugin detection of VoIP port configuration on Cisco switch ports. For an additional configuration requirement for plugin-provided detection of VoIP port configuration, see [MAC Read/Write Method](#).

This requirement is not relevant for managed Cisco Small Business 300 Series switches.

- Cisco Catalyst 2950 switches using SNMPv3
- Cisco ISR routers
- Cisco Nexus switches
- Dell - for Switch Plugin performance of Neighbor table read operations. See [IPv6 Support](#).

- Hirschmann switches
- HPE-Comware:
  - IPv4 switches
  - For Switch Plugin performance of Neighbor table read operations. See [IPv6 Support](#).
- Juniper:
  - IPv4 switches
  - Dual-stack switches, for Switch Plugin performance of Neighbor table read operations. See [IPv6 Support](#).

CLI parameters **can** be configured for the plugin to manage the following network devices:

- 3COM switches in order to apply the *Assign to VLAN* action on detected endpoints connected to a 3COM hybrid port.
- Brocade and Enterasys Matrix N-Series switches in order to apply ACL actions (*Endpoint Address ACL* and *Access Port ACL*) on detected endpoints that are connected to these switches.
- Cisco switches in order to:
  - Use the **Set port alias on action** option on the switch. See [Switch Advanced Settings](#) for details about this option.
  - Apply ACL actions (*Endpoint Address ACL* and *Access Port ACL*) on detected endpoints that are connected to these switches.
  - Apply the *Assign Security Group Tag* action on the switch.
- Comtec switches in order to:
  - Apply the *Assign to VLAN* action on detected endpoints that are connected to these switches.
  - Use the *ARP Permissions* option **Write: Clear Redundant IP Addresses associated with MAC Address**.
- DASAN switches in order to:
  - Apply the *Assign to VLAN* action on detected endpoints that are connected to these switches.
  - Use the *ARP Permissions* option **Write: Clear Redundant IP Addresses associated with MAC Address**.
- ExtremeXOS switches in order to apply the *Assign to VLAN* action on detected endpoints that are connected to these switches.
- H3C switches in order to apply the *Assign to VLAN* action on detected endpoints; endpoints that are connected to H3C switches as follows:
  - On detected endpoints located behind a VoIP device that is connected to an H3C trunk port.
  - On detected endpoints connected to an H3C access port or an H3C hybrid port.
- Huawei switches in order to apply the *Assign to VLAN* action on detected endpoints that are connected to these switches.



- When configuring the plugin to manage switches using the *Generic* vendor option.

**To add CLI information:**


1. Select **Use CLI** to activate CLI access.
  - When configuring the Switch Plugin to manage a Cisco Small Business 300 Series switch, do not select **Use CLI**. The plugin interoperates with the 300 series switch using SNMP only.
  - When configuring the Switch Plugin to manage either a Juniper switch or a Layer 3 device (a supported vendor firewall or a Linux router), **Use CLI** is permanently selected (cannot be cleared); SNMP is not available for communication between the Switch Plugin and these network devices.
  - When configuring the Switch Plugin to manage an Arista switch, **Use CLI** is permanently selected (cannot be cleared).

2. In the **Connection Type** field, select the connection type that you want to use to enable communication from the Switch Plugin to the switch.


When configuring the Switch Plugin to manage either a Juniper switch or a Layer 3 device (a supported vendor firewall or a Linux router), **SSH** is the permanently selected connection type.

3. In the **User** and **Password** fields, type a user name and a password, respectively, for plugin log in to the switch. Confirm the provided password.

For plugin management of Juniper switches, the user you configure must have *superuser* permission on the Juniper switch.

 *Do not use the root log in for CLI access to Juniper EX series switches.*

4. If you do not want to grant the plugin write privileges on the switch, clear the **Enable privileged access** option in the Privileged Access Parameters section and continue with step 6.

 *For managing Check Point-FW Layer 3 devices, never disable the **Enable privileged access** option (option is enabled by default). The enabled option instructs the plugin to interoperate in expert mode with the Check Point firewall.*

5. In the **Privileged Access Parameters** section, define privileged access credentials:
  - Select **No password** if the switch setup does not require a password.
  - Select **Use login parameters** if the user name and password entered at step 3 can also be used for privileged access.
  - Select **Custom** if privileged access requires a second user name and password pair, and type the user name and password.

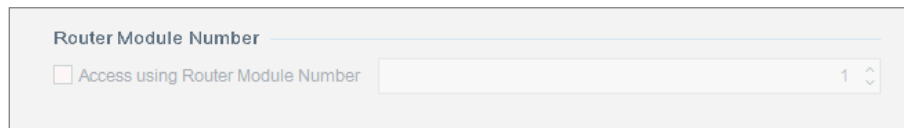
6. If SSH is the selected communication type, then, in the **SSH Fingerprint** section, the following fields are available for configuration:
  - a. Select the **Use SSH Fingerprint** option. By default, this option is not selected.

Enabling this option instructs the plugin to establish an SSH connection that is secured using an `ssh-rsa` fingerprint, for purposes of CLI communication with the managed network device.
  - b. Select either one of the following methods by which the plugin obtains the `ssh-rsa` fingerprint to use:
    - > **Learn SSH Fingerprint at every plugin start** - Selecting this option instructs the plugin to query the switch to obtain the `ssh-rsa` fingerprint, every time the plugin is started. By default, selection of **Use SSH Fingerprint** results in the selection of this option.
    - > **Use login parameters** - Select this option to define, in the input box, the `ssh-rsa` fingerprint that the Switch Plugin must use.

When using an SSH connection to establish CLI communication with a managed network device, if the Switch Plugin determines that the `ssh-rsa` fingerprint that it possesses does not meet minimum Common Criteria requirements, then the plugin does not establish the CLI connection.

7. In the **Router Module Number** section (*Enterasys only*):

When the plugin uses a CLI connection with a managed Enterasys switch, then, following plugin log in to the switch and establishment of the CLI connection, the plugin must always then enable `router` mode on the switch, either with a provided router module number or without one.



The screenshot shows a configuration panel with the title "Router Module Number". Below the title is a checkbox labeled "Access using Router Module Number". To the right of the checkbox is a text input field containing the number "1" and a small up/down arrow icon.

This section provides the **Access using Router Module Number** checkbox and associated field, which are used to instruct the plugin regarding enabling `router` mode on the switch, as follows:

- Clear the **Access using Router Module Number** checkbox to instruct the plugin to only send the `router` command, when enabling `router` mode on an Enterasys switch. By default, the **Access using Router Module Number** checkbox is not selected.
  - Select the **Access using Router Module Number** checkbox to instruct the plugin to send the `router` command together with the value defined in the associated field, when enabling `router` mode on an Enterasys switch. The field's default and minimum value is 1.
8. Select **Next**.

## SNMP Configuration

Use the SNMP page of the Add Switch wizard to specify the SNMP version and to define the SNMP credentials the plugin must use with the switch. SNMP credentials must be defined for plugin switch management, as follows:

- All vendors, except Juniper
  - When the *Generic* vendor option is configured for plugin switch management
- 📄 *SNMP configuration is not relevant for plugin management of Layer 3 devices.*

### *Plugin SNMP Use with H3C Switches*

When SNMP is used by the plugin to manage H3C switches, a switch configuration requirement might be applicable to the managed H3C switches. For details, see [Configuring H3C Switches for SNMP](#).

### *Plugin SNMP Use with Juniper Switches*

Plugin SNMP queries are not supported for Juniper switches.

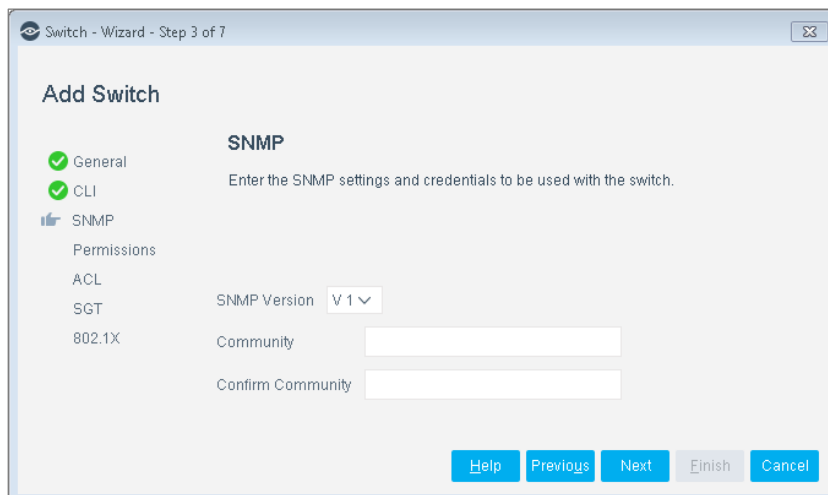
SNMP can be used for port status (link-up/link-down) traps. No configuration is required to work with SNMPv1 or SNMPv2c. For SNMPv3 traps, enter any Juniper SNMPv3 settings to be used with the switch.

## SNMPv1 and SNMPv2c Configuration

- 📄 *If you are using the switch-as-template feature (see [Use Switch Configuration as a Template](#)), it is strongly recommended that you use a different community for each switch vendor.*

### In the SNMP pane:

1. In the **SNMP Version** field, select either **V1** or **V2** from the drop-down menu.



2. In the **Community** field, enter a community relevant to your SNMP version selection.
3. Select **Next**. The Permissions pane opens.

## SNMPv3 Configuration

Switch Plugin management of a Cisco switch using SNMPv3 communication requires defining several options that are not required for earlier SNMP versions. Examples include: mib view, security group, username and password, authentication protocol and privacy protocol. If these options are not defined, plugin SNMPv3 communication with a managed Cisco switch might be affected. For more information, refer to standard SNMPv3 documentation.

### In the SNMP pane:

1. In the **SNMP Version** field, select **V3** from the drop-down menu. The following fields display:

The screenshot shows a wizard window titled "Switch - Wizard - Step 3 of 7". The main content area is titled "Add Switch" and "SNMP". It contains a list of configuration steps on the left: General (checked), CLI (checked), SNMP (selected), Permissions, ACL, SGT, and 802.1X. The main area has the following fields and options:

- SNMP Version:** A dropdown menu set to "V3".
- User:** A text input field.
- Authentication:** A section with a checked checkbox "Use Authentication" and a dropdown menu "Authentication Protocol" set to "HMAC-SHA".
- Password:** A text input field.
- Confirm Password:** A text input field.
- Privacy:** A section with a checked checkbox "Use Privacy" and a dropdown menu "Privacy Protocol" set to "DES".
- Password:** A text input field.
- Confirm Password:** A text input field.

At the bottom, there are five buttons: "Help", "Previous", "Next", "Finish", and "Cancel".

2. For plugin SNMP **V3** communication, configure the following fields:
3. In the **User** field, enter a user name.
4. Select **Use Authentication** to enable authentication.
5. If you enabled the **Use Authentication** option, you must also define:
  - a. In the **Authentication Protocol** field, select an authentication protocol for the plugin to use. The following authentication protocol options are available:
    - > HMAC-MD5
    - > HMAC-SHA
  - b. In the **Password** field, enter a password for the plugin to use

6. Select **Use Privacy** to enable privacy.
  - 📄 *Configuring the plugin to use **Privacy** requires that you also configure the plugin to use **Authentication**.*
7. If you enabled the **Use Privacy** option, you must also define:
  - a. In the **Privacy Protocol** field, select an encryption protocol for the plugin to use. The following encryption protocol options are available:
    - > DES
    - > AES-128
    - > AES-192 (*Cisco only*)
    - > AES-256 (*Cisco only*)
  - b. In the **Password** field, enter a password for the plugin to use
8. Select **Next**. The Permissions pane opens.

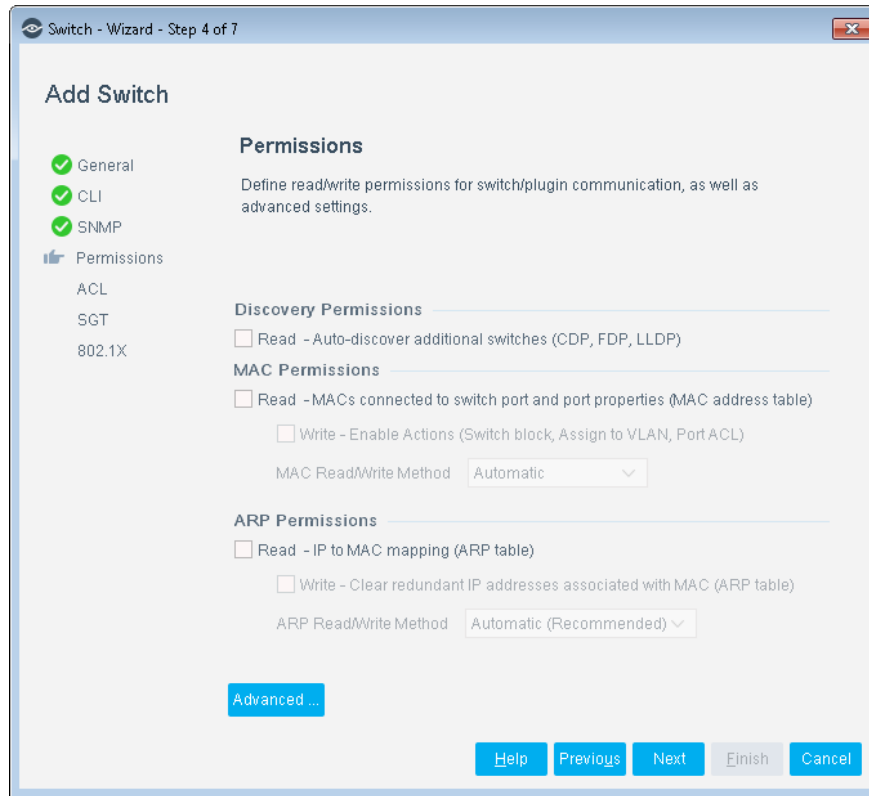
#### *Plugin SNMPv3 Use with Cisco Switches*

In order for the Switch Plugin to use SNMPv3 communication to manage Cisco switches, additional configuration is required on each of the involved Cisco switches. For example, when using VLANs with Cisco switches, a VLAN context must be defined for the desired security group. For details, see [Configuring Cisco Switches for SNMPv3](#).

## Permissions Configuration

Use the **Permissions** page of the Add Switch wizard to define read and write permissions and advanced permission settings.

For plugin management of a switch, whether by SNMP, CLI or a combination of both methods, make sure that the involved users have the necessary read and write permissions defined on the managed switch and defined for the plugin. For example, in the CLI page/tab, plugin CLI write permission requires both selection of the **Enable privileged access** option and definition of privileged access credentials.



## Discovery Permissions

*Read: Auto-discover additional switches (CDP, FDP, LLDP)*

Enable or disable the auto-discovery feature to run periodically. See [Auto-Discovery – Discover Neighboring Switches](#) for more information about how this feature works.

By default, switches run auto-discovery every 10 minutes (600 seconds). To change this setting for the current switch, select **Advanced** to open the Switch Advanced Settings dialog box and change the value of the **Auto-discover additional switches** field.

If you are configuring the plugin to manage a switch that does not support auto-discovery, this field is disabled.

## MAC Permissions

Enabling MAC read permission allows CounterACT to read a switch's MAC address table and thereby, can discover connected endpoints and their network interface. This ability supports CounterACT with applying plugin restrict actions to the relevant switch port.

*Read: MACs connected to switch port and port properties (MAC address table)*

Enable or disable the mechanism used by the plugin to query the switch for connected endpoints and port attributes. When configuring the plugin to manage a generic switch, ForeScout recommends enabling this permission option.

By default, this information is queried once every 60 seconds. To change this setting for the current switch, select **Advanced** to open the Switch Advanced Settings dialog

box and change the value of the **Read MACs connected to switch port and port properties (MAC address table)** field.

*Write: Enable Actions (Switch Block, Assign to VLAN, ACL)*

Enable or disable the Switch Plugin permission to apply the *Assign to VLAN* action, *the Switch Block* action and ACL actions on endpoints detected on the managed switch. When configuring the plugin to manage a generic switch, ForeScout recommends enabling this permission option.

See [Restrict Actions](#) for more information about Switch Plugin-provided actions.

Clearing this checkbox, while the any of these actions are currently applied on endpoints detected on the managed switch, results in the Switch Plugin releasing the affected endpoints from the applied action.

*MAC Read/Write Method*

For the plugin MAC read/write method used per network device vendor, see [Appendix 1: See and Control Capabilities Summary](#).

When configuring (add/edit) the plugin to manage a Cisco switch, the **MAC Read/Write Method** field is available for use. From the drop-down list, select the method that the plugin uses to perform the following tasks when managing a Cisco switch:

- Read:
  - The MAC Address table
  - The switch properties, for example, ports, VLANs, aliases
- Write:
  - For applying the *Assign to VLAN* action
  - For applying the *Switch Block* action

The following read/write methods are available to select:

- **Automatic**
- **SNMP (RW)**
- **SNMP (RW) and CLI**
- **SNMP (RO) and CLI**

Method	READ	WRITE	Notes
<b>Automatic</b>	<ul style="list-style-type: none"> <li>▪ SNMP</li> <li>▪ CLI (see notes)</li> </ul>	<ul style="list-style-type: none"> <li>▪ SNMP</li> </ul>	<ol style="list-style-type: none"> <li>1. Read commands are performed using SNMP with the following exceptions: <ul style="list-style-type: none"> <li>- Cisco ISR</li> <li>- Cisco IOS version 12.1 or below and the plugin is configured to use SNMPv3 to manage the switch</li> </ul> </li> <li>2. When managing these switches, the majority of read commands are performed using SNMP and a minority of read commands are performed using CLI.</li> <li>3. <i>Limitation:</i> If this method is selected, the plugin cannot apply the <i>Assign to VLAN</i> action on Cisco 2950 switches running IOS version 12.1, due to this switch model's SNMP implementation.</li> </ol>
<b>SNMP (RW)</b>	<ul style="list-style-type: none"> <li>▪ SNMP</li> </ul>	<ul style="list-style-type: none"> <li>▪ SNMP</li> </ul>	The limitation provided in method <b>Automatic</b> , note <b>3</b> , also applies to this method.
<b>SNMP (RW) and CLI</b>	<ul style="list-style-type: none"> <li>▪ SNMP</li> <li>▪ CLI</li> </ul>	<ul style="list-style-type: none"> <li>▪ SNMP</li> </ul>	<ol style="list-style-type: none"> <li>1. The majority of read commands are performed using SNMP; a minority of read commands are performed using CLI.</li> <li>4. The limitation provided in method <b>Automatic</b>, note <b>3</b>, also applies to this method.</li> </ol>
<b>SNMP (RO) and CLI</b>	<ul style="list-style-type: none"> <li>▪ CLI</li> <li>▪ SNMP</li> </ul>	<ul style="list-style-type: none"> <li>▪ CLI</li> </ul>	<ol style="list-style-type: none"> <li>1. The majority of read commands are performed using CLI; a minority of read commands are performed using SNMP.</li> <li>2. Select this method: <ul style="list-style-type: none"> <li>- For plugin management of a Cisco Nexus (recommended)</li> <li>- When CLI is the preferred method for plugin application of the <i>Assign to VLAN</i> and the <i>Switch Block</i> actions</li> </ul> </li> </ol>



- 📖 *Although a MAC Read/Write Method is not selected for plugin management of Arista switches, the plugin uses the **SNMP (RO) and CLI** method to perform reads on Arista switches.*

Selecting either the **SNMP (RW) and CLI** method or the **SNMP (RO) and CLI** method is required for any of the following:

- The **Switch Port Configurations** property to be available.
- Switch Plugin detection of VoIP port configuration on Cisco switch ports. (This requirement is not relevant for managed Cisco Small Business 300 Series switches.)

### ARP Permissions/ARP Table (IPv4) and Neighbor Table (IPv6) Permissions

When configuring the plugin to manage a Brocade, Cisco, HPE Comware, Avaya, DELL or Juniper switch, the Console displays the section title **ARP Table (IPv4) and Neighbor Table (IPv6) Permissions**. Otherwise, the Console displays the section title to be **ARP Permissions**.

#### ARP Table

In an IPv4 network device, the **ARP table** holds the association between IPv4 addresses and MAC addresses.

Enabling the **Read** option allows the plugin to read the ARP table of the managed network device. ARP table reading is used by the plugin for ARP learning - learning the IP address to MAC address mapping information of the managed network device. ARP table reading is available for all plugin-managed network devices (supported switches and supported Layer 3 devices).

- 📖 *For the plugin to query the Linux router ARP table, the configured user path on the Linux router must include the directory containing the **arp** command.*

Enabling the **Write** option allows the plugin to write to the ARP table of the managed network device. ARP table writing is used by the plugin to clear redundant IP addresses to MAC address entries from the ARP table of the managed network device. ARP table writing is available for most plugin-managed network devices, as follows:

- Available for all supported switches, except HPE-Comware
- Not available for all supported Layer 3 devices, except Juniper SRX firewall

#### Neighbor Table

In an IPv6 network device (both IPv6-only and dual-stack network devices), the **Neighbor table** holds the association between IPv6 addresses and MAC addresses. Dual-stack switches maintain both an ARP table and a Neighbor table. The Switch Plugin performs only read operations on a Neighbor table.

#### *Read: IP to MAC Mapping*

The Switch Plugin performs read operations on both ARP and Neighbor tables.

If you select **Read: IP to MAC Mapping**, the Switch Plugin discovers:

- Each connected endpoint that the managed switch adds to its ARP table

- For Brocade/Foundry and Cisco dual-stack switches, each connected IPv6 endpoint that the managed switch adds to its Neighbor table. See [IPv6 Support](#).

Select this option if you are working in an environment where endpoints can only be learned via the Switch Plugin (for example, CounterACT channels have not been defined). Also, when configuring the plugin to manage a generic switch, ForeScout recommends enabling this permission option.

By default, the Switch Plugin queries the ARP table every 10 minutes (600 seconds). To change this setting for the current switch, select **Advanced** to open the Switch Advanced Settings dialog box and change the value of the **Read IP to MAC Mapping** field.

When CLI is the method selected to read the ARP table of a managed Cisco or Enterasys switch, the plugin learns additional ARP table information, specifically, the age of ARP table entries. With this information, the plugin can ignore redundant IP addresses associated with the same MAC address.

For the plugin read method used per network device vendor, see the *ARP Table (IPv4) Neighbor Table (IPv6)* column in [Appendix 1: See and Control Capabilities Summary](#).

#### *ARP Read Method*

The **ARP Read Method** field only displays for Enterasys switches.

When configuring (add/edit) the plugin to manage an Enterasys switch, the **ARP Read Method** drop-down list is presented. Use this drop-down list to define the method that the plugin uses to read the ARP table of the Enterasys switch.

When the **Read: IP to MAC Mapping** checkbox is selected, then the **ARP Read Method** drop-down list is available for use.

The screenshot shows a dialog box titled "ARP Permissions". It contains two unchecked checkboxes: "Read - IP to MAC mapping (ARP table)" and "Write - Clear redundant IP addresses associated with MAC (ARP table)". Below the checkboxes is a label "ARP Read/Write Method" followed by a dropdown menu currently showing "Automatic (Recommended)". At the bottom left of the dialog is a blue button labeled "Advanced ...".

The following methods are available to select for plugin read of a managed Enterasys switch ARP table:

- **SNMP** - the default selection. Instructs the plugin to use SNMP to query the switch ARP table.
- **CLI** - instructs the plugin to use CLI commands to query the switch ARP table.

#### *Write: Clear Redundant IP Addresses associated with MAC Address*

The Switch Plugin only performs write operations on ARP tables.

The IP address of an endpoint can change (for example, if the endpoint is moved from one VLAN to another). When an endpoint IP address changes, the old IP

address is still associated with the endpoint MAC address in the ARP table, and the Switch Plugin may then learn the old IP address of the endpoint.

Selecting the **Write: Clear Redundant IP Addresses associated with MAC Address** option instructs the plugin to periodically delete redundant IP addresses from the ARP table, which is then followed by a plugin read of the ARP table to discover the current IP address associated with the MAC. This operation is also referred to as *refresh ARP table*.

Clearing redundant IP addresses from a managed switch ARP table occurs, following any of these events:

- A plugin ARP table query, triggered by the **Read: IP to MAC Mapping** option, that results in the discovery of more than one IP address for the same MAC address
- When the plugin knows that an IP address has become redundant, for example:
  - After applying the *Assign to VLAN* action, the *Endpoint Address ACL* action defined with the *MAC ACL* parameter or the *Switch Block* action
  - Upon a detected endpoint being deleted from CounterACT

The plugin uses either SNMP commands or CLI commands to clear redundant IP addresses from the ARP table of a managed switch. For the plugin write method used per network device vendor, see the *ARP Table (IPv4) Neighbor Table (IPv6)* column in [Appendix 1: See and Control Capabilities Summary](#).

- 📖 *With a managed Juniper switch, the plugin CLI clear the ARP table command is always followed by the plugin CLI commit command.*

#### *Read/Write Method*

The **Read/Write Method** field only displays for Cisco switches.

When configuring (add/edit) the plugin to manage a Cisco switch and the **Read: IP to MAC Mapping** option is selected, then the **Read/Write Method** field is available for use.

- For the ARP table, the plugin uses the selected method to perform both read and write operations on this table.
- For the Neighbor table, the plugin uses the selected method to perform read operations on this table.

Methods available for plugin to perform its read/write operations on the relevant table of a managed Cisco switch:

- Selecting **Automatic (Recommended)**, the drop-down list default selection, instructs the plugin to perform its operations on the relevant switch table via CLI, when **Use CLI** is selected in the [CLI page](#). Otherwise, the plugin uses SNMP to query the table. When configuring the Switch Plugin to manage a Cisco Small Business 300 Series switch, selecting the **Automatic (Recommended)** option is the same as selecting the **SNMP** option.
- **SNMP** - instructs the plugin to use SNMP to perform its operations on the relevant switch table.

- **CLI** - instructs the plugin to use CLI commands to perform its operations on the relevant switch table.

### Switch Advanced Settings

Selecting **Advanced** in the Permissions page opens the **Switch Advanced Settings** window. This window provides the advanced settings for plugin management of a switch that are available to configure.

**Switch Advanced Settings**

**Performance tuning**

Auto-discover additional switches every  seconds

Read MACs connected to switch port and port properties (MAC address table) every  seconds

Read IP to MAC Mapping every  seconds

Read IP to MAC mapping protection between subsequent queries  seconds

When SNMP is used to read IP to MAC mapping, refresh reported entries every  seconds

**Settings**

SNMP parameters

SSH parameters

Ignore actions on port names:

Ignore actions on port aliases:

Don't learn on port name:

In the above port-related fields, provide regular expressions and/or plain text separated by the semicolon (;).  
For plain text, prefix each special character with the backslash (\).  
For example, aa.\*;bb.\*;ifc4 \(\Slot 1 Port 4\)

Detect endpoints connected to trunk ports

Maximum connected endpoints per port

Set port alias on action

**IP to MAC mapping**

Read - IP to MAC mapping (ARP table) for VRFs

Connectivity Groups

Allow IP Discovery from Connectivity Group

**Default VLAN**

Default VLAN ID/Name

Only assign vacant ports to default VLAN

**Configuration Flags**

Configuration flags

**NAT Layer 3 Translation**

ARP translation ...

The available settings are vendor specific and are based on the **Vendor** field selection that was made in the General page. Not all of the settings (fields and options) described in this section are available for use with every supported vendor, whether switch vendor or Layer 3 device vendor. The advanced settings for plugin management of a switch are as follows:

- [Auto-discover additional switches](#)
- [Read MACs connected to switch port and port properties](#)
- [Read IP to MAC Mapping](#)
- [Read IP to MAC mapping protection between subsequent queries](#)
- [When SNMP is used to read IP to MAC mapping, refresh reported entries](#)
- [ARP Table OID](#)
- [SNMP parameters](#)
- [SSH parameters](#)
- [Ignore actions on port names](#)
- [Ignore actions on port aliases](#)
- [Don't learn on port name](#)
- [Detect endpoints connected to trunk ports](#)
- [Maximum connected endpoints per port](#)
- [Set port alias on action](#)
- [Read – IP to MAC mapping \(ARP table\) for VRFs](#)
- [Connectivity Groups](#)
- [Allow IP Discovery from Connectivity Group](#)
- [Assign to VLAN by configuration group assignment](#)
- [Default VLAN ID/Name](#)
- [Only assign vacant ports to default VLAN](#)
- [Configuration flags](#)
- [ARP Translation](#)

### Performance Tuning

Use this section to update discovery frequencies.

#### *Auto-discover additional switches*

For a description of this performance tuning setting, see the [Discovery Permissions](#) section. Since the plugin does not support the auto-discovery feature for generic switches and Linux routers, therefore, this setting cannot be configured for plugin management of either a generic switch or a Linux router.

#### *Read MACs connected to switch port and port properties*

For a description of this performance tuning setting, see the [MAC Permissions](#) section. Since Linux routers do not have a MAC address table, therefore, this setting cannot be configured for plugin management of a Linux router.

### *Read IP to MAC Mapping*

For a description of this performance tuning setting, see the [ARP Permissions/ARP Table \(IPv4\) and Neighbor Table \(IPv6\) Permissions](#) section.

### *Read IP to MAC mapping protection between subsequent queries*

This performance tuning setting defines the minimum period, in seconds, that the Switch Plugin must always wait between subsequent ARP table queries of the network device. More specifically, this setting defines the minimum wait time between when the previous query ended and the new query is begun. The setting default is 30 seconds.

### *When SNMP is used to read IP to MAC mapping, refresh reported entries*

This performance tuning setting defines how frequently the Switch Plugin must refresh the CounterACT device with the ARP table information of a previously known table entry. The ARP table of an L3-enabled network device records the association between IP address and MAC address of an endpoint connected to the device.

### *ARP Table OID*

This setting is only displayed when configuring the plugin to manage a generic switch and is required to be configured. For purposes of SNMP communication with the switch, select the OID where the ARP table is found in the switch MIB.

## Settings

### *SNMP parameters*

Use this option to control the timeout and retry number for SNMP requests sent to the switch. You may need to do this to handle SNMP timeout problems. These problems may occur if the network or switch is extremely busy.

- **Timeout** – how long (in seconds) that the Switch Plugin waits for a response from the SNMP agent on the switch. The default timeout is 25 seconds.
- **Retry** – number of times to retry sending an SNMP message to the endpoint. The default number of retries is 2. The maximum number of retries is 20.

For example, to indicate a timeout of 30 seconds and a maximum of three retries, enter the following in the field:

```
-t 30 -r 3
```

### *SSH parameters*

The **SSH Parameters** field only appears for switch vendors that support CLI communication with the plugin. Use of this field is relevant when the plugin is configured to manage the switch using CLI via an SSH connection.

Provide any SSH parameters that you want included in the SSH client command line that the plugin executes when logging in to and establishing CLI communication with a managed switch. The plugin concatenates the text provided in the **SSH Parameters** field to the end of its SSH client command line.

For example, providing the parameter `-o PubkeyAuthentication=no` in the **SSH Parameters** field, results in the following SSH client command line for use with a managed Cisco switch:

```
ssh <IP address> -l networking -o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null -o NoHostAuthenticationForLocalhost=yes
-o PubkeyAuthentication=no
```

#### *Ignore actions on port names*

Enter a comma-separated list of port names or numbers that are ignored when applying the *Switch Block*, *the Assign to VLAN* and the ACL actions and the Pre-Connect ACL. Regular expressions are valid for use in this field.

Currently blocked endpoints, when connected to ports that you define in this field, are released (no longer blocked).

#### *Ignore actions on port aliases*

Enter a string in this field; ports on the switch whose alias field contains the specified string are ignored when applying the *Switch Block*, *the Assign to VLAN* and the ACL actions and the Pre-Connect ACL. Regular expressions are valid for use in this field.

Currently blocked endpoints when connected to ports that you define in this field, are released (no longer blocked).

#### *Don't learn on port name*

Enter port names or numbers at which endpoint learning should not take place. Enter a comma between each port name. Regular expressions are valid for use in this field.

#### *Detect endpoints connected to trunk ports*

Enable this option to instruct the plugin to detect endpoints that are connected to the trunk ports of a managed switch. The plugin resolves and displays in the Console the switch properties of these connected endpoints, including the VLAN-related properties of **Switch Port VLAN**, **Switch Port VLAN Name** and **Switch Port VLAN Change**.

 *With managed 3com, Extreme, Force10 and Huawei switches, the plugin does not resolve these VLAN-related properties for trunk port-connected endpoints.*

See [General Considerations for Action Use](#) about the *Assign to VLAN* action and trunk port-connected endpoints.

Use of this option requires that you provide, in the **Don't learn on port name** field of this window, the uplink port names of the managed switch. Doing so, instructs the plugin to ignore learn events for the uplink ports provided in the field.

If needed for use of this option, modify the **Maximum connected endpoints per port** field to increase its value to allow plugin detection of multiple endpoints concurrently connected to the same switch port. The field's default value is 10 (endpoints). The field's updated value must reflect the maximum number of endpoints that can be concurrently connected to the same port.

#### *Maximum connected endpoints per port*

Configure the value of the **Maximum connected endpoints per port** field to define the maximum number of endpoints that can be concurrently connected to the same port. The Switch Plugin uses this limiting value when evaluating the ports of a

managed switch. Any port, regardless of its port type, that is identified by the plugin to exceed the defined limit is ignored by the plugin. The field's default value is 10.

#### *Set port alias on action*

The **Set port alias on action** field only displays for Cisco switches.

Use of this option requires:

- **Use CLI** enabled in the [CLI page](#).
- Selection of the **Enable privileged access** option in the **Privileged Access Parameters** section of the [CLI page](#).
- **Write - Enable Actions (Switch Block, Assign to VLAN, ACL)** enabled, in the [MAC Permissions](#) section of the Permissions page.
- Configuration of the managed switch to allow privileged command-line access from the CounterACT device. See [Configuring Switches for ACL Integration](#) for the switch configuration procedure.

Specify whether information about the latest switch action performed on the port is prepended to the port alias field on the switch. This information can be retrieved by users responsible for the switch who do not have access to the CounterACT Console.

If no previous action of this type has been performed on the port, the information is prepended to the existing switch alias text. If a previous action of the same type was performed, the information about the current action overwrites the information about the previous action of the same type but leaves the remainder of the existing text intact.

The information added to the port alias text is formatted as follows:

- *Assign to VLAN* action:  
 \_\_\_\_CA:<Appliance\_IP\_address>:<timestamp>:V:<previous\_VLAN\_ID>-<new\_VLAN\_ID>:act:NAC\_\_\_\_
- ACL actions:  
 \_\_\_\_CA:<Appliance\_IP\_address>:<timestamp>:A:<ACL\_name>:act:NAC\_\_\_\_
- *Switch Block* action:  
 \_\_\_\_CA:<Appliance\_IP\_address>:<timestamp>:B:act:NAC\_\_\_\_
- Assign port to the default VLAN:  
 \_\_\_\_CA:<Appliance\_IP\_address>:<timestamp>:V:<previous\_VLAN\_ID>-<default\_VLAN\_ID>:DEF:NAC\_\_\_\_
- Pre-Connect ACL:  
 \_\_\_\_CA:<Appliance\_IP\_address>:<timestamp>:AD:<Default\_ACL\_name>:DEF:NA  
 C\_\_\_\_

Where <timestamp> has the format **mm:dd:hh:mm:ss**.



## IP to MAC Mapping

*Read – IP to MAC mapping (ARP table) for VRFs*

The **Read - IP to MAC mapping (ARP table) for VRFs** checkbox is displayed for the following Layer 3 switches that implement VRF:

- Alcatel
- Arista
- Avaya (Nortel)
- HPE running a Comware operating system
- Cisco

For these Layer 3 switches that implement VRF, specify whether the plugin is to read the IP to MAC mapping from each VRF ARP table, in addition to reading the mapping from the ARP table.

To enable the **Read - IP to MAC mapping (ARP table) for VRFs** option, make sure that the following options are also configured:

- In the CLI page, **Use CLI** is selected.
- In the ARP Permissions section of the Permissions page, **Read: IP to MAC Mapping** is selected.
- (*Cisco only*) In the ARP Permissions/ARP Table (IPv4) and Neighbor Table (IPv6) Permissions section of the Permissions page, the **Read/Write Method** selected is either **Automatic** or **CLI**.

### *Connectivity Groups*

Enter *Connectivity Group* name(s). A Connectivity Group defines a group of **adjacent** network devices (any combination of L2 devices, L3-enabled devices and L2/L3-enabled devices). A network device can be assigned to any number of Connectivity Groups. Multiple group names must be comma-separated.

The Switch Plugin uses a Connectivity Group's L3-enabled network devices that are configured to *Allow IP Discovery from Connectivity Group*, when carrying out the *Expedite IP Discovery* action. For information about this action, see [Expedite IP Discovery](#).

### *Allow IP Discovery from Connectivity Group*

Select this option when configuring an L3-enabled network device. This option lets the Switch Plugin query the L3-enabled device for ARP table data in support of other devices assigned to the same [Connectivity Group](#), when carrying out the *Expedite IP Discovery* action. For information about this action, see [Expedite IP Discovery](#).

## Configuration Group

*Assign to VLAN by configuration group assignment*

The **Assign to VLAN by configuration group assignment** checkbox only displays for Juniper switches.

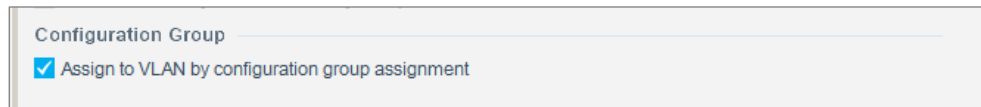
For Juniper EX switches, when working in environments with configuration groups, the plugin can assign a switch port to a configuration group, instead of assigning it to

a VLAN. This capability enables CounterACT users to configure multiple groups on a switch, for example:

- a Guest\_Group
- a Corporate\_Group

In the switch, each defined configuration group must include VLAN. The Switch Plugin moves ports between VLANs by moving ports between configuration groups.

Select the **Assign to VLAN by configuration group assignment** checkbox to enable use of the action.



To specify the configuration group to which endpoints are assigned, see [Assign to VLAN](#), [Switch-Specific Considerations for Action Use](#).

### Default VLAN

Since the plugin does not support the Default VLAN feature for generic switches and Linux routers, therefore, all settings provided in this section cannot be configured for plugin management of either a generic switch or a Linux router.

#### *Default VLAN ID/Name*

To assign ports to a default VLAN, select **Default VLAN ID/Name** and type the ID or name of the VLAN in the text box.

- 📄 **Default VLAN ID/Name** is enabled only if **Write: Enable Actions (Switch Block, Assign to VLAN, ACL)** is selected in the **MAC Permissions** section of the **Permissions** page.

All ports on managed switches are assigned to the default VLAN, except:

- Trunk ports.
- CDP, FDP and LLDP ports.
- Ports that have more than a specified number of endpoints connected to the port. (This value is set in the **Maximum assigned users per port to default VLAN** field in the Edit general parameters dialog box. See [Maximum assigned users per port to default VLAN](#) for details.)
- Ports that have been assigned to a VLAN using the *Assign to VLAN* action.
- Switch ports that have been blocked by the *Switch Block* action.
- Ports that are excluded from actions by the *Ignore actions on port names* and *Ignore actions on port aliases* configurations. See [Switch Advanced Settings](#) for information about these configurations.

For additional control, you can modify:

- The maximum number of endpoints per port for the port to be assigned to the default VLAN. See [Maximum assigned users per port to default VLAN](#) for details.

- The time period to wait until the Switch Plugin tries to reassign a port to the default VLAN (if the assignment failed due to the number of endpoints connected to the port). See [Time period to halt assignments to default VLAN \(hours\)](#) for details.

#### *Only assign vacant ports to default VLAN*

To only assign vacant ports to the default VLAN, select **Default VLAN ID/Name** and then select **Only assign vacant ports to default VLAN**. Vacant ports include VoIP ports. This is useful if your policy dictates that an end-point must be inspected for compliance before it gets into a production VLAN (a *pre-connect* inspection). For example, in a conference room where it is likely that guest endpoints will frequently connect and reconnect, you can set up a guest VLAN, and set the *Vacant Port* assignment to that VLAN. A port is considered vacant if its operational status (link state) is down for more than 3.5 minutes.

### Configuration Flags

#### *Configuration flags*

To enable *per-switch* advanced configuration features, type the relevant flag in this field.

- To enable a feature, type `<property_name>:<value>` in the field.
- To restore the feature to its *default* value, delete the string.
- Strings for different advanced features must be separated by a comma.
- Per-switch configuration of a flag always takes precedence over the global configuration of that flag.

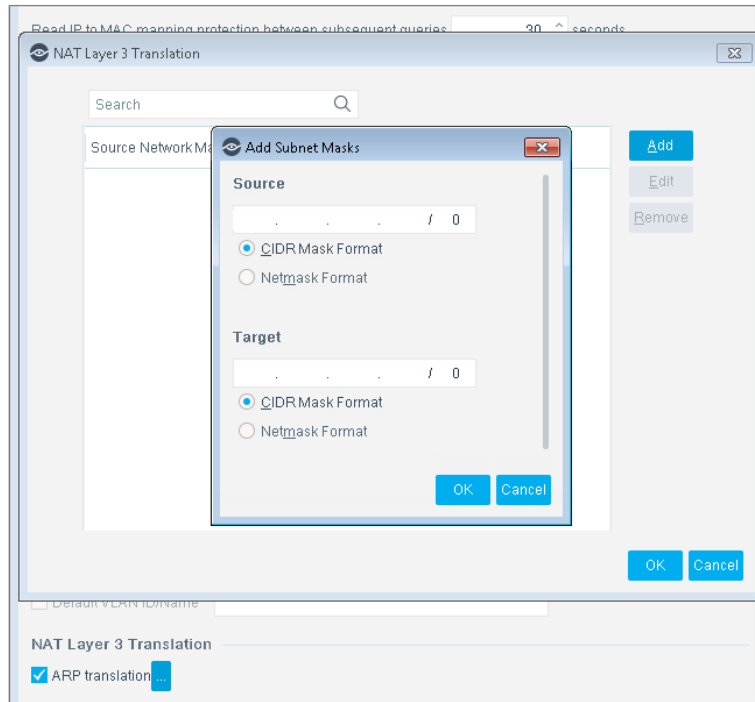
Supported configuration flags are listed and explained in [Appendix 2: Troubleshooting, Workarounds and Feature Functionality Support](#).

See also [Advanced configuration flags](#) for *global* advanced configuration features.


### NAT Layer 3 Translation

#### *ARP Translation*

Detect and control IPv4 endpoints, including *dual-stack endpoints*, that are behind NAT devices located on layer 3 switches. Include these endpoints as part of your managed network. Using the **ARP Translation** option, translate endpoint IPv4 addresses learned by remote switches into local addresses that can be used as part of the internal network range.



**To configure NAT layer 3 translation, do the following:**

1. In the **NAT Layer 3 Translation** section, select the **ARP translation** checkbox and then select the accompanying button . The NAT Layer 3 Translation window opens.
2. In the window, select **Add**. The Add Subnet Masks dialog opens.
3. In the **Source** section, do the following:
  - a. Select the address format to use. By default, The **CIDR Mask Format** option is selected.
  - b. In the associated field, specify a source IPv4 address range from the remote switch ARP table.
4. In the **Target** section, do the following:
  - a. Select the address format to use. By default, The **CIDR Mask Format** option is selected.
  - b. In the associated field, specify a target IPv4 address range from your internal network.

## ACL Configuration – Cisco and Brocade Switches

In the ACL page of the Add Switch wizard, define the Switch Plugin ACL configuration for interoperability with either managed Cisco or managed Brocade switches. The available options are described in the following sections.

- 📄 When configuring the Switch Plugin to manage a Cisco Small Business 300 Series switch, **Use CLI** must be disabled in the CLI page, resulting in the ACL page being disabled for configuration. The plugin does not support applying ACL actions on the Cisco Small Business 300 series switch, since ACL support requires plugin-switch CLI interoperation and the plugin interoperates with the 300 series switch using SNMP only.

For plugin IPv6 support exceptions with ACL-related functionality, see [IPv6 Support](#).

For details about the Switch Plugin ACL capabilities, see [Appendix 6: Working with ACL Capabilities](#).

The screenshot shows the 'Switch - Wizard - Step 5 of 7' configuration window. The title bar indicates the current step. The main content area is titled 'Add Switch' and is divided into several sections:

- General:** Includes 'General', 'CLI', 'SNMP', and 'Permissions' sections, all of which are marked with a green checkmark.
- ACL:** This section is currently selected in the sidebar. It contains:
  - Enable ACL:** A checkbox that is currently unchecked.
  - Block hosts learned via downstream devices:** A checkbox that is unchecked.
  - Add ACL access group to physical ports:** A checkbox that is checked.
  - Keep ACL access group on ports after action canceled:** A checkbox that is unchecked.
  - IP ACL:** A section with:
    - Add CounterACT authentication servers permit rules:** A checked checkbox.
    - Use system-defined name (forescout\_acl):** A selected radio button.
    - Define custom name:** An unselected radio button with an adjacent text input field.
    - Enable basic ACL on action failure:** An unchecked checkbox.
  - Specify basic ACL rules:** A large empty text area.
  - If rule numbering is not supported:** A section with:
    - Use ACL without rule numbering:** A selected radio button.
    - Use basic ACL settings on action failure:** An unselected radio button.
  - MAC ACL:** A section with:
    - Enable MAC ACL:** An unchecked checkbox.
    - MAC ACL Name:** A text input field.
  - Pre-Connect Mode:** A section with:
    - Enable Pre-Connect Mode:** An unchecked checkbox.
    - Select from ACL Repository:** A dropdown menu labeled 'Select ACL...'.
    - Select an option:** A section with:
      - Link-Up ACL:** A selected radio button.

At the bottom of the window, there are five buttons: 'Help', 'Previous', 'Next', 'Finish', and 'Cancel'.

### Enable ACL

Enable or disable ACL configuration defined on this page. This option must be enabled to use either the *Access Port ACL* action or the *Endpoint Address ACL* action

(IP address-based ACL or MAC addressed-based ACL). For the *Access Port ACL* action, this is the only option to enable in the page.

#### *Block hosts learned via downstream devices*

This option is used with the *Endpoint Address ACL* action.

Enable or disable the blocking of endpoints on the access port or, if not found on the access port, on a trunk port. Enabling this option allows the Switch Plugin to apply the ACL to detected endpoints that reside on a downstream switch device that, for example, does not support ACL use. By default, this option is disabled.

#### *Add ACL access group to physical ports*

This option is used with the *Endpoint Address ACL* action.

By default, this option is enabled. When enabled, the Switch Plugin adds the relevant ACL rules to the switch *access list* and applies the ACL on endpoint-connected switch ports (*access group* is the ACL on a switch port).

When this option is disabled, the Switch Plugin only adds the relevant ACL rules to the switch *access list*; the plugin does not also apply the ACL on endpoint-connected switch ports (*access group* is the ACL on a switch port). In this case, the CounterACT user must then manually add the ACL to the appropriate switch port(s).

#### *Keep ACL access group on ports after action canceled*

This option is used with the *Endpoint Address ACL* action.

When this option is enabled, the Switch Plugin leaves an ACL, which was previously applied by an *Endpoint Address ACL* action, on its port after the action is cancelled for an endpoint (whether manually or by a policy). The ACL (access group) remains on the port until either the plugin is stopped or Switch Plugin garbage collection occurs. The plugin does not remove the relevant ACL rules from the switch *access list*. By default, this option is disabled.

Operating in this manner, the plugin reduces the amount of CLI configuration changes in the switch that, in turn, yields a reduction in both CPU and memory usage of the switch.

## **IP ACL**

This section defines the parameters used to support IP address blocking of detected endpoints, applied using the *Endpoint Address ACL* action.

#### *Add CounterACT authentication servers permit rules*

Selecting this option adds rules to the ACL that permit communication between detected endpoints and CounterACT authentication servers. When the applied action, which adds these rules, is later cancelled, these CounterACT authentication server permit rules are still maintained on the switch, due to performance considerations. Only stopping the plugin or performing a Clear CounterACT ACLs removes added CounterACT authentication server permit rules from the managed switch.

Do not clear this checkbox (this option is enabled by default). If you clear the checkbox, CounterACT may not have access to the blocked endpoints and configured authentication servers.

*Use system-defined name / Define custom name*

Select between the following ACL naming options for the ACL (type IP ACL) that the plugin applies using the *Endpoint Address ACL* action:

- Use the system-defined ACL name, **forescout\_acl**. This option is the default selection.
- Define a custom ACL name in the associated field.

*Enable basic ACL on action failure*

Select this checkbox to address any of the following managed switch scenarios:

- If the switch does not support ACL TCP flags (in which case plugin application of the *Endpoint Address ACL* action fails), following the action's failure, you can still have the Switch Plugin instruct the managed switch to block endpoint traffic by defining ACL rules in the **Specify basic ACL rules** box.
  - 📖 *When this option is enabled, then the Switch Plugin (a) does not add default rules and (b) ignores the **Add CounterACT authentication servers permit rules** option, if enabled.*
  - 📖 *When defining the *Endpoint Address ACL* action, the action option **Use Basic ACL on action failure** must be selected.*
- If the switch does not support ACL rule numbering (*ACL rule sequence numbers*), you can still have the Switch Plugin instruct the managed switch to block endpoint traffic by defining ACL rules in the **Specify basic ACL rules** box. Also, see [If rule numbering is not supported](#).

*Specify basic ACL rules*

This box is available for data entry, only when the **Enable basic ACL on action failure** option is selected. In the box, enter basic ACL rules to be used if your Switch does not support comprehensive ACL blocking. See [IP Address Blocking Capability](#) for details. Enter rules based on your switch requirements.

Examples of basic ACL rules:

ACL Rule	Description
<b>Deny ip host HOST_IP any</b>	Block all IP traffic <i>from</i> the detected endpoint. When using this type of rule: <ul style="list-style-type: none"> <li>▪ Sessions <i>to</i> the endpoint will not be initiated because the endpoint will not return a <b>SYN-ACK</b> message.</li> <li>▪ UDP traffic will not be transmitted from the endpoint.</li> </ul>
<b>Deny tcp host HOST_IP any</b>	Block all TCP traffic <i>from</i> the detected endpoint. When using this rule, session to the endpoint will not be initiated because the endpoint will not return a <b>SYN-ACK</b> message.
<b>Deny tcp host HOST_IP any eq 80</b>	Block HTTP access <i>from</i> the detected endpoint. In this case one can block access to more than one port, but it must be in the same direction.

ACL Rule	Description
<b>Deny tcp host HOST_IP any eq 23</b>	Block Telnet access <i>from</i> the detected endpoint. In this case one can block access to more than one port, but it must be in the same direction.
<b>Deny tcp host HOST_IP eq 3389 any</b>	Block RDP (Remote Desktop Application) access <i>to</i> the detected endpoint. In this case one can block access to more than one port, but it must be in the same direction.

### If rule numbering is not supported

The Switch Plugin provides the following IP ACL configuration options, should a managed switch *not* support the use of *ACL rule sequence numbers* (ACL rule numbering):

- **Use the ACL without rule numbering** - Every addition or cancellation of ACL rule(s) requires the switch to re-write its entire ACL list, due to it not using ACL rule sequence numbers. Switch re-write of its ACL list can affect the CPU utilization (high), depending upon re-write frequency and ACL list size.
- **Use basic ACL settings on action failure** - selecting this option instructs the plugin to add to the ACL list on the switch, the ACL rule(s) defined in the **Specify basic ACL rules** box, whenever the plugin fails to apply the *Endpoint Address ACL* action.

When this option is selected, the following ACL pane/tab configuration for the managed switch is also required:

- The **Enable basic ACL on action failure** option must also be selected.
- In the **Specify basic ACL rules** box, a minimum of one ACL rule must be defined.

📖 *When defining the Endpoint Address ACL action, the action option **Use Basic ACL on action failure** option must be selected.*

### MAC ACL

The **MAC ACL** section displays for Cisco switches only. MAC ACL capability is only available for use on managed Cisco switches.

This section defines the parameters used to support MAC address blocking of detected endpoints, applied using the *Endpoint Address ACL* action. When a MAC ACL is applied, the switch blocks all traffic sent from the affected, endpoint MAC address. The **MAC ACL** section is displayed for Cisco switches only.

#### Enable MAC ACL

Enable or disable working with the MAC ACL on this switch. MAC ACL blocking enables blocking of endpoints based on their MAC address. Traffic from the endpoint to the switch is blocked.

In the textbox, type the name of the ACL as it appears in the switch. MAC ACL blocking is not supported when the endpoint's switch port is defined with both an IP and MAC ACL or if you are working with a Cisco 2950 switch that is limited to



Standard Image (SI) support. Make sure that the MAC ACL name is different from the IP ACL name, if you are using both features.

### Pre-Connect Mode

The Pre-Connect Mode capability is only available for use on managed Cisco switches and, hence, the **Pre-Connect Mode** section only displays when configuring Cisco switches.

In the **Pre-Connect Mode** section, the CounterACT user can select an ACL from the Switch Plugin ACL Repository for the plugin to apply as the Pre-Connect ACL on **qualified** switch **access ports** on a managed Cisco switch.

Pre-Connect Mode value:

- Extends CounterACT enforcement by applying **immediate** ACL control to switch access ports without having to first wait for policy evaluation and plugin application of an ACL action [*Access Port ACL, Endpoint Address ACL*].
- Provides flexible use of the capability based on CounterACT Console configuration options, as follows:
  - Only apply the Pre-Connect ACL to occupied access ports (**Fail-Open**)
  - Apply the Pre-Connect ACL to both occupied access ports and vacant switch ports (**Fail-Close**)
  - Override all non-CounterACT ACLs applied to access ports by applying the Pre-Connect ACL
  - Never apply the Pre-Connect ACL to access ports having a currently applied non-CounterACT ACL
  - Exclude ports from Pre-Connect ACL application by use of the **Ignore actions on port** options. See [Switch Advanced Settings](#) for information about these options.

An applied Pre-Connect ACL remains in effect on all the relevant access ports of the switch until one of the following events occurs:

- The plugin applies an ACL action, either an *Access Port ACL* action or an *Endpoint Address ACL* action, on affected port(s). The applied Pre-Connect ACL is removed from the affected port(s).
- All connected endpoints disconnect from a port on which the Pre-Connect ACL is applied and the **Link-Up ACL** option is enabled. The applied Pre-Connect ACL is removed from the affected port(s).
- The Switch Plugin is stopped. The applied Pre-Connect ACL is removed from the managed switch.

The Pre-Connect Mode capability is only available for access ports of managed Cisco switches that meet the following criteria:

- The access port is not excluded from actions by the **Ignore actions on port names** and **Ignore actions on port aliases** options. See [Switch Advanced Settings](#) for information about these options.
- The access port **does not have a plugin ACL action** [*Access Port ACL, Endpoint Address ACL*] **currently applied** to it.

If the Switch Plugin fails to apply the Pre-Connect ACL on a managed switch, a Switch Alert message displays in the Switch tab about the failure to apply the ACL on the switch. Pre-Connect ACL application fails for any of the following reasons:

- Plugin fails to write the Pre-Connect ACL rules on the switch
- Plugin succeeds to write the Pre-Connect ACL rules on the switch but fails to link the ACL to the access ports of the switch

To prohibit plugin application of the Pre-Connect ACL on switch access ports where CDP is in use, see [Allow Pre-Connect ACL on switch CDP ports](#).

The **Set port alias on action** option can be enabled for use with the Switch Plugin application of the Pre-Connect ACL to an access port of a managed switch. See [Switch Advanced Settings](#) for information about this option.

Use of Pre-Connect Mode involves configuring the following settings:

#### *Enable Pre-Connect Mode*

Select this option to enable use of the Pre-Connect Mode for the managed switch. This option requires the following options to be enabled:

- In the ACL pane, both of the following options are selected:
  - The **Enable ACL** option
  - The **Add ACL access group to physical ports** option
- In the Permissions pane, the MAC Permission options of **Read** and **Write** are selected.

Clearing the **Enable Pre-Connect Mode** option disables use of the Pre-Connect Mode for the managed switch.

#### *Select from ACL Repository*

Select an ACL from the ACL Repository for the plugin to provision as the Pre-Connect ACL for the managed switch.

For the dropdown list to contain entries, ACLs must exist in the ACL Repository. For information about working with the ACL Repository, see [The ACL Repository](#).

#### *Link-Up ACL*

Enable the **Link-Up ACL** option to instruct the plugin to only apply the Pre-Connect ACL to switch access ports having a minimum of one connected endpoint (**Fail-Open**). This Pre-Connect Mode option is selected by default.

- When **Link-Up ACL** is selected, then after a switch access port has no connected endpoints, the plugin keeps the Pre-Connect ACL applied to the port for an additional period that is, by default, 120 seconds. When this additional period expires, the plugin removes the Pre-Connect ACL from the switch port. To modify this period, see both the switch-specific option [Override global setting: Delay release of Pre-Connect ACL \(seconds\)](#) and the global option [Delay release of Pre-Connect ACL \(seconds\)](#).

#### *Default ACL*

Enable the **Default ACL** option to instruct the plugin to apply the Pre-Connect ACL to switch access ports, regardless of whether these ports have a connected endpoint or have no connected endpoint (**Fail-Close**).

- When **Default ACL** is selected, then after a switch access port has no connected endpoints (port is vacant), the plugin keeps the Pre-Connect ACL applied to the port. The plugin only removes the Pre-Connect ACL from the vacant switch port, if one of the following conditions are true:
  - An endpoint next connects (port is again occupied) and the plugin applies an ACL action to this endpoint.
  - The Switch Plugin is stopped.

#### *Override all ACLs existing on port*

Enable this option to instruct the plugin to override any non-CounterACT ACL currently applied to switch access ports and, instead, apply the Pre-Connect ACL to these switch access ports. This option is available for use with both the **Link-Up ACL** and the **Default ACL** options.

Clear the selected option to instruct the plugin not to apply the Pre-Connect ACL to switch access ports, whenever a non-CounterACT ACL is currently applied to these switch access ports.

#### *Override global setting: Delay release of Pre-Connect ACL (seconds)*

Enabling this option keeps the Pre-Connect ACL of the managed Cisco switch applied to an applicable switch access port for an additional period of time, as of the access port having no connected endpoints (port is vacant), instead of immediately releasing the Pre-Connect ACL from the affected port. By default, the delayed release period is 120 seconds. To modify the value in the field, either enter a value or use the up/down arrow keys to specify a value.

This option is available for use for the specific Cisco switch, when the plugin is configured to manage it as follows:

- The **Enable Pre-Connect Mode** option is enabled
- The **Link-Up ACL** option is selected.

When this option is enabled, its delayed release period value overrides the value defined in the global option **Delay release of Pre-Connect ACL**. For details, see [Global Configuration Options for the Switch Plugin](#).

#### *Keep Pre-Connect ACL Access List on Managed Switches When Plugin Stops*

When the Switch Plugin is stopped, the Pre-Connect ACL of the managed Cisco switch is removed from the switch, including both the provisioned access list and all links to switch ports. CounterACT environments experiencing frequent Switch Plugin stops/starts can elect to have the Switch Plugin maintain the provisioned access list of the Pre-Connect ACL on managed switches and only remove the Pre-Connect ACL from the affected switch access ports. The Switch Plugin property controlling this behavior is `config.acl_pluginstop_keeps_rules_on_switch.value`, which by default is set to `false`.

#### **To keep the Pre-Connect ACL access list on managed Cisco switches when plugin stops:**

1. From the Console, stop the Switch Plugin (**Options > Modules > Network > Switch > Stop**).

2. To modify property per Appliance, do the following:
  - a. On the Appliance, log in to the CounterACT CLI.
  - b. Run the following fstool command:

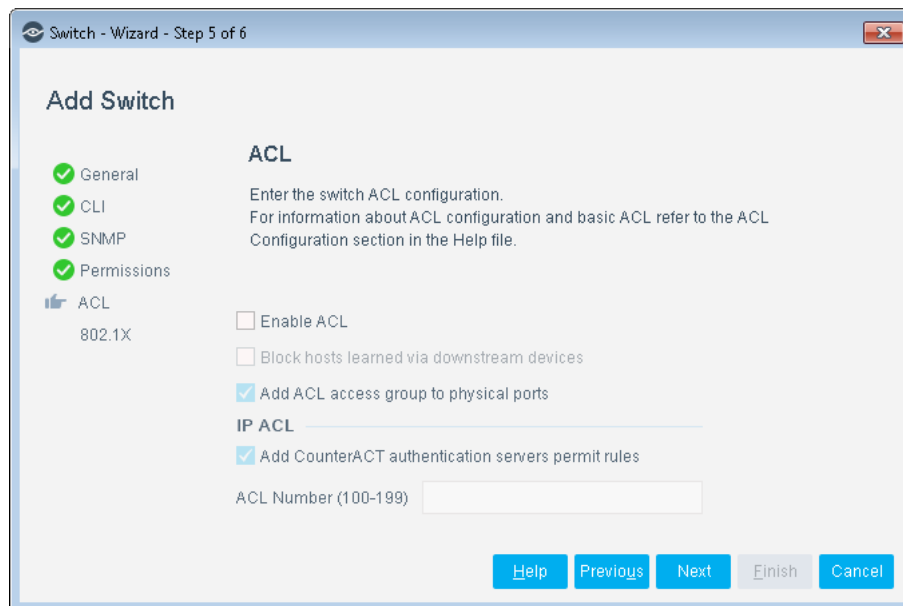
```
fstool sw set_property
config.acl_pluginstop_keeps_rules_on_switch.value true
```
3. To modify property for all CounterACT devices [Enterprise Manager and all Appliances], do the following:
  - a. On the Enterprise Manager, log in to the CounterACT CLI.
  - b. Run the following fstool command:

```
fstool oneach -c fstool sw set_property
config.acl_pluginstop_keeps_rules_on_switch.value true
```
4. From the Console, start the Switch Plugin (**Options > Modules > Network > Switch > Stop**).

## ACL Configuration – Enterasys Matrix N-Series Switches

In the ACL page of the Add Switch wizard, define the Switch Plugin ACL configuration for interoperation with managed Enterasys Matrix N-Series switches. The available options are described in the following sections.

For details about the Switch Plugin ACL capabilities, see [Appendix 6: Working with ACL Capabilities](#).



### Enable ACL

Enable or disable the use of the *Endpoint Address ACL* action (IP address-based ACL) configuration defined on this page.

#### *Block hosts learned via downstream devices*

This option is used with the *Endpoint Address ACL* action.

Enable or disable the blocking of endpoints on the access port or, if not found on the access port, on a trunk port. Enabling this option allows the Switch Plugin to apply the ACL to detected endpoints that reside on a downstream switch device that, for example, does not support ACL use. By default, this option is disabled.

#### *Add ACL access group to physical ports*

This option is used with the *Endpoint Address ACL* action.

By default, this option is enabled. When enabled, the Switch Plugin adds the relevant ACL rules to the switch *access list* and applies the ACL on endpoint-connected switch ports (*access group* is the ACL on a switch port).

When this option is disabled, the Switch Plugin only adds the relevant ACL rules to the switch *access list*; the plugin does not also apply the ACL on endpoint-connected switch ports (*access group* is the ACL on a switch port). In this case, the CounterACT user must then manually add the ACL to the appropriate switch port(s).

## **IP ACL**

This section defines the parameters used to support IP address blocking of detected endpoints, applied using the *Endpoint Address ACL* action.

#### *Add CounterACT authentication servers permit rules*

Selecting this option adds rules to the ACL that permit communication between detected endpoints and CounterACT authentication servers. When the applied action, which adds these rules, is later cancelled, these CounterACT authentication server permit rules are still maintained on the switch, due to performance considerations. Only stopping the plugin or performing a Clear CounterACT ACLs removes added CounterACT authentication server permit rules from the managed switch.

Do not clear this checkbox (this option is enabled by default). If you clear the checkbox, CounterACT may not have access to the blocked endpoints and configured authentication servers.

#### *ACL Number (100-199)*

Type the number of the extended ACL to use on the switch. (ACLs on Enterasys switches are defined by number rather than name.)

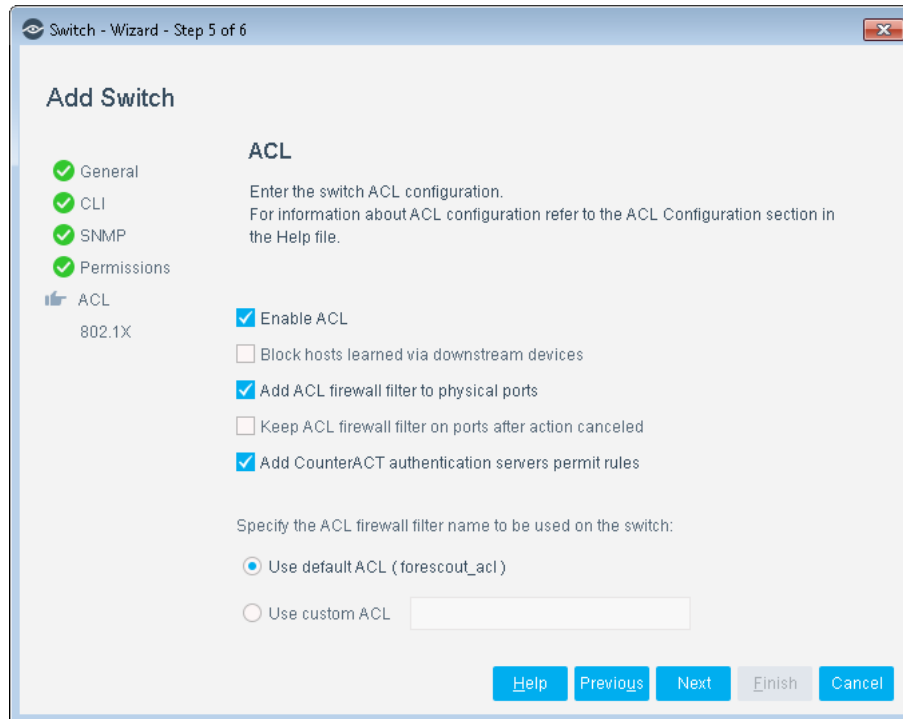
## **ACL Configuration – Juniper Switches**

In the ACL page of the Add Switch wizard, define the Switch Plugin ACL configuration for interoperation with managed Juniper switches. The available options are described in the following sections.

The Juniper-specific term for an ACL is *firewall filter*. A firewall filter can simultaneously contain both IP ACL rules and MAC ACL rules. At any given time, only one firewall filter can be applied to a Juniper switch port.

For plugin IPv6 support exceptions with ACL-related functionality, see [IPv6 Support](#).

For details about the Switch Plugin ACL capabilities, see [Appendix 6: Working with ACL Capabilities](#).



#### *Enable ACL*

Enable or disable the use of the Endpoint Address ACL (IP address-based ACL or MAC addressed-based ACL) configuration defined on this page.

#### *Block hosts learned via downstream devices*

This option is used with the *Endpoint Address ACL* action.

Enable or disable the blocking of endpoints on the access port or, if not found on the access port, on a trunk port. Enabling this option allows the Switch Plugin to apply the ACL firewall filter to detected endpoints that reside on a downstream switch device that, for example, does not support ACL firewall filter use. By default, this option is disabled.

#### *Add ACL firewall filter to physical ports*

This option is used with the *Endpoint Address ACL* action.

By default, this option is enabled. When enabled, the Switch Plugin adds the relevant ACL firewall filter to the switch ACL list and applies the ACL firewall filter on endpoint-connected switch ports.

When this option is disabled, the Switch Plugin only adds the relevant ACL firewall filter to the switch ACL list; the plugin does not also apply the ACL firewall filter on endpoint-connected switch ports. In this case, the CounterACT user must then manually add the ACL firewall filter to the appropriate switch port(s).

#### *Keep ACL firewall filter on ports after action canceled*

This option is used with the *Endpoint Address ACL* action.

When this option is enabled, the Switch Plugin leaves the ACL firewall filter, which was previously applied by an *Endpoint Address ACL* action, on its port after the

action is cancelled for an endpoint. The ACL firewall filter remains on the port until either the plugin is stopped or Switch Plugin garbage collection occurs. The plugin does not remove the relevant rules from the ACL firewall filter. By default, this option is disabled.

Operating in this manner, the plugin reduces the amount of CLI configuration changes in the switch that, in turn, yields a reduction in both CPU and memory usage of the switch.

#### *Add CounterACT authentication servers permit rules*

This option is used with IP ACL rules of an *Endpoint Address ACL* action and supports the IP address blocking of detected endpoints. Selecting this option adds rules to the ACL that permit communication between detected endpoints and CounterACT authentication servers. When the applied action, which adds these rules, is later cancelled, these CounterACT authentication server permit rules are still maintained on the switch, due to performance considerations. Only stopping the plugin or performing a Clear CounterACT ACLs removes added CounterACT authentication server permit rules from the managed switch.

Do not clear this checkbox (this option is enabled by default). If you clear the checkbox, CounterACT may not have access to the blocked endpoints and configured authentication servers.

#### *Specify the ACL firewall filter name to be used on the switch*

Select the name of the ACL firewall filter to be used by the Endpoint Address ACL action on the Juniper switch. Select either one of the following options:

- **forescout\_ac1** - the CounterACT-supplied, default ACL firewall filter name.
- **Custom** - upon selecting this option, enter an ACL firewall filter name in the associated field.

## Security Group Tagging Configuration

The plugin supports the Security Group Tagging functionality of a Cisco TrustSec domain. A Cisco TrustSec domain is a collection of authorized and authenticated Cisco switches and routers. These switches and routers secure and control the IP traffic within the domain, by using the information that is added in the TrustSec header of all IP packets to enforce the domain's access control policy.

Within the Cisco TrustSec domain, an assigned Security Group Tag (SGT) is either carried through the network or imposed on the endpoint. Imposing an SGT on endpoint IP traffic generated in the domain requires the following:

- The endpoint is assigned an SGT to be imposed. An SGT is a number in the range of 1 - 65,535.
- Any TrustSec domain switch that handles IP traffic processes the SGT Exchange Protocol (SXP) in either one of the following manners:
  - As an *SXP Speaker* switch. Switches that are SXP Speakers understand the protocol, identify that the IP packet requires its SGT assignment to be imposed and then forward the IP packet to an SXP Listener switch, based on configured, SXP network connections.

- As an *SGT-enabled* switch. Switches that are SGT-enabled have the ability to impose the SGT assignment in an IP packet (Cisco terms this ability *inline tagging*).

In support of the Security Group Tagging functionality of a Cisco TrustSec domain, the Switch Plugin provides the following:

- The *Assign Security Group Tag* action to assign an SGT to IP addresses, these being CounterACT-detected endpoints. The applied action can be canceled.
- The **SGT** property. Resolving this property provides the currently assigned SGT, if any, of an endpoint.

Ensure that the plugin can perform the *Assign Security Group Tag* action and resolve the **SGT** property for CounterACT-detected endpoints that are located on managed Cisco switches by performing the following actions:

1. Configure the Switch Plugin to use CLI communication with the managed Cisco switch. For details, see [CLI Configuration](#).
2. Enable the advanced configuration flag `assign_sgt` in the **Edit general parameters** dialog box of the Switch tab. For details, see [Advanced configuration flags](#), [Enable a Feature](#).
3. For the managed Cisco switch, configure the plugin to read/write switch SGT information. See [SGT Pane/Tab](#).
4. Test the managed Cisco switch configuration to verify that the plugin successfully reads/writes the switch's SGT information and that the switch has the necessary Security Group Tagging configuration, meaning that the switch is either *SGT-enabled*, an *SXP Speaker* or both.
5. After successful test results, save the updated switch plugin configuration (in the Switch tab, select **Apply**).

### SGT Pane/Tab

For a managed Cisco switch, configure the plugin to read/write switch SGT information. This is accomplished either when adding a switch to be managed by the plugin, using the Add Switch wizard > SGT pane, or when editing an existing managed switch, using the Edit Switch > SGT tab.





To configure plugin performance of SGT-related processing on the managed Cisco switch:

1. In the SGT pane/tab, enable the **Read/Write Switch SGT Information**.
2. Define the default SGT that the plugin must use when canceling the *Assign Security Group Tag* action that is applied on an endpoint. The following options are available:
  - **Re-assign original SGT to endpoint:** Selecting this option instructs CounterACT to return the SGT assignment that existed on the endpoint immediately prior to CounterACT applying any *Assign Security Group Tag* action on the endpoint.
  - **Clear endpoint of SGT assignment:** Selecting this option instructs CounterACT to delete the SGT assignment that exists on the endpoint. This option results in the affected endpoint having no assigned SGT.


## 802.1X Integration

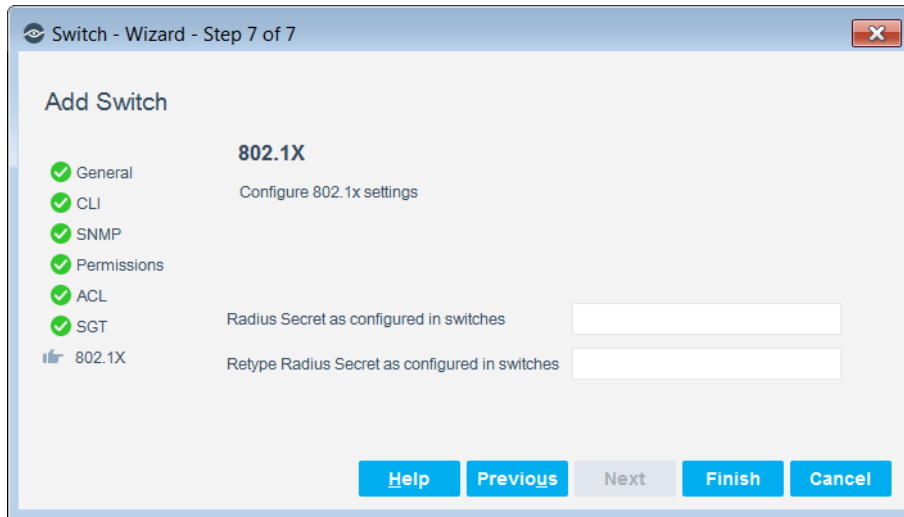
The Add Switch wizard opens the 802.1X pane, as the final pane in the plugin configuration process.

Configure the fields in the 802.1X pane if your CounterACT deployment is responsible for providing RADIUS-based authentication and authorization of detected endpoints attempting to connect to your organization's network via its switches.

**In the 802.1X pane:**

1. In the **RADIUS Secret as configured in switches** field, enter the necessary RADIUS secret to allow communication between the CounterACT RADIUS server and the managed switches in your organization's network.

 *The identical RADIUS Secret must be configured for all switch devices that are deployed in the same IP address range. The plugin does not validate for this requirement.*

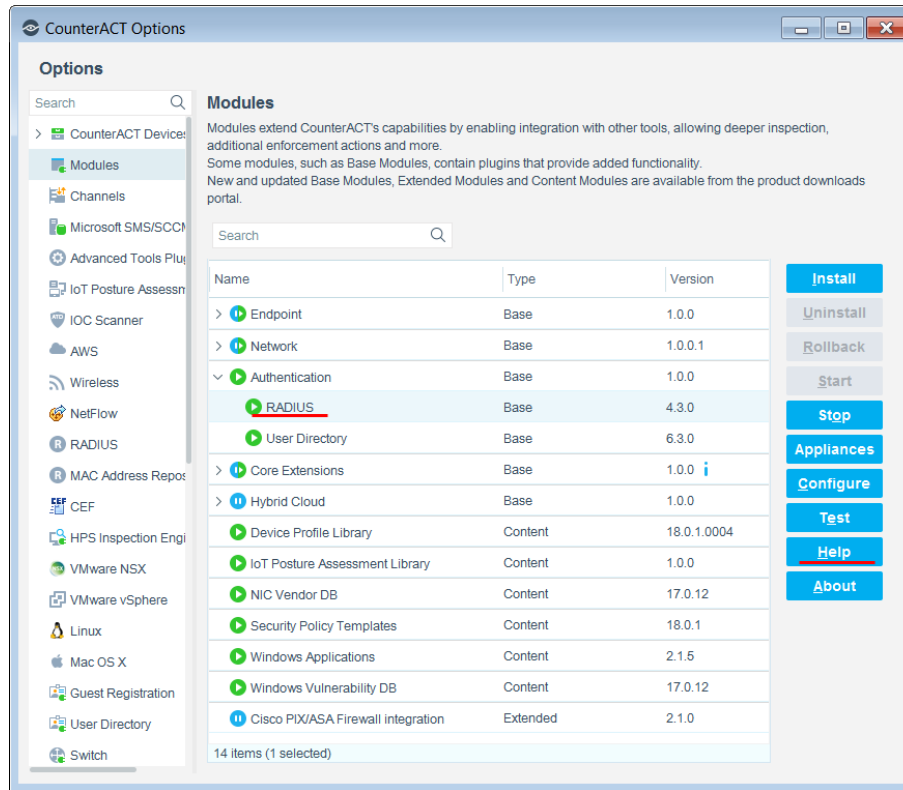


2. Select **Finish**. The Switch tab re-displays containing the configured entry.

Review information about 802.1X and switch integration before working with this capability.

**To review RADIUS Plugin information:**

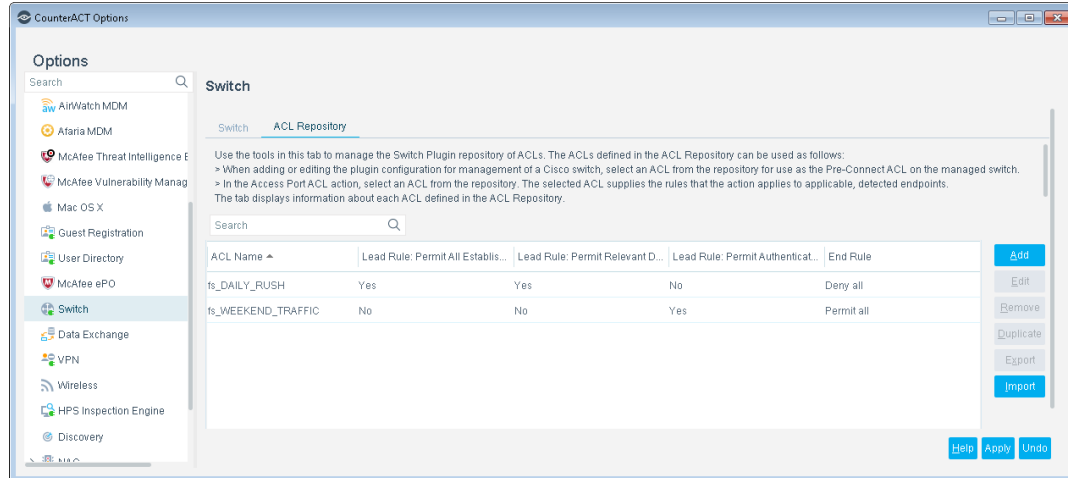
1. In the Console, select **Tools > Options > Modules**. The Module pane opens.
2. In the Module pane, select the **Authentication** module. The plugins, which are installed as part of the CounterACT Authentication Module display.
3. In the Modules pane, select the **RADIUS** entry from the table listing.
4. Select **Help**.



## The ACL Repository

The ACL Repository tab is located in the Switch pane. Use this tab to manage the Switch Plugin repository of ACLs. ACLs defined in this repository are only for use on managed Cisco switches for the following purposes:

- Pre-Connect Mode - select an ACL from the repository for use as the Pre-Connect ACL of a managed switch. See [Pre-Connect Mode](#).
- In an *Access Port ACL* Action - select an ACL from the repository for inclusion in an *Access Port ACL* action. The selected ACL supplies the rules that the action applies to applicable detected endpoints, either due to a policy condition match or a manual application of the action. See [Restrict Actions](#), [Access Port ACL](#).



The tab provides the following repository management capabilities:

- **Add** - define a new ACL in the repository
- **Edit** - edit an existing repository ACL
- **Remove** - delete an ACL from the repository
- **Duplicate** - copy an ACL from the repository and edit its content to define a new ACL in the repository
- **Export** - export the selected repository ACLs into an XML formatted (.xml) file. As part of the process, you supply a password to protect the ACL data in the file being exported.
- **Import** - import into the repository the ACLs defined in an XML formatted (.xml) file. As part of the process, you supply the password that was used to protect the ACL data, when the file was exported. The Console displays warnings about any issues detected in the ACL data awaiting import.

After performing any of the above actions, select **Apply** in the ACL Repository tab to save the modified plugin configuration.

Repository ACLs are composed of the following information:

Field/Option	Description
<b>ACL Name</b>	<p>Required field. This field accepts any combination of alphanumeric characters and the underscore character (_). When defining the ACL name, make sure to follow the switch's rules about valid ACL name.</p> <p>The Switch Plugin automatically prefixes the defined ACL name with the characters <b>fs_</b>. For example, the CounterACT user provides the name <b>Eastern</b> in the ACL Name field. The official plugin name of the ACL is <b>fs_Eastern</b>.</p> <p>Customize the ACL name prefix, to characters other than the default value of <b>fs_</b>, by modifying the property <b>config.acl_name_prefix.value</b>, which controls the prefix value. See the procedure <a href="#">Customize the ACL Name Prefix</a>.</p> <p>When editing a repository ACL, you cannot modify the <b>ACL Name</b> field; it is view-only.</p>

Field/Option	Description
<b>ACL Rules</b>	<p>CounterACT does not inspect and does not alter the provided rules; the plugin's role is to deliver the ACL to a switch device.</p> <p>Note the following issues:</p> <ul style="list-style-type: none"> <li>▪ <i>When defining rules, you must follow the switch's rules about valid ACL rule content.</i></li> </ul> <p>For example, if syntax, not supported by the switch device, is used in an ACL rule, such that this rule cannot be added to the switch access list, then including this rule will result in a plugin failure to write the associated access list on the switch. Hence, using unsupported rule syntax must be avoided.</p> <ul style="list-style-type: none"> <li>▪ <i>Do not include rule numbers in the rules that are defined in the <b>ACL Rules</b> text box.</i></li> </ul> <p>Failure to follow this restriction results in plugin failure to apply the ACL on the switch, whether as a Pre-Connect ACL or in an <i>Access Port ACL</i> action. A Switch Alert message displays in the Switch tab about the failure to apply the ACL on the switch.</p>
<b>Lead Rule: Permit all established connections</b>	<p>When adding an ACL to the repository, this <i>lead rule</i> option is selected by default.</p> <p>Selecting this option adds the following lead rule to the ACL:</p> <p style="text-align: center;"><b>permit tcp any any established</b></p> <p>This rule permits all established connections through the ACL by using the <i>established</i> keyword, which identifies that IP communication packets belong to an existing connection.</p> <p>In the ACL, lead rules are added before all rules defined in the <b>ACL Rules</b> text box.</p>

Field/Option	Description
<b>Lead Rule:</b> <b>Permit relevant CounterACT devices</b>	<p>When adding an ACL to the repository, this <i>lead rule</i> option is selected by default.</p> <p>Selecting this option instructs the Switch Plugin, running on an Appliance, to add a permit lead rule in the ACL for each relevant CounterACT device. The relevant CounterACT devices requiring a permit lead rule in the ACL are:</p> <ul style="list-style-type: none"> <li>▪ The Enterprise Manager</li> <li>▪ The managing Appliance of the target switch, where the plugin applies the ACL</li> <li>▪ Any other Appliance having an IP assignment that includes the IP address of any endpoint that the Switch Plugin learns about, when any of the following CounterACT events occur: <ul style="list-style-type: none"> <li>- The IP address of an endpoint changes</li> <li>- An endpoint, connected to a switch being managed by the Appliance, is restricted by an applied ACL action.</li> <li>- All endpoints that the Appliance learns about when reading the ARP table (IP to MAC mapping) of a managed switch.</li> </ul> </li> </ul> <p>Rule example: <b>permit ip any host 109.41.73.125</b>, where <b>109.41.73.125</b> is the <i>&lt;IP address of the managing Appliance of the target switch &gt;</i></p> <p>The Switch Plugin, running on an Appliance, periodically checks whether or not there are any changes in its list of relevant CounterACT devices. If change occurred, the plugin updates the lead permit rules of the affected ACLs (rules added for Appliances joining the list; rules deleted for Appliances removed from the list). By default, the plugin performs this check every 60 seconds. The Switch Plugin property <b>config.acl_appliances_sync.value</b> controls the frequency of this check. The plugin re-applies the updated ACLs on the affected switch.</p>
<b>Lead Rule:</b> <b>Permit CounterACT authentication servers</b>	<p>Selecting this option adds <i>lead rules</i> to the ACL that permit communication between detected endpoints and CounterACT authentication servers.</p>
<b>End Rule:</b> <b>Deny all traffic</b>	<p>When adding an ACL to the repository, this end rule option is selected by default.</p> <p>Selecting this option adds the following end rule to the ACL:</p> <ul style="list-style-type: none"> <li>▪ <b>deny any any</b></li> </ul> <p>This rule denies all IP communication, both incoming and outgoing, through the ACL.</p> <p>At any given time, only one end rule option can be selected. In the ACL, the end rule is added after all lead rules and all rules defined in the <b>ACL Rules</b> text box.</p>

Field/Option	Description
<b>End Rule:</b> <b>Permit all traffic</b>	Selecting this option adds the following end rule to the ACL: <ul style="list-style-type: none"> <li>▪ <b>permit any any</b></li> </ul> This rule permits all IP communication, both incoming and outgoing, through the ACL. At any given time, only one end rule option can be selected. In the ACL, the end rule is added after all lead rules and all rules defined in the <b>ACL Rules</b> text box.

About repository ACLs:

- **Minimum rule requirement:** Either one rule is provided in the **ACL Rules** text box or one lead rule option is selected.
- **Rule placement:** Lead rules are positioned in the ACL before rules defined in the **ACL Rules** text box.
- **Lead Rule 0:** As part of plugin application of a repository ACL, whether as a Pre-Connect ACL or in an *Access Port ACL* action, the plugin automatically adds *lead rule 0* to the applied ACL. *Lead rule 0* is always added on the switch before all other lead rules. No explicit user action is required. The addition of *lead rule 0* ensures that the managing CounterACT device is *always* able to communicate, via CLI, with its managed switches.

Lead Rule 0:

```
permit tcp host <managing CounterACT IP address> host <managed switch IP address> eq <configured CLI connection type>
```

where the value of **eq** is either:

- 22, when the plugin's configured CLI connection type is **SSH**
- 23, when the plugin's configured CLI connection type is **Telnet**

#### To customize the ACL name prefix:

1. On the Enterprise Manager, log in to the CounterACT CLI.
2. Run the following `fstool` command:
 

```
fstool sw set_property config.acl_name_prefix.value <acl_name_prefix>
```

  - When defining the **acl\_name\_prefix**, make sure to follow the switch rules about valid ACL name
  - The **acl\_name\_prefix** can be any combination of alphanumeric characters and the underscore character (`_`)
  - There is no limit on the length of the **acl\_name\_prefix**
3. Re-install the currently installed Switch Plugin version. This re-install only affects the Enterprise Manager.
4. Exit the Console.
5. Log in to the Console.



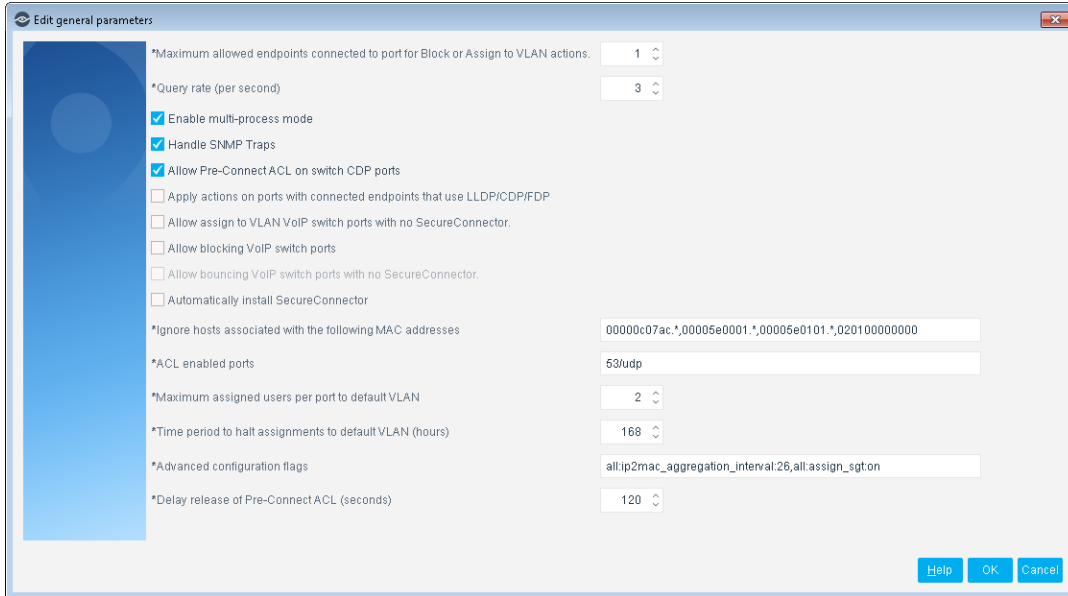
## Global Configuration Options for the Switch Plugin

This section describes options that are globally applied to all switches configured for Switch Plugin management. The plugin provides the following global options:

- [Maximum allowed endpoints connected to port for Block or Assign to VLAN actions](#)
- [Query rate \(per second\)](#)
- [Enable multi-process mode](#)
- [Handle SNMP Traps](#)
- [Allow Pre-Connect ACL on switch CDP ports](#)
- [Apply actions on ports with connected endpoints that use LLDP/CDP/FDP](#)
- [Allow blocking VoIP switch ports](#)
- [Allow Assign to VLAN VoIP switch ports with no SecureConnector](#)
- [Allow bouncing VoIP switch ports with no SecureConnector](#)
- [Automatically install SecureConnector](#)
- [Ignore hosts associated with the following MAC addresses](#)
- [ACL enabled ports](#)
- [Maximum assigned users per port to default VLAN](#)
- [Time period to halt assignments to default VLAN \(hours\)](#)
- [Advanced configuration flags](#)
- [Delay release of Pre-Connect ACL \(seconds\)](#)

**To open the Edit general parameters dialog box:**

1. Select **Options** in the Switch tab toolbar. The **Edit general parameters** dialog box opens.



### Maximum allowed endpoints connected to port for Block or Assign to VLAN actions

A *Switch Block* or an *Assign to VLAN* action is applied on a port only if the number of endpoints that are connected to that port does not exceed the defined value of this option. ***VoIP devices that are connected to that port do NOT count towards this limit.***

Defining a low value for this option means that the plugin will not block or reassign ports that are connected to other switches, routers or hubs. For example, if another hub is connected to a switch port, there will usually be numerous users behind the port.

You can also use the option as a security mechanism. If, for example, numerous endpoints are located on a single hub port but only one of them matches your policy, you can prevent unnecessary blocking of compliant endpoints by limiting the number of blocked endpoints. (If one endpoint matches the policy but several endpoints are located on the port, then defining a high value means that all endpoints are blocked or quarantined – regardless of their policy compliance status.)

If the defined **Maximum allowed endpoints connected to port for Block or Assign to VLAN actions** value is exceeded, the *Switch Block* or *Assign to VLAN* action icon in the All Hosts pane indicates that the action failed.

Policy	User Name	MAC Address	Switch	Switch	Switch	Switch	Switch	Switch	Actions
sw t...		000c29e...	10.33...	on qa ...	Fa0/17	2	Up	333	
sw t...		000c29d...	10.33...	on qa ...	Fa0/17	2	Up	333	

When the defined value of the option is exceeded, the All Hosts pane tooltip displays:

**Failure (mac[XXX]) - port [XXX] has multi users)**

### Query rate (per second)

This is the maximum number of switches that will be queried per second. The Switch Plugin proceeds through all switches one-by-one, and then starts again. Depending

on the number of switches configured, the value here may not allow the plugin to fulfill the query rate set in the **When SNMP is used to read IP to MAC mapping, refresh reported entries** parameter in the Switch Advanced Settings dialog box (see [Performance Tuning](#) for details).

If refreshing the ARP table is important, be sure to set this value high enough.

### Enable multi-process mode

Selecting this option enables multi-process operation of the Switch Plugin on all Appliances. By default, the Switch Plugin operates on all Appliances in multi-process mode (option checkbox selected).

When **Enable multi-process mode** is selected, each Appliance runs multiple, parallel device management processes, thereby increasing the real-time, switch management capacity of CounterACT. When this option is not selected, the Switch Plugin on each Appliance runs in standard, single-process mode.

For additional deployment considerations and information about multi-process operation of the Switch Plugin on Appliances, see [Appendix 7: Improve Switch Management for Large Deployments](#).

### Handle SNMP Traps

Select this option to enable Switch Plugin handling of the SNMP traps it receives from managed switch devices. Clear the **Handle SNMP Traps** checkbox to disable plugin handling of received SNMP traps; the plugin then ignores all received SNMP traps.

#### *SNMP Trap Processing*

Switch Plugin handles SNMPv1, SNMPv2 and SNMPv3 traps. The types of SNMP traps that the plugin handles are:

- SNMP link status traps [the *Link Up* trap and the *Link Down* trap]
- The MAC notification *MAC Address Learned* trap (Cisco only)

Selecting the **Handle SNMP Traps** option configures the Switch Plugin to receive SNMP traps sent from switches whenever a switch detects an endpoint connecting to or disconnecting from the network.

- When the advanced configuration flag `forward_snmp_traps` is disabled (the default state of this flag), each Appliance operates as follows:
  - The Switch Plugin processes SNMP traps sent from switch devices that the Appliance manages.
  - The Switch Plugin ignores SNMP traps sent to the Appliance by a switch device that the Appliance does not manage (sending switch device is managed by another Appliance).
- When the advanced configuration flag `forward_snmp_traps` is enabled, each Appliance operates as follows:
  - The Switch Plugin processes SNMP traps sent from switch devices that the Appliance manages.

- The Switch Plugin forwards SNMP traps sent by a switch device that the Appliance does not manage to the Appliance managing the sending switch device.

The plugin uses direct inter-Appliance communication infrastructure to forward SNMP traps to the target Switch Plugin running on the relevant Appliance. This infrastructure provides for direct communication between Appliances. Refer to the *Enterprise Manager/Appliance Communication CounterACT Technical Notes* for further information about direct inter-Appliance communication. See [Additional CounterACT Documentation](#) for information on how to access this document.

- For information about enabling the `forward_snmp_traps` advanced configuration flag, see [Enable or Control Features](#).

When the Switch Plugin receives an SNMP *Link Up* trap or a MAC notification *MAC Address Learned* trap, it triggers a CounterACT admission event (a network event that indicates the admission of an endpoint into the network) and allows the CounterACT Console to know almost immediately about the change.

Receipt of an SNMP *Link Up* trap for an endpoint from a managed switch, causes the plugin to then check for and, if necessary, wait for the receipt of an associated *MAC Address Learned* trap for the endpoint, as follows:

- Plugin checks for the receipt, during the preceding 5 second interval, of the associated *MAC Address Learned* trap.
- If a previously received trap is not found, plugin waits to receive an associated *MAC Address Learned* trap, during the following 5 second interval.
- If no associated *MAC Address Learned* trap is received, during the following 5 second interval, the plugin performs a MAC query on the managed switch to learn additional MAC address detail about the endpoint.

The check-for-receipt/wait-for-receipt interval is controlled by the property `config.query_mac_post_traps_delay.value`, which is maintained in the CounterACT `local.properties` file. You can modify the property's value to shorten or lengthen the interval, using the following `fstool` command line:

```
fstool sw set_property config.query_mac_post_traps_delay.value
<interval length>
```

See [Configuring MAC Notification Traps on Cisco Switches](#) for information about configuring a Cisco switch to send MAC notification traps to CounterACT.

### *SNMP Traps Ignored*

The Switch Plugin ignores the following received traps:

- Traps from a switch not being managed by the plugin.  
*Exception:* When the community string of the received trap matches the community string of a managed switch that has **Use switch configuration as template** selected (see [Use Switch Configuration as a Template](#)), then the plugin does handle the trap sent to it from the unmanaged switch.
- The MAC notification *MAC Address Removed* trap. This is due to the trap being an unreliable indicator of endpoint disconnection from a switch, in scenarios where the endpoint is connected to either a VoIP device or a hub.

### Allow Pre-Connect ACL on switch CDP ports

When Pre-Connect Mode is enabled for use on a managed Cisco switch, enable the **Allow Pre-Connect ACL on switch CDP ports** option to allow the Switch Plugin to apply the Pre-Connect ACL on ports that have connected endpoints using the Cisco discovery protocol (CDP). By default, the **Allow Pre-Connect ACL on switch CDP ports** option is enabled. See [Pre-Connect Mode](#).

In the **Edit general parameters** window, a similar option is available for the apply/not apply of specific Switch Plugin actions on switch ports where a discovery protocol is in use, see the option **Apply actions on ports with connected endpoints that use LLDP/CDP/FDP**.

### Apply actions on ports with connected endpoints that use LLDP/CDP/FDP

Selecting this option allows the Switch Plugin to apply the *Switch Block* action and the *Assign to VLAN* action on ports with connected endpoints, where such endpoints use one of the following discovery protocols: LLDP, CDP or FDP.

### Allow blocking VoIP switch ports

Select this option to use the *Switch Block* action in a VoIP environment. Clear this option to prevent use of the *Switch Block* action for blocking VoIP ports. For a list of switches that support VoIP blocking, see [VoIP Support](#).

### Allow Assign to VLAN VoIP switch ports with no SecureConnector

This option lets you use the *Assign to VLAN* action in a VoIP environment when SecureConnector is not installed on endpoints connected to VoIP switch ports.

- ☰ *If SecureConnector is not installed on an endpoint, the endpoint will not receive a new IP address automatically (unless **Allow bouncing VoIP Switch Ports with no SecureConnector** is selected) and must be manually provided with a new IP address.*

### Allow bouncing VoIP switch ports with no SecureConnector

Select this option to bounce the switch VoIP ports when performing the *Assign to VLAN* action. Note that this means that calls from VoIP devices (IP phones) are disconnected when the endpoint is assigned to a new VLAN.

This option is enabled only if **Allow assign to VLAN VoIP switch ports with no SecureConnector** is selected.

- ☰ *In the case of an endpoint located behind a VoIP device, if the VoIP device is connected to a PoE port on the switch but powered by an external power supply, bouncing the switch port does not cause a link-down on the endpoint and the endpoint must be manually provided with a new IP address.*

### Automatically install SecureConnector


Select this option to silently install SecureConnector on an endpoint (if it is not already installed) when performing an *Assign to VLAN* action.

If you do not select this option, VoIP ports on the switch will either be bounced or require manual assignment of new IP addresses.

### Ignore hosts associated with the following MAC addresses

Use this option to tell the plugin to ignore endpoints that are associated with the listed MAC addresses. Comma-separated regular expressions can be entered in this field. By default, the following MAC addresses are listed in this field:


- `0007b400.*` (a Cisco virtual MAC address range, used with the Gateway Load Balancing Protocol)
- `00000c07ac.*` (HSRP traffic)
- `00005e0001.*` and `00005e0101.*` (VRRP traffic)
- `020100000000` (the heartbeat for Windows Server 2003 load-balancing)

 *To restore the default setting, clear the field of all entries and select **OK**. In the Options window, select **Apply** to save the Switch Plugin configuration update. Saving the configuration update causes a restart of the Switch Plugin in all CounterACT devices.*

### ACL enabled ports

Use this option to ensure that specific ports are available for restricted endpoints when working with the rules of an *Endpoint Address ACL* action. The ports that you enter here remain available regardless of the *Endpoint Address ACL* actions defined in the plugin.

By default, 53/UDP (DNS) is enabled.

 *To restore the default setting, clear the field of all entries and select **OK**. In the Options window, select **Apply** to save the Switch Plugin configuration update.*

### Maximum assigned users per port to default VLAN

This option specifies the maximum number of endpoints connected to a port so that, if a default VLAN is specified (see [Default VLAN](#)), the port may be assigned to the default VLAN.

### Time period to halt assignments to default VLAN (hours)

This option specifies the time period to wait until the Switch Plugin begins reassigning ports to the default VLAN. For example, if the maximum number of endpoints per port is set to 4 in the preceding option and the value here is set to 5 hours, the port will not be assigned to the default VLAN for 5 hours, even if the number of endpoints on the port falls to 4 within the 5 hours.


### Advanced configuration flags

Advanced configuration flags are used to:

- [Enable or Control Features](#)
- Implement Workarounds – see [Appendix 2: Troubleshooting, Workarounds and Feature Functionality Support](#)

Enable *global* advanced configuration features by defining the appropriate flag in the **Advanced configuration flags** field. Advanced configuration flags apply to all switches configured to work with the plugin.

To enable per switch advanced configuration features, see [Configuration Flags](#).

 *Per-switch configuration of a flag always takes precedence over the global configuration of that flag.*

**To enable a *global* advanced configuration feature:**

1. In the Console toolbar, select the **Options** icon.
2. In the **Options** window navigation tree, select **Switch**. The **Switch** tab displays.
3. In the **Switch** tab, select the **Options...** button. The **Edit General Parameters** window opens.
4. In the **Advanced configuration flags** field, , use any of the following statements, as applicable:
  - `<vendor>:<flag_name>:on` (enables the flag)
  - `<vendor>:< flag_name>:<decimal_value>` (enables the flag and assigns it the provided value)
  - `<vendor>:< flag_name>:<text_string>` (enables the flag and assigns it the provided text)

For `<vendor>`, `all` enables the flag for all supported switch vendors; a specific supported vendor name enables the flag only for the switches of the specified vendor, for example, `cisco`, `nortel`, `enterasys`. For certain flags, only `all` is valid for use in the `<vendor>` field. Other flags are only intended for use with a specific supported vendor and therefore, only that vendor name is valid for use in the `<vendor>` field. These constraints are identified in the relevant flag usage description.

In the field, use the comma (,) to separate between multiple, advanced configuration flag statements.

5. Select **OK** and then select **Apply**.

**To disable a *global* advanced configuration feature:**

1. In the Console toolbar, select the **Options** icon.
2. In the **Options** window navigation tree, select **Switch**. The **Switch** tab displays.
3. In the **Switch** tab, select the **Options...** button. The **Edit General Parameters** window opens.
4. In the **Advanced configuration flags** field, do any of the following:
  - Delete the relevant, advanced configuration flag statement.
  - If the `on` parameter is being used to enable the flag, then modify the relevant, advanced configuration flag statement, as follows:  
`<vendor>:< flag_name>:off`
5. Select **OK** and then select **Apply**.

### *Enable or Control Features*

Several advanced configuration flags are provided for use with specific Switch Plugin features. These flags serve either one of the following purposes:

- [Enable a Feature](#)
- [Control a Feature](#)

#### **Enable a Feature**

The following advanced configuration flags enable a plugin feature:

- [acl\\_action\\_type](#)
- [assign\\_sgt](#)
- [forward\\_snmp\\_traps](#)
- [verify\\_disconnect\\_of\\_data\\_endpoint](#)

#### *acl\_action\_type*

The `acl_action_type` flag enables use of the *Access Port ACL* action. To enable use of the action, configure `acl_action_type` as follows:

- `all:acl_action_type:Access_Port_ACL`

To use the *Endpoint Address ACL* action, make sure that the above configuration statement does not appear in the **Advanced configuration flags** field (since the **default** setting of this flag is `all:acl_action_type:IP_ACL`, which enables use of the *Endpoint Address ACL* action, therefore explicit flag configuration is not necessary).

Flag Constraint: Only `all` is valid for use in the `<vendor>` field.

At any given time, only one of these ACL actions, either the *Endpoint Address ACL* action or the *Access Port ACL* action, can be enabled for use.

#### **To switch between the enablement of these two actions, do the following:**

1. Stop the Switch Plugin on all CounterACT devices. Doing so, results in the cancellation of currently applied, switch restrict actions.
2. In the **Advanced configuration flags** field of the Edit general parameters window, define the `acl_action_type` flag to enable the desired action for use, as described in this section.
3. Start the Switch Plugin on all CounterACT devices.

#### *assign\_sgt*

The `assign_sgt` flag enables plugin use of the SGT-related components *Assign Security Group Tag* action and the **SGT** property. To enable use of the SGT-related components, configure `assign_sgt` as follows:

- `all:assign_sgt:on`

By default, this flag is disabled, `all:assign_sgt:off`. When this flag is disabled, the *Assign Security Group Tag* action and the **SGT** property are unavailable for use and do not appear in the Console. When the action and property are currently included in existing policies and the `assign_sgt` flag is disabled, the action and the property are



marked as **Obsolete** in the relevant policies. For information about Cisco Security Group Tagging functionality, see [Security Group Tagging Configuration](#).

#### *forward\_snmp\_traps*

When a switch device sends SNMP traps about endpoint connection to or disconnection from the network to an Appliance that does not manage the sending switch device and the **forward\_snmp\_traps** flag is enabled, plugin processing ensures that the received SNMP traps are forwarded for handling to the Appliance that manages the sending switch device.

By default, Switch Plugin forwarding of SNMP traps is disabled. Plugin forwarding of SNMPv1, SNMPv2 and SNMPv3 traps is supported.

#### **To enable Switch Plugin forwarding of SNMP traps:**

1. In the **Advanced configuration flags** field, configure **forward\_snmp\_traps** flag as follows:  
`all:forward_snmp_traps:on`
2. Make sure that the **Handle SNMP Traps** checkbox is selected (default option setting).

#### *verify\_disconnect\_of\_data\_endpoint*

The **verify\_disconnect\_of\_data\_endpoint** flag enables the Switch Plugin to use a CDP query with managed Cisco switches in order to determine, more frequently and more reliably, the disconnect status of the data endpoint that is connected behind the VoIP device on a VoIP port (voice VLAN, data VLAN). To enable global use of the CDP query by the plugin, configure **verify\_disconnect\_of\_data\_endpoint** as follows:

- `cisco:verify_disconnect_of_data_endpoint:on`

By default, this configuration flag is disabled (**off**) both globally, all Cisco switches, and per Cisco switch.

- 📖 *When a data endpoint, which is connected behind a VoIP device, disconnects from the VoIP device just before a Switch Plugin restart, then after restart, the plugin initially reports the data endpoint as being online. The actual status (offline) of the data endpoint is then correctly reported when the plugin next performs its periodic MAC address table query of the managed switch. The query period is defined in the setting **Read MACs connected to switch port and port properties** located in the Switch Advanced Settings window.*

Furthermore, use of the CDP query also requires that the plugin is configured to manage the Cisco switches, as follows:

- In the CLI pane/tab, **Use CLI** is enabled
- In the Permissions pane/tab > MAC Permissions section > **MAC Read/Write Method** field, either one of the following MAC read/write methods is selected:
  - **SNMP (RW) and CLI**
  - **SNMP (RO) and CLI**

### Control a Feature

The following advanced configuration flag controls the plugin *Expedite IP Discovery* action:

- `ip2mac_aggregation_interval`

This flag defines an interval that controls the frequency of ARP table queries made by the Switch Plugin, as a result of the Expedite IP Discovery action, to a *Connectivity Group's* designated, L3-enabled network devices in order to obtain IP to MAC mapping data. The interval is maintained per designated, L3-enabled network device. The `ip2mac_aggregation_interval` flag prevents overloading L3-enabled network devices with such queries.

During a given interval, the Switch Plugin aggregates all IP discovery resolve requests for endpoints connected to network devices that are assigned to the same *Connectivity Group*. At interval expiration, the plugin issues its ARP table query to the designated, L3-enabled network devices that are serving the specific *Connectivity Group*.

To define the IP discovery query interval, configure the `ip2mac_aggregation_interval` as follows:

- `all:ip2mac_aggregation_interval:<interval>`

where `<interval>` specifies a number of seconds. The default `<interval>` is 10.

Flag Constraint: Only `all` is valid for use in the `<vendor>` field.

For example, if the defined `<interval>` is 25, all IP discovery resolve requests that the plugin receives for a specific L3-enabled network device, as a result of *Expedite IP Discovery* actions, are delayed for up to 25 seconds prior to that switch device being queried. During the interval, the plugin aggregates consecutive IP discovery resolve requests, thereby minimizing the traffic load on the network and the switch device.

### Delay release of Pre-Connect ACL (seconds)

Enabling this option keeps the Pre-Connect ACL of managed Cisco switches applied to an applicable switch access port for an additional period of time, as of the access port having no connected endpoints (port is vacant), instead of immediately releasing the Pre-Connect ACL from the affected port. By default, the delayed release period is 120 seconds. To modify the value in the field, either enter a value or use the up/down arrow keys to specify a value.

This global option is in effect for all Cisco switches that the plugin is configured to manage as follows:

- The **Enable Pre-Connect Mode** option is enabled
- The **Link-Up ACL** option is selected.

For details, see [Pre-Connect Mode](#).

## 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.

## Edit Switch Configurations in the Plugin

This section describes how to edit switch configurations in the Switch Plugin.

 *Editing a new switch is not described in detail; the tabs of the Edit Switch window are equivalent to the pages of the Add Switch wizard. Refer to the relevant subsection of [Add Switches to the Switch Plugin](#).*

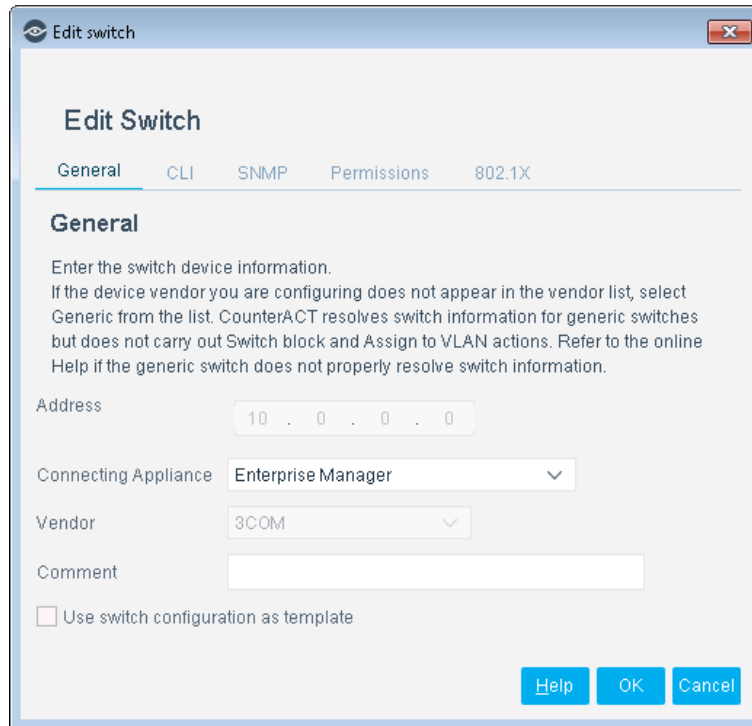
### To edit an existing switch:

1. Select **Options** from the **Tools** menu. The CounterACT **Options** window opens.
2. Select **Switch**. The Switch tab opens.
3. Select a switch in the Switch tab.

You can select more than one switch and edit their configurations, provided that all selected switches are from the same vendor. This feature is described in the following section.

4. Select **Edit**. The Edit Switch dialog box opens displaying the **General** tab.

 *When editing a switch, the **Address** and **Vendor** fields are read-only.*



5. Select the tab containing the settings that you need to edit. The tabs that display for edit can vary based on switch vendor.

For more information, refer to:

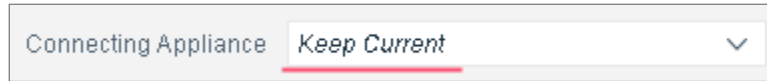
- **General** tab: [General Configuration](#)
  - **CLI** tab: [CLI Configuration](#)
  - **SNMP** tab: [SNMP Configuration](#)
  - **Permissions** tab: [Permissions Configuration](#)
  - **ACL** tab: [ACL Configuration – Cisco and Brocade Switches](#), [ACL Configuration – Enterasys Matrix N-Series Switches](#) or [ACL Configuration – Juniper Switches](#).
  - **SGT** tab: [Security Group Tagging Configuration](#)
  - **802.1X** tab: [802.1X Integration](#)
6. After making all necessary changes, select **OK**.
  7. Select **Apply** to apply your changes to the Switch Plugin.

## Editing Multiple Switches

When editing multiple switches, different switches may have different configured values. If you change the value of a parameter, all selected switches take the new value; all other parameters retain their original values on a per-switch basis.

This is indicated in the Edit Switch dialog box as follows:

- Text boxes and drop-down lists: If these controls contain different text (or one of them is empty), Keep Current is displayed in the control. For example (from the General tab):

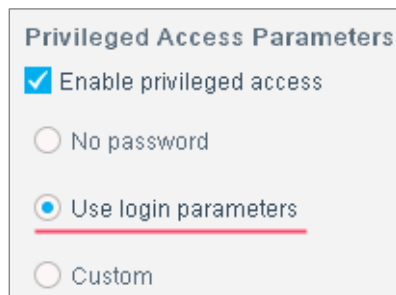


- Checkboxes: If a checkbox is selected for some, but not all, of the switches, a gray (rather than black) check is displayed in the checkbox. For example (from the General tab):

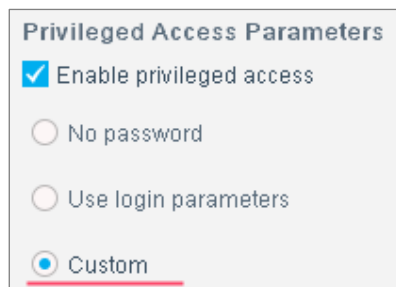


- Radio buttons: If different switches have different radio buttons selected, no radio button is selected in the dialog box. For example (in the CLI tab):

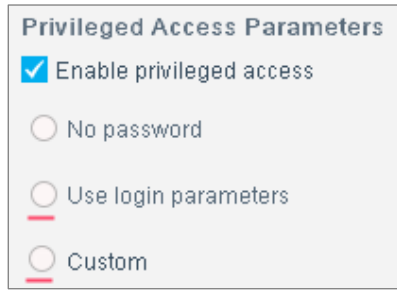
– Switch #1:



– Switch #2:

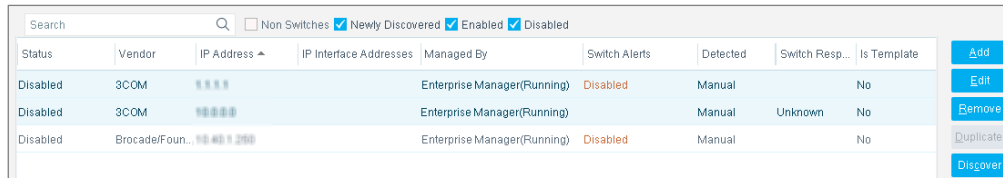


- Multi-edit both switches (no radio button selected):



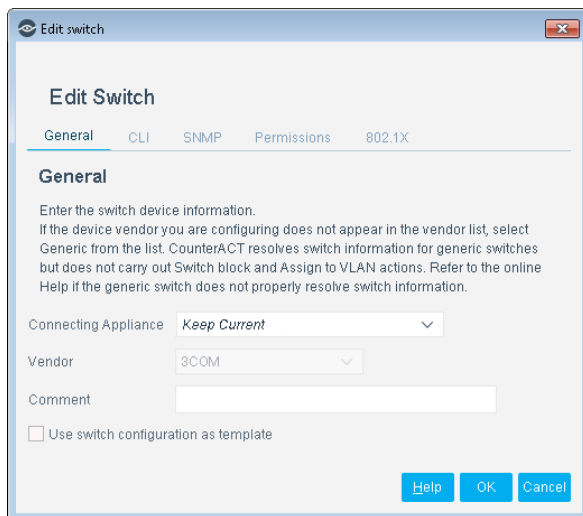
**To edit multiple switches:**

1. In the Switch tab, select the switches that you want to edit in the Switch tab. Make sure that all selected switches are from the same vendor.



2. Select **Edit**. The Edit Switch dialog box opens displaying the General tab.

*When editing multiple switches, the **Address** field is not displayed and the **Vendor** field is read-only.*



3. Select the tab containing the settings that you need to edit. The tabs that display for edit can vary based on switch vendor.

For more information, refer to:

- **General** tab: [General Configuration](#)
- **CLI** tab: [CLI Configuration](#)
- **SNMP** tab: [SNMP Configuration](#)

- **Permissions** tab: [Permissions Configuration](#)
  - **ACL** tab: [ACL Configuration – Cisco and Brocade Switches](#), [ACL Configuration – Enterasys Matrix N-Series Switches](#) or [ACL Configuration – Juniper Switches](#).
  - **SGT** tab: [Security Group Tagging Configuration](#)
  - **802.1X** tab: [802.1X Integration](#)
4. After making all necessary changes, select **OK**.
  5. Select **Apply** to apply your changes to the Switch Plugin.

## Verify 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 Switch Configuration

The switch configuration test accomplishes the following:

- Verifies Switch Plugin communication with the selected network devices.
- Verifies that the Switch Plugin has the read and the write access required for the permissions that you specified. Specifically, read access is required to use any permission and write access is required to apply the following plugin-provided switch actions: *Access Port ACL*, *Assign Security Group Tag*, *Assign to VLAN*, *Endpoint Address ACL* and *Switch Block*.

Test failures may also be the result of errors not related to read or write failures. Be sure to read the information displayed in the **Message** column if there is a failure.

You can test an individual plugin configuration for the management of a network device or simultaneously test multiple plugin configurations for the management of multiple network devices.

## Running the Test

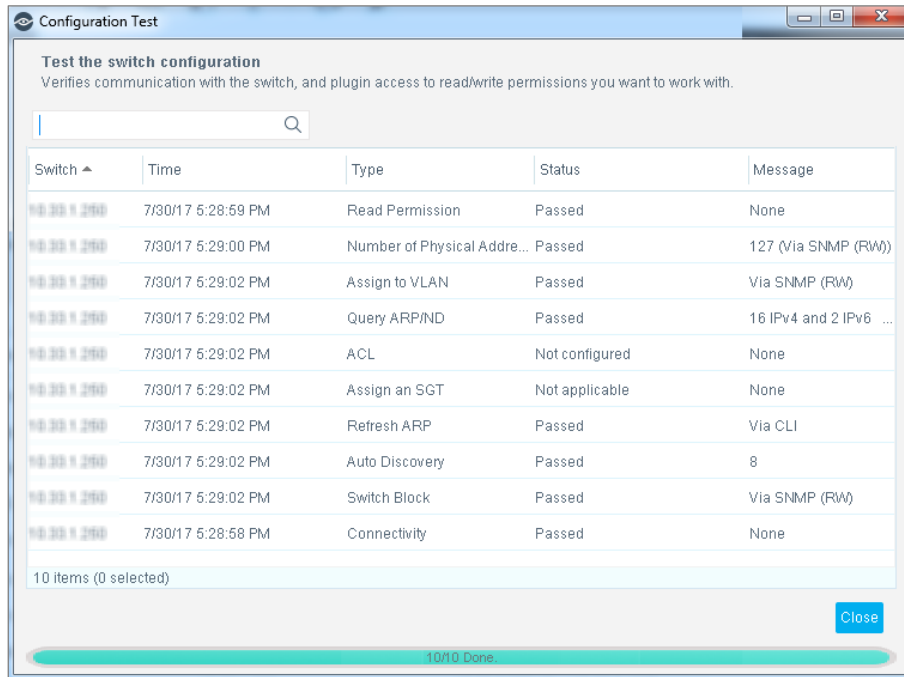
It is recommended that you run the test:

- On initial plugin configuration.
- On plugin configurations that may be problematic, as indicated when the **Status** field in the Switch tab displays an **Error**, **Warning** or **Information** icon.

### To perform the test:

1. Ensure that the plugin is running.

2. In the Switch tab, select the network devices - switch, firewall or Linux router - that you want to test.
3. Select **Test**. The Configuration Test dialog box opens.



The tests may take a few minutes. The test results for the switches that you selected are listed in the dialog box. The Message column includes, where relevant, the configured read or write method.

## Test Failure Scenarios

This section describes the following plugin configuration test failure scenarios:

- [Read and Write Failure](#)
- [Write Failure](#)
- [Assign an SGT Failure](#)
- [Connectivity with Firewall Failure](#)
- [Switch ACL Support Failure](#)

### Read and Write Failure

If the test fails for both reading and writing:

- The Status column reads *Failed*.
- The Message column reads *Fail to read mib (<MIB OID>) [No response from remote host <IP address>]*.

Switch	Time	Type	Status	Message
10.1.24.249	Jan 1, 2007	Read Permission	Failed	Fail to read mib [1.3.6.1.2.1.1.6.0] error[No response from remote host '10.1.24.249']
10.1.24.249	Jan 1, 2007	QueryHosts	Failed	Fail to read mib (1.3.6.1.4.1.9.9.68.1.2.1.1.2) [No response from remote host '10.1.24.249']
10.1.24.249	Jan 1, 2007	Actions Permission	Failed	Fail to read mib (1.3.6.1.2.1.2.2.1.7) [No response from remote host '10.1.24.249']



### Write Failure

If the test fails for writing only:

- The Status column reads *Passed* for all tested items except actions, which require write permissions.
- The Message column for the Action reads *Fail to Write mib (<MIB OID>)* and indicates the reason.

If the switch IP address does not exist or the community is wrong:

- The Status column reads *Failed*.
- The Message column reads *No response from remote host <IP address>*.

If the MIB does not exist on the switch (for example, when the OS of the switch is different than that supported for the switch model):

- The Status column reads *Failed*.
- The Message column reads *Fail to Write mib (<MIB OID>) to status () error*.

Switch	Time	Type	Status	Message
10.1.24.248	Jan 11, 2007	Read Permission	Passed	
10.1.24.248	Jan 11, 2007	Query Hosts	Passed	31 Addresses Learned
10.1.24.248	Jan 11, 2007	Query ARP	Passed	3 Addresses Learned
10.1.24.248	Jan 11, 2007	Auto Discovery	Passed	2 Addresses Learned
10.1.24.248	Jan 11, 2007	Network Policy Actions	Failed	Fail to Write mib (1.3.6.1.2.1.2.2.1.8.1) to status () error[Received noAccess(0) error-status at error-index 1]

[Appendix 4: MIBs Used by the Switch Plugin](#) lists MIBs that must be included on the switch.

### Assign an SGT Failure

The **Assign an SGT** test for a managed switch yields any of the following results:

- *Not applicable* - the required advanced configuration flag `assign_sgt` is disabled on the managed Cisco switch.
- *Not applicable* - for any switch vendor that does not support SGT, this is every plugin-supported vendor other than Cisco.
- *Not configured* - the **Read/Write Switch SGT Information** setting is disabled on the managed Cisco switch.
- *Failed* - either the plugin could not read the managed Cisco switch's SGT information or the plugin read the managed Cisco switch's SGT information and determined that the switch does not support SGT; SGT and SXP capabilities are either not configured or disabled.
- *Passed* - the plugin read the managed Cisco switch SGT information and determined that the switch supports SGT; SGT and/or SXP capabilities are configured and enabled.

### Connectivity with Firewall Failure

In the **Connectivity** test step for the management of a firewall, the Switch Plugin attempts to log in to the firewall. If log in to the firewall fails, the configuration test displays the *Login refused* message for this test step. The failure to log in to the firewall can be caused by any of the following reasons:

- Plugin use of wrong credentials
- Incorrect plugin parsing of the device prompt

- Connection problem

If the **Connectivity** test step for the management of a firewall fails, the **Query ARP** test step consequently displays the following message: *CLI connection is invalid[Login refused]*.

#### *Switch ACL Support Failure*

When the **switch ACL support** test step fails and the following information displays in the **Message** column of the test:

*Unsupported Interface <interface name> for ACLs*

This failure can be caused by plugin selection of a virtual interface of the switch on which to perform this test step, instead of selecting a physical interface.

If the *<interface name>* reported in the failure message is actually a virtual interface, prevent a reoccurrence of this test step failure by adding the tested port to the list of ports prohibited for use when verifying switch ACL support. This list is maintained in the CounterACT `local.properties` file. Add ports to this list using either their port description or a unique portion of their port description.

- 📖 *The Switch Plugin also consults this list after being started, prior to verifying switch **ACL** support of a managed switch.*

In the `fstool` command line, you can use the **OR** operand (`|`) to assign multiple port descriptions to the `config.sw_acl_illegal_port_name.value` property. Also, this property is not case sensitive.

#### **To add a port to the list of ports prohibited for use when verifying switch ACL support:**

1. Stop the Switch Plugin.
2. Add ports to this list using any of the following command lines:
  - a. `fstool sw set_property config.sw_acl_illegal_port_name.value <port description>`  
 For example, `fstool sw set_property config.sw_acl_illegal_port_name.value excluded`
  - b. `fstool sw set_property config.sw_acl_illegal_port_name.value "<port description1|...|port descriptionN>"`  
 For example, `fstool sw set_property config.sw_acl_illegal_port_name.value "--uncont|--cont|EXCLUDE"`
3. Start the Switch Plugin.

After adding port(s) to the list, re-perform the test of plugin configuration for the managed switch.

#### **Further Support**

If you require further details concerning the reasons for test failures, you can run an `fstool` command from your CounterACT device. The command output is a snapshot of the switch MIBs, which can then be analyzed by the ForeScout support team.

**To produce a MIB snapshot when the switch uses SNMP:**

1. Run the following from the CounterACT device:

```
fstool sw snmpwalk
```

Output similar to the following will be displayed:

```
CounterACT Utility Tool
```

```
~~~~~
```

```
Get SNMPWALK from Configured Switches
```

```
Please wait, reading switch list from database...
```

```
Open database - Success
```

```
The following switches are configured to work on the appliance:
```

1. 171.33.1.253 using SNMP version [2] vendor [cisco]
2. 171.34.1.250 using SNMP version [2] vendor [extreme]
3. 171.33.1.250 using SNMP version [2] vendor [cisco]

```
Select a switch for SNMPWALK by entering its number in the list. For multiple switch selection, separate numbers by commas.
```

```
Select switch: 2
```

```
Selected switch [171.34.1.250] model [extreme]
```

```
Take SNMPWALK on (s)electd OIDs, (a)ll OIDs, or OID (f)ile:
```

2. Type **a**, unless you have been instructed to type **s** or **f** by ForeScout support.

Output similar to the following will be displayed:

```
trying . >>/tmp/171.34.1.250.extreme.walk
```

3. Complete the form that opens up when you run `fstool sw snmpwalk` and submit it to the ForeScout support team for debugging assistance.

**To produce a MIB snapshot when the switch uses the NETCONF protocol:**

1. Run the following from the CounterACT device:

```
fstool sw netconf
```

Output similar to the following will be displayed:

```
CounterACT Utility Tool
```

```
~~~~~
```

```
Get NETCONF XMLs from Configured Switches
```

```
Please wait, reading switch list from database...
```

```
Open database - Success
```

```
The following switches are configured to work on the appliance:
```

1. 116.39.1.250 using SNMP version [2] vendor [alcatel]
2. 116.39.1.248 using NETCONF vendor [juniper]
3. 116.34.1.250 using SNMP version [2] vendor [extreme]

```
Select a switch for NETCONF XML query by entering its number in the list. For multiple switch selection, separate numbers by commas.
```

```
Select switch: 2
```

```
Open session to switch [116.39.1.248] vendor [juniper]
```

```
Take NETCONF XMLs on (a) all XMLs (s)electd XMLs or XMLs (f)ile:
```

2. Type **a**, unless you have been instructed to type **s** or **f** by ForeScout support.

Output similar to the following will be displayed:

```
trying . >>/tmp/116.39.1.248.juniper.walk
```

## View Managed Switch Information

View plugin configuration details for the switches being managed, switch information learned by the plugin and real-time, plugin activity information. Two options are available for viewing this information:

- In the **Switch** tab
- In the **Properties** dialog box of a selected network device - switch, firewall or Linux router

### Switch Tab Display

The Console **Switch** tab displays information about the network devices that the plugin is configured to manage.

Status	Vendor	IP Address	IP Interface Address...	Managed By	Detected By	Switch Alerts	Detected	Switch Response Time	Is Template
✓	Cisco	19.44.1.250		Enterprise Manager(Running)			Manual	0.019	No
Newly Discovered	Cisco	46.44.1.249		Enterprise Manager(Running)	26.44.1.250	New	Auto Discovery		No
Newly Discovered	Cisco	46.33.1.248		Enterprise Manager(Running)	26.44.1.250	New	Auto Discovery		No

3 items (1 selected)

These devices are associated with one of the following display categories:

- Enabled (being managed)
- Disabled (read/write permissions not configured for management of device)
- Newly Discovered (via auto-discovery)
- Non Switch (a network device entry that is manually designated as *not a switch* by the CounterACT user)

The **Switch** tab can display the following network device information:

Column	Description
ACL Status	
Actions	
ARP Table OID	
ARP Translation	

Column	Description
<b>Auto Discovery</b>	<p>Identifies whether the managed switch is <b>enabled</b> to/<b>disabled</b> from performing auto-discovery of additional switches.</p> <p>In the Console, the performance of auto-discovery is enabled/disabled in the Permissions pane/tab &gt; Discovery Permissions section.</p>
<b>Auto Discovery Rate</b>	<p>The frequency at which the managed switch performs its periodic auto-discovery of additional switches. By default, this frequency is every 600 seconds (10 minutes).</p> <p>In the Console, this frequency is defined in the Permissions pane/tab &gt; Advanced &gt; Switch Advanced Settings window &gt; Performance tuning section.</p>
<b>Auto Discovery Status</b>	
<b>Block via downstream switches</b>	<p>Identifies whether the plugin option <b>Block hosts learned via downstream devices</b> is enabled or disabled for the managed switch.</p> <p>In the Console, this option is defined in the ACL pane/tab.</p>
<b>Comment</b>	<p>Displayed by default.</p> <p>The presented text is taken from the <b>Comment</b> field of the General pane/tab.</p>
<b>Connectivity Groups</b>	<p>The Connectivity Groups to which the managed switch is assigned. This information is defined in the <b>Connectivity Groups</b> field of the Switch Advanced Settings window (Permissions pane/tab &gt; Advanced).</p>
<b>Detected</b>	<p>Displayed by default.</p> <p>Identifies how the Switch Plugin learned of the table entry. Possible column values are:</p> <ul style="list-style-type: none"> <li>▪ <b>Manual</b> - table entry was manually added by a CounterACT user.</li> <li>▪ <b>Auto Discovery</b> - table entry resulted from being auto-discovered by a managed switch.</li> </ul>
<b>Detected By</b>	<p>Displayed by default.</p> <p>The IP address of the managed switch that auto-discovered the table entry.</p>
<b>Detection Time</b>	<p>The date/time that the table entry was auto-discovered.</p>
<b>IP Address</b>	<p>Displayed by default.</p> <p>The IP address of the switch that the plugin uses for its management of the switch. This information is defined in the <b>IP Address</b> field of the General pane/tab.</p>

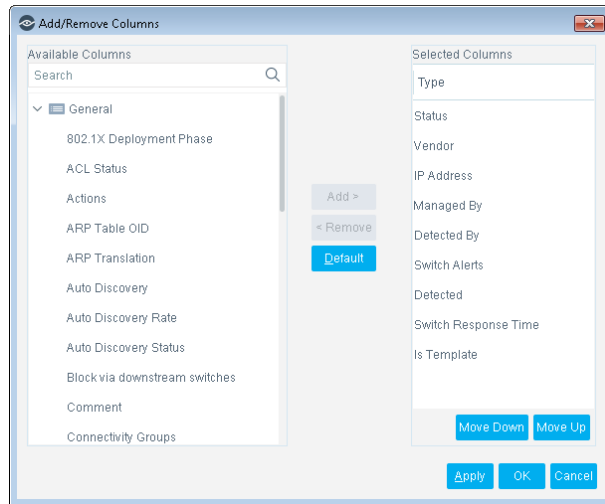
Column	Description
<b>IP Interface Addresses</b>	<p>Displayed by default.</p> <p>Additional IP addresses - IPv4 addresses and/or IPv6 addresses - of the network device as known by the plugin. Switches can have more than one IP address, for example, Layer 3 switches. When you add a new switch to the plugin, only a single IP address can be configured. The Switch Plugin automatically learns the other IP addresses of the switch and reports them to the Console, which displays them in this column entry.</p>
<b>Is Template</b>	<p>Displayed by default.</p> <p>Identifies whether or not the plugin configuration for the managed switch is designated for use as a template for newly discovered, yet unmanaged switches having the same SNMP community.</p>
<b>L3 for Group</b>	<p>The IP addresses of plugin-managed, L3-enabled network devices that are defined to serve the Connectivity Groups to which the managed switch is assigned. Such L3-enabled network devices are used in the <i>Expedite IP Discovery</i> action.</p>
<b>Last Trap Received</b>	<p>Time of plugin receipt of the most recent SNMP trap from the switch.</p>
<b>Location</b>	
<b>Managed By</b>	<p>Displayed by default.</p> <p>The CounterACT device, which is identified either by name or IP address, currently responsible for managing the switch and either one of the following statuses:</p> <ul style="list-style-type: none"> <li>▪ The status of the Switch Plugin on the CounterACT device</li> <li>▪ The status of the CounterACT device, currently responsible for managing the switch, when that CounterACT device is disconnected.</li> </ul>
<b>Number of MACs Found</b>	<p>The number of MAC address entries in the MAC address table of the managed switch, which was learned from the Switch Plugin's most recent query of this table.</p>
<b>OS</b>	<p>Operating system information of the network device.</p>
<b>Permission</b>	<p>The MAC address table permissions that are defined for plugin management of the switch. Possible column values are:</p> <ul style="list-style-type: none"> <li>▪ <b>Read</b></li> <li>▪ <b>Read/Write</b></li> </ul> <p>In the Console, these permissions are defined in the Permissions pane/tab &gt; MAC Permissions section.</p>

Column	Description
<b>Query ARP Rate</b>	The frequency, in seconds, at which the plugin periodically queries the ARP table of the network device. By default, this frequency is every 600 seconds (10 minutes).  In the Console, this frequency is defined in the Permissions pane/tab > Advanced > Switch Advanced Settings window > Performance tuning section.
<b>Query ARP Status</b>	Number of ARP table entries (MAC address to IP address mapping entries) that the plugin learns from reading the ARP table of the network device.
<b>Query Hosts Rate</b>	The frequency, in seconds, at which the plugin periodically queries the MAC address table of the managed switch. By default, this frequency is every 60 seconds (1 minute).  In the Console, this frequency is defined in the Permissions pane/tab > Advanced > Switch Advanced Settings window > Performance tuning section.
<b>SGT Enabled, SXP Speaker</b>	Relevant only for managed Cisco switches that are located within a Cisco TrustSec domain.  Identifies the managed switch as being either <i>SGT-enabled</i> , an <i>SXP Speaker</i> or both.
<b>SNMP Version</b>	The SNMP version of the network device.
<b>Status</b>	Displayed by default.  Current status of the network device as known to the plugin. Statuses include <i>Newly Discovered</i> , <i>Disabled</i> , the <i>No errors</i> , <i>No warnings</i> icon and the <i>No response from the switch</i> icon.
<b>Switch Alerts</b>	Displayed by default.  Key processing information about the network device that the plugin wants to bring to the attention of the CounterACT user. For a list of these plugin processing alerts, see <a href="#">Appendix 8: Switch Alerts</a> .
<b>Switch Hostname</b>	Switch name as defined in the managed switch.
<b>Switch Response Time</b>	Displayed by default.
<b>Vendor</b>	Displayed by default.  Switch vendor name.

Columns can be added to and removed from the **Switch** tab display.

**To add columns to and remove columns from the Switch tab:**

1. Right-click any **Switch** tab column header. A dropdown menu opens, which contains the following options: Add/Remove Columns, Remove Column and Best Fit Column.
2. Select **Add/Remove Columns**. The Add/Remove Columns dialog box opens.



3. Do any of the following:
  - a. From the **Add Columns** pane, select one or more column options you want to add to the **Switch** tab display and select **Add**. The **Selected Columns** pane is updated to reflect the added column selection(s).
  - b. From the **Selected Columns** pane, select one or more column options you want to remove from the **Switch** tab display and select **Remove**. The **Selected Columns** pane is updated to reflect the removed column selection(s).
4. Do any of the following:
  - a. Select **Apply**. The **Switch** tab display is updated with the added/removed column(s) and the Add/Remove Columns dialog box remains open.
  - b. Select **OK**. The Add/Remove Columns dialog box closes and the **Switch** tab display is updated with the added/removed column(s).

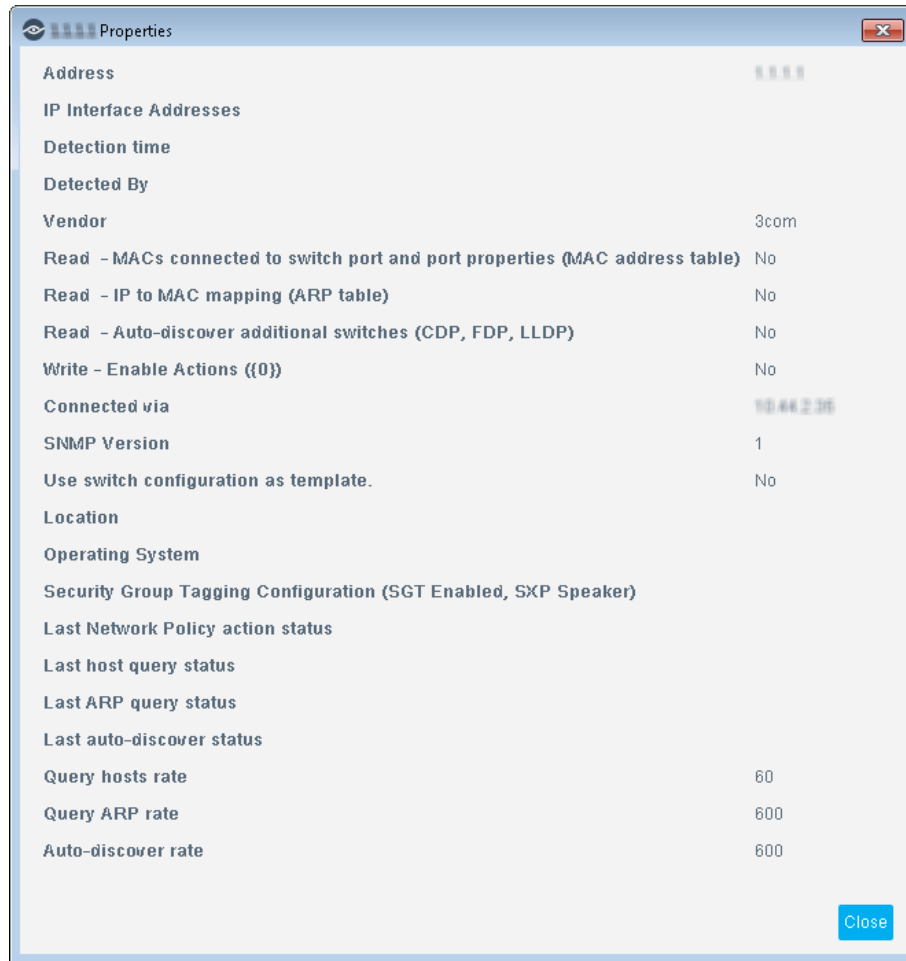
### Properties Dialog Box Display

For a network device that is selected in the **Switch** tab, you can display its **Properties** dialog box. The **Properties** dialog box provides the same information about the network device as does the **Switch** tab display.

#### To view the Properties dialog box details:

1. In the **Switch** tab, right-click an entry. A dropdown menu opens.
2. From the menu, select **Properties**. The **Properties** dialog box for the selected network device opens.





## Replicate Switch Configuration

The Switch Plugin provides three methods for copying switch configurations from one switch to another:

- [Duplicate Existing Switch](#)  
Copy the configuration of an existing switch to one or more new switches that you specify by IP address.
- [Use Switch Configuration as a Template](#)  
Copy the configuration of an existing switch to unmanaged switches that belong to the same SNMP community as they are detected.
- [Auto-Discovery – Discover Neighboring Switches](#)  
Copy the configuration of an existing switch to one or more neighboring unmanaged switches, discovered using an auto-discovery protocol.

## Duplicate Existing Switch Configuration

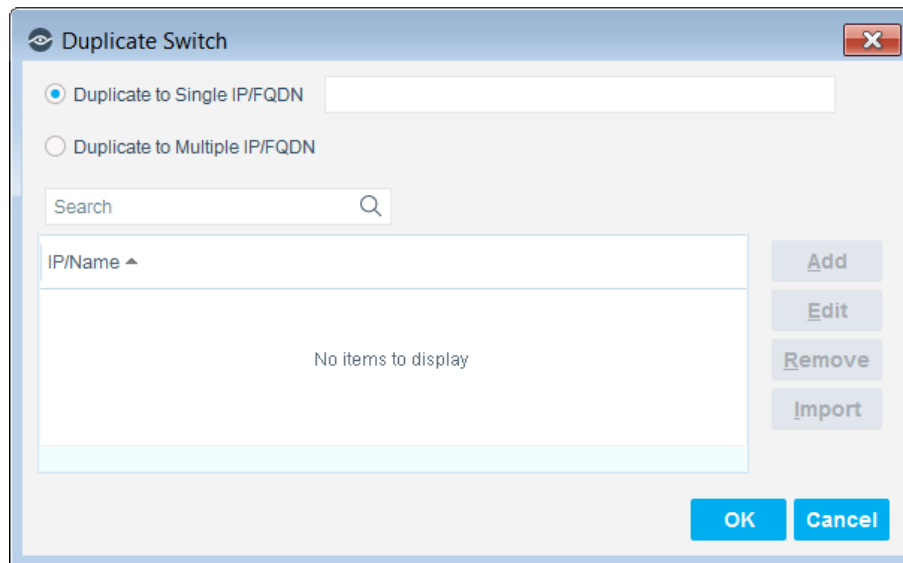
You can add one or more new switches to the Switch Plugin by copying the configuration of an existing switch to the new switches. You must provide the IP/FQDN of each new switch, which can be any of the following:

- An IPv4 address
- An FQDN
- An IPv6 address

Alternatively, you can import a list of IP/FQDN from a CSV file rather than having to manually enter them.

### To duplicate an existing switch:

1. Select **Options** from the **Tools** menu. The CounterACT Options window opens.
2. Select **Switch**. The Switch pane opens.
3. In the Switch tab, select a switch entry.
4. Select **Duplicate**. The Duplicate Switch dialog box opens.



### To make a single duplicate of a switch:

1. Select the **Duplicate to Single IP/FQDN** option (the default selection).
2. Enter the IP/FQDN of the new switch in the associated field.
3. Select **OK**.

The Edit Switch dialog box opens with the selected switch's parameters and the new switch's (read-only) IP/FQDN. All parameters can be edited.

4. Select **OK** to save the new switch.
5. Select **Apply** to add the new switch to the Switch Plugin configuration.

**To make multiple duplicates of a switch:**

1. Select the **Duplicate to Multiple IP/FQDN** option.

The **Add** and **Import** buttons are enabled.

2. Do one of the following:

- Select **Add** to add the IP/FQDN of the new switches one-by-one.
- Select **Import** to import a list of IP/FQDN from a CSV file.

3. Select **OK**.


The Edit Switch dialog box opens with the selected switch's parameters but no **Address** field. All parameters can be changed to a different value for all the new switches. (You can also edit individual switches after you have saved all the new switches.)

4. Select **OK** to save the new switches.


5. Select **Apply** to add the new switches to the Switch Plugin configuration.

## Use Switch Configuration as a Template

You can specify that a switch be used as a template for unmanaged switches that belong to the same SNMP community as the existing switch.

 *This feature does not support SNMPv3.*

When an unmanaged switch sends an SNMP trap, and the community string of the unmanaged switch matches the community string of the template switch, all of the template switch settings *including vendor* (except the IP address) are applied to the newly-detected switch. Switches detected in this manner are added to the Switch Plugin automatically and there is no need to restart the Switch Plugin.

 *It is strongly recommended that you use a different community for each switch vendor.*

**To specify that a switch is to be used as a template:**

1. In the General page/tab, select the **Use switch configuration as template** checkbox. See the [Use switch configuration as template](#) option description in the [General Configuration](#) section.

Since the plugin adds the unmanaged switch in the Approved (managed) state, prior to evaluating the addition of that switch, a delay is incorporated into plugin processing. This delay is used to ensure that the IP address of the unmanaged switch is not an additional IP address of a currently managed switch (additional IP addresses of currently managed switches display in the Console Switch tab **IP Interface Addresses** column). The processing delay is as follows:

- After the receipt of an SNMP trap from a switch and before the plugin begins evaluating the addition of that switch, 10 minutes have had to elapse since the most recent plugin start time. Only SNMP traps, received after that 10-minute period has elapsed, trigger plugin evaluation of a switch addition. The 10-minute period is the default period.

Modify this period, per Appliance, using the `config.add_by_template_delay.value` property in the `local.properties` file. To maintain the same Switch Plugin wait period throughout your entire CounterACT deployment, make sure to modify this wait period with the identical value in all your CounterACT devices.

## Auto-Discovery – Discover Neighboring Switches

You can configure a single switch and then rely on the Switch Plugin *auto-discovery* feature to detect neighboring switches. You can enable auto-discovery on these newly-discovered switches which can then discover their neighbors.

Plugin auto-discovery with switches of supported vendors is performed regardless of whether the plugin is configured to manage the switch using an IPv4 address, an FQDN or an IPv6 address. Switch Plugin auto-discovery is supported for the switches of the following vendors:

- Arista
- Avaya (Nortel)
- Brocade
- Cisco
- Enterasys
- H3C
- HPE - for switches running either a Comware operating system or a ProVision/ProCurve operating system

The Switch Plugin handles the CDP, FDP and LLDP discovery protocols, with the exception of CDP on a loopback interface of a switch. Switches use a specific discovery protocol.

- CDP, FDP and LLDP only support the discovery of neighboring switch IPv4 addresses.

For the discovery protocol in use by the switches of specific vendors, see [Appendix 1: See and Control Capabilities Summary](#).

Discovered switches inherit basic attributes of the switch that detected them, including the switch vendor, the CounterACT device managing the switch, CLI credentials and the SNMP version, settings and credentials. Read and write permissions, advanced settings and ACL configuration are not inherited and must be edited manually.

In order for the Switch Plugin to add a discovered switch as **Newly Discovered**, the switch must have the same SNMP community as the plugin-managed switch that discovered it.

Note that enabling newly discovered switches includes restarting the Switch Plugin.

By default, every switch enabled for auto-discovery runs auto-discovery every 10 minutes. This value can be changed on a per-switch basis, see [Read: Auto-discover additional switches \(CDP, FDP, LLDP\)](#). When a new switch is discovered, a

notification appears in the CounterACT Console, see [Notification of Auto-Discovered Switches](#).

During a failover scenario, the Switch Plugin auto-discovery feature is affected as follows:

- Managed Switch *Failover* to a *Recipient* Appliance: All neighboring switch devices that the Switch Plugin, on the *recipient* Appliance, learns about from the auto-discovery efforts of a failed-over managed switch device remain managed by the Switch Plugin on the *recipient* Appliance.
- Managed Switch *Failback* to the *Original* Appliance: When failback occurs, only the failed-over managed switch device is re-assigned back to the *original* Appliance.

For information about CounterACT *Failover Clustering* and the Switch Plugin, see [Failover Clustering Support](#).

### To auto-discover neighboring switches:

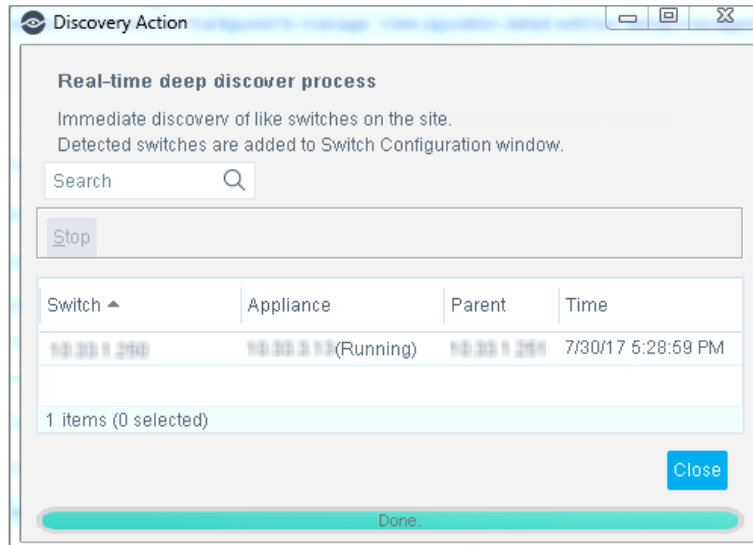
1. Select **Options** from the **Tools** menu. The CounterACT Options window opens.
2. Select **Switch**. The Switch pane opens.
3. In the Switch tab, select **Add** and configure a switch. Make sure that in the **Vendor** field of the General pane, you select a vendor that supports auto-discovery. See [Add Switches to the Switch Plugin](#).
4. In the Permissions pane, make sure to select **Read: Auto-discover additional switches (CDP, FDP, LLDP)**.
5. Select **Apply**.
6. Select the switch that you just added and then select **Discover**.

Status	Vendor	IP Address	Managed By	Detected By	Switch Alerts	Detected	Switch Response Time	Is Template	
Disabled	3COM	10.44.2.35	10.44.2.35(Running)		Disabled	Manual		No	Apply
Disabled	Avaya/Nor...	10.44.2.35	10.44.2.35(Running)		Disabled	Manual		No	Edit
Disabled	3COM	10.44.2.35	10.44.2.35(Running)			Manual	Unknown	No	Remove
									Duplicate
									Discover

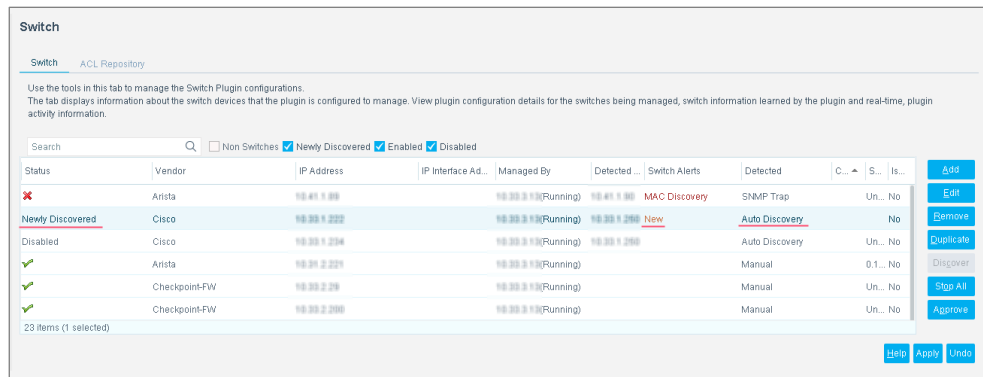
A confirmation dialog opens.

7. Select **Yes**.

The Discovery Action dialog box opens. Neighboring switches are displayed in the dialog box as they are discovered. If no switches are discovered, **No items to display** is displayed in the Discovery Action dialog box.



8. Select **Close**.
9. The **Status**, **Switch Alert** and **Detected** fields in the Switch tab indicate that unmanaged switches have been auto-discovered.



If no switches were discovered, an **Information** icon is displayed in the **Status** field.

Status	Vendor	IP Address	Managed By	Switch Alerts	Detected
	Avaya/Nortel	10.30.1.260	10.30.3.13(Initializing)	Auto Discovery	Manual
<div style="background-color: yellow; padding: 5px;"> <b>No errors</b>  <b>No warnings</b>  <b>Information</b>  <u>No switches detected</u>                      Press 'F2' for focus                 </div>	Cisco	10.30.1.260	10.30.3.13(Initializing)		Manual
	Router-Linux	10.30.1.262	10.30.3.13(Initializing)		Manual
	Cisco	10.30.1.260	10.30.2.11(Running)	Not a switch	SNMP Trap
	Checkpoint-FW	10.30.2.29	10.30.3.13(Initializing)		Manual

10. Select a newly-discovered switch and then select **Edit**.
11. Configure the switch. See [Edit Switch Configurations in the Plugin](#).
  - a. Enable the auto-discovery feature. See [Read: Auto-discover additional switches \(CDP, FDP, LLDP\)](#).
  - b. Enable desired read and write permissions. See [Permissions Configuration](#).
  - c. For switches using ACL, enable and configure ACL in the **ACL** tab of the Edit Switch window. See [Edit Switch Configurations in the Plugin](#).
12. Select **Approve** to approve Switch Plugin management of the newly/auto-discovered switch.

Status	Vendor	IP Address	IP Interface Ad...	Managed By	Detected ...	Switch Alerts	Detected	C...	S...	Is...
<span style="color: red;">✘</span>	Arista	10.41.1.88	10.30.0.13(Running)	10.41.1.88	MAC Discovery	SNMP Trap	Un...	No		
Newly Discovered	Cisco	10.30.1.222	10.30.0.13(Running)	10.30.1.200	New	Auto Discovery	Un...	No		
Disabled	Cisco	10.30.1.204	10.30.0.13(Running)	10.30.1.200		Auto Discovery	Un...	No		
<span style="color: green;">✔</span>	Arista	10.31.2.221	10.30.0.13(Running)			Manual	0.1...	No		
<span style="color: green;">✔</span>	Checkpoint-FW	10.30.2.29	10.30.0.13(Running)			Manual	Un...	No		
<span style="color: green;">✔</span>	Checkpoint-FW	10.30.2.200	10.30.0.13(Running)			Manual	Un...	No		

The status of the switch changes from **Newly Discovered** to **Disabled**.

13. Repeat the preceding three steps for each switch that you want to approve.
14. After you have approved and edited all the discovered switches, select **Apply**.  
The status of each switch is updated to ✔ (Enabled) when read and write permissions are successfully assigned.

## Notification of Auto-Discovered Switches

Every switch enabled for auto-discovery periodically runs auto-discovery. When a switch detects a new switch via the auto-discovery feature, the Switch Plugin notifies the CounterACT Console and a **New Switch Detected** icon appears in the Console status bar. Click the icon to open the Switch tab and configure the switch.



New Switch Indicator

Once you open the Switch tab, the icon is removed from the status bar.

## Non-Switch Devices

Occasionally devices other than switches may be discovered and added to the switch list, for example, wireless access points or routers. You can change the status of these devices to **Not a switch**. Use the *Non Switches* filter at the top of the Switch tab to hide and display these devices.

**To define the status of a device as *Not a switch*:**

1. Right-click the newly-discovered device and select **Not a switch**.

The status of the switch changes to .

**To hide or display non-switch devices:**

1. Select or clear **Non Switches** in the Switch tab.

Status	Vendor	IP Address	Managed By	Detected By	Switch Alerts	Detected	Switch Response Time	Is Template	
Disabled	3COM	1.1.1.1	10.44.2.35(Running)		Disabled	Manual		No	Add Edit Remove Duplicate Discover
Disabled	AvayaNor...	12.21.221.1	10.44.2.35(Running)		Disabled	Manual		No	
Disabled	3COM	10.0.0.0	10.44.2.35(Running)			Manual	Unknown	No	

**To redefine a non-switch device as a switch:**

1. Display non-switch devices by selecting **Non Switches**.
2. Right-click a non-switch device and select **Approve**.

## Duplicate Switch Restrictions

The Switch Plugin does not allow CounterACT users to approve any *Newly Discovered* switch device that the plugin designated as a duplicate switch device. The duplicate switch designation pertains whenever the IP address of that *Newly Discovered* switch device is known to the plugin as an *additional IP address* of a currently managed switch. Additional IP addresses of a currently managed switch display in the Switch tab **IP Interface Addresses** column of that managed switch. When the plugin identifies a *Newly Discovered* switch device to be a duplicate switch device, it displays the alert *Duplicate Switch* in the **Switch Alerts** column of the Switch tab. For each such alert, the plugin provides the associated tooltip *This switch is a duplicate of switch <IP address>*.

The Console restricts the CounterACT user from completing any of the following related activities in the Switch tab:

- Select for approval/double-click on a newly discovered, duplicate switch device.
- Attempt to define a new switch that the plugin identifies to be a duplicate switch device.
- Selects for approval multiple, newly discovered, duplicate switch devices.

The plugin notifies the CounterACT user of the activity restriction with the display of an error message.



# Working with Switch Information at the CounterACT Console

This section introduces how to view and use switch information at the CounterACT Console. The following topics are described:

- [Viewing Switch Information in the All Hosts Pane](#)
- [CounterACT Policies](#)
- [Clear ACLs from All Switch Ports](#)

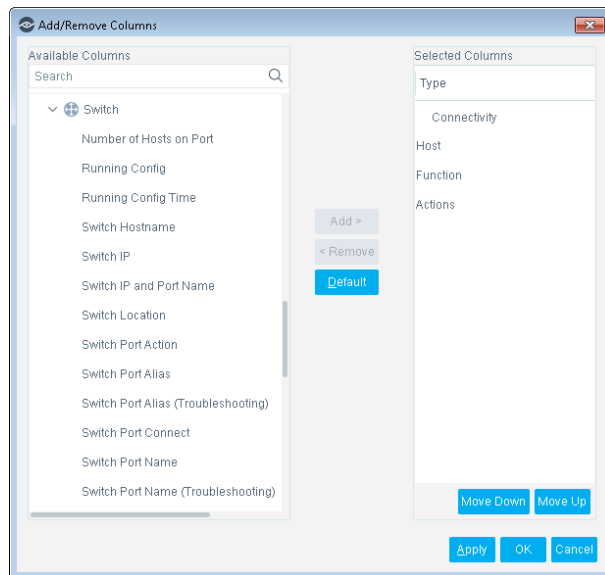
More detailed information about these topics is provided in the *Working at the CounterACT Console* chapter of the *CounterACT Administration Guide*.

## Viewing Switch Information in the All Hosts Pane

In the Console, view information obtained by the plugin in the All Hosts pane.

### To display switch information:

1. In the **All Hosts** pane, right-click a table column and select **Add/Remove Columns**. The **Add/Remove Columns** window opens.



2. In the **Available Columns** pane, select switch-related items. This information appears in the **All Hosts** pane of the Console.

The screenshot displays the ForeScout interface. At the top, there are navigation tabs for Home, Asset Inventory, and Policy. The main area is titled 'All Hosts' and shows a table of host information. The table has columns for Host, Host IP, MAC Address, Switch Port Name, and Switch IP and Port Name. One host is selected, and its profile is shown below the table. The profile includes a search bar and a 'General' section with the following details:

Category	Property	Value
General	IPv4 Address:	10.33.1.233
Network Access	Admission:	Offline host became online
More	Linux Manageable (SecureConnector):	No
	MAC Address:	58ac7803f2d0
	NIC Vendor:	CISCO SYSTEMS, INC
	Nmap-Banner (Ver. 5.3):	22/tcp Cisco SSH 1.25 protocol 1.5 23/tcp Cisco router 80/tcp Cisco IOS http config 23/tcp Cisco IOS telnetd
	OS Class (Obsolete):	Cisco
	OS Fingerprint:	22/tcp Cisco SSH 1.25 protocol 1.5;23/tcp Cisco router

In the **All Hosts** pane, the **IPv6 Address** column displays the additional IP addresses of an entry that are IPv6 addresses, for both plugin managed switch entries and detected/connected endpoint entries. The **IPv6 Address** column does not display by default; select **Add/Remove Columns > Available Columns** pane > **Properties > Device Information** and add this column to the pane's display.

## View Information in the Profile Tab

The **Profile** tab contains detailed information about the switch connection of a detected endpoint.

**Host Details**

Profile Compliance All Policies Policy Actions

IPv4 Address: 10.33.1.250 Function: Router or Switch  
 MAC Address: 88ae780300d0 Operating System: Cisco IOS  
 Vendor and Model: Cisco Router or Switch

Search [Q] [^] [v]

NIC Vendor:		CISCO SYSTEMS, INC
Number of Hosts on Port:		4
Switch IP:	+	10.33.1.250
Switch IP and Port Name:	+	10.33.1.250 Fa2/3
Switch Location:	+	QA-LAB
Switch Port ACL:	+	
Switch Port Action:		None
Switch Port Alias:	+	_QA_Net_Eth
Switch Port Connect:		Connected
Switch Port Name:	+	Fa2/3
Switch Port PoE Connected Device:	+	N/A
Switch Port PoE Power Consumption:		0
Switch Port VLAN:		331
Switch Port VLAN Name:	+	VLAN0331
Switch Port Voice Device:		No
Switch Vendor:	+	Cisco
Switch VoIP Port:		No
WLAN Client Connectivity Status:		No
<b>More</b>		
Switch Hostname:	+	CAT#4506>SAP.dom33.la
Switch OS:	+	Cisco IOS Software, Cataly

### To display the Profile tab:

1. In the Console, navigate to the **Home** tab.
2. In the **All Hosts** pane, double-click a detected endpoint.

The **Host Details** window of the selected endpoint opens.

3. In the window, select the **Profile** tab.

Much of the switch connection detail for a detected endpoint is provided by resolved switch properties. For a description of these properties, see [Switch Properties](#).

In addition to the resolved switch property information, other switch connection detail about a selected endpoint is provided in the tab and described in the following sections.

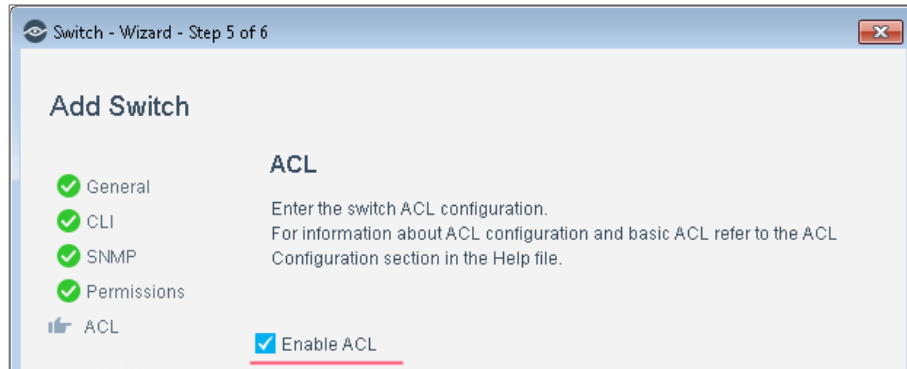
### Switch Port Host ACL Locations – Candidates

This entry lists all the switch ports that the detected endpoint is connected to. This information is taken from the MAC table of each switch in which the endpoint is

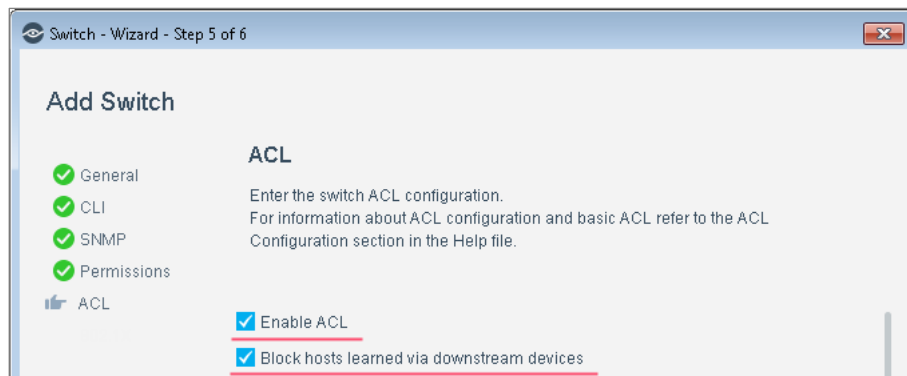
recorded (all identified instances of layer 2 forwarding information to the detected endpoint). Information provided in the following format:

`<switch IP address>:<card model><card #>/<port #>`

- If the access port is known *and* **Enable ACL** is configured for the switch, the entry lists the switch IP address and access port.



- If the access port is not known *and* both **Enable ACL** and **Block hosts learned via downstream devices** are configured for the switch, the entry lists any trunk ports.



The entry lists more than one candidate if there is more than one eligible trunk port.

```
10.33.1.222:Fa0/2
10.33.1.250:Fa0/2
```

### Switch Port Host ACL Locations – Enforced


This entry lists all the switch ports that the detected endpoint is connected to and that have an ACL applied to the port. This information is provided in the following format:

`<switch_IP_address>:<card_model><card_#>/<port_#>:<ACL_name>`

## Endpoints Connected to a Brocade Switch Port VLAN with Virtual Routing Interface

For a detected endpoint that is connected to a Brocade switch port VLAN and that VLAN is configured with a virtual routing interface, be aware of the following atypical, switch connection detail in the **Profile** tab display of such an endpoint:

- The **Switch IP/FQDN and Port Name** property - contains either the IP address or the fully qualified domain name of the switch and the port name (the physical Ethernet interface information of the port). This is expected.
- The **Switch Port Host ACL Locations - Candidates** property - contains the VLAN/virtual routing interface information of the port. This is *atypical*.
- After plugin application of the *Endpoint Address ACL* action on such a detected endpoint, the **Switch Port Host ACL Locations - Enforced** property - contains the VLAN/virtual routing interface information of the port. This is *atypical*.

 *To display switch information details about a Brocade switch port VLAN that is configured with a virtual routing interface, the network administrator must run, on the Brocade switch device, the **show running config** command specifying the port VLAN/virtual routing interface.*

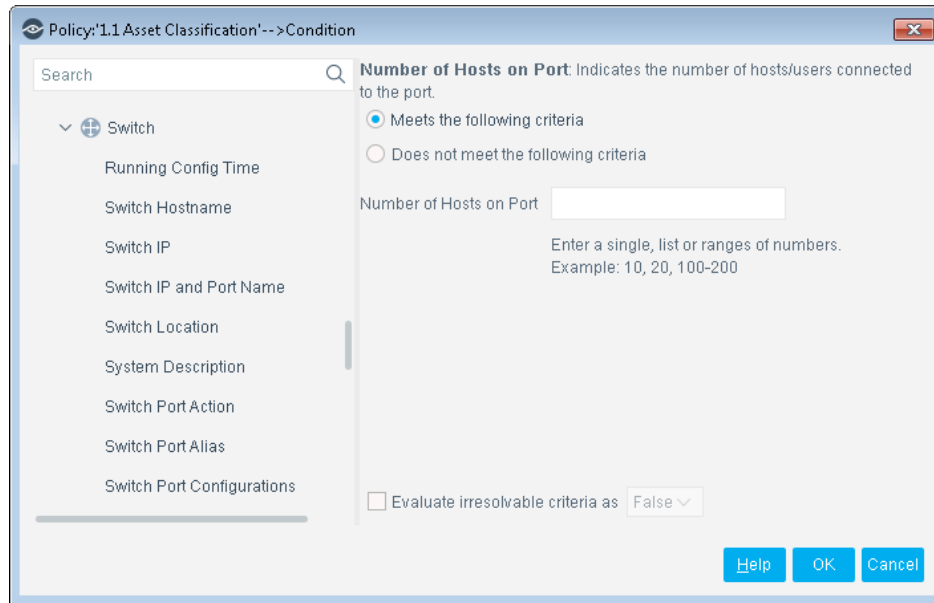
## CounterACT Policies

Use CounterACT policy tools to monitor and control endpoints that are connected to switches. The following topics are described:

- [Switch Properties](#)
- [Restrict Actions](#)
- [Remediate Actions](#)
- [Detect and Ignore Switch Virtual Interfaces](#)

## Switch Properties

You can create a policy that applies to endpoints that are connected to a specific managed switch by specifying the switch's properties.



The Switch Plugin detects switch information according to the criteria you specify when defining a policy rule. The following tables describe the policy properties to use with the Switch Plugin:

- [Basic Switch Properties](#)
- [Network Device Compliance Properties](#)
- [Switch Track Changes Properties](#)

### Basic Switch Properties

The following policy properties resolve basic information about a managed switch:

Property	Description
<b>Number of Hosts on Port</b>	The number of endpoints connected to a specific port. You can write a condition for this number to instruct the Switch Plugin to detect ports with more than one endpoint (MAC address) if, for example, a hub and a guest computer have been connected together with a company endpoint on a company switch port. Ports connecting between switches are excluded from this calculation.
<b>SGT</b>	The Security Group Tag (SGT) assigned to an endpoint. An SGT is a number in the range of 1 - 65,535. Endpoints with an assigned SGT are connected to a managed Cisco switch in a Cisco TrustSec domain. When the property is currently included in existing policies and the advanced configuration flag <b>assign_sgt</b> is disabled, the property is marked as <b>Obsolete</b> in the relevant policies. For details about this flag, see <a href="#">Advanced configuration flags, Enable a Feature</a> .
<b>Switch Hostname</b>	The switch name as defined in the managed switch.

Property	Description
<b>Switch IP/FQDN</b>	Either the IP address or the fully qualified domain name of the switch.
<b>Switch IP/FQDN and Port Name</b>	Either the IP address or the fully qualified domain name of the switch and the port name (the physical Ethernet interface information of the port). The format is <code>&lt;IP address/FQDN&gt;: &lt;port&gt;</code> .
<b>Switch Location</b>	The switch location based on the switch MIB.
<b>Switch OS</b>	The operating system of the switch device to which the endpoint is connected.
<b>Switch Port ACL</b>	The name of the ACL applied to the switch port.
<b>Switch Port Action</b>	The actions ( <i>Blocked</i> or <i>Assign to VLAN</i> ) that are assigned to the switch port.
<b>Switch Port Alias</b>	The description of the port as defined in the switch configuration and modified by the Switch Plugin.
<b>Switch Port Configurations</b>	<p><i>For use with Cisco and Arista devices only.</i></p> <p>The configuration detail of the switch interface to which an endpoint is connected.</p> <p>For this property to be resolvable, the Switch Plugin must be configured to use CLI to learn the endpoints that are connected to the managed switch. See Permissions Configuration, <a href="#">MAC Read/Write Method</a>.</p>
<b>Switch Port Connect</b>	The physical connectivity between the endpoint and the switch port.
<b>Switch Port PoE Connected Device</b>	<p><i>For use with Cisco devices only.</i></p> <p>Description of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed Cisco switch. For example, Cisco IP Phone 6921.</p>
<b>Switch Port PoE Power Consumption</b>	<p><i>For use with Cisco devices only.</i></p> <p>Power consumption of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed Cisco switch. The power consumption value provided is in milliwatts (mW). For example, 750.</p> <p>When either a non-PoE device or no device is connected to the PoE-enabled switch port, the property value is zero (0).</p> <p>For switch vendors that the plugin does not support switch port PoE, the Console displays the following information for this property: <i>Vendor is currently not supported for this property.</i></p>
<b>Switch Port Name</b>	The hard-coded port name.
<b>Switch Port VLAN</b>	The VLAN associated with the switch port.
<b>Switch Port VLAN Name</b>	The name of the VLAN associated with the switch port.
<b>Switch Port Voice Device</b>	Whether the endpoint connected to the switch port is a VoIP device.

Property	Description
<b>Switch Port Voice VLAN</b>	The switch port VLAN to which the VoIP endpoint is connected.
<b>Switch Vendor</b>	The switch vendor name.
<b>Switch Virtual Interface</b>	Identifies whether the switch interface is a Switch Virtual Interface or not. The property is supported for managed switches only.
<b>Switch VoIP Port</b>	Whether the switch port is a VoIP port.
<b>System Description</b>	Detects the system description information provided by the managed device. System description information is as specified by the network device SNMPv2-MIB property <code>sysDescr (1.3.6.1.2.1.1.1)</code> .

### Network Device Compliance Properties

For any Cisco network device managed by the Switch Plugin, use the following policy properties to create policies that determine network device compliance:

Property	Description
<b>Running Config</b>	<p><i>For use with Cisco devices only.</i></p> <p>Detects <i>running config</i> information of switches managed by CounterACT, as generated by the <b>show running-config</b> command.</p> <p>The Switch Plugin resolves this property for information at the following instances: (a) After plugin start and initially detecting the switch and (b) Whenever <i>running config</i> information changes.</p> <p>Before working with this property, several configuration tasks must be performed.</p> <p>As the amount of information provided by the resolved Running Config property can be very extensive, you can filter this information.</p> <p>See <a href="#">Appendix 5: Using Network Device Compliance Policies</a>.</p>
<b>Running Config Time</b>	<p><i>For use with Cisco devices only.</i></p> <p>Contains the timestamp, MM/DD/YY HH:MM:SS AM/PM, of the plugin's <i>running config</i> information query of the device.</p> <p>Before working with this property, several configuration tasks must be performed. See <a href="#">Appendix 5: Using Network Device Compliance Policies</a>.</p>



Property	Description
<b>Interface Table</b>	<p><i>For use with Cisco devices only.</i></p> <p>Detects the specific interface configuration provided in a device <i>running config</i> for the interface.</p> <p>Per interface, the resolved property provides the following information:</p> <ul style="list-style-type: none"> <li>▪ Interface Name - The interface name and when available the interface location information.</li> <li>▪ Interface Configuration (raw) - the specific, interface configuration, as provided in a device <i>running config</i>.</li> </ul> <p>Before working with this property, several configuration tasks must be performed. See <a href="#">Appendix 5: Using Network Device Compliance Policies</a>.</p>

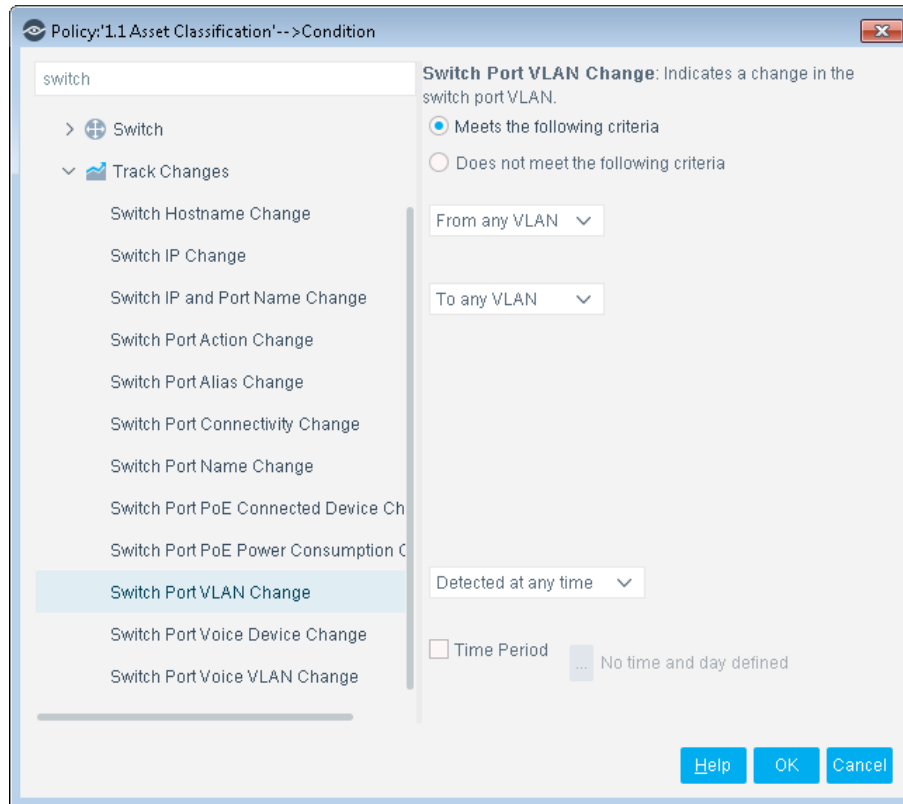
Network device compliance properties are only resolved for a managed switch's **Host IP** address and not for any of the managed switch's entries having an IP Interface Address. (**IP Interface Address** was formerly termed **More IPs** in the Console).

Instead, the Console handles network device compliance property information for switch entries whose **Host IP** address is an IP Interface Address in the following manner:

- A property value of **N/A** is displayed.
- Next to the property value, the following informational message is available:  
*Address <IP\_Interface\_Address> is an **IP Interface Address** for host <Primary\_IP\_Address>. To view network compliance property values for this host, select Host IP <Primary\_IP\_address> in the **All Hosts** pane (above).*

### Switch Track Changes Properties

*Track Changes* properties check whether a property value has changed. For each *Track Changes* property there is an equivalent property in the *Switch* folder that checks values of the property. For example, there is a *Switch Port VLAN Change* property in the *Track Changes* folder and a *Switch Port VLAN* property in the *Switch* folder.



Policy change properties to use with the Switch Plugin are described in the following table:

Property	Description
<b>SGT Change</b>	Identifies a change in an endpoint's assigned Security Group Tag (SGT). An SGT is a number in the range of 1 - 65,535. Endpoints with an assigned SGT are connected to managed Cisco switch in a Cisco TrustSec domain.
<b>Switch Hostname Change</b>	Identifies a change in the switch name that is defined in the managed switch.
<b>Switch IP/FQDN and Port Name Change</b>	Identifies that a change in value occurred in the <b>Switch IP/FQDN and Port Name</b> property.
<b>Switch IP/FQDN Change</b>	Identifies that a change in value occurred in the <b>Switch IP/FQDN</b> property.
<b>Switch Port ACL Change</b>	Identifies a change in the name of the ACL applied to the switch port.
<b>Switch Port Action Change</b>	Whether any actions ( <i>Blocked</i> or <i>Assign to VLAN</i> ) that are assigned to the switch port have changed.
<b>Switch Port Alias Change</b>	Whether the description of the port (as defined in the switch configuration and modified by the Switch Plugin) has changed.
<b>Switch Port Connectivity Change</b>	Whether the physical connectivity between the endpoint and the switch port has changed.

Property	Description
<b>Switch Port Name Change</b>	Whether the hard-coded port name has changed.
<b>Switch Port PoE Connected Device Change</b>	<i>For use with Cisco devices only.</i> Identifies a change in PoE device that is connected to the PoE-enabled switch port.
<b>Switch Port PoE Power Consumption Change</b>	<i>For use with Cisco devices only.</i> Identifies a change in power consumption of the PoE device that is connected to the PoE-enabled switch port.
<b>Switch Port VLAN Change</b>	Whether the VLAN associated with the switch port has changed.
<b>Switch Port Voice Device Change</b>	Whether the device type of the endpoint connected to the switch port has changed between VoIP and non-VoIP.
<b>Switch Port Voice VLAN Change</b>	Whether the switch port VLAN to which the VoIP endpoint is connected has changed.
<b>Switch Running Config Change</b>	<i>For use with Cisco devices only.</i> Detects <i>running config</i> information changes in the device. Before working with this property, several configuration tasks must be performed. See <a href="#">Appendix 5: Using Network Device Compliance Policies</a> .

## Restrict Actions

This section provides an overview of the CounterACT **Restrict** actions available with the Switch Plugin.

During a failover scenario, applied switch restrict actions continue to be applied as part of failover and failback operation. For information about CounterACT *Failover Clustering* and the Switch Plugin, see [Failover Clustering Support](#).

- 📄 *There might be occurrences during failover and failback operation, in which an applied, switch restrict action is temporarily cancelled by the Switch Plugin. However, as soon as CounterACT re-discovers and re-evaluates the affected endpoints, the Switch Plugin re-applies the action that was in effect at failover/failback on the endpoints, as necessary.*

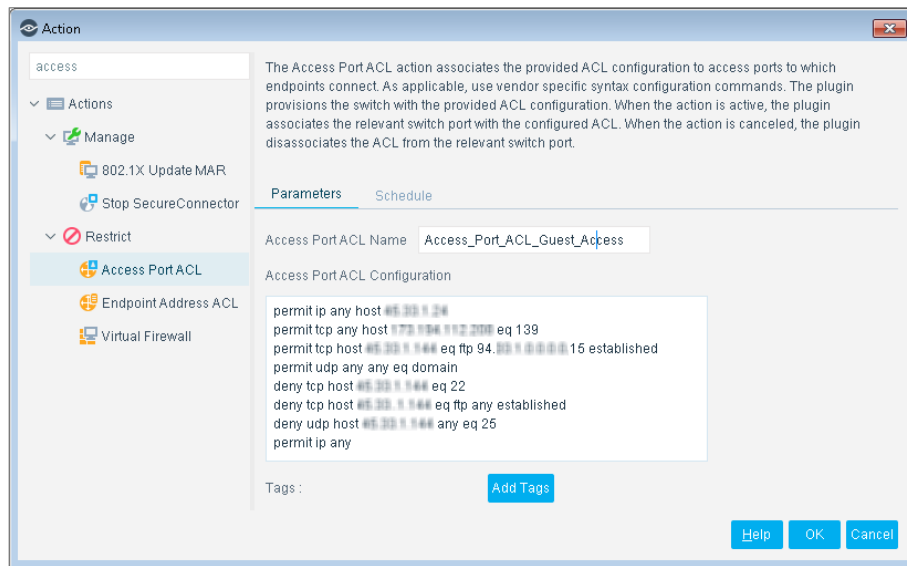
The following restrict actions are available:

- [Access Port ACL](#)
- [Assign Security Group Tag](#)
- [Assign to VLAN](#)
- [Endpoint Address ACL](#)
- [Switch Block](#)

## Access Port ACL

Use the *Access Port ACL* action to define an ACL that addresses one or more than one access control scenario, which is then applied to an endpoint's switch access port. Access control scenarios are typically role or classification driven, for example, registered guest or compliance, and **not endpoint IP specific**. For example, implement an ACL action that denies corporate network access to guests but permits Internet access, regardless of endpoint IP address (no IP address dependency).

In the ACL configuration, take advantage of the full set of switch capabilities. CounterACT does not inspect and does not alter the provided content; the plugin's role is one of delivery vehicle to provision a network switch.



For plugin IPv6 support exceptions with ACL-related functionality, see [IPv6 Support](#).

In the action's Parameters tab, do:

1. Specify the rules that an *Access Port ACL* action applies on a switch access port using one of the following methods:
  - **Select from ACL Repository:** Select this option and then choose from the drop-down list an ACL from the ACL Repository. This option is the default selection for the action.
  - **Define ACL Name:** Select this option and enter an ACL name in the associated field. Then, in the **Define ACL Rules** text box, define one or more rules.

*When defining an Access Port ACL, you must follow the switch's rules about valid ACL name and ACL rule content.* For example, if syntax, not supported by the switch device, is used in an ACL rule, such that this rule cannot be added to the switch access list, then including this rule will result in a plugin failure to write the associated access list on the switch. Hence, using unsupported rule syntax must be avoided.

When you provide rules in the **Define ACL Rules** text box, then, as part of plugin application of this ACL, the plugin automatically adds **lead rule 0** to the applied ACL. *Lead rule 0* is always added on the switch before all other provided rules. No explicit user action is required. The addition of

*lead rule 0* ensures that the managing CounterACT device is *always* able to communicate, via CLI, with its managed switches.

Lead Rule 0:

```
permit tcp host <managing CounterACT IP address> host <managed  
switch IP address> eq <configured CLI connection type>
```

where the value of `eq` is either:

- > 22, when the plugin's configured CLI connection type is **SSH**
- > 23, when the plugin's configured CLI connection type is **Telnet**

2. Use the **ACL Action Priority** field to assign a priority to the *Access Port ACL* action being defined. The range of valid field values is 1 - 100 with 1 being the highest priority and 100 being the lowest priority. The default value of this field is 1.

The Switch Plugin uses the assigned priority of an *Access Port ACL* action when deciding between two *Access Port ACL* actions, in the following situation:

When two endpoints are connected to the same port and the Switch Plugin must determine which one of the two *Access Port ACL* actions must be applied on the port.

Keep the *Access Port ACL* action that is currently applied on the switch port or replace it with another *Access Port ACL* action, which CounterACT currently requested the plugin to apply on the switch port.

An example of this situation is a switch port having both a connected VoIP device and an endpoint connected to the VoIP device.

To decide between the two *Access Port ACL* actions, the plugin takes the following action(s):

- a. Compares their assigned **ACL Action Priority**. The *Access Port ACL* action having the higher priority takes precedence and is the action that the plugin applies/maintains on the switch port.
- b. When the two *Access Port ACL* actions have the same **ACL Action Priority**, the plugin then compares their action timestamp. The *Access Port ACL* action having the more recent action timestamp takes precedence and is the action that the plugin applies/maintains on the switch port.

If the plugin determines:

- That the currently applied *Access Port ACL* action must be kept on the switch port, then the requested-to-be-applied *Access Port ACL* action fails and the appropriate error message is issued for the action failure.
- That the currently applied *Access Port ACL* action must be replaced on the switch port by the requested-to-be-applied *Access Port ACL* action, then the currently applied *Access Port ACL* action fails and the appropriate error message is issued for the action failure.

At any given time, only one ACL action, either the *Access Port ACL* action or the *Endpoint Address ACL* action, can be enabled for use. To switch between the enablement of these two actions, see the procedure in [acl\\_action\\_type](#).

For the ACL capabilities that are available to use with the Switch Plugin for supported, vendor switches, see Appendix 6, section [Switch Vendor ACL Support](#).

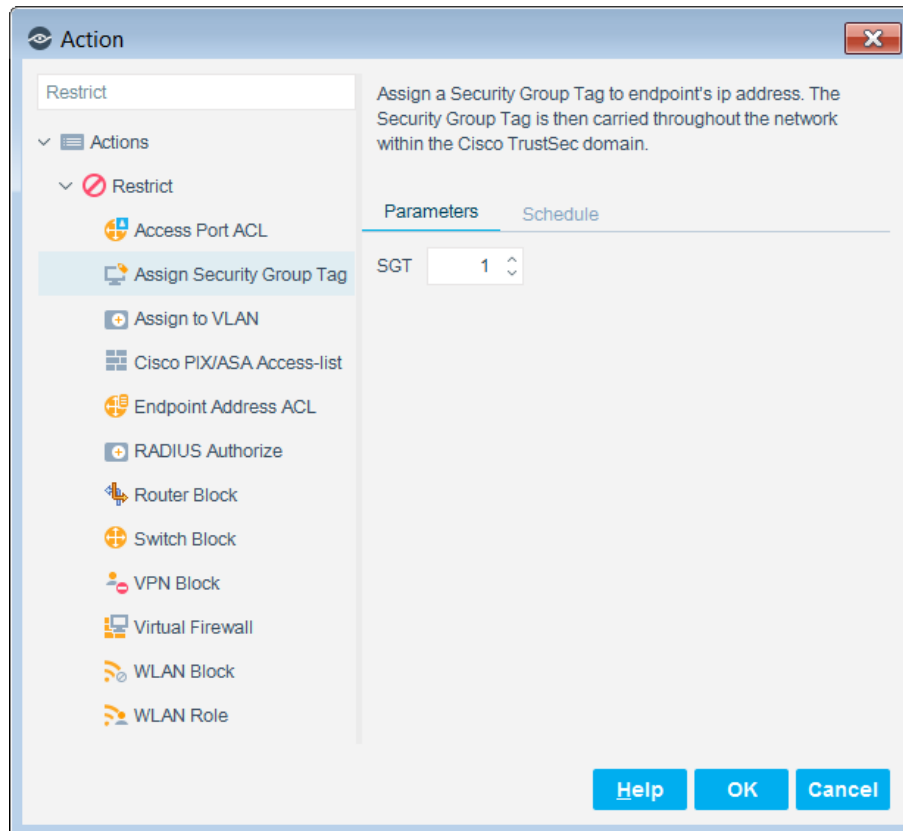
- 📄 *Switch Plugin Garbage Collection: By default, once an hour, the plugin releases from a switch those Access Port ACLs that are not in use because the Access Port ACL action has been canceled for the relevant endpoint. Per endpoint, the operation removes the Access Port ACL from the specific port (the access group). To modify the default, removal period, contact customer support at [support@forescout.com](mailto:support@forescout.com).*

### Assign Security Group Tag

Use the *Assign Security Group Tag* action to assign a Security Group Tag (SGT) to CounterACT-detected endpoints. Endpoints with an assigned SGT are connected to a managed Cisco switch in a Cisco TrustSec domain. An SGT is a number in the range of 1 - 65,535.

- 📄 *There might be Cisco switches that accept a lower number for the maximum SGT, for example, 65,533 or 65,519. Prior to using the Assign Security Group Tag action, make sure to verify the SGT range accepted by the managed Cisco switches in your organization's Cisco TrustSec domain.*

For an overview of Switch Plugin support of the Security Group Tagging functionality of a Cisco TrustSec domain, see [Security Group Tagging Configuration](#).



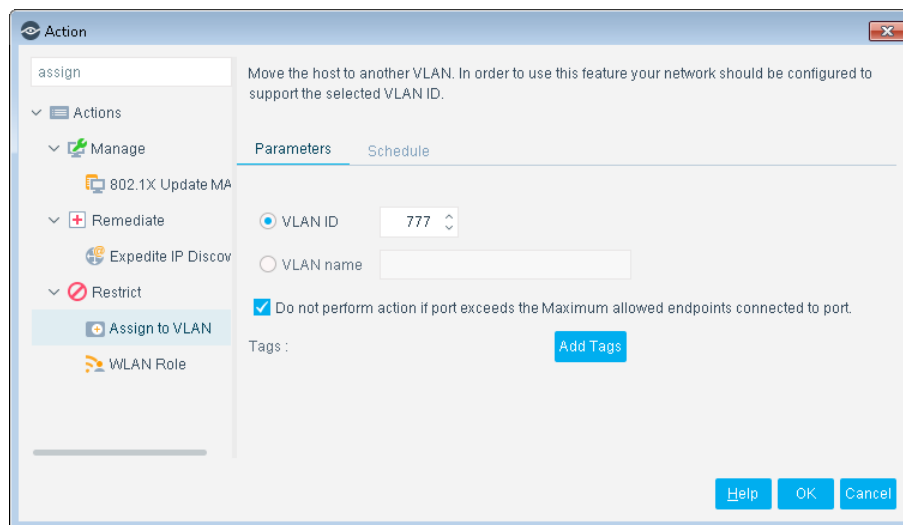
When the *Assign Security Group Tag* action is currently included in existing policies and the advanced configuration flag `assign_sgt` is disabled, the action is marked as **Obsolete** in the relevant policies. For details about this flag, see [Advanced configuration flags](#), [Enable a Feature](#).

The applied *Assign Security Group Tag* action can be canceled for CounterACT-detected endpoints. Action cancellation is accomplished either

- Manually - in the **Home** tab > **All Hosts** pane > right-click an applicable endpoint entry > **Cancel Actions** > select *Undo Security Group Tag Assignment*.
- By policy evaluation - when CounterACT-detected endpoints no longer match the policy condition associated with the applied action.

## Assign to VLAN

Use the *Assign to VLAN* action to assign endpoints to a VLAN, rather than turning off their switch ports. This enables secured remote connection to endpoints for the purpose of deploying patches, but still prevents the propagation of unwanted traffic to other sections of the network.



### General Considerations for Action Use

When the Switch Plugin applies the *Assign to VLAN* action using a VLAN that is tagged on the port, the VLAN becomes untagged on the port. This behavior does not impair *Assign to VLAN* functionality; when the applied *Assign to VLAN* action is cancelled, the untagged VLAN is deleted from the port.

- For the *Assign to VLAN* action, ForeScout recommends to avoid the use of a VLAN that either is or might be tagged on a port to which endpoints are connected. Use of a tagged VLAN that is the port's voice VLAN causes the *Assign to VLAN* action to fail.

The plugin does not support the application of the *Assign to VLAN* action in the following scenarios:

- For a VoIP device, if there is a VoIP device between the switch and the endpoint (a VoIP port with a connected VoIP phone and a connected PC

behind the phone). The *Assign to VLAN* action is, however, supported for the endpoint and requires that either one of the following is in effect:

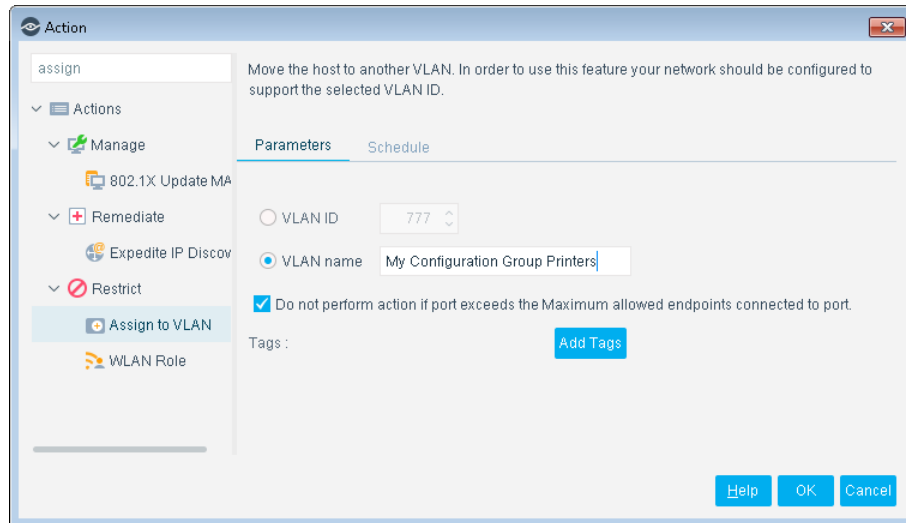
- SecureConnector is installed in the endpoint.
  - The global switch VoIP port protection is overridden. See [Global Configuration Options for the Switch Plugin](#).
- For detected endpoints that are connected to trunk ports.
    - 📄 *Plugin detection of endpoints connected to trunk ports requires that the option **Detect endpoints connected to trunk ports** is enabled for plugin management of the specific switch.*

See [Appendix 3: Setting Up a VLAN](#) for details about how to create an isolated VLAN with secured access.

#### *Switch-Specific Considerations for Action Use*

- With managed Alcatel switches, do not use VLAN 1 with the *Assign to VLAN* action. The switch does not allow endpoint assignments to the VLAN 1 of general ports.
- With managed Comtec, DASAN and ExtremeXOS switches, using the *Assign to VLAN* action requires that both CLI and SNMP credentials are configured and have write permission. This requirement is due the fact that for these switches the plugin uses both CLI (assign port) and SNMP (bounce port) to perform the action.
- With managed H3C switches, when the plugin uses CLI to perform the *Assign to VLAN* action, be aware that as part of completing the *Assign to VLAN* action, the plugin uses SNMP to bounce the port on the switch. Therefore, ensure that the SNMP community, used by the plugin, is configured on the switch with read/write capability.
- With managed Huawei switches:
  - If the plugin is configured to use CLI communication, the plugin applies the *Assign to VLAN* action using CLI.
  - As part of completing the *Assign to VLAN* action, the plugin uses SNMP to bounce the port on the switch. Therefore, ensure that the SNMP community, used by the plugin, is configured on the switch with read/write capability.
  - When the plugin applies the *Assign to VLAN* action using CLI, then in order for the plugin to bounce Huawei hybrid PoE (Power over Ethernet) ports, as part of completing the *Assign to VLAN* action on endpoints connected to such ports, the configuration flag `cli_hybrid_port_bounce_poe` must be enabled. For details about enabling this flag, see [Appendix 2: Troubleshooting, Workarounds and Feature Functionality Support](#).
- With managed Juniper EX switches, if the **Assign to VLAN by configuration group assignment** checkbox is enabled in the Switch Advanced Settings window, specify the configuration group to which endpoints are assigned, as follows:
  - In the **VLAN name** field of the *Assign to VLAN* action, enter the configuration group name.





- With a managed 3COM switch model 4400, when the Switch Plugin applies the *Assign to VLAN* action on endpoints connected to this switch model, there is a difficulty to attain electrical shut down of the newly assigned ports as part of the bounce operation initiated by the plugin. Since the plugin cannot shut down these newly assigned ports, endpoints are not assigned their new IP address and the action fails. To successfully apply the *Assign to VLAN* action on endpoints connected to this switch model, it is recommended to have SecureConnector installed on these endpoints.

### Endpoint Address ACL


Use the *Endpoint Address ACL* action to define and apply any of the following, connected endpoint handling:

- [IP ACL](#)
- [MAC ACL](#)

At any given time, only one ACL action, either the *Access Port ACL* action or the *Endpoint Address ACL* action, can be enabled for use. To switch between the enablement of these two actions, see the procedure in [acl\\_action\\_type](#).

- 📄 *When the plugin applies the *Endpoint Address ACL* action on a Brocade layer 3 switch interface that is included in a Brocade virtual interface, the plugin applies this action on the Brocade virtual interface and not on the individual, target interface. Doing so, results in the *Endpoint Address ACL* action being applied on every interface that is included in the Brocade virtual interface.*

For the ACL capabilities that are available to use with the Switch Plugin for supported, vendor switches, see Appendix 6, section [Switch Vendor ACL Support](#).

 *Switch Plugin Garbage Collection: By default, once an hour, the plugin releases from a switch those IP ACLs and MAC ACLs that are not in use because the Endpoint Address ACL action has been canceled for the relevant endpoint. Per endpoint, the operation removes both the relevant rules from the switch IP access list and the ACL from the specific port (the access group). To modify the default, removal period, contact customer support at [support@forescout.com](mailto:support@forescout.com).*

For plugin IPv6 support exceptions with ACL-related functionality, see [IPv6 Support](#).

#### *IP ACL*

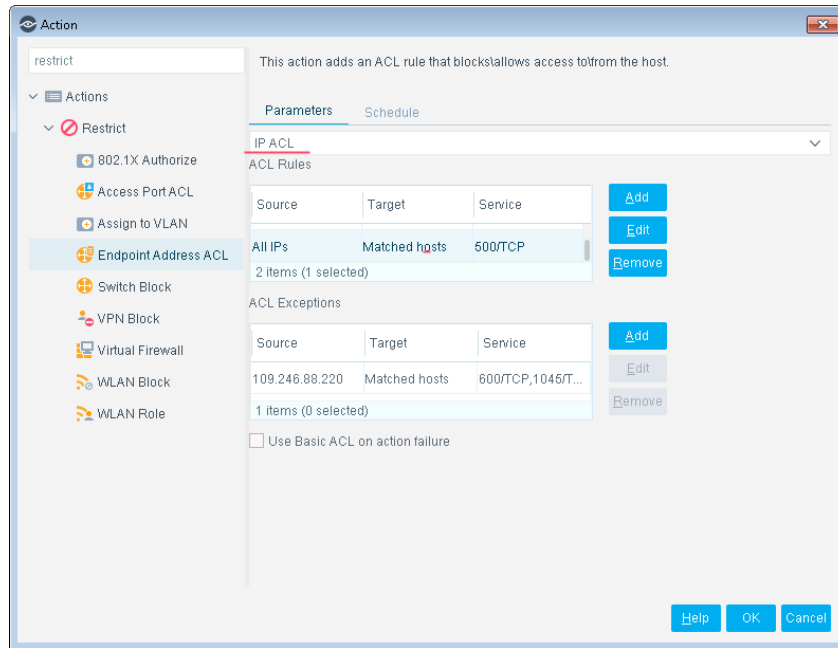
The **IP ACL** option instructs a switch to close (ACL rule) or to open (ACL exception) network zones, services or protocols to either traffic to or traffic from specific, endpoint IP addresses connected to the switch.

If the plugin is configured to manage a switch with the ACL option **Add CounterACT authentication servers permit rules**, then, when the action is applied, the plugin adds rules to the ACL that permit communication between detected endpoints and CounterACT authentication servers. When the applied action is later cancelled, these CounterACT authentication server permit rules are still maintained on the switch, due to performance considerations. Only stopping the plugin or performing a Clear CounterACT ACLs removes added CounterACT authentication server permit rules from the managed switch.

If a managed switch does not support either ACL TCP flags or ACL rule numbering (*ACL rule sequence numbers*), use the *Endpoint Address ACL* action to instruct the switch to block endpoint traffic using basic ACL rules, previously defined in [Specify basic ACL rules](#). To accomplish this, the action option **Use Basic ACL on action failure** option must be selected.

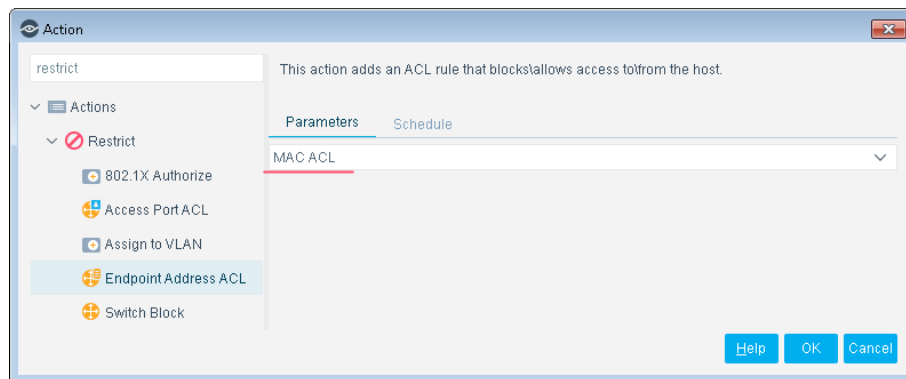
The action option **Use Basic ACL on action failure** is not supported for Juniper switches.

Plugin application of this action on connected *dual-stack* endpoints, using the **IP ACL** option, only restricts the IPv4 traffic of these endpoints.



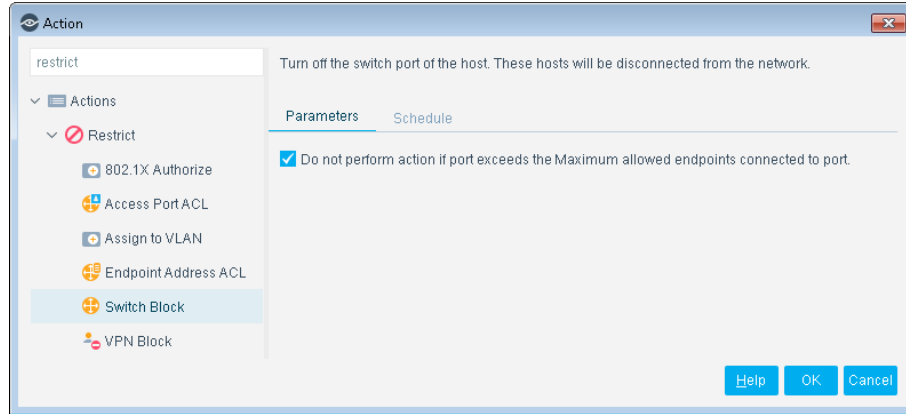
### MAC ACL

The **MAC ACL** option instructs a switch to block all traffic sent from the affected, endpoint MAC address.



### Switch Block

Use the *Switch Block* action to completely isolate endpoints from your network by turning off their switch port and preventing endpoints from communicating with the network.



If there is a VoIP device between the switch and the endpoint, that is, a VoIP port with a connected VoIP phone and a connected PC behind the phone, using the *Switch Block* action requires that global switch VoIP port protection is overridden. See [Global Configuration Options for the Switch Plugin](#).

### **Action Impact**

When using the *Switch Block* action either in a policy or by manual application, be aware of the following impact:

- Application of the *Switch Block* action on detected endpoints that match the **Host is online** property of a policy condition results in these endpoints no longer matching the **Host is online** property. Overlooking this policy condition change might trigger other, unintended policy re-evaluation of the affected endpoints.

Construct a policy rule condition that ensures matching endpoints that are online yet also unaffected by the *Switch Block* action, by combining the following criteria in the rule's condition:

- **Host is online AND Not Switch Port Action - Blocked**

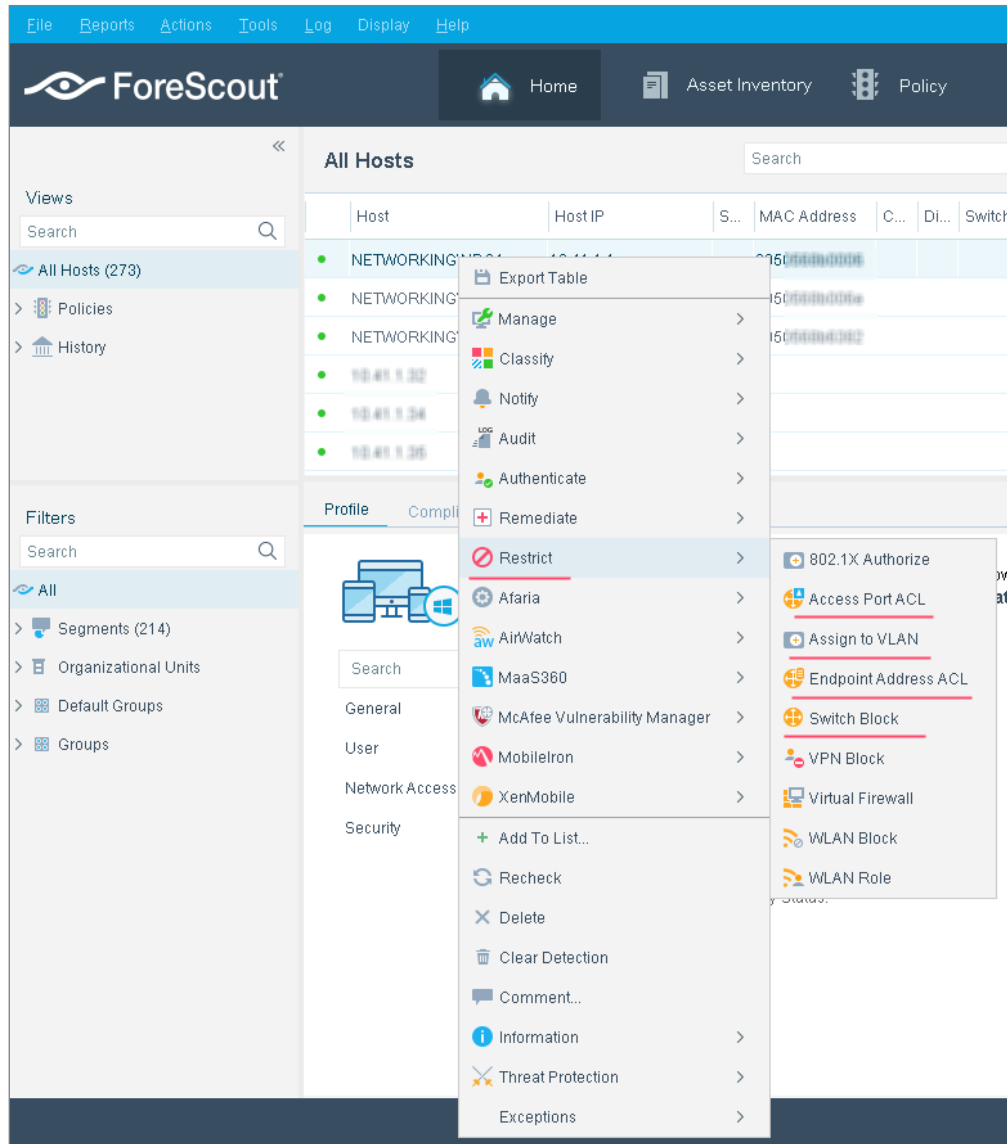
### **Working with Restrict Actions**

To work with restrict actions, you can:

- Manually apply these actions on endpoints from the Console.
- Create policies that carry out these actions.

#### **To manually define an action at the Console:**

1. Select the **Home** icon from the Console toolbar. The **Home** tab opens.
2. In the **All Hosts** pane, right-click an endpoint and select **Restrict**.
3. Select any one of the restrict actions **Access Port ACL**, **Assign Security Group Tag**, **Assign to VLAN**, **Endpoint Address ACL** or **Switch Block**.



### To define an action via a CounterACT policy:

1. Select the **Policy** icon from the Console toolbar. The **Policy** tab opens.
2. In the **Policy Manager** pane, select **Add** and create a policy.
3. In the **Action** section of the policy, select one of **Access Port ACL**, **Assign Security Group Tag**, **Assign to VLAN**, **Endpoint Address ACL** or **Switch Block**. The associated, action definition dialog opens.

For example:

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

Parameters    Schedule

---

VLAN ID   

VLAN name   

Do not perform action if port exceeds the Maximum allowed endpoints connected to port.

Tags :

## Action Thresholds

*Action thresholds* are designed to automatically implement safeguards when rolling out policy actions. Consider a situation in which you defined multiple policies that utilize *Access Port ACL*, *Assign to VLAN*, *Endpoint Address ACL* and *Switch Block* actions. If an extensive number of endpoints match these policies, you may block more network endpoints than you anticipated.

An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single CounterACT device. By working with thresholds, you gain more control over how many network endpoints are simultaneously restricted in one way or another. Refer to the *CounterACT Administration Guide (Policy Management > Policy Safety Features > Working with Action Thresholds)* for details. See [Additional CounterACT Documentation](#) for information on how to access this guide.

The following table lists the default action thresholds for restrict actions:

Restrict Action	Default Threshold
<b>Access Port ACL</b>	2%
<b>Assign to VLAN</b>	2%
<b>Endpoint Address ACL</b>	2%
<b>Switch Block</b>	2%

## Remediate Actions

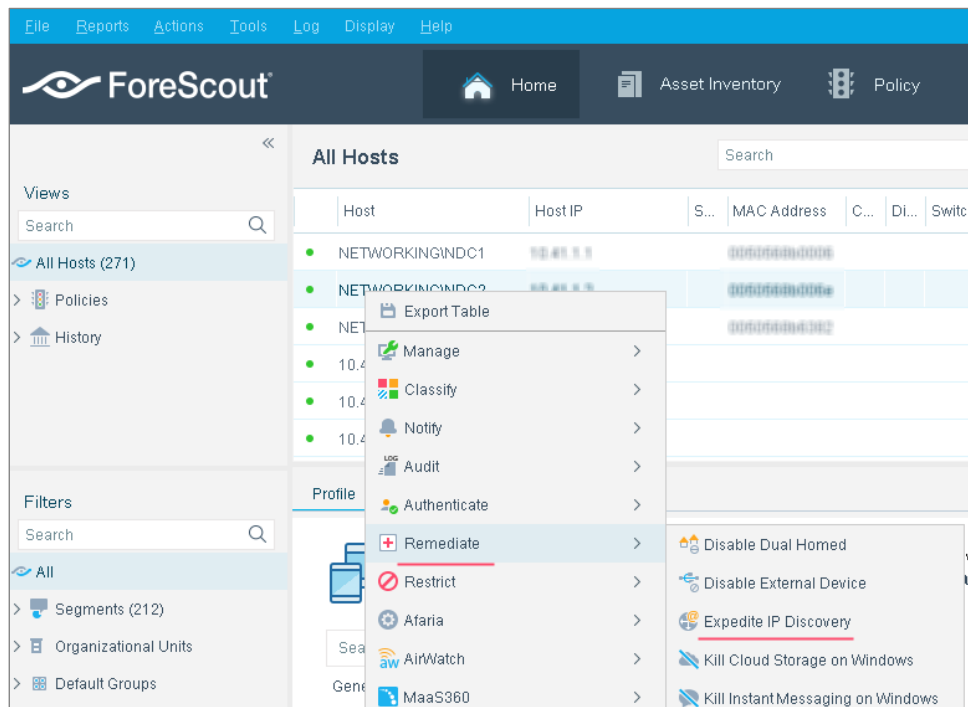
This section provides an overview of the CounterACT **Remediate** actions available with the Switch Plugin. The following remediate actions are available:

- [Expedite IP Discovery](#)

### Expedite IP Discovery

Use the *Expedite IP Discovery* action to address situations of delayed endpoint IP discovery. The action expedites the resolution of endpoint IP addresses (IP discovery

resolve requests) by the Switch Plugin querying the ARP table of designated, **adjacent**, L3-enabled network devices.



#### *Symptom of Delayed Endpoint IP Discovery*

Consider using the action if you identify a high failure rate of actions that is due to the IP address of the detected endpoint being unknown (unresolved).

#### *Root Causes of Delayed Endpoint IP Discovery*

Delayed endpoint IP discovery can be caused by any of the following reasons:

- Endpoint is connected to an L2 network device
- Connecting network device does not permit IP discovery
- No configured SPAN port (traffic mirroring is turned off)
- Misconfigured SPAN port
- Regular polling of connecting network device or an adjacent upstream device is too slow

#### *Action Usage Dependencies*

In order to use the action, verify the following:

- The detected endpoints are connected to an access switch that is configured in the Switch Plugin.
- In the Switch Plugin configuration, the access switch is assigned to a minimum of one *Connectivity Group*; configured using either the Add Switch wizard or the Edit Switch window, **Permissions** > **Advanced** > **IP to MAC mapping** section. See [IP to MAC Mapping](#).

- At least one L3-enabled network device is configured in the Switch Plugin that:
  - has the option **Read: IP to MAC Mapping** enabled; configured using either the Add Switch wizard or the Edit Switch window, **Permissions > ARP Permissions** section. See [ARP Permissions/ARP Table \(IPv4\) and Neighbor Table \(IPv6\) Permissions](#).
  - has the option **Allow IP Discovery from Connectivity Group** enabled; configured using either the Add Switch wizard or the Edit Switch window, **Permissions > Advanced > IP to MAC mapping** section. See [IP to MAC Mapping](#).
  - is assigned to the same *Connectivity Group* as the access switch. See [IP to MAC Mapping](#).
- The `ip2mac_aggregation_interval` advanced configuration flag is configured with the appropriate interval. See [Advanced configuration flags](#).

A *Connectivity Group* defines a group of **adjacent** network devices (any combination of L2, L3-enabled, L2/L3-enabled). When the access switch, to which detected endpoints are connected, cannot be used to resolve endpoint IP addresses, and the Switch Plugin performs the *Expedite IP Discovery* action:

1. The plugin queries the *Connectivity Group's* L3-enabled network devices that are configured to *Allow IP Discovery from Connectivity Group*.
2. The plugin obtains their ARP table data (IP to MAC mapping) and resolves detected endpoint IP addresses.

#### *Remediate Delayed Endpoint IP Discovery*

To remediate situations of delayed endpoint IP discovery, create a policy that identifies managed endpoints with unknown (unresolved) IP address and performs the *Expedite IP Discovery* action on such endpoints.

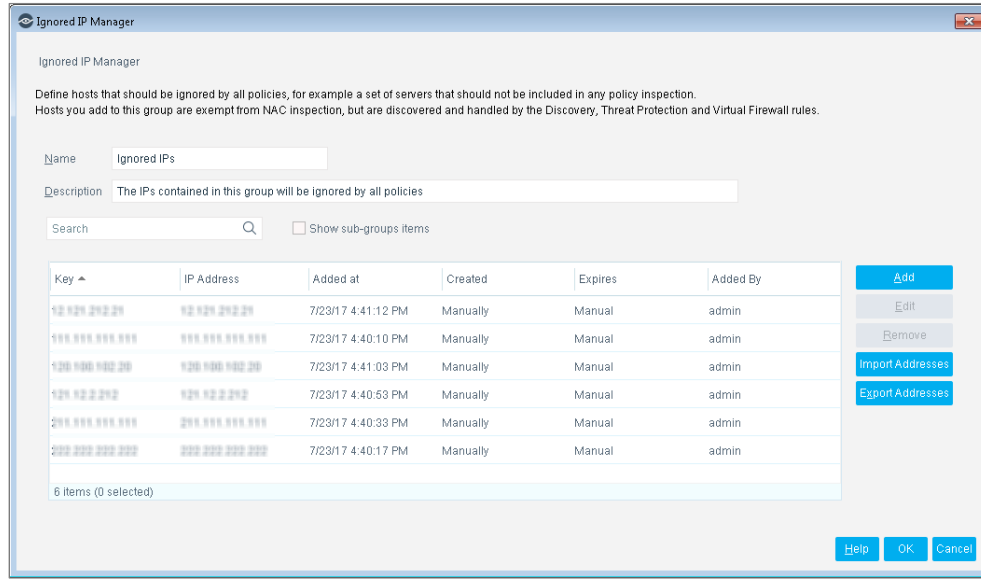
## Detect and Ignore Switch Virtual Interfaces

The Switch Plugin does not properly identify the Switch Virtual Interfaces (SVIs) of managed switches; the plugin detects these SVIs as separate interfaces. In large deployments having an extensive number of SVIs, detected SVIs are displayed as separate interfaces in the Console All Hosts pane. This impacts usability as the All Hosts pane becomes cluttered and causes configuration overhead, for example, when defining a policy Scope.

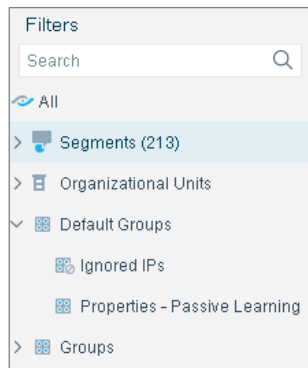
Use the policy template **Ignore Switch Virtual Interfaces** to create a CounterACT policy that detects SVIs by evaluating the Switch Virtual Interface property of managed switches. The policy adds matched SVIs to CounterACT's **Ignored IPs** group. These IP addresses are excluded from all policy inspection and remain assigned to the **Ignored IPs** group until manually removed. In the Console, open the Policy Wizard and access the policy template by selecting **Policy** tab > **Add** > **Templates** > **Ignore IPs** > **Ignore Switch Virtual Interfaces**.

- 📖 *CounterACT does not count IP addresses assigned to the **Ignored IPs** group towards license usage.*





Display ignored IP addresses in the All Hosts pane, by selecting from the Filters pane the **Ignored IPs** filter.



You can manually remove SVIs from the Ignored IPs group using the Console's **Ignored IP Manager** window.

#### To remove SVI entries from the Ignored IPs group:

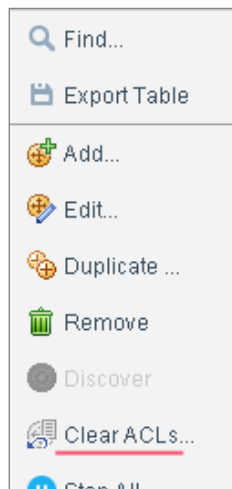
1. In the Filters pane of the Console **Home** tab, open the **Default Groups**.
2. Double-click the **Ignored IPs** filter option. The **Ignored IP Manager** window displays.
3. From the table, select the Key/IP Address of the entries that you want to remove and select **Remove**.
4. Select **OK** and then select **Yes** to apply your changes.

## Clear ACLs from All Switch Ports

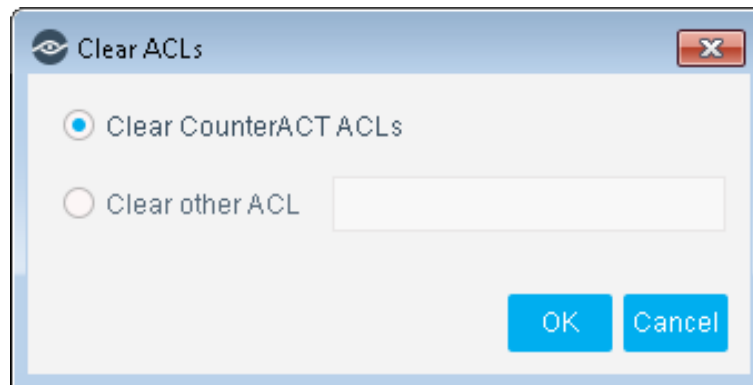
Eliminate ACLs from a switch, whether CounterACT Endpoint Address ACLs or a non-CounterACT defined ACL.

### To clear ACLs:

1. In the Switch tab, select **Stop All...** and stop Switch Plugin operation in all your CounterACT devices.
2. In the Switch tab, select one or more switches, right-click and select **Clear ACLs**.



The **Clear ACLs** dialog box opens.

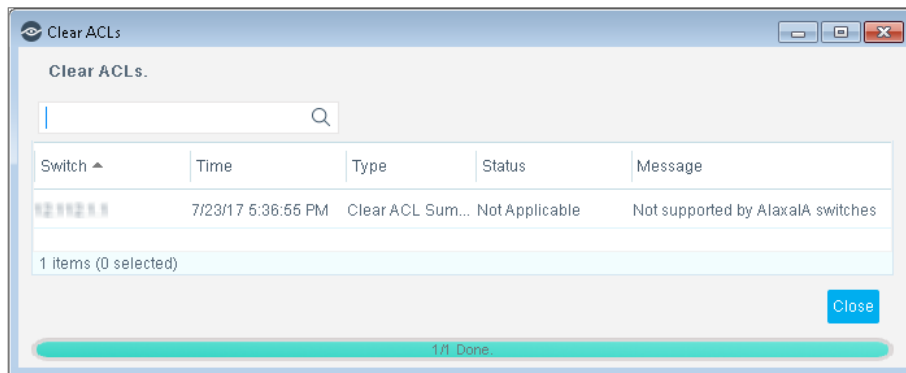


3. Do one of the following:
  - Select **Clear CounterACT ACLs** to release in a selected switch the CounterACT-applied Endpoint Address ACLs. An Endpoint Address ACL contains either an IPL ACL, a MAC ACL or, in the case of a Juniper switch, both of these types of ACL rules; the Juniper switch ACL firewall filter can simultaneously contain both IP ACL rules and MAC ACL rules. With a Cisco switch, selecting **Clear CounterACT ACLs** also releases the CounterACT-applied Pre-Connect ACL.

- Select **Clear other ACL** and enter in the accompanying field the ACL name of any ACL to release it in a selected switch, regardless of ACL origin.
4. Select **OK**.
- A new process starts, which logs in to each selected switch, and performs the following actions:

- Releases the identified ACL(s) from all ports in the switch.
- Removes the identified ACL(s) from the switch ACL list.

The **Clear ACLs** results window opens and displays the results of the requested clear action.



The **Clear ACLs** results window displays the following information for each selected switch:

- *Clear ACL Summary* – With status *Succeeded*, *Failed* or *Not applicable*

For switches that support ACL actions (Cisco, Brocade, Enterasys and Juniper), the following results are also displayed:

- *Clear ACL from Switch ACL List* – Result can be *Not found*, *Cleared* or *Error* (if the clear failed)
- *Clear ACL from Switch Ports*:
  - Result can be *Not found*, *Cleared* (with number of cleared interfaces) or *Error* (if the clear failed)
  - Result per interface, *Cleared* with the name of the ACL cleared or *Failed to clear* with an error message if the clear failed

*Clear Alias from Switch Ports* - the process also removes the ACL part from the port alias.

## Switch Setup

This section describes the configuration that must be applied in the switches of specific vendors to enable these switches to interoperate with the Switch Plugin.

- [Configuring Cisco Switches for SNMPv3](#)

- [Configuring H3C Switches for SNMP](#)
- [Configuring Huawei Switches](#)
- [Configuring NETCONF on Juniper EX Series Switches](#)
- [Configuring MAC Notification Traps on Cisco Switches](#)
- [Configuring Switches for ACL Integration](#)

## Configuring Cisco Switches for SNMPv3

In order for the Switch Plugin to use SNMPv3 to communicate with a Cisco switch, perform the following on the Cisco switch:

- [Define the Group Configuration](#)
- [Define the User Configuration](#)
- [Define the View Configuration](#)

### Define the Group Configuration

If the Cisco switch supports *match prefix*, enter the following command lines in the switch to define the group:

1. `snmp-server group <group name> v3 auth read <view name> write <view name>`
2. `snmp-server group <group name> v3 priv context vlan`
3. `snmp-server group <group name> v3 priv context vlan- match prefix`

If the Cisco switch does not support *match prefix*, enter the following command lines in the switch:

1. `snmp-server group <group name> v3 auth read <view name> write <view name>` (no context)
2. For each defined switch VLAN (VLAN context), enter the following line:  
`snmp-server group <group name> v3 auth context vlan-<VLAN number> read <view name> write <view name>`

Example: The switch does not support *match prefix*, the group to define is `nacgroup`, the view to define is `nacview` and VLANs 4, 19 and 27 are defined on the switch. The following command lines would be entered:

```
snmp-server group nacgroup v3 auth read nacview write nacview
snmp-server group nacgroup v3 auth context vlan-4 read nacview write nacview
snmp-server group nacgroup v3 auth context vlan-19 read nacview write nacview
snmp-server group nacgroup v3 auth context vlan-27 read nacview write nacview
```

## Define the User Configuration

Enter the following command line in the switch to define the user:

```
snmp-server user <user name> <group name> v3 auth <authentication
protocol> <authentication password> [priv <privacy protocol> <privacy
password>]
```

Command line parameters enclosed within brackets [ ] are optional.

Example: User `cisco` belongs to group `nacgroup` that works with the authentication protocol `sha` and the authentication password `cisco1234`, the following command line would be entered:

```
snmp-server user cisco nacgroup v3 auth sha cisco1234
```

## Define the View Configuration

When defining the view, include the entire SNMP view (`.iso`). Enter the following command line in the switch to define the view:

```
snmp-server view <view name> iso included
```

# Configuring H3C Switches for SNMP

When SNMP is used by the plugin to interoperate with managed H3C switches having hybrid ports, the following switch configuration is required:

- On a hybrid port, configure all candidate VLANs as *untagged*.

```
[Net31_SW2-GigabitEthernet1/0/22]
[Net31_SW2-GigabitEthernet1/0/22]
[Net31_SW2-GigabitEthernet1/0/22]dis this
#
interface GigabitEthernet1/0/22
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 311 to 313 untagged
 port hybrid pvid vlan 311
 voice vlan 314 enable
#
return
[Net31_SW2-GigabitEthernet1/0/22]
```

## Configuring Huawei Switches

Switch Plugin management of hybrid ports on a Huawei switch – learning VLAN information and applying switch actions on the ports – requires including the following port definition statement immediately after the `pvid` statement, per hybrid port on the switch:

- `undo port hybrid vlan 1`

## Configuring NETCONF on Juniper EX Series Switches

The Juniper Junos operating system supports NETCONF, an XML-based protocol that enables users to install, manipulate and delete the configuration of network devices. When configuring the Switch Plugin to manage Juniper EX series switches, the procedures described in [Add Switches to the Switch Plugin](#) apply, with one difference - the Switch Plugin must use NETCONF to manage these switches. To work with NETCONF, you must perform both of the following:

- Enable the service on the Juniper switch, as described in the procedures provided below
- Configure SSH credentials for Switch Plugin CLI access (see [CLI Configuration](#))

### To configure NETCONF using the command-line console of the switch:

1. Type the following at the command line:

- `cli`
- `configure`
- `set system services netconf ssh`

### To configure NETCONF using the Switch Configuration window of the switch:

1. Select the following options:

- CLI Tools
- Point & Click CLI
- system
- services
- netconf
- ssh
- OK

## Configuring MAC Notification Traps on Cisco Switches

SNMP *MAC notification traps* are supported for Cisco switches only. Configure Cisco switches to send SNMP *MAC notification traps* to CounterACT.

CounterACT provides an *fstool* command to support configuring single Cisco switches to send these traps. You can also configure the traps directly from the switch using the CLI.

In addition to configuring Cisco switches to send SNMP *MAC notification traps*, the Switch Plugin must be enabled to handle the SNMP traps it receives from managed switch devices. Accomplish this by selecting in the Console, the **Handle SNMP Traps** checkbox in the **Edit general parameters** window.

## Configuring MAC Notification Traps – Configuration from CounterACT

Configure a single, managed Cisco switch to send its SNMP MAC notification traps to CounterACT. This requires, first, running an *fstool* command from the CounterACT device and then, second, running switch CLI commands.

### To configure a single Cisco switch:

1. Run the following from the CounterACT device:

```
fstool sw traps
```

Output similar to the following will be displayed:

```
CounterACT Utility Tool
~~~~~

SNMP Switch Configuration for MAC Notification Traps
Please wait, reading switch list from database...

Open database [trails] - Success

The following switches are configured to work on the appliance:

1. 10.39.1.250 using SNMP version [2] vendor [alcatel]
2. 10.37.1.250 using SNMP version [2] vendor [nortel]
3. 10.39.1.251 using SNMP version [1] vendor [3com]
4. 10.39.1.253 using SNMP version [3] authentication [true] privacy
   [true] vendor [foundry]
5. 10.33.1.250 using SNMP version [2] vendor [cisco]
6. 10.39.1.248 using NETCONF vendor [juniper]
7. 10.31.1.250 using SNMP version [2] vendor [generic]
8. 10.38.1.250 using SNMP version [2] vendor [enterasys]
9. 10.34.1.250 using SNMP version [2] vendor [extreme]

Select a switch by entering its number in the list. For multiple
switch selection, separate numbers by commas.

Select switch: 5

Connecting switch [10.33.1.250]

(e)nable Notification/(d)isable Notification:e
Starting Switch Configuration for MAC Notification Traps
Updating Switch Succeeded
** Please Add This Line Manually to Switch Configuration:
    snmp-server host <CA Address> <Community>
```

Example: Switch ports - before *fstool sw traps* configuration

```
interface GigabitEthernet1/0/2
 switchport access vlan 301
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 302
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 303
 switchport mode access
!
```

Example: Switch ports - after `fstool sw traps` configuration

```
interface GigabitEthernet1/0/2
switchport access vlan 301
switchport mode access
snmp trap mac-notification change added
snmp trap mac-notification change removed
!
interface GigabitEthernet1/0/3
switchport access vlan 302
switchport mode access
snmp trap mac-notification change added
snmp trap mac-notification change removed
!
interface GigabitEthernet1/0/4
switchport access vlan 303
switchport mode access
snmp trap mac-notification change added
snmp trap mac-notification change removed
!
```

2. Enter the switch CLI in Enable mode and type the following:

```
configure terminal
```

3. Type the following:

```
snmp-server host <Appliance_IP_address> <community>
```

Use the IP address of the CounterACT device that manages this switch.

## Configuring MAC Notification Traps – Configuration from the Switch

Configure the sending of SNMP *MAC notification traps* directly from Cisco switches using the CLI. This is recommended if you have a central configuration tool for all switches that allows making this change once and applying it to all the switches.

The configuration commands to use vary, depending on the version of Cisco IOS running on the switches.

### Configuring MAC Notification Traps – IOS 12.2 (35) and Below

The configuration from the CLI of the switch is performed, for example, as follows:

1. `snmp-server enable traps MAC-Notification`
2. `mac-address-table notification`
3. `snmp-server host <CounterACT_device_IP_address> <community>`

Use the IP address of the CounterACT device that manages these switches.

Configure each non-trunk interface of the switch, using the command `interface FastEthernet0/:`

4. Run the following command to receive a MAC notification trap on link-up:  
`snmp trap mac-notification added`
5. Run the following command to receive a MAC notification trap on link-down:  
`snmp trap mac-notification removed`



## Configuring MAC Notification Traps – IOS 12.2 (55) and Above

The configuration from the CLI of the switch is performed, for example, as follows:

1. `snmp-server enable traps MAC-Notification`
2. `mac-address-table notification change`
3. `snmp-server host <CounterACT_device_IP_address> <community>`

Use the IP address of the CounterACT device that manages these switches.

Configure each non-trunk interface of the switch, using the command `interface FastEthernet0/:`

4. Run the following command to receive an SNMP MAC notification trap on link-up:  
`snmp trap mac-notification change added`
5. Run the following command to receive an SNMP MAC notification trap on link-down:  
`snmp trap mac-notification change removed`

## Configuring Switches for ACL Integration

In order for the plugin to apply ACL actions in managed switches, you must allow command-line (CLI) access from the CounterACT device to the switches.

**To set up the switch:**

1. Create a privilege level with access to at least the following commands. (To skip this step, use privilege level 15.)

Context	Command
exec	<code>show running-config</code>
exec	<code>show access-lists</code>
exec	<code>config t</code>
configure	<code>access-list</code>
configure	<code>interface</code>
configure	<code>ip access-list</code>
interface	<code>ip access-group</code>
ipenacl	<code>permit</code>
ipenacl	<code>deny</code>

The following example sets privilege level 7:

```
enable secret level 7 0 <enable_password>
privilege ipenacl level 7 permit
privilege ipenacl level 7 deny
privilege interface level 7 ip access-group
privilege configure level 7 access-list
privilege configure level 7 interface
```

```
privilege configure level 7 ip access-list
privilege exec level 7 show running-config
privilege exec level 7 show access-lists
privilege exec level 7 config t
```

2. Set up a user name with a password and a privileged password. For example:

```
username test privilege 7 secret 0 <initial_password>
```

3. If there is an ACL controlling SSH access to the switch, modify the ACL to permit the Switch Plugin to access the switch.
4. If you choose to manually configure the ports on which the ACL will be applied, do so by using a command like the following for the appropriate interfaces:

```
interface <interface_name>
ip access-group forescout_acl in
```

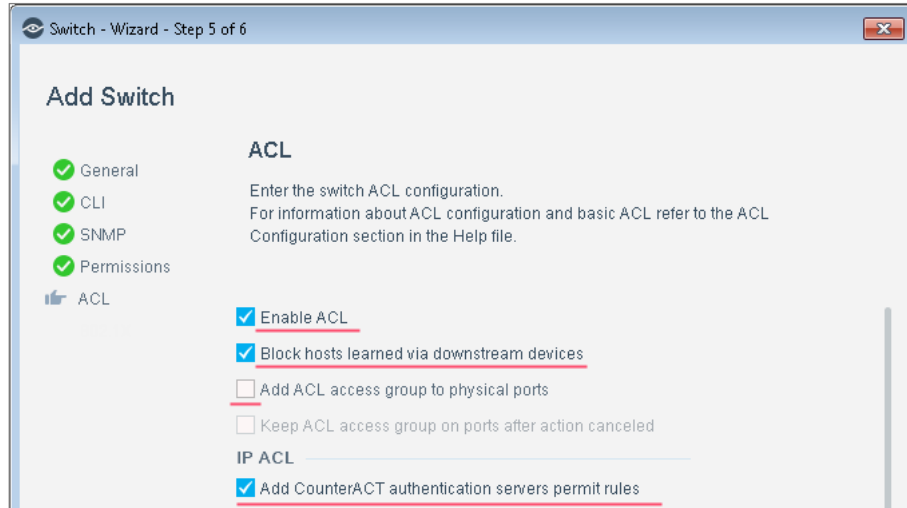
## Layer 3 Switch Support for ACL

Layer 3 switches (for example, Cisco ISR Catalyst 2801) do not support full-featured port-based ACLs. These switches can still be used for ACL blocking.

### To work with these switches:

1. For Access Port ACL and Endpoint Address ACL, verify that the switch supports Layer 3 routing.
2. For Endpoint Address ACL, add the following command to the ACL configuration on the relevant interface VLAN on the switch:

```
ip access-group forescout_acl in
```
3. For Access Port ACL, select **Enable ACL** in the Switch Plugin ACL page (see [ACL Configuration – Cisco and Brocade Switches](#)).
4. For Endpoint Address ACL, configure the Switch Plugin ACL page (see [ACL Configuration – Cisco and Brocade Switches](#)) as follows:
  - a. Select **Enable ACL**
  - b. Select **Block hosts learned via downstream devices**
  - c. Clear selection of **Add ACL access group to physical ports**
  - d. Maintain selection of **Add CounterACT authentication servers permit rules**



- Some switch devices (for example, Cisco Series 800 Routers) do not have a MAC address table. The Endpoint Address ACL action cannot be applied because the Switch Plugin does not know at which port the endpoint is connected to the switch and therefore the ACL cannot be set.

## Appendix 1: See and Control Capabilities Summary

This section provides table summaries of the capabilities that the Switch Plugin supports per network device vendor. The supported capabilities are grouped as follows:

- [SEE Capabilities](#)
- [CONTROL Capabilities](#)

In the provided tables:

- A highlighted (*light blue*) cell identifies a supported capability.
- SNMP/CLI/Netconf: Identifies the communication protocol used. **Unless otherwise indicated, the plugin uses the listed protocol to accomplish both reads and writes.**
- Plugin performance of ARP table and Neighbor table operations is identified by the prefaces **ARP:** and **Nghbr:** respectively; when not specified, only plugin ARP table operations are performed.

For detailed information about specific, switch vendor models and operating system versions that are validated for Switch Plugin management, refer to the *WIRED INTEGRATIONS (SWITCHES)* section in the *CounterACT Network Devices Compatibility Matrix*. You can access this matrix in one of the following locations, depending on the licensing mode your deployment is using:

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#), Documentation Page.

See [Additional CounterACT Documentation](#) (*Identifying Your Licensing Mode in the Console*) to learn which licensing mode your deployment is using.

### SEE Capabilities

The following table summarizes the SEE capabilities that the Switch Plugin supports per network device vendor.

- CDP/FDP/LLDP: Identifies the discovery protocol used by the managed switches and supported by the plugin.

SEE						
Network Device Vendor	MAC Table	ARP Table (IPv4) Nghbr Table (IPv6)	SNMP Trap Receipt Link Up/Down	Auto Discovery	VoIP Detection	Resolve PoE Port Info
3COM	SNMP	SNMP			SNMP	

	<b>SEE</b>					
<b>Network Device Vendor</b>	<b>MAC Table</b>	<b>ARP Table (IPv4) Nghbr Table (IPv6)</b>	<b>SNMP Trap Receipt Link Up/Down</b>	<b>Auto Discovery</b>	<b>VoIP Detection</b>	<b>Resolve PoE Port Info</b>
<b>Alaxala</b>	SNMP	SNMP				
<b>Alcatel</b>	SNMP	SNMP read-VRF ARP by CLI			SNMP	
<b>Apresia</b>	SNMP	SNMP				
<b>Arista</b>	CLI	CLI (including read-VRF ARP)		CDP		
<b>Avaya (Nortel)</b>	SNMP	ARP: SNMP read-VRF ARP by CLI Nghbr: SNMP/CLI read only		LLDP	SNMP	
<b>Brocade</b>	SNMP	ARP: SNMP Nghbr: CLI read only		FDP	SNMP	
<b>Cisco<sup>(*)</sup></b>	SNMP/CLI	ARP: SNMP/CLI read-VRF ARP by CLI Nghbr: SNMP/CLI read only	MAC Notification traps also supported	CDP	SNMP/CLI	SNMP
<b>Comtec</b>	SNMP	read- SNMP, write-CLI				
<b>DASAN</b>	SNMP	read- SNMP, write-CLI				
<b>Dax</b>	SNMP	SNMP				
<b>Dell</b>	SNMP	ARP: SNMP Nghbr: CLI read only				
<b>D-Link</b>	SNMP	SNMP				
<b>Enterasys</b>	SNMP	read- SNMP/CLI, write- SNMP		LLDP	SNMP	

	<b>SEE</b>					
<b>Network Device Vendor</b>	<b>MAC Table</b>	<b>ARP Table (IPv4) Nghbr Table (IPv6)</b>	<b>SNMP Trap Receipt Link Up/Down</b>	<b>Auto Discovery</b>	<b>VoIP Detection</b>	<b>Resolve PoE Port Info</b>
<b>Enterasys Matrix N-Series</b>	SNMP	read-SNMP/CLI, write-SNMP		LLDP	SNMP	
<b>Extreme</b>	SNMP	SNMP				
<b>Extreme XOS</b>	SNMP	SNMP				
<b>Force10</b>	SNMP	SNMP			SNMP	
<b>Generic</b>	SNMP/CLI	SNMP/CLI				
<b>H3C</b>	SNMP	SNMP		LLDP	SNMP	
<b>Hirschmann</b>	SNMP/CLI	SNMP/CLI				
<b>HPE-Comware OS</b>	CLI	ARP: CLI read only (including read-VRF ARP) Nghbr: CLI read only		LLDP	CLI	
<b>HPE-Provision/ProCurve OS</b>	SNMP	SNMP		LLDP	SNMP	
<b>Huawei</b>	SNMP	SNMP				
<b>Juniper EX</b>	Netconf	ARP: Netconf Nghbr: Netconf read only			Netconf	
<b>Linksys</b>	SNMP	SNMP				
<b>NEC</b>	SNMP	SNMP				
<b>Firewall: Check Point</b>		CLI read only VSX supported				
<b>Firewall: Cisco ASA</b>		CLI read only				
<b>Firewall: Forcepoint Stonesoft</b>		CLI read only				
<b>Firewall: Fortinet</b>		CLI read only VDOM supported				
<b>Firewall: Juniper SRX</b>		CLI				

<b>SEE</b>						
<b>Network Device Vendor</b>	<b>MAC Table</b>	<b>ARP Table (IPv4) Nghbr Table (IPv6)</b>	<b>SNMP Trap Receipt Link Up/Down</b>	<b>Auto Discovery</b>	<b>VoIP Detection</b>	<b>Resolve PoE Port Info</b>
<b>Firewall: Palo Alto Networks</b>		CLI read only				
<b>Router: Linux OS</b>		CLI read only				

(\*) For managed Cisco Small Business 300 Series switches, SNMP is the only read method used to detect VoIP port configuration.

### CONTROL Capabilities

The following table summarizes the CONTROL capabilities that the Switch Plugin supports per network device vendor.

<b>CONTROL</b>			
<b>Network Device Vendor</b>	<b>Assign to VLAN Action</b>	<b>Switch Block Action</b>	<b>ACL Actions</b>
<b>3COM</b>	SNMP/CLI	SNMP	
<b>Alaxala</b>	SNMP	SNMP	
<b>Alcatel</b>	SNMP	SNMP	
<b>Apresia</b>	SNMP	SNMP	
<b>Arista</b>	CLI	CLI	
<b>Avaya (Nortel)</b>	SNMP	SNMP	
<b>Brocade</b>	SNMP	SNMP	CLI Endpoint Address ACL <sup>(*)</sup>
<b>Cisco<sup>(β)</sup></b>	SNMP/CLI	SNMP/CLI	CLI Pre-Connect ACL <sup>(*)</sup> , Endpoint Address ACL <sup>(*)</sup> , Access Port ACL <sup>(*)</sup>
<b>Comtec</b>	CLI	SNMP	
<b>DASAN</b>	CLI	SNMP	
<b>Dax</b>	SNMP	SNMP	
<b>Dell</b>	SNMP	SNMP	
<b>D-Link</b>	SNMP	SNMP	
<b>Enterasys</b>	SNMP	SNMP	
<b>Enterasys Matrix N-Series</b>	SNMP	SNMP	CLI Endpoint Address ACL

	<b>CONTROL</b>		
<b>Network Device Vendor</b>	<b>Assign to VLAN Action</b>	<b>Switch Block Action</b>	<b>ACL Actions</b>
<b>Extreme</b>	SNMP	SNMP	
<b>Extreme XOS</b>	SNMP/CLI	SNMP	
<b>Force10</b>	SNMP	SNMP	
<b>Generic</b>		SNMP	
<b>H3C</b>	SNMP/CLI	SNMP	
<b>Hirschmann</b>	SNMP/CLI	SNMP	
<b>HPE-Comware OS</b>	CLI	SNMP	
<b>HPE-Provision/ProCurve OS</b>	SNMP	SNMP	
<b>Huawei</b>	SNMP/CLI	SNMP	
<b>Juniper EX</b>	Netconf	Netconf	Netconf <i>Endpoint Address ACL<sup>(&amp;)</sup></i>
<b>Linksys</b>	SNMP	SNMP	
<b>NEC</b>	SNMP	SNMP	
<b>Firewall: Check Point</b>			
<b>Firewall: Cisco ASA</b>			
<b>Firewall: Forcepoint Stonesoft</b>			
<b>Firewall: Fortinet</b>			
<b>Firewall: Juniper SRX</b>			
<b>Firewall: Palo Alto Networks</b>			
<b>Router: Linux OS</b>			

(β) The plugin does not support applying ACL actions on the Cisco Small Business 300 Series switch, since the plugin interoperates with these switches using only SNMP and ACL support requires plugin-switch CLI interoperation.

(&) For exceptions to plugin IPv6 support of ACL-related functionality, see [IPv6 Support](#).



## Appendix 2: Troubleshooting, Workarounds and Feature Functionality Support

This appendix covers the following topics:

- [Troubleshooting](#)
- [Configuration Flags for Workarounds](#)
- [Configuration Flags Supporting Plugin Functionality](#)

### Troubleshooting

This section provides troubleshooting solutions for the following issues:

- [Plugin VoIP Detection for Cisco Trunk Port Configuration Exception](#)

### Plugin VoIP Detection for Cisco Trunk Port Configuration Exception

For exceptional situations in which the involved Cisco trunk ports cannot have their voice VLANs configured using `switchport voice vlan <n>`, the Switch Plugin can still provide VoIP detection for these trunk ports, however, the following configurations must be in effect:

#### Cisco Switch Configuration

- Each involved Cisco switch trunk port must be configured with only two, allowed VLANs.
- One of these two VLANs must be configured as a native VLAN

Trunk port configuration example:

```
switchport trunk native vlan 309
switchport trunk allowed vlan 309,311
```

#### Switch Plugin Configuration

- In the **Advanced configuration flags** field of the Edit general parameters window, enable the `determine_voip_by_allowed_vlans` flag as follows:

```
cisco:determine_voip_by_allowed_vlans:on
```

By default, this flag is disabled (flag assignment is `off`).

- The plugin is configured to manage the involved Cisco switch(es) using either one of the following MAC read/write methods:
  - SNMP (RW) and CLI
  - SNMP (RO) and CLI

In the Console's Switch tab, select **Add/Edit** a switch > Permissions pane/tab > MAC Permissions section > **MAC Read/Write Method** field.

## Configuration Flags for Workarounds

This section provides workarounds that address device management issues. Configuration flags are used to enabled/disabled each of these workarounds. The following issues are addressed:

- [Disable Reporting of Last Trap Received](#)
- [Control the Update Frequency of Number of MACs Found](#)
- [Support for Handling Multiple Entries for Same MAC](#)
- [Support for VoIP for Enterasys Switches](#)
- [Ignore Untagged Ports on Avaya \(Nortel\) Switches](#)
- [Ignore Entity Mapping MIB when Detecting Physical Port](#)
- [Pad MAC Addresses Missing Any Leading Zeros](#)
- [Ignore Link Down Traps After Assign to VLAN Action](#)

[Configuration Flags](#) address specific plugin switch management issues *at the per switch level*. [Advanced configuration flags](#) address issues at the global switch level and are enabled either for all plugin-managed switches or for all plugin-managed switches of a specific vendor.

### Disable Reporting of Last Trap Received

#### Issue:

By default, the Console reports **Last Trap Received** information in the **Switch** tab. When there is a high frequency of traps received from the switch, the information that is retrieved for the **Last Trap Received** column in the **Switch** tab generates extensive traffic between CounterACT devices and the Console.

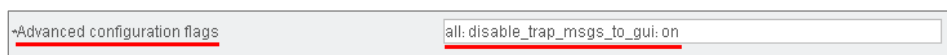
#### Workaround:

Use the new configuration flag, *disable\_trap\_msgs\_to\_gui*, to reduce the extensive amount of generated traffic. When activated, this flag halts the plugin's report of **Last Trap Received** information in the **Switch** tab. Activation of this flag affects all your configured switches.

#### To activate this flag:

1. In the Console, select **Options > Switch > Options....** The **Edit general parameters** window opens.
2. In the **Advanced configuration flags** field, enter the statement:

```
all:disable_trap_msgs_to_gui:on
```



- 📄 *Even if halted for the **Switch** tab, **Last Trap Received** information continues being reported in the plugin test results.*

To disable the feature, do either of the following actions:

- Delete the string from the **Advanced configuration flags** field.
- Modify the string to be: `all:disable_trap_msgs_to_gui:off`.

## Control the Update Frequency of Number of MACs Found

### Issue:

In large deployments (multiple managed switches, multiple connecting endpoints), information retrieved for the **Number of MACs found** column in the **Switch** tab generates extensive traffic between the CounterACT devices and the Console.

### Workaround:

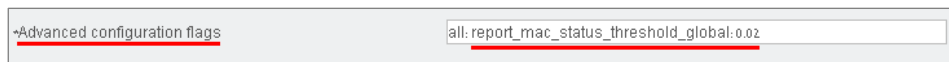
Use two new configuration flags to reduce the extensive amount of generated traffic. When activated, these flags control the frequency at which the **Number of MACs found** information is updated for re-display. The flag's control is based on a defined percent of required, information change. For example, if the defined value of the flag is 0.05, then updates of **Number of MACs found** information will only occur if existing information changes by  $\geq 5\%$ .

Use these configuration flags, `report_mac_status_threshold_global` and `report_mac_status_threshold`, either in combination with each other or alone.

### To globally activate this control for all your switches:

1. In the Console, select **Options > Switch > Options...** The **Edit general parameters** window opens.
2. In the **Advanced configuration flags** field, enter the statement:  
`all:report_mac_status_threshold_global:<decimal_value>` , where provided value represents a percentage out of 100.

The global activation value **overrides** the global default value of 0.01 (1%).



### To globally disable the feature for all your switches:

- Delete the statement from the **Advanced configuration flags** field.

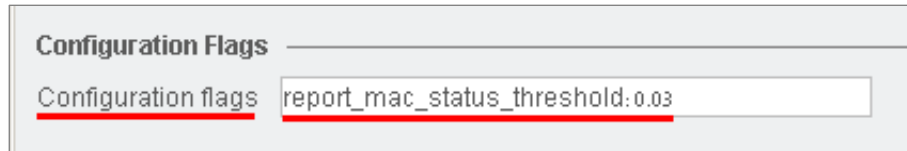
### To activate this control per configured switch:

1. In the Console, select **Options > Switch > switch entry > Edit > Permissions > Advanced...** . The **Switch Advanced Settings** window opens.

2. In the **Configuration flags** field, enter the statement:

`report_mac_status_threshold:<decimal_value>`, where provided value represents a percentage out of 100.

A per switch activation value *overrides* the global value.



**To disable the feature, do the following:**

- Delete the statement from the **Configuration flags** field.

## Support for Handling Multiple Entries for Same MAC

### Issue:

The Switch Plugin learns the same MAC address on more than one access port on a single switch, meaning, a single switch, one MAC address table and several entries in the table with same MAC. When this happens, the plugin might initiate unnecessary admission events and resolve host properties with inaccurate information. This issue might occur with endpoints having the following setup:

(a) Oracle/SUN Solaris M5000 box is installed and (b) the OBP (OpenBootProm) option (SPARC BIOS) *set local mac-address* is set to FALSE.

### Workaround:

Instruct the Switch Plugin to ignore endpoints in which the same MAC address was learned on more than one access port by using the *Global Advanced Configuration Flags* feature.

This workaround is available for Cisco switches using CLI.

**To enable this feature:**

1. Select **Tools > Options** and then select **switch** from the **Options** pane.
2. In the **Advanced configuration flags** field of the Edit general parameters dialog box, type the following string:

`cisco:cli_ignore_duplicate_mac:on.`



**To disable the feature, do either of the following actions:**

- Delete the string from the **Advanced configuration flags** field.
- Modify the string to be: `cisco:cli_ignore_duplicate_mac:off.`

## Support for VoIP for Enterasys Switches

### Issue:

The plugin identifies VoIP ports on Enterasys switches as trunk ports instead of access ports.

### Workaround:

Instruct the Switch Plugin to define VoIP ports as access ports by using the global advanced configuration flags feature, see [Advanced configuration flags](#).

To enable this feature, in the **Advanced configuration flags** field of the Edit general parameters dialog box, type the following string:

```
enterasys:enable_voip:on.
```



To disable the feature, either delete the string or change it to

```
enterasys:enable_voip:off.
```

## Ignore Untagged Ports on Avaya (Nortel) Switches

### Issue:

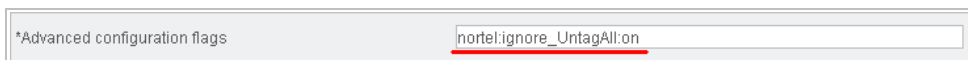
The plugin defines non-voice ports on Avaya (Nortel) switches that belong to more than one VLAN as trunk ports; you might want to leave untagged ports that belong to more than one VLAN as access ports.

### Workaround:

Instruct the Switch Plugin to leave untagged ports on Avaya (Nortel) switches as access ports, even when the plugin would normally define them as trunk ports, by using the global advanced configuration flags feature, see [Advanced configuration flags](#).

To enable this feature, in the **Advanced configuration flags** field of the Edit general parameters dialog box, type the following string:

```
nortel:ignore_UntagAll:on.
```



To disable the feature, either delete the string or change it to

```
nortel:ignore_UntagAll:off.
```

## Ignore Entity Mapping MIB when Detecting Physical Port

### Issue:

The Switch Plugin uses two MIBs to identify physical ports on a switch:

- entPhysicalClass (1.3.6.1.2.1.47.1.1.1.1.5)
- entAliasMappingIdentifier (1.3.6.1.2.1.47.1.3.2.1.2)

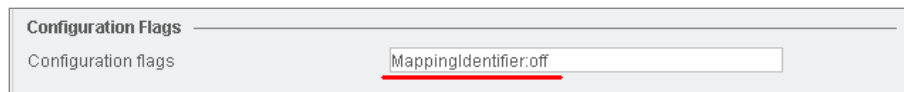
If a physical port is missing from 1.3.6.1.2.1.47.1.3.2.1.2 (the entity mapping MIB), the plugin assumes that the port cannot be an access port and ignores any endpoints attached to the port.

### Workaround:

Instruct the Switch Plugin to ignore the entity mapping MIB by using the per-switch advanced configuration flags feature, see [Configuration Flags](#).

To enable this feature for a switch, in the **Configuration flags** field of the Switch Advanced Settings dialog box, type the following string:

```
MappingIdentifier:off.
```



If the feature is enabled, all ports in 1.3.6.1.2.1.47.1.1.1.1.5 with a value of 10 are assumed to be physical ports.

To disable the feature, type:

```
MappingIdentifier:on.
```

To restore the default value, leave the field empty.

By default, the feature is disabled (meaning, the entity mapping MIB is *not* ignored).

## Pad MAC Addresses Missing Any Leading Zeros

### Issue:

With Linux routers running Check Point Firewall version EPSO 6.2, when the Switch Plugin reads the device ARP table to report the endpoint MAC-to-IP entries, the plugin erroneously invalidated any MAC address it received with skipped leading zeros (0) in the address sequence. For example, the 12 hexadecimal character MAC address `21:01:8e:0b:05:2f` is stored by such Linux routers as the 9 hexadecimal character MAC address `21:1:8e:b:5:2f`.


### Workaround:

To correct this Linux router processing issue, use the `pad_mac_addr` configuration flag. By default, this flag is enabled per managed Linux router.

The enabled `pad_mac_addr` flag instructs the plugin to pad MAC addresses received from the Linux router with leading zeros, when found to be missing from the address sequence, before validating the address.


`pad_mac_addr` can be enabled/disabled on a per-device basis (configuration flag) and on a global device basis (advanced configuration flag). The per-device configuration of the flag always takes precedence over the global configuration of the flag.

### To enable/disable the flag per managed Linux Router:

 *By default, this flag is enabled for managed Linux Routers*

1. In the Console, select **Options** > **Switch** > Linux router entry > **Edit** > **Permissions** > **Advanced**. The **Switch Advanced Settings** window opens.
2. In the **Configuration flags** field, perform either of the following:
  - a. To disable the flag, enter the command:  
`pad_mac_addr:off`
  - b. To enable the flag, enter the command:  
`pad_mac_addr:on`  
or delete the `pad_mac_addr:off` command from the **Configuration flags** field, which restores the per-device flag to its default value of `on` (enabled).

### To globally enable/disable the flag for all managed Linux Routers:

 *A per-device configuration of the flag always takes precedence over the global configuration of the flag.*

1. In the Console, select **Options** > **Switch** > **Options...**. The **Edit general parameters** window opens.
2. In the **Advanced configuration flags** field, perform either of the following:
  - a. To globally disable the flag, enter the statement:  
`all:pad_mac_addr:off`
  - b. To globally enable the flag, enter the statement:  
`all:pad_mac_addr:on`  
or delete the `all:pad_mac_addr:off` command from the **Configuration flags** field, which restores the global flag to its default value of `on` (enabled).

## Ignore Link Down Traps After Assign to VLAN Action

### Issue:

Following plugin apply of the *Assign to VLAN* action, which includes a bounce of the affected port, when a **link down trap** notification from the managed switch device was regularly received by the plugin with a delay of several seconds, the plugin handled this notification as an action failure and cancelled the applied action. This resulted in the plugin entering into an *apply action-cancel action* processing loop and the affected port continuously alternating between two VLANs.

### Workaround:

Enable the advanced configuration flag `ignore_received_link_down_traps` to instruct the Switch Plugin to ignore receipt of link down traps for a defined period, following its application of the *Assign to VLAN* action. The flag affects all managed switches.

By default:

- The `ignore_received_link_down_traps` flag is disabled.
- The ignore period is 60 seconds.

### To enable/disable the flag for all managed switches:

1. In the Console, select **Options > Switch > Options**. The **Edit general parameters** window opens.
2. In the **Advanced configuration flags** field:
  - a. To globally enable the flag, enter the statement:  
`all:ignore_received_link_down_traps:on`
  - b. To globally disable the flag, enter the statement:  
`all:ignore_received_link_down_traps:off`  
or delete the `all:ignore_received_link_down_traps:on` statement.

### To modify the ignore traps period:

1. Log in to the CounterACT device CLI.
2. Submit the following command:

```
fstool sw set_property
conf.ignore_received_link_down_traps_period.value <seconds>
```

where `<seconds>` is the period during which link down traps are ignored. The default ignore period is 60 seconds.



## Configuration Flags Supporting Plugin Functionality

This section describes configuration flags that must be used to support Switch Plugin feature functionality. The following configuration flags provide feature functionality support:

- [cli\\_hybrid\\_port\\_bounce\\_poe](#)

[Configuration Flags](#) address specific plugin switch management issues *at the per switch level*. [Advanced configuration flags](#) address issues at the global switch level and are enabled either for all plugin-managed switches or for all plugin-managed switches of a specific vendor.

### cli\_hybrid\_port\_bounce\_poe

Enabling the `cli_hybrid_port_bounce_poe` configuration flag is required in order for the Switch Plugin to bounce Huawei switch hybrid PoE (Power over Ethernet) ports, as part of completing the *Assign to VLAN* action on endpoints connected to such ports.

By default, the `cli_hybrid_port_bounce_poe` flag is disabled.

#### To enable/disable the flag per switch:

1. In the Console, select **Options > Switch > Huawei switch entry > Edit > Permissions > Advanced**. The **Switch Advanced Settings** window opens.
2. In the **Configuration flags** field, perform either of the following:
  - a. To enable the flag, enter the statement:  
`cli_hybrid_port_bounce_poe:on`
  - b. To disable the flag, enter the statement:  
`cli_hybrid_port_bounce_poe:off`  
or delete the `cli_hybrid_port_bounce_poe:on` statement from the **Configuration flags** field (restores the per-device flag to its default value of disabled).

You can globally enable/disable this configuration flag for all your managed Huawei switches. A per-device configuration of the flag always takes precedence over the global configuration of the flag.

#### To globally enable/disable the flag for all managed Huawei switches:

1. In the Console, select **Options > Switch > Options**. The **Edit general parameters** window opens.
2. In the **Advanced configuration flags** field, perform either of the following:
  - a. To globally enable the flag, enter the statement:  
`huawei:cli_hybrid_port_bounce_poe:on`

- b. To globally disable the flag, enter the statement:  
`huawei:cli_hybrid_port_bounce_poe:off`  
or delete the `huawei:cli_hybrid_port_bounce_poe:on` statement from the **Advanced configuration flags** field (globally restores the flag to its default value of disabled).

## Appendix 3: Setting Up a VLAN

You can move endpoints to a VLAN, rather than turning off their switch ports. This enables secured remote connection to endpoints for the purpose of deploying patches, but still prevents unwanted traffic to other sections of the network. This type of blocking requires an isolated VLAN with secured access only. (The steps required to create such a VLAN are the same as those required to implement any other company-wide VLAN.)

### To create an isolated VLAN with secured access only:

1. Choose an unused VLAN number.
2. Define the VLAN on the relevant routers—a single router if the VLAN is continuous among all managed switches, multiple routers if it is not. The term *continuous* here means that a broadcast packet in the VLAN on any managed switch is able to reach all other managed switches. This is true if all switches are interconnected using unrestricted trunk links.
3. (**Recommended**) Define the VLAN on every switch prior to the activation of the plugin. As a backup procedure, this is done by the Switch Plugin automatically when assigning a port to the VLAN on a switch that is not properly configured.
4. Define routing between the VLAN and the rest of the network. This step is not required in most environments, where routing protocols are dynamic.
5. Define a DHCP relay on the routers (*ip helper address* in Cisco terminology).
6. Define an address pool on the DHCP servers for this VLAN.
7. Restrict traffic between the VLAN and the rest of the network according to your access policy. This is usually done using an access list on the routers.

You should allow:

- DHCP traffic between the LAN and the DHCP servers
- DNS traffic
- Any other traffic allowed from the VLAN (for example, access to authentication servers which may result in un-quarantining, access to other company or Internet resources, etc.)

Deny all other traffic.

## Appendix 4: MIBs Used by the Switch Plugin

This section lists switch MIB requirements. If the Switch Plugin test fails for a switch, the switch might not meet specific MIB requirements. Use the following procedure to determine whether a required MIB exists on a switch or not:

1. Log in to the CounterACT device CLI
2. Submit the following command:

```
fstool run snmpwalk <switch_ip_address> -v <version> -c <community>  
<oid>
```

Required MIBs for the switches of the following vendors:

- [General MIBs](#)
- [3COM](#)
- [Alcatel](#)
- [Apresia](#)
- [Avaya \(Nortel\)](#)
- [Brocade](#)
- [Cisco](#)
- [Comtec](#)
- [D-Link](#)
- [Dasan](#)
- [Dax](#)
- [Dell](#)
- [Enterasys](#)
- [Extreme](#)
- [H3C](#)
- [HP](#)
- [Hirschmann](#)
- [Huawei](#)
- [Linksys](#)
- [NEC](#)

**General MIBs**

.1.3.6.1.2.1.2.2.1.6  
.1.3.6.1.2.1.1.6.0  
.1.3.6.1.2.1.1.3.0  
.1.3.6.1.2.1.2.2.1.2  
.1.3.6.1.2.1.31.1.1.1.1  
.1.3.6.1.2.1.2.2.1.7  
.1.3.6.1.2.1.1.7.0  
.1.3.6.1.2.1.1.1.0  
.1.3.6.1.2.1.1.2.0  
.1.3.6.1.2.1.2.2.1.8  
.1.3.6.1.2.1.2.2.1.1  
.1.3.6.1.2.1.4.1.0  
.1.3.6.1.2.1.17.4.3.1.2  
.1.3.6.1.2.1.17.7.1.2.2.1.2  
.1.3.6.1.2.1.17.7.1.4.2.1.3  
.1.3.6.1.2.1.17.1.4.1.2  
.1.3.6.1.2.1.3.1.1.2  
.1.3.6.1.2.1.4.22.1.2  
.1.3.6.1.2.1.4.22.1.4  
.1.0.8802.1.1.2.1.4.2.1.3  
.1.0.8802.1.1.2.1.4.1.1  
.1.3.6.1.4.1.45.1.6.13.2.1.1.3  
.1.3.6.1.2.1.17.2.15.1.8  
.1.3.6.1.2.1.17.2.15.1.3  
.1.3.6.1.2.1.17.2.15.1.9  
.1.3.6.1.2.1.17.1.1.0  
.1.3.6.1.2.1.17.7.1.4.3.1.1  
.1.3.6.1.2.1.17.7.1.4.3.1.2  
.1.3.6.1.2.1.17.7.1.4.3.1.4  
.1.3.6.1.2.1.47.1.1.1.1.5  
.1.3.6.1.2.1.47.1.3.2.1.2  
.1.3.6.1.2.1.4.21.1  
.1.3.6.1.2.1.4.20.1.1  
.1.3.6.1.6.3.1.1.5.3  
.1.3.6.1.6.3.1.1.5.4  
.1.3.6.1.6.3.1.1.4.1.0  
.1.3.6.1.4.1.9.9.402.1.2.1.9  
.1.3.6.1.2.1.105.1.1.1.9  
.1.3.6.1.2.1.31.1.1.1.18  
.1.3.6.1.2.1.47.1.1.1.1.13  
.1.3.6.1.2.1.4.34.1.3.2.16

.1.3.6.1.6.3.18.1.3.0  
.1.3.6.1.4.1.9.9.215.2  
.1.3.6.1.4.1.9.9.215.1.1.8.1.3.1  
.1.3.6.1.2.1.4.35.1.4  
.1.3.6.1.2.1.31.1.1.1.2  
.1.3.6.1.2.1.1.5.0

## **3COM**

### *3Com SuperStack 3*

.1.3.6.1.4.1.43.10.1.14.1.1.1.2  
.1.3.6.1.2.1.31.1.2.1.3  
.1.3.6.1.4.1.43.10.1.14.1.2.1.2  
.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.2.1.4  
.1.3.6.1.2.1.17.7.1.4.2.1.5

### *3Com 4500*

.1.3.6.1.4.1.43.45.1.2.23.1.1.1.1.5  
.1.3.6.1.4.1.43.45.1.2.23.1.1.3.1.4  
.1.3.6.1.4.1.43.45.1.2.23.1.1.3.1.2  
.1.3.6.1.4.1.43.45.1.2.23.1.2.1.1.1.2  
.1.3.6.1.4.1.43.45.1.2.23.1.2.1.1.1.3  
.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.43.45.1.2.23.1.3.2.1.2

## **Alcatel**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.2.1.5  
.1.3.6.1.4.1.89.48.22.1.1  
.1.3.6.1.4.1.6486.800.1.2.1.8.1.1.1.1.1

### *Alcatel 6000*

.1.3.6.1.4.1.6486.800.1.2.1.3.1.1.2.1.1.5

## **Apresia**

### *Apresia 2024G*

.1.3.6.1.4.1.278.2.8.5.1.3.1.9  
.1.3.6.1.4.1.278.2.8.5.2.2.1.2  
.1.3.6.1.4.1.278.2.8.5.1.3.1.2  
.1.3.6.1.4.1.278.2.8.5.1.3.1.10

*Apresia 3124GT, Apresia 4328GT, Apresia 4224GT-PSR*

.1.3.6.1.4.1.278.2.27.2.2.2.3  
.1.3.6.1.4.1.278.2.27.2.2.2.4  
.1.3.6.1.4.1.278.2.27.2.2.2.2

**Avaya (Nortel)**

.1.3.6.1.4.1.2272.1.3.3.1.7  
.1.3.6.1.4.1.2272.1.3.3.1.4  
.1.3.6.1.4.1.2272.1.3.2.1.11  
.1.3.6.1.4.1.2272.1.3.2.1.2  
.1.3.6.1.4.1.2272.1.4.10.1.1.1  
.1.3.6.1.4.1.2272.1.13.5.1.4  
.1.3.6.1.4.1.2272.1.13.5.1.10  
.1.3.6.1.4.1.2272.1.13.5.1.11  
.1.3.6.1.4.1.2272.1.14.18.1.3  
.1.3.6.1.4.1.2272.1.14.20.1.4  
.1.3.6.1.4.1.2272.1.3.3.1.8  
.1.3.6.1.2.1.55.1.12.1.2  
.1.3.6.1.4.1.2272.1.14.22.1.6  
.1.3.6.1.2.1.105.1.1.1.3

*Avaya (Nortel 1600)*

.1.3.6.1.4.1.2272.1.3.3.1.13

*Avaya (Nortel Old)*

.1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.1.2.2.1.6  
.1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.1.1.2.1.3  
.1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.1.1.2.1.2

**Brocade**

.1.3.6.1.4.1.1991.1.1.3.3.1.1.11  
.1.3.6.1.4.1.1991.1.1.3.2.6.1.3  
.1.3.6.1.4.1.1991.1.1.3.2.7.1.1  
.1.3.6.1.4.1.1991.1.1.3.3.1.1.50  
.1.3.6.1.4.1.1991.1.1.3.3.1.1.38  
.1.3.6.1.4.1.1991.1.1.3.20.1.2.1.1.5  
.1.3.6.1.4.1.1991.1.1.3.20.1.2.1.1  
.1.3.6.1.4.1.1991.1.1.3.2.7.1.22

*Foundry BigIron RX*

.1.3.6.1.4.1.1991.1.1.3.3.5.1.13  
.1.3.6.1.4.1.1991.1.1.3.2.6.1.1  
.1.3.6.1.4.1.1991.1.1.3.2.6.1.4

*Foundry EdgIron 2402*

.1.3.6.1.2.1.17.7.1.4.5.1.1

**Cisco**

.1.3.6.1.4.1.9.9.276.1.5.1.1.1  
.1.3.6.1.4.1.9.9.215.1.1.8.1.2  
.1.3.6.1.4.1.9.9.68.1.2.2.1.2  
.1.3.6.1.4.1.9.9.68.1.2.2.1.1  
.1.3.6.1.4.1.9.9.68.1.2.1.1.2  
.1.3.6.1.4.1.9.9.68.1.2.1.1.3  
.1.3.6.1.4.1.9.9.68.1.5.1.1.1  
.1.3.6.1.4.1.9.9.46.1.3.1.1.4  
.1.3.6.1.4.1.9.9.23.1.2.1.1.4  
.1.3.6.1.4.1.9.9.23.1.2.1.1  
.1.3.6.1.4.1.9.5.1.4.1.1.11  
.1.3.6.1.4.1.9.5.1.9.3.1.3  
.1.3.6.1.4.1.9.5.1.9.3.1.7  
.1.3.6.1.4.1.9.5.1.9.3.1.8  
.1.3.6.1.4.1.9.5.1.9.3.1.5  
.1.3.6.1.4.1.9.9.46.1.6.1.1.13  
.1.3.6.1.4.1.9.9.215.1.1.1.0  
.1.3.6.1.4.1.9.9.215.1.1.5.0  
.1.3.6.1.4.1.9.9.215.1.2.1.1.2  
.1.3.6.1.4.1.9.9.215.1.2.1.1.1

*Cisco Small Business 300 Series*

.1.3.6.1.4.1.9.6.1.101.48.22.1.1

**Comtec**

1.3.6.1.4.1.35270.533.2.20.2.1.1  
1.3.6.1.4.1.35270.533.2.6.5.1.1  
1.3.6.1.4.1.35270.533.1.3.1.1.11  
1.3.6.1.4.1.35270.533.1.3.1.1.12  
1.3.6.1.4.1.35270.533.2.3.1.1.1.1

**D-Link***DGS 3100, DGS 3200*

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.2.1.4.0  
.1.3.6.1.2.1.17.7.1.4.2.1.5.0



*DGS 1224T*

.1.3.6.1.4.1.171.10.76.5.13.1.1.3  
.1.3.6.1.4.1.171.10.76.5.13.1.1.4  
.1.3.6.1.4.1.171.10.76.5.13.1.1.2

*DES 1252*

.1.3.6.1.4.1.171.10.75.4.13.1.1.3  
.1.3.6.1.4.1.171.10.75.4.13.1.1.4  
.1.3.6.1.4.1.171.10.75.4.13.1.1.2

*DGS 1248*

.1.3.6.1.4.1.171.10.76.6.13.1.1.3  
.1.3.6.1.4.1.171.10.76.6.13.1.1.4  
.1.3.6.1.4.1.171.10.76.6.13.1.1.2

**Dasan**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.3.1

**Dax**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.6339.100.5.1.1.2  
.1.3.6.1.2.1.17.7.1.4.2.1.4.0  
.1.3.6.1.2.1.17.7.1.4.2.1.5.0

**Dell**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.2.1.4.0  
.1.3.6.1.2.1.17.7.1.4.2.1.5.0  
.1.3.6.1.4.1.674.10895.5000.2.89.48.22.1.1  
.1.3.6.1.4.1.89.48.62.1.1  
.1.3.6.1.2.1.55.1.8.1.2

*Dell 6200*

.1.3.6.1.4.1.674.10895.5000.2.6132.1.1.1.2.13.1.26  
.1.3.6.1.4.1.674.10895.5000.2.6132.1.1.1.2.13.1.43

*Dell PowerConnect*

.1.3.6.1.4.1.89.48.22.1.1

**Enterasys**

.1.3.6.1.2.1.17.7.1.4.5.1.1

## Extreme

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.1916.1.16.1.1.4  
.1.3.6.1.4.1.1916.1.16.1.1.3

### ExtremeXOS

.1.3.6.1.4.1.1916.1.2.1.2.1.10  
.1.3.6.1.4.1.1916.1.2.1.2.1.2  
.1.3.6.1.4.1.1916.1.2.6.1.1.1  
.1.3.6.1.4.1.1916.1.2.6.1.1.2  
.1.0.8802.1.1.2.1.3.7.1.3  
.1.3.6.1.4.1.1916.1.1.2.2.1.1

## H3C

.1.3.6.1.4.1.2011.2.23.1.2.1.1.1.3  
.1.3.6.1.4.1.25506.8.35.1.1.1.5 **or** .1.3.6.1.4.1.2011.2.23.1.1.1.1.5  
.1.3.6.1.4.1.25506.2.9.1.1.2  
.1.3.6.1.4.1.25506.8.35.2.1.1.1.2  
.1.3.6.1.4.1.25506.8.35.2.1.1.1.3  
.1.3.6.1.4.1.25506.8.35.2.1.1.1.18  
.1.3.6.1.2.1.105.1.1.1.3.1  
.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.2011.10.2.9.2

## HP

.1.3.6.1.4.1.11.2.14.11.5.1.9.16.1.1.3  
.1.3.6.1.2.1.17.7.1.4.2.1.5.0  
.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.11.2.3.7.11.90.0.2  
.1.3.6.1.2.1.16.9.1.1.2.75  
.1.3.6.1.2.1.16.9.1.1.2.76  
.1.3.6.1.2.1.105.1.1.1.3.1  
.1.3.6.1.2.1.105.1.1.1.3

### HP 4000m

.1.3.6.1.4.1.11.2.14.11.5.1.3.1.1.4.1.5  
.1.3.6.1.4.1.11.2.14.11.5.1.3.1.1.8.1.1  
.1.3.6.1.2.1.47.1.2.1.1.2.1

**Hirschmann**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.3.1  
.1.3.6.1.2.1.17.7.1.4.3.1.3

**Huawei**

.1.3.6.1.2.1.17.7.1.4.2.1.5.0  
.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.2011.5.25.42.2.1.3.1.4  
.1.3.6.1.4.1.2011.5.25.42.1.1.1.3.1.3  
.1.3.6.1.4.1.2011.5.25.195.3.1.3

**Linksys**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.2.1.17.7.1.4.2.1.5.0

**NEC**

.1.3.6.1.2.1.17.7.1.4.5.1.1  
.1.3.6.1.4.1.119.2.3.126.2.23.1.2.1.1.1.3  
.1.3.6.1.4.1.119.2.3.126.2.23.1.1.1.1.5  
.1.3.6.1.4.1.119.2.3.126.2.23.1.1.3.1.4  
.1.3.6.1.4.1.119.2.3.126.2.23.1.1.3.1.2  
.1.3.6.1.4.1.119.2.3.126.2.23.1.2.1.1.1.2

## Appendix 5: Using Network Device Compliance Policies

Determine the compliance of Cisco network devices managed by the Switch Plugin. Use device compliance information to create CounterACT policies that accomplish the following types of proactive enforcement:

- Forbid SNMP Community String *public* settings.
- Require system logging to always be enabled.
- Forbid directed broadcast.
- Forbid SNMP access without ACL
- Forbid remote startup configuration from unwarranted sources.
- Detect accidental configuration errors. For example, prevent DHCP services from being mistakenly enabled or prevent accidental hostname changes.
- Ensure that AAA services are properly configured and enabled, for example, require authenticated login.

The screenshot shows the ForeScout interface with a table of hosts and a detailed view of a device's running configuration. The table has columns for Host, Host IP, Segment, Policy AAA Serv..., MAC Address, and Comment. A row is highlighted with a green dot, indicating a match. The detailed view shows the device's IPv4 Address, MAC Address, Function, Operating System, and Vendor and Model. A blue box highlights a specific configuration line in the running config: `no aaa new-model`.

Host	Host IP	Segment	Policy AAA Serv...	MAC Address	Comment
192.24.1.250	192.24.1.250	Net31	AAA Service ...	1920-455a-75a	

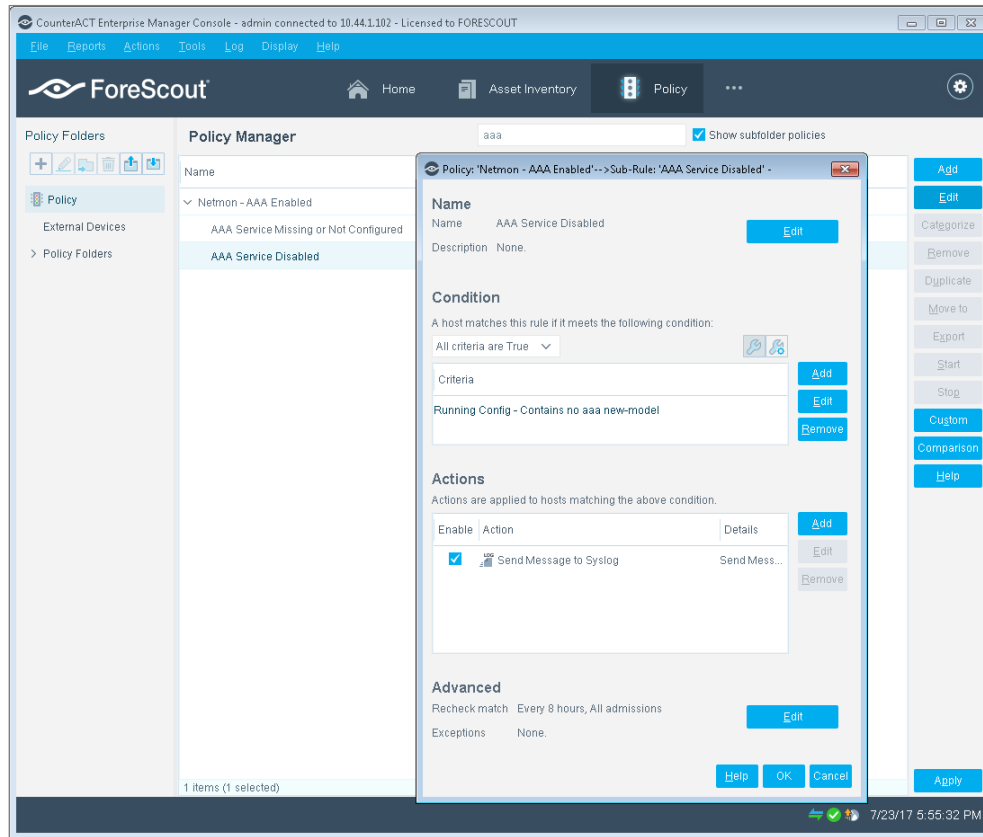
running config

Profile Compliance All Policies

IPv4 Address: 192.24.1.250 Function: Router or Switch  
 MAC Address: 1920-455a-75a Operating System: Cisco IOS  
 Vendor and Model: Cisco Router or Switch

```

type default
user-name qaadmin
creation-time 1474375013
privilege 0
password 0 qaadmin
type default
user-name qaadmin
creation-time 1490258484
password 0 qaadmin
no aaa new-model
!
aaa authentication login SSH none
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network Dudu local
aaa accounting identity default start-stop group radius
aaa accounting system default start-stop group radius
!
  
```




## How It Works

Several switch properties enable policies to detect and obtain *running config* information that is generated by managed, Cisco network devices that have the **show running-config** command run on them. Use the following switch network device compliance properties to create a variety of compliance policies:

Property	Description
<b>Running Config</b>	<p>Detects <i>running config</i> information of switches managed by CounterACT, as generated by the <b>show running-config</b> command.</p> <p>The Switch Plugin resolves this property for information at the following instances: (a) After plugin start and initially detecting the switch and (b) Whenever <i>running config</i> information changes (thereby, reduces load on the targeted network devices).</p>
<b>Running Config Time</b>	<p>Contains the timestamp, MM/DD/YY HH:MM:SS AM/PM, of the plugin's <i>running config</i> information query of the device.</p>

Property	Description
<b>Interface Table</b>	<p>Detects the specific interface configuration provided in a device <i>running config</i> for the interface.</p> <p>Per interface, the resolved property provides the following information:</p> <ul style="list-style-type: none"> <li>▪ Interface Name - The interface name and when available the interface location information.</li> <li>▪ Interface Configuration (raw) - the specific, interface configuration, as provided in a device <i>running config</i>.</li> </ul>

 *Network device compliance properties - Running Config, Running Config Time and Interface Table - are only resolved for a managed switch's Host IP address and not for any of the managed switch's entries having an IP Interface Address (formerly termed in the Console More IPs).*

In addition, detect and compare configuration changes, using the following switch track changes property:

Property	Description
<b>Switch Running Config Change</b>	Detects <i>running config</i> information changes in the device.

## Prerequisites for Network Device Compliance Property Use

Perform the following configuration tasks before working with the network device compliance properties:

- [Define User with Privileged Permissions](#)
- [Configure the Plugin](#)
- [Activate the cdm Configuration Flag](#)

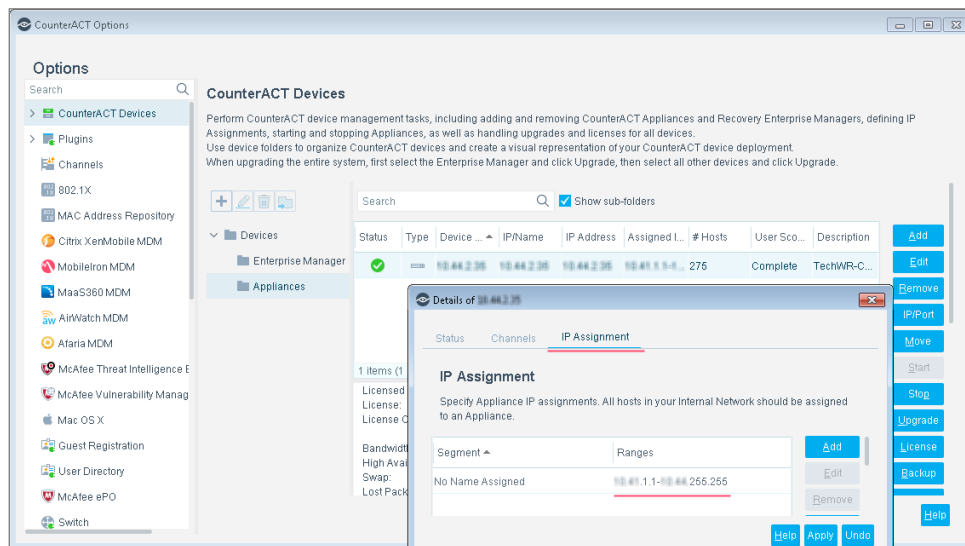
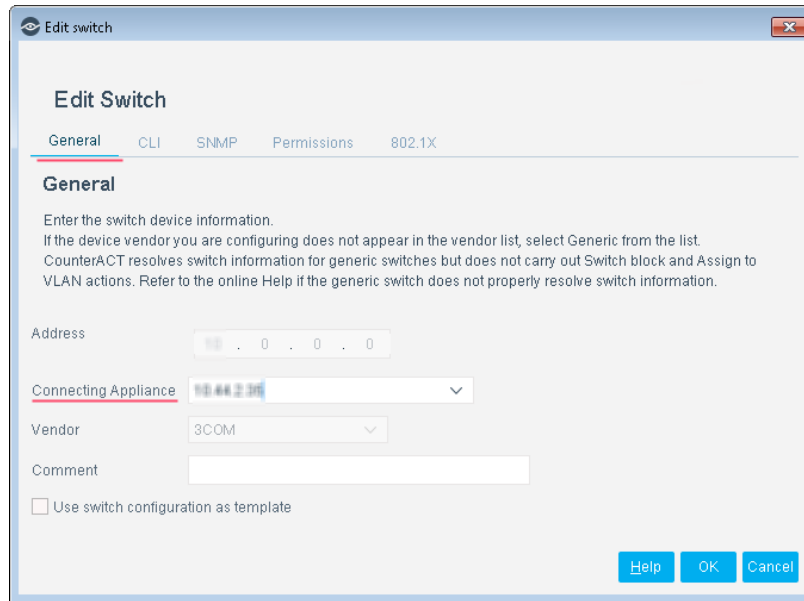
### Define User with Privileged Permissions

Verify that the user defined on the network device has privileged permissions.

### Configure the Plugin

Verify that the plugin configuration for the switch includes the following:

- The CLI option defined with privileged access.
- The MAC Read/Write method defined with SNMP and CLI permissions.
- The **Connecting Appliance** assigned to the switch contains the switch's IP address in the Appliance **IP Assignment** range.



This helps ensure consistent compliance validation and saves network utilization. Refer to the *CounterACT Administration Guide* for information about Appliance **IP Assignment**. See [Additional CounterACT Documentation](#) for information on how to access this guide.

**To define the necessary CLI and MAC Permissions settings, do the following:**

1. In the **CLI** tab, select the **Use CLI** checkbox.
2. In the **Privileged Access Parameters** section of the **CLI** tab, select the **Enable privileged access** checkbox.

The screenshot shows the 'Edit Switch' dialog box with the 'CLI' tab selected. The dialog has a title bar 'Edit switch' and a close button. Below the title bar are tabs for 'General', 'CLI', 'SNMP', 'Permissions', and '802.1X'. The 'CLI' tab is active and contains the following content:

**Edit Switch**

General CLI SNMP Permissions 802.1X

**CLI**

Configure the plugin to connect to the managed switch using CLI credentials - either Telnet or SSH credentials.

Use CLI

Connection Type SSH ▾

User

Password

Confirm Password

**Privileged Access Parameters**

Enable privileged access

No password

Use login parameters

Custom

User a

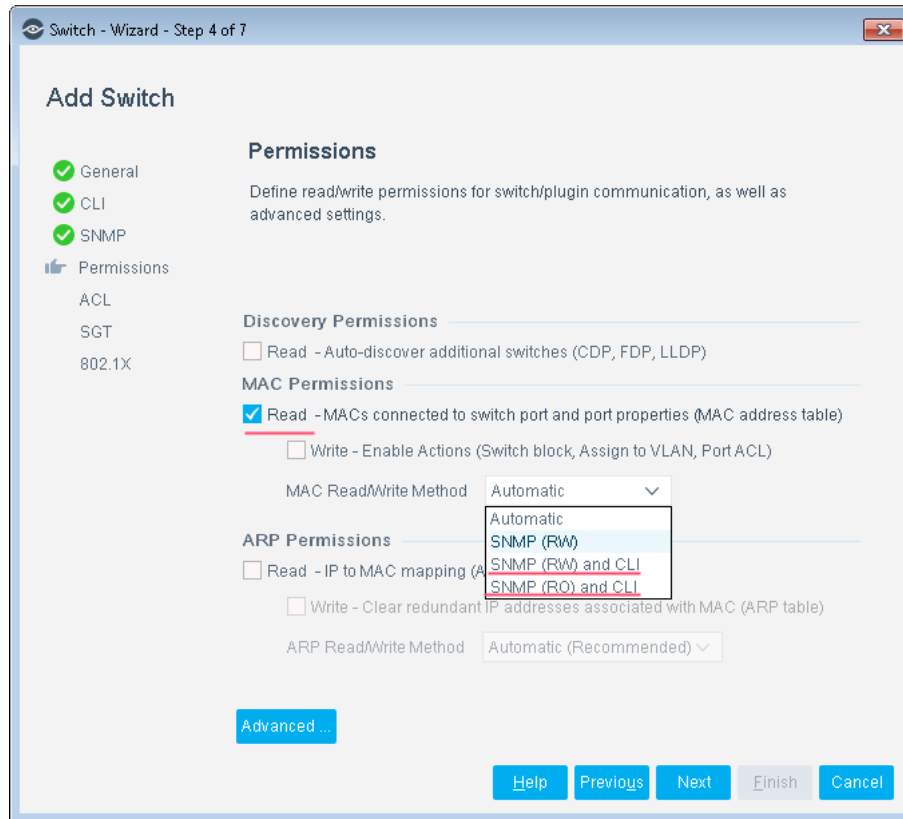
Password \*\*\*

Confirm Password \*\*\*

Buttons: Help, OK, Cancel

3. In the **MAC Permissions** section of the **Permissions** tab, do the following:
  - Select the **Read** checkbox.
  - In the **MAC Read/Write Method** dropdown, select either one of the following options: **SNMP (RW) and CLI** or **SNMP (RO) and CLI**.





## Activate the cdm Configuration Flag

In order to use the network device compliance properties, that is, enable resolution of these policy properties, you must activate the **cdm** advanced configuration flag.

### To activate the cdm flag:

1. In the **Tools** menu, select **Options**.
2. In the Switch tab, select one or more switches, as relevant.
3. Select **Edit** and then select **Permissions**.
4. Select **Advanced**. The Switch Advanced Settings window opens.

**Switch Advanced Settings**

**Performance tuning**

Auto-discover additional switches every  seconds

Read MACs connected to switch port and port properties (MAC address table) every  seconds

Read IP to MAC Mapping every  seconds

Read IP to MAC mapping protection between subsequent queries  seconds

When SNMP is used to read IP to MAC mapping, refresh reported entries every  seconds

**Settings**

SNMP parameters

SSH parameters

Ignore actions on port names:

Ignore actions on port aliases:

Don't learn on port name:

In the above port-related fields, provide regular expressions and/or plain text separated by the semicolon (;).  
For plain text, prefix each special character with the backslash (\).  
For example, aa.\*bb.\*;fc4 \Slot 1 Port 4\

Detect endpoints connected to trunk ports

Maximum connected endpoints per port

Set port alias on action

**IP to MAC mapping**

Read - IP to MAC mapping (ARP table) for VRFs

Connectivity Groups

Allow IP Discovery from Connectivity Group

**Default VLAN**

Default VLAN ID/Name

Only assign vacant ports to default VLAN

**Configuration Flags**

Configuration flags

**NAT Layer 3 Translation**

ARP translation ...

**Restore defaults** **OK** **Cancel**

5. In the **Configuration flags** field, enter `cdm:on`.

Stop resolution of the network device compliance properties by deactivating the `cdm` advanced configuration flag.

**To deactivate the cdm flag:**

- In the **Configuration flags** field of the Switch Advanced Settings window, enter `cdm:off`.

## Tuning

The following tuning options are available when working with the Running Config property:

- [Filter Resolved Running Config Information](#)
- [Adjust the Device Properties Query Rate](#)

### Filter Resolved Running Config Information

The amount of information provided by the resolved Running Config property can be very extensive. Filter this information by instructing CounterACT to ignore specific information, thereby eliminating information that is not required for the compliance verification, for example, comments or descriptions. Information filtering prevents overloading CounterACT and any third-party systems that CounterACT might share this information with.

In the **Switch Advanced Settings** window, use the configuration flag `running_config_content_filter` to define a filter for use with the information provided by the resolved Running Config property.

#### To define the filter configuration flag:

1. Select **Options** from the **Tools** menu.
2. In the **Switch** tab, select one or more switches, as relevant.
3. Select **Edit** and then select **Permissions**.
4. Select **Advanced**. The **Switch Advanced Settings** window opens.

**Switch Advanced Settings**

**Performance tuning**

Auto-discover additional switches every: 600 seconds

Read MACs connected to switch port and port properties (MAC address table) every: 60 seconds

Read IP to MAC Mapping every: 600 seconds

Read IP to MAC mapping protection between subsequent queries: 30 seconds

When SNMP is used to read IP to MAC mapping, refresh reported entries every: 16200 seconds

**Settings**

SNMP parameters: [Text Field]

SSH parameters: [Text Field]

Ignore actions on port names: [Text Field]

Ignore actions on port aliases: [Text Field]

Don't learn on port name: [Text Field]

In the above port-related fields, provide regular expressions and/or plain text separated by the semicolon (;).  
For plain text, prefix each special character with the backslash (\).  
For example, aa.\*bb.\*;ifc4 \Slot 1 Port 4\

Detect endpoints connected to trunk ports

Maximum connected endpoints per port: 10

Set port alias on action

**IP to MAC mapping**

Read - IP to MAC mapping (ARP table) for VRFs

Connectivity Groups: [Text Field]

Allow IP Discovery from Connectivity Group

**Default VLAN**

Default VLAN ID/Name: [Text Field]

Only assign vacant ports to default VLAN

**Configuration Flags**

Configuration flags: running\_config\_content\_filter:<regular expression>

**NAT Layer 3 Translation**

ARP translation ...

Restore defaults OK Cancel

5. In the **Configuration flags** field, enter the statement:  
**running\_config\_content\_filter:<regular expression>**

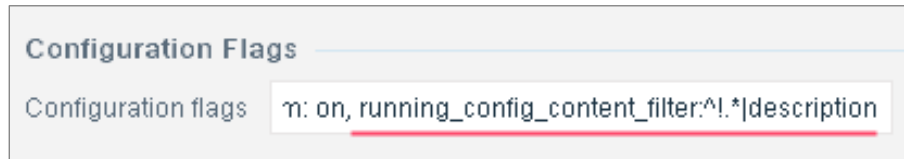
The regular expression contains the filtering criteria to be applied.

During filter processing, when a line of information is found to match any one of the criteria provided in the regular expression it is eliminated from the resulting information output.

### Filter Example

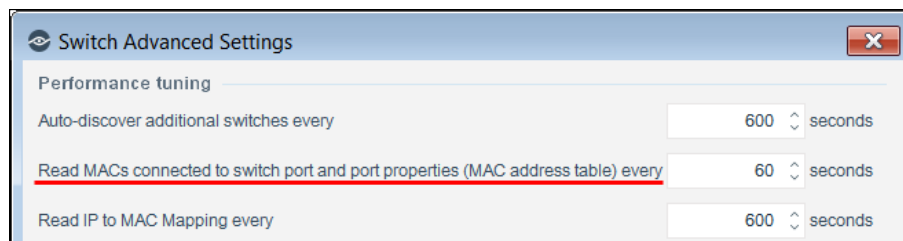
To eliminate any line of information, provided by the resolved *running config* property, that contains either a comment or the word *description*, provide the statement:

```
running_config_content_filter:^\!.*|description
```



## Adjust the Device Properties Query Rate

By default, the Switch Plugin queries device properties for updates every 10 minutes, regardless of the policy recheck interval. Running Config is an example of a device property. This query rate can be adjusted per device in the **Switch Advanced Settings** window, using the **Read MACs connected to switch port and port properties (MAC address table)** value; this field's default value is 60 seconds.



The device properties query rate is calculated as follows:

**Read MACs connected to switch port and port properties (MAC address table)** value multiplied by 10.

- 📖 *In addition to being used to calculate the device properties query rate, the **Read MACs connected to switch port and port properties (MAC address table)** value defines the Read MAC query rate.*

**To adjust the device properties query rate for a configured switch device, do the following:**

1. In the Console toolbar, select **Options**.
2. In the navigation pane, select **Switch**.
3. In the **Switch** tab, select the relevant switch.
4. Select **Edit** and then select the **Permissions** tab.
5. Select **Advanced...** . The **Switch Advanced Settings** window opens.
6. In the **Read MACs connected to switch port and port properties (MAC address table)** field, use the up/down arrow keys to modify the value.
7. Select **OK** > **OK** > **Apply**. The Switch Plugin configuration is updated.

## Appendix 6: Working with ACL Capabilities

This section presents an overview of Switch Plugin access control list (ACL) capabilities for the management of switches. ACLs, applied on a switch, perform packet filtering on traffic traveling through the switch and are commonly used to restrict the network usage of connecting endpoints. The Switch Plugin offers CounterACT operators the following ACL capabilities for switch management:

- The [Endpoint Address ACL Action](#)
- The [Access Port ACL Action](#)
- The [Pre-Connect Mode](#)

For plugin IPv6 support exceptions with ACL-related functionality, see [IPv6 Support](#).

Additionally, this section provides the following supporting information for working with plugin ACL capabilities:

- [Identifying Supported ACL Blocking](#)
- [Switch Vendor ACL Support](#)
- [What to Do](#)

### Endpoint Address ACL Action

The *Endpoint Address ACL* action applies an ACL that delivers blocking protection *when* endpoints connect to the network. Other benefits of Endpoint Address ACL blocking include:

- Access limitations on flat networks, when there is no opportunity to assign endpoints to a VLAN.
- Blocking specific endpoints and not all endpoints on a switch port.
- Limiting access to endpoints at their connection point to the network without the need to reassign to VLAN to achieve the same access limitations.
- More robust control of UDP traffic.
- Block endpoints on a backbone switch via the trunk connection, when the endpoint connected to the switch does not support ACL or is connected to an unmanaged switch.

The following types of Endpoint Address ACL blocking are available:

- Close or open network zones, services or protocols on specific endpoint IP addresses or groups of them directly at the switch. See [IP Address Blocking Capability](#) for details.
- Block traffic from an endpoint to a switch based on the endpoints MAC address. See [MAC Address Blocking Capability](#) for details.

## IP Address Blocking Capability

Use IP ACL rules that instruct a switch to execute any of the following:

- Block all traffic from network address(es) to targeted port(s)/service(s) in detected endpoint(s), based on endpoint IP addresses.
- Block all traffic from detected endpoint(s), based on endpoint IP addresses, to targeted port(s)/service(s) in network address(es).
- Allow blocking exceptions

For switches that support IP ACL blocking, use the *Endpoint Address ACL* action to define the ACL rules. The rules will apply to all endpoints on the switch detected as a result of your policy. When incorporating the action into a policy you can apply different rules to different network segments.

See [What to Do](#) for information about configuration required when working with IP address ACL blocking.

## MAC Address Blocking Capability

Use MAC ACL rules to instruct a switch to block detected endpoints based on their MAC address. All traffic from the endpoint to the switch is blocked. This is useful, for example, when you want to control traffic at Layer 2 and the switch cannot be configured to block IP addresses. For switches that support MAC ACL blocking, use the *Endpoint Address ACL* action to apply blocking based on MAC address.

See [What to Do](#) for information about configuration required when working with MAC address ACL blocking.

## Access Port ACL Action

The *Access Port ACL* action applies a network operator-defined ACL, addressing one or more than one access control scenario, which is applied to an endpoint's switch access port. These access control scenarios are typically role or classification driven, for example, registered guest or compliance, and not endpoint IP specific. This differs from Endpoint Address ACL blocking, where CounterACT limits the rules of the ACL – only allowing the adding/removing of endpoint addresses to the ACL's permit/deny rules. The plugin does not inspect or change the ACL configuration, but acts as a delivery vehicle to provision a network switch.

With Access Port ACLs, a network operator has total control over the ACL configuration and can take advantage of the full set of switch capabilities, regardless of endpoint IP address status (has IP, does not have IP, has multiple assigned IPs, has multiple assigned IPs that change with time). For example, define an ACL configuration that denies corporate network access to guests but permits Internet access, regardless of endpoint IP address (no IP address dependency).

Access Port ACLs are applied to switch access ports, which can be any of the following IP interfaces:

- A switch port
- A switch port assigned to a single VLAN

- A switch port assigned to a single VLAN and a VoIP VLAN
- 📄 *An Access Port ACL is not intended for application on ports serving multiple endpoints; specifically, trunk ports and uplink ports are not supported.*

## Use Cases

- A network operator seeking basic, access control with minimal impact to end users and network infrastructure. Needs to enforce network restrictions for corporate endpoints and guest endpoints and quarantine other endpoints without changing VLAN assignments or requiring pre-registration of IP/ MAC configuration.
- For a high security deployment that either does not use RADIUS or handles endpoints that cannot perform 802.1X authentication (avoid extended delays of MAB timeouts). Needs to restrict network access until a successful authentication/compliance inspection completes.
- Network operator using vendor specific APIs, for example, ACL restriction rules (conditions), traffic shaping (QoS) and logging.

## Reduced Switch Processing Load

Use of Access Port ACL reduces switch processing load. Because ACL content is not IP address dependent, each application to a switch access port:

- Does not require the switch to re-compile its entire ACL configuration
- Does not suspend switch ACL treatment for the applied/associated ports, while the ACL configuration is re-evaluated for packet filtering rules

See [What to Do](#) for information about configuration required when working with Access Port ACLs.

## Pre-Connect Mode

The Pre-Connect Mode capability, which is only available for use on managed Cisco switches, extends CounterACT enforcement by applying **immediate** ACL control to switch access ports without having to first wait for policy evaluation and plugin application of an ACL action [*Access Port ACL, Endpoint Address ACL*].

In the **Pre-Connect Mode** section of the ACL pane/tab, select an ACL from the Switch Plugin ACL Repository for the plugin to apply as the Pre-Connect ACL on **qualified** switch **access ports** on a managed Cisco switch.

Flexible application of the Pre-Connect ACL is accomplished using the following configuration options:

- Only apply the Pre-Connect ACL to occupied access ports (**Fail-Open**)
- Apply the Pre-Connect ACL to both occupied access ports and vacant switch ports (**Fail-Close**)
- Override all non-CounterACT ACLs applied to access ports by applying the Pre-Connect ACL

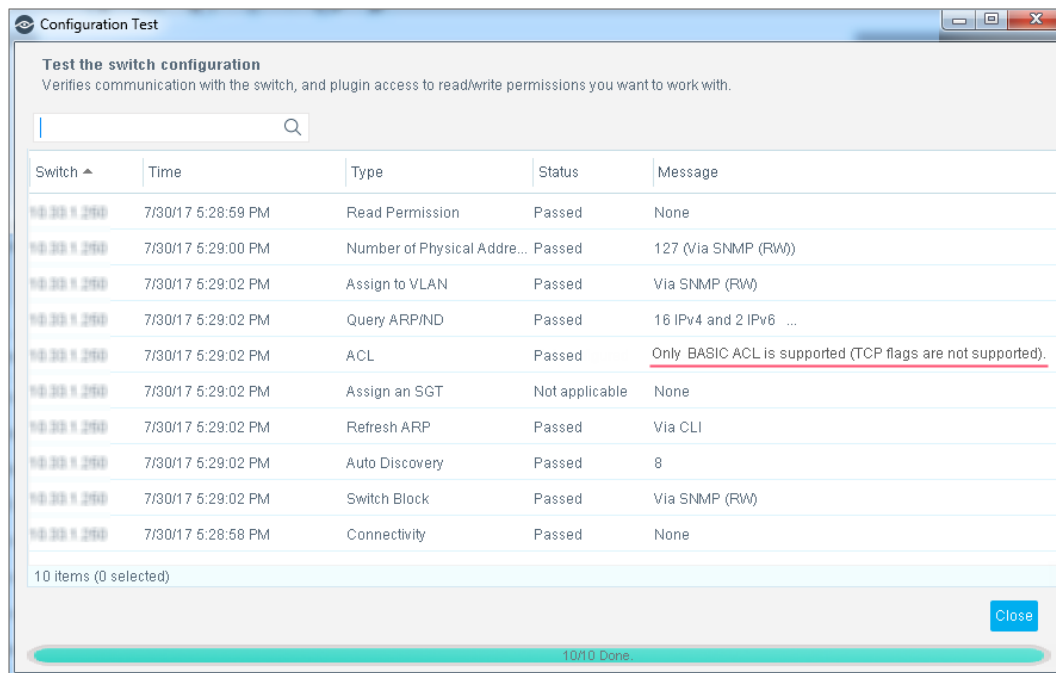


- Never apply the Pre-Connect ACL to access ports having a currently applied non-CounterACT ACL

For additional details see [Pre-Connect Mode](#). For details about working with the ACL Repository, see [The ACL Repository](#).

## Identifying Supported ACL Blocking

The test of the plugin configuration for managing a particular switch produces results that identify the kind of ACL blocking supported by that switch.



Switch	Time	Type	Status	Message
10.30.1.250	7/30/17 5:28:59 PM	Read Permission	Passed	None
10.30.1.250	7/30/17 5:29:00 PM	Number of Physical Addre...	Passed	127 (Via SNMP (RW))
10.30.1.250	7/30/17 5:29:02 PM	Assign to VLAN	Passed	Via SNMP (RW)
10.30.1.250	7/30/17 5:29:02 PM	Query ARP/ND	Passed	16 IPv4 and 2 IPv6 ...
10.30.1.250	7/30/17 5:29:02 PM	ACL	Passed	Only BASIC ACL is supported (TCP flags are not supported).
10.30.1.250	7/30/17 5:29:02 PM	Assign an SGT	Not applicable	None
10.30.1.250	7/30/17 5:29:02 PM	Refresh ARP	Passed	Via CLI
10.30.1.250	7/30/17 5:29:02 PM	Auto Discovery	Passed	8
10.30.1.250	7/30/17 5:29:02 PM	Switch Block	Passed	Via SNMP (RW)
10.30.1.250	7/30/17 5:28:58 PM	Connectivity	Passed	None

10 items (0 selected)

Close

10/10 Done

See [Test Failure Scenarios](#) for details.

## Switch Vendor ACL Support

The following tables define the ACL capabilities that are available to use with the Switch Plugin for supported, vendor switches:

- [Brocade Switches \(except for IronWare switches\)](#)
- [Brocade IronWare Switches](#)
- [Cisco Switches \(except for Catalyst 2950 switches and Small Business 300 Series switches\)](#)
- [Cisco Catalyst 2950 Switches – Standard Image Software](#)
- [Cisco Catalyst 2950 Switches – Enhanced Image Software](#)
- [Enterasys Switches](#)
- [Juniper Switches](#)

**Brocade Switches (except for IronWare switches)**

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Supported	Not supported	Not supported	<b>Endpoint Address ACL:</b> Comprehensive ACL rule supported

**Brocade IronWare Switches**

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Use <b>Basic ACL on action failure</b> option supported. ACL rule numbering not supported.	Supported	Not supported	<b>Endpoint Address ACL:</b> <ul style="list-style-type: none"> <li>▪ Cannot use IP and MAC ACL rules simultaneously on the same port.</li> <li>▪ For managed Brocade Layer 3 switches, stackable models ICX6430 and ICX6450 that run IronWare OS version .07.4 and above, the plugin supports applying the <i>Endpoint Address ACL</i> action on detected endpoints, when these endpoints are connected to a port VLAN that is configured with a virtual routing interface (the plugin applies the <i>Endpoint Address ACL</i> action on the VLAN's virtual routing interface, instead of the VLAN's Ethernet interface).</li> </ul>

**Cisco Switches (except for Catalyst 2950 switches and Small Business 300 Series switches)**

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Supported	Supported	Supported	<b>Endpoint Address ACL:</b> Comprehensive ACL rule supported

**Cisco Catalyst 2950 Switches – Standard Image Software**

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Not supported	Not supported	Supported	

ACL support is available for Cisco Catalyst 2950x switches that are limited to Standard Image (SI) support, including:

- Catalyst 2950-12 Standard Image (SI)
- Catalyst 2950-24 Standard Image (SI)
- Catalyst 2950SX-24 Standard Image (SI)

**Cisco Catalyst 2950 Switches – Enhanced Image Software**

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Use Basic ACL on action failure option supported. ACL rule numbering not supported.	Supported	Supported	<b>Endpoint Address ACL:</b> Cannot use IP and MAC ACL rules simultaneously on the same port.

ACL support is available for Cisco 2950x switches that support the installation of Enhanced Image (EI). These include:

- Catalyst 2950T-24 Enhanced Image (EI)
- Catalyst 2950C-24 Enhanced Image (EI)
- Catalyst 2950G-12-EI Enhanced Image (EI)
- Catalyst 2950G-24-EI Enhanced Image (EI)
- Catalyst 2950G-24-EI-DC Enhanced Image (EI)
- Catalyst 2950G-48-EI Enhanced Image (EI)

**Enterasys Switches**

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Supported	Not supported	Not supported	<b>Endpoint Address ACL:</b> Comprehensive ACL rule supported

### Juniper Switches

Endpoint Address ACL		Access Port ACL	Comments
Based on IP Address	Based on MAC Address		
Supported <b>Use Basic ACL on action failure</b> option is not supported.	Supported	Not supported	

## What to Do

In order to use the Switch Plugin ACL capabilities with a managed switch, the following must be performed:

- Using either the Add Switch wizard or the Edit Switch window, configure the **Write – Enable Actions** for MAC permissions. See [MAC Permissions](#).
- Using either the Add Switch wizard or the Edit Switch window, configure ACL capabilities per switch being configured to interoperate with the Switch Plugin. See any of the following:
  - [ACL Configuration – Cisco and Brocade Switches](#)
  - [ACL Configuration – Enterasys Matrix N-Series Switches](#)
  - [ACL Configuration – Juniper Switches](#)
- Setup your switches to work with the Switch Plugin and the ACL capability. See [Configuring Switches for ACL Integration](#).
- To work with plugin-provided ACL actions:
  - Using either the Add Switch wizard or the Edit Switch window, configure the advanced configuration flag `acl_action_type` with the appropriate ACL action type for either Access Port ACL or Endpoint Address ACL. See [Enable a Feature](#).
  - Define the required action in policies – either *Access Port ACL* action or *Endpoint Address ACL* actions (IP address-based ACL or MAC addressed-based ACL). See [Restrict Actions](#).

## Appendix 7: Improve Switch Management for Large Deployments

This section discusses implementing a multi-process plugin architecture; such an architecture significantly increases the real-time, switch management capacity of CounterACT. This approach is useful in very large networks with many L2/L3 switches.

The following topics are covered:

- [Multi-Process Switch Plugin Architecture](#)
- [Deploy Plugin Multi-Process Operation](#)
- [Determining the Number of Sub-Processes to Run](#)
- [Administer Plugin Multi-Process Operation per Appliance](#)

### Multi-Process Switch Plugin Architecture

When the Switch Plugin operates in multi-process mode, it initiates and sustains several simultaneous processes - one parent process and a variable number of switch management child processes. The parent process communicates between parallel switch management child processes and the CounterACT infrastructure. This architecture allows numerous, concurrent switch management sessions to run, multiplying the capacity of the Switch Plugin as compared with single-process versions of the Switch Plugin.

### Number of Sub-Processes to Run

When operating in multi-process mode, the Switch Plugin determines the number of sub-processes to run on each Appliance based on its consideration of the following factors:

- The number of active switch devices that the Appliance manages (active switch devices do not have any of the following statuses: *disabled*, *newly discovered* or *not a switch*)
- The CounterACT-established maximum number of switch devices that any single sub-process should manage
- The number of Appliance CPUs
- The amount of Appliance RAM

## Deploy Plugin Multi-Process Operation

In order to deploy Switch Plugin multi-process operation in CounterACT Appliances, you must perform the following administrative tasks:

- [Engineer Appliance Management Processing Load](#)
- [Enable Multi-Process Operation for the Plugin](#)

### Engineer Appliance Management Processing Load

Deploying Switch Plugin multi-process operation in your CounterACT Appliances requires you to be aware of the management processing load that will be required of these Appliances and, if necessary, adjust that processing load among Appliances.

For the recommended maximum number of switches that an Appliance can manage, refer to the [ForeScout Licensing and Sizing Guide](#). Use the provided information to plan for the use of Switch Plugin multi-process operation in CounterACT Appliances.

### Enable Multi-Process Operation for the Plugin

By default, the Switch Plugin operates in multi-process mode on all Appliances. In the **Edit general parameters** window, multi-process operation on all Appliances is enabled by default.

To disable multi-process operation on all Appliances and make the Switch Plugin run in standard, single-process mode on all Appliances, see [Global Configuration Options for the Switch Plugin](#).

## Determining the Number of Sub-Processes to Run

The Switch Plugin enhanced method for determining the number of sub-processes to run takes into consideration the following factors:

- The number of active switch devices that the Appliance manages (active switch devices do not have any of the following statuses: *disabled*, *newly discovered* or *not a switch*)
- The CounterACT-established maximum number of switch devices that any single sub-process should manage
- The number of Appliance CPUs
- The amount of Appliance RAM

In earlier versions of the Switch Plugin, the number of sub-processes put into operation by the plugin was determined using either of the following methods:

- A specific number of sub-processes property was defined in a properties file.
- A ratio property was defined in the properties file, which was then multiplied by the number of Appliance CPUs. The resulting product was used.

Neither of these existing methods takes into consideration the number of switches being managed by the Appliance.

## Plugin Multi-Process Operation Post-Upgrade

This section describes the multi-process operation method in effect for the Switch Plugin after upgrading to the current version.

- [Multi-Process Operation Unavailable in Previous Plugin Version](#)
- [Multi-Process Operation Available in Previous Plugin Version](#)

### Multi-Process Operation Unavailable in Previous Plugin Version

In any version prior to 8.7.0, Switch Plugin multi-process operation was **not available** for use. Upgrading from a version prior to 8.7.0 to the current version enables plugin multi-process operation using the enhanced method for determining the number of multi-processes to run.

### Multi-Process Operation Available in Previous Plugin Version

In all versions 8.7.0 and above, Switch Plugin multi-process operation **was available** for use. Upgrading from any version 8.7.0 or above to the current version maintains the existing plugin multi-process operation (enabled/disabled and the associated property values). It is recommended that your Switch Plugin use the enhanced method for determining the number of sub-processes to run, provided in the current version.

#### To use the enhanced method on all Appliances:

1. From the Console, stop the Switch Plugin on all CounterACT devices (the Enterprise Manager and all Appliances).  
(Select **Options** > **Modules**>**Network**> **Switch**> select **Stop**. In the Select Appliances window, select all CounterACT devices. Once plugin processing completes, the Switch Plugin status is **Not running**.)
2. Log in to the CLI on the Enterprise Manager.
3. Run the following commands using an SSH connection:
  - a. `fstool oneach -c fstool sw remove_property config.fssubproc_count.value`
  - b. `fstool oneach -c fstool sw remove_property config.fssubproc_cpuration.value`
  - c. `fstool oneach -c fstool sw remove_property config.fssubproc_manual_mode.value`
4. From the Console, start the Switch Plugin on all CounterACT devices.  
(Select **Options** > **Modules**>**Network**> **Switch**>click **Start** >. In the Select Appliances window, select all CounterACT devices. Once plugin processing completes, the Switch Plugin status initially displays as **Initializing** and then must update to **Running**.)

## Administer Plugin Multi-Process Operation per Appliance

Administer multi-process operation of the Switch Plugin per specific Appliances, using `fstool` commands. The following administrative capabilities are available:

- [Disable Multi-Process Operation of the Switch Plugin for an Appliance](#)
- [Force Appliance Use of the Switch Plugin Configured Settings](#)

### Disable Multi-Process Operation of the Switch Plugin for an Appliance

If **Enable multi-process mode** option is *selected* in the **Edit general parameters** window of the Switch Plugin, then multi-process operation of the Switch Plugin is enabled on all Appliances.

#### To disable multi-process operation of the Switch Plugin for a specific Appliance:

1. Log in to the CLI on the CounterACT Appliance.
2. Run the following commands:
  - a. `fstool sw set_property config.fssubproc_manual_mode.value true`
  - b. `fstool sw set_property config.fssubproc_count.value 1`
  - c. `fstool sw restart`

### Force Appliance Use of the Switch Plugin Configured Settings

Should you want to force an Appliance to return to operate according to the Switch Plugin settings as configured in the Console - in this specific case, operate per configured **Enable multi-process mode** option in the **Edit general parameters** window of the Switch Plugin - then perform the following procedure:

#### To force a specific Appliance to return to operate according to the configured Switch Plugin settings:

1. Log in to the CLI on the CounterACT Appliance.
2. Run the following commands:
  - a. `fstool sw remove_property config.fssubproc_manual_mode.value`
  - b. `fstool sw restart`



## Appendix 8: Switch Alerts

This section presents the processing alerts that the plugin can display about switches and Layer 3 devices. The plugin displays alerts in the **Switch Alerts** column of the Switch tab; hovering your cursor over either the **Status** column or the **Switch Alerts** column results in the display of the associated message/tooltip.

Alert Display Legend:

- Warning and informational alerts appear in orange text
- Error alerts appear in red text

Switch Alert	Type	Cause(s)	Message/Tooltip
<b>Permissions</b>	Error	Failed action: <ul style="list-style-type: none"> <li>▪ Assign to VLAN</li> <li>▪ Switch Block</li> </ul> regardless of whether application of the action was initiated by policy, manually or plugin configuration test.	<i>Failed to block/assign to VLAN</i>
<b>ARP</b>	Error in Layer 3, otherwise, Warning	When ARP permissions are configured for plugin management of a switch: <ul style="list-style-type: none"> <li>▪ No ARP entries found</li> <li>▪ Failed ARP test step in plugin configuration test</li> </ul>	<i>No ARP entries found</i>
<b>MAC Discovery</b>	Warning in Layer 3, otherwise, Error	When MAC permissions are configured for plugin management of a switch: <ul style="list-style-type: none"> <li>▪ No MAC entries found</li> <li>▪ Failed MAC test step in plugin configuration test</li> </ul>	<i>No MAC entries found</i>
<b>Auto Discovery</b>	Information	When Auto Discovery permissions are configured for plugin management of a switch: <ul style="list-style-type: none"> <li>▪ No switches detected</li> <li>▪ Failed Auto Discovery test step in plugin configuration test</li> </ul>	<i>No switches detected</i>
<b>ACL</b>	Error	Failed to establish SNMP connection	<i>No response from remote host &lt;switch_name&gt;</i>
		Failed to establish CLI connection – incorrect user name	<i>Failed log in to &lt;switch_IP_address&gt; error [Login Incorrect]</i>

Switch Alert	Type	Cause(s)	Message/Tooltip
		Failed to establish CLI connection – incorrect password	<i>Login Incorrect. CLI connection is invalid [Login Incorrect]</i>
		Failed to establish ACL connection – ACL test step in plugin configuration test	<i>ACL connection failed: Login Incorrect</i>
		Failed writing the Pre-Connect ACL rules on managed switch	<i>Cannot apply Pre-Connect ACL: Failure to provision switch with the ACL configuration</i>
		Failed writing the Pre-Connect ACL port on managed switch	<i>Cannot apply Pre-Connect ACL: Failure to link the provisioned ACL configuration to switch port(s)</i>
		Failed to apply ACL action	Per action application failure, a specific error
<b>No Connectivity</b>	Error	<ul style="list-style-type: none"> <li>▪ No queries returned results within the established <b>CONNECTIVITY TIMEOUT</b> period</li> <li>▪ No response from the switch</li> </ul>	<i>No response from the switch</i>
<b>Duplicate Switch</b>	Warning	The IP address of this switch is an IP interface address of another managed switch	<i>This Switch is a duplicate of switch &lt;switch_name &gt;</i>
<b>[blank - no entry]</b>	Information	Read/write permissions are not configured for plugin management of the switch. In the Switch tab, such a switch entry displays the status of <i>Disabled</i>	<i>Permissions have not been defined. The switch will not be queried or perform any actions</i>
<b>Configuration</b>	Information	The plugin configuration changed and <b>Apply</b> was not selected	<i>Select 'Apply' to set new configuration</i>
<b>Permission Pending</b>	Information	<p>The MAC permission <b>Write: Enable Actions</b> is enabled for plugin management of an added switch and both of the following conditions are true:</p> <ul style="list-style-type: none"> <li>▪ Plugin configuration test not yet performed</li> <li>▪ None of the relevant actions (<i>Assign to VLAN, Switch Block</i>) completed</li> </ul>	<i>Connecting to the switch...</i>

Switch Alert	Type	Cause(s)	Message/Tooltip
<b>MAC Discovery Pending</b>	Information	<p><b>MAC Permissions</b> are enabled for plugin management of an added switch and both of the following conditions are true:</p> <ul style="list-style-type: none"> <li>▪ Plugin configuration test not yet performed</li> <li>▪ The plugin MAC query did not complete</li> </ul>	<i>Connecting to the switch...</i>
<b>ARP Pending</b>	Information	<p><b>ARP Permissions</b> are enabled for plugin management of an added switch and both of the following conditions are true:</p> <ul style="list-style-type: none"> <li>▪ Plugin configuration test not yet performed</li> <li>▪ The plugin ARP query did not complete</li> </ul>	<i>Connecting to the switch...</i>
<b>Auto Discovery Pending</b>	Information	<p><b>Discovery Permissions</b> are enabled for plugin management of an added switch and both of the following conditions are true:</p> <ul style="list-style-type: none"> <li>▪ Plugin configuration test not yet performed</li> <li>▪ The plugin Auto Discovery query did not complete</li> </ul>	<i>Connecting to the switch...</i>
<b>New</b>	Information	New switch is discovered by another switch	<i>Discovered by Switch. Right-Click to define status as Approve or Not a Switch</i>
<b>Not a switch</b>	Information	CounterACT user marks the network device as <i>Not a Switch</i>	
<b>No managing appliance</b>	Error	Managing appliance not configured	<i>No managing appliance</i>
<b>Managing appliance disconnected</b>	Error	Managing appliance disconnected	<i>Managing appliance disconnected</i>

## Network Module Information

The Switch Plugin is installed with the CounterACT Network Module.

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

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

The Network Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release and may also be made available in between CounterACT releases.

The plugins listed above are installed and rolled back with the Network Module. Refer to the *CounterACT Network Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

## Additional CounterACT Documentation

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

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

### Documentation Downloads

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

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

### Product Updates Portal

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

#### To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.

2. Select the CounterACT version you want to discover.

### Customer Portal


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

#### To access documentation on the ForeScout Customer Portal:

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

### Documentation Portal

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

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

#### To access the Documentation Portal:

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

### CounterACT Help Tools

Access information directly from the CounterACT Console.

#### **Console Help Buttons**

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

#### **CounterACT Administration Guide**

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

#### **Plugin Help Files**

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

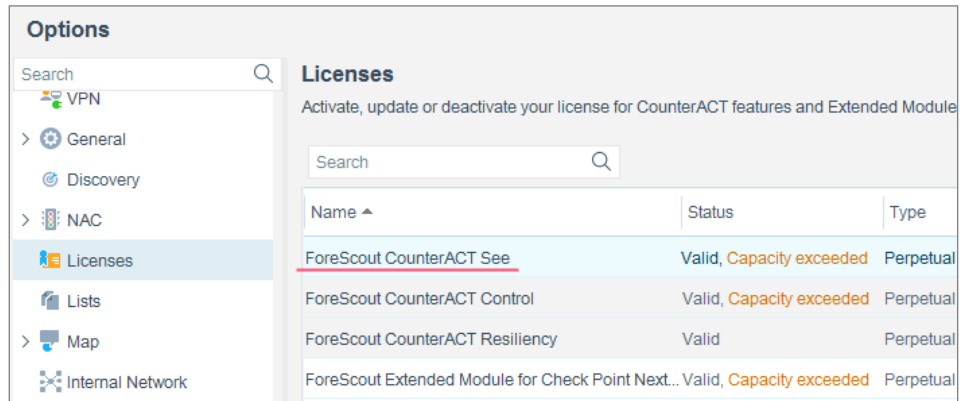
#### **Documentation Portal**

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

### Identifying Your Licensing Mode in the Console

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

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



The screenshot shows the 'Options' console page with the 'Licenses' section selected. The 'Licenses' section includes a search bar and a table with columns for Name, Status, and Type. The table lists four licenses, with the first one, 'ForeScout CounterACT See', highlighted in blue.

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

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

## Legal Notice

© 2018 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.

2018-04-10 09:21