

Policy Enforcer

Policy Enforcer Connectors Guide



Modified: 2018-07-17

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Policy Enforcer Policy Enforcer Connectors Guide

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Part 1	Connectors for Third-Party Switches, Wireless Access Controller, Public Cloud, and Private Cloud	
Chapter 1	Policy Enforcer Connectors	3
	Policy Enforcer Settings	3
	Policy Enforcer Connector Overview	6
	Benefits of Policy Enforcer Connector	7
	Creating a Policy Enforcer Connector for Public and Private Clouds	7
	Creating a Policy Enforcer Connector for Third-Party Switches	15
	Editing and Deleting a Connector	18
	Editing a Connector	18
	Deleting a Connector	19
	Viewing VPC or Projects Details	20
	Integrating ForeScout CounterACT with Juniper Networks SDSN	22
	Configuring the DEX Plug-in	22
	Configuring the Web API Plug-in	25
	Creating ForeScout CounterACT Connector in Security Director	27
	ClearPass Configuration for Third-Party Plug-in	30
	Cisco ISE Configuration for Third-Party Plug-in	37

PART 1

Connectors for Third-Party Switches, Wireless Access Controller, Public Cloud, and Private Cloud

- [Policy Enforcer Connectors on page 3](#)

CHAPTER 1

Policy Enforcer Connectors

- [Policy Enforcer Settings on page 3](#)
- [Policy Enforcer Connector Overview on page 6](#)
- [Creating a Policy Enforcer Connector for Public and Private Clouds on page 7](#)
- [Creating a Policy Enforcer Connector for Third-Party Switches on page 15](#)
- [Editing and Deleting a Connector on page 18](#)
- [Viewing VPC or Projects Details on page 20](#)
- [Integrating ForeScout CounterACT with Juniper Networks SDSN on page 22](#)
- [ClearPass Configuration for Third-Party Plug-in on page 30](#)
- [Cisco ISE Configuration for Third-Party Plug-in on page 37](#)

Policy Enforcer Settings

To access this page, in the Security Director UI, navigate to **Administration > Policy Enforcer > Settings**.

Before You Begin

- Policy Enforcer Release version and Security Director Release version must be compatible. The Settings page shows the current release version of Policy Enforcer. If there is an incompatibility, an error message is shown that there is a mismatch between Security Director and Policy Enforcer release versions. To know more about the supported software versions, see *Policy Enforcer Release Notes*.

You cannot proceed further if the Policy Enforcer and Security Director Release versions are incompatible.

- A valid Policy Enforce VM password is required to have a fully functional Policy Enforcer. If the password is valid, a message is shown at the top of the Settings page that the Policy Enforcer Space user (pe_user) password is currently valid and the date by when the password expires. The pe_user has the same capabilities as the super user.

If the password is invalid, an error message is shown at the top of the Settings page. To fix this issue, login to the Policy Enforcer VM, change the root password, and then enter a new value in the Settings page.

- Policy Enforcer with Security Director can be used in four different configuration types. For each configuration type, certain features are available. Read the following topic:

Sky ATP Configuration Type Overview before you make a Sky ATP Configuration Type selection on the Policy Enforcer Settings page.

- If you are using Sky ATP without SDSN or Cloud Feeds only, you must still download Policy Enforcer and create a policy enforcer virtual machine.
- Sky ATP license and account are needed for all configuration types (Sky ATP with SDSN, Sky ATP, and Cloud Feeds only). If you do not have a Sky ATP license, contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium license. If you do not have a Sky ATP account, when you configure Sky ATP, you are redirected to the Sky ATP server to create one. Please obtain a license before you try to create a Sky ATP account. Refer to *Policy Enforcer Installation Overview* for instructions on obtaining a Sky ATP premium license.

To set up a Sky ATP Configuration Type, you must do the following:

1. Enter the IP address for the policy enforcer virtual machine. (This is the IP address you configured during the PE VM installation. You can locate this IP address in the vSphere Center portal.)
2. Enter the password for the policy enforcer virtual machine. (This is the same password you use to login to the VM with your root credentials. Note that the username defaults to root)



NOTE: Refer to *Deploying and Configuring the Policy Enforcer with OVA files* for instructions on downloading Policy Enforcer and creating your policy enforcer virtual machine.

3. Select a Sky ATP Configuration Type. If you do not select a type, Policy Enforcer works in *default mode*. (See *Sky ATP Configuration Type Overview* for more information.)
 - **Sky ATP with SDSN**—All Policy Enforcer features and threat prevention types are available.



NOTE: If you upgrade from cloud feeds or Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention. Use guided setup to expedite the process configuring threat prevention policies.

See the following topics to configure Sky ATP with SDSN:

- *Using Guided Setup for Sky ATP with SDSN*
- *Configuring Sky ATP with SDSN (Without Guided Setup) Overview*
- **Sky ATP**—All threat prevention types are available: Command and control server, Geo IP, and Infected hosts.



NOTE: If you upgrade from cloud feeds only to Sky ATP, you cannot roll back again. Upgrading resets all devices previously participating in threat prevention, and you must re-enroll them with Sky ATP. Use the setup wizard to expedite the process configuring threat prevention policies.

See the following topics to configure Sky ATP:

- *Using Guided Setup for Sky ATP*
- *Configuring Sky ATP (No SDSN and No Guided Setup) Overview*
- **Cloud feeds only**—Command and control server, infected hosts, and Geo IP are the threat prevention types available.

See the following topic to configure Cloud feeds only:

- *Configuring Cloud Feeds Only*
- **No Selection**—Custom feeds only. Infected hosts is the prevention type available.

See the following topic to configure “no selection”:

- *Using Guided Setup for No Sky ATP (No Selection)*

4. Polling timers affect how often the system polls to discover endpoints. There are two polling timers, one that polls network wide and one that polls site wide. They each have default settings, but you can change those defaults to poll more or less often.
 - Network wide polling interval (value in hours): The default is 24 hours. You can set this range from between 1 to 48 hours. This timer polls all endpoints added to the secure fabric.
 - Site wide polling interval (value in minutes): The default is 5 minutes. You can set this range from 1 minute to 60 minutes. This timer polls infected endpoints moving within the sites that are a part of Secure fabric.
5. Click the **Download** button to view or save Policy Enforcer data logs to your local system. These logs are in a compressed file format.

Related Documentation

- *Comparing the SDSN and non-SDSN Configuration Steps*
- *Using Guided Setup for Sky ATP with SDSN*
- *Using Guided Setup for Sky ATP*
- *Configuring Cloud Feeds Only*
- *Using Guided Setup for No Sky ATP (No Selection)*
- *Policy Enforcer Dashboard Widgets*

Policy Enforcer Connector Overview

Configure a connector for third-party products (non-Juniper Networks) to unify policy enforcement across all network elements. This protects endpoints, wired and wireless, connecting to third-party devices as well as Juniper devices.

For Policy Enforcer to provide threat remediation to endpoints connecting through third-party devices, it must be able to authenticate those devices and determine their state. It does this using a tracking and accounting threat remediation plug-in to gather information from a RADIUS server and enforce policies such as terminate session and quarantine.



NOTE: All third-party switches being used with Policy Enforcer must support AAA/RADIUS and Dynamic Authorization Extensions to RADIUS protocol (RFC 3579 and RFC 5176).



NOTE: All Cisco Systems switch models that adhere to Radius IETF attributes and support Radius Change of Authorization from Aruba ClearPass are supported by Policy Enforcer for threat remediation.

Once configured, the connector uses an API to gather endpoint MAC address information from the RADIUS server. If a host is found to be suspicious, the RADIUS server sends a CoA to disconnect the active session and quarantine the host. Once the threat has been mitigated, the interface can return to the network again, but must be authorized to do so by Policy Enforcer using the plug-in and information gathered from the RADIUS server.

Once you have a connector configured, the following information is provided on the Connectors main page.

Table 1: Connectors Information- Main Page

Field	Description
Name	The name you entered for the connector.
Type	This field always reads Third Party Switch at this time.
Status	<p>The current status of the connector. (Active or Inactive.)</p> <p>Hover over the status to see more details of connector instances and their respective status.</p> <p>The following statuses are shown:</p> <ul style="list-style-type: none"> Active status with green icon—All connector instances inside a connector are active Inactive status with red icon—All connector instances inside a connector are inactive Active status with red icon—One of the connectors is inactive and other connectors are active. In progress status with green icon—All connectors are still in progress. Pending (not in progress) status with green icon—All connectors are still pending.

Table 1: Connectors Information- Main Page (continued)

Field	Description
Description	Specifies the description of a connector.
Identity Server	Specifies the IP address of the product management server.
IP Address	The IP address of the ClearPass RADIUS server.

Benefits of Policy Enforcer Connector

- **Custom threat feed and automation** - Automates the threat remediation workflows for third-party products.
- **RESTful APIs** - Provides a network vendor agnostic mechanism for threat remediation. Enables you to automate configuration and management of physical, logical, or virtual devices.

Related Documentation

- [ClearPass Configuration for Third-Party Plug-in on page 30](#)
- [Cisco ISE Configuration for Third-Party Plug-in on page 37](#)
- [Creating a Policy Enforcer Connector for Third-Party Switches on page 15](#)

Creating a Policy Enforcer Connector for Public and Private Clouds

To access this page, select **Administration > Policy Enforcer > Connectors**.

Before You Begin

- For Amazon Web Services (AWS) connector:
 - Create access key and password for your AWS account. This will be a unique username and password for your Amazon account required to create a connector. See [Managing Access Keys for Your AWS Account](#).
 - Create Virtual Private Clouds(VPC) for the required region. See [Getting Started With Amazon VPC](#).
 - Instantiate the vSRX instance in the required VPC and set the tag identifier, for example AWS_SDSN_VSRX. This tag identifier must match with the vSRX instance tag key in AWS.

- Create a Security Group in AWS required to create a threat prevention policy for the AWS connector.
- Deploy workloads in the required VPC and set the resource tags to the workloads.

To configure threat remediation for a public or private cloud, you must install and register the threat remediation plug-in with Policy Enforcer as follows:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Click the create icon (+).

The Create Connector page appears.

3. Complete the configuration using the information in [Table 2 on page 8](#).

4. Click **OK**.



NOTE: Once configured, you select the connector name as an Enforcement Point in your Secure Fabric.

Table 2: Fields on the Create Connector Page for AWS and Contrail

Field	Description
<i>General</i>	
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63 characters maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Connector Type	Select Amazon Web Services or Contrail from the list to connect to your secure fabric and create policies for this network.
IP Address/URL	Enter the IP (IPv4 or IPv6) address or URL of AWS or Contrail. For AWS, this field is set to www.aws.amazon.com , by default. This is where all VPCs are located. You cannot edit this field.
Port	For AWS connector, the port is set to 443 by default and you cannot edit this field. For Contrail connector, provide the port number as 8081.

Table 2: Fields on the Create Connector Page for AWS and Contrail (continued)

Field	Description
Username	<p>Enter the username of the server for the selected connector type.</p> <p>For AWS, enter the generated access key for your Amazon account. This is not same as your Amazon account username.</p>
Password	<p>Enter the password for the selected connector type.</p> <p>For AWS, enter your secret password generated along with your access key. This is not same password as your amazon account.</p>
<i>Network Details</i>	
Connector Type: AWS Virtual Private Clouds	<p>One or more virtual networks under the AWS account are discovered. They are called virtual private cloud (VPC). Only VPCs having vSRX instances deployed are managed. The VPCs are region specific. Select a region from the Region list and the corresponding VPCs are listed. By default, the VPCs for the first available region are listed.</p> <p>Security Director suggests a default Secure Fabric site name for the VPC, in the <code><connector name>_<vpc name>_site</code> format. Click the Secure Fabric site name to edit it. When you edit the name, you will also see the other Secure Fabric sites that do not have any switches or connectors assigned to them. You can also assign these Secure Fabric sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the Secure Fabric site name is reverted to its previous name.</p> <p>You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one option. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further.</p> <p>You can get a detailed view of the VPC by hovering over the name and clicking the Detailed View icon. See “Viewing VPC or Projects Details” on page 20.</p> <p>NOTE: You can perform search on VPCs. Search is not supported for the site names.</p>

Table 2: Fields on the Create Connector Page for AWS and Contrail (continued)

Field	Description
Connector Type: Contrail	Tenant information determined from the Contrail connector is listed.
Project	<p>Security Director suggests a default site name for the project, in the <code><connector name>_<project name>_site</code> format. Click the site name to edit it. When you edit the site name, you will also see the other sites that do not have any switches or connectors assigned to them. You can also assign these sites to the connectors. If the edited site name is already existing with a connector or a switch, an alert message is shown and the site name is reverted to its previous name.</p> <p>You must enable either Threat Remediation or Next Generation Firewall options or both. You cannot create a connector instance without enabling at least one of the two options. If you navigate to the next page without enabling these options, an error message is shown insisting the user to enable either Threat Remediation or Next Generation Firewall to proceed further.</p> <p>You can get a detailed view of the project by hovering over the name and clicking the Detailed View icon. See "Viewing VPC or Projects Details" on page 20.</p> <p>NOTE: You can perform search on Project names. Search is not supported for the site names.</p>
Subnets	<p>The subnet information for Contrail and AWS is determined from the respective systems. For AWS, subnets are the availability zones and for Contrail, subnets are virtual networks. You can create Policy Enforcement Groups for one or more of the subnets, if threat remediation is selected.</p> <p>Both AWS and Contrail subnets are allocated to be within the tenant IP Address Management (IPAM) scheme.</p>
Configuration	

Table 2: Fields on the Create Connector Page for AWS and Contrail (continued)

Field	Description
Configuration	

Table 2: Fields on the Create Connector Page for AWS and Contrail (continued)

Field	Description
	<p><i>Metadata</i></p> <p>Specifies the resource tag information and the resource tag values that you have determined from the projects or VPC. The tag information appears only if the Next Generation Firewall option is enabled.</p> <p>For AWS connector, the resource tag values are fetched from AWS for all the endpoints and then mapped them to the Security Director generated metadata names.</p> <p>Based on the resource tag name, Security Director checks if a metadata with the same resource tag name is already available. If available, it automatically maps the resource tag name to its metadata. If there is no match found, Security Director suggests a new metadata name for the corresponding tag. The suggested metadata name is same as the resource tag name. You can also edit the suggested metadata name and customize the resource tag name.</p> <p>However, in the Generated MetaData Name column, you cannot use the following predefined metadata names:</p> <ul style="list-style-type: none"> • Tenant • Provider • Controller <p>If you provide these names, an appropriate error message is shown to choose a different name.</p> <p>Select the Map option to map the resource tag to the generated Security Director Metadata while creating the connector instance. If the Map option is not selected, the connector instance is created for a project or VPC without any resource tags. For example, if you have multiple resource tags for a project, you can choose one or more resource tags to map to the corresponding generated metadata, by selecting the Import option. The project or VPC with the selected resource tags are created when the connector instance is created.</p> <p>Mapping of Contrail and AWS connector resource tags to Security Director metadata enables you to create the next generation firewall policy definitions for the source and destination rules, based on the metadata expressions. Policy Enforcer dynamically determines the matching VM instances in AWS or Contrail connector to the metadata expressions and pushes the IP address content as dynamic address groups to the enforcement points in the tenant specific vSRX firewall instance.</p> <p>In the Configuration Value column, provide any additional information required for this particular connector connection. For example, if the connector type is ForeScout CounterACT, you are required to provide the WebAPI username and password. Similarly for other connectors if the additional configuration parameters are required, they are listed in this column.</p>

Table 2: Fields on the Create Connector Page for AWS and Contrail (continued)

Field	Description
	<p>After the successful completion, the subnet you have created is mapped to that particular connector instance.</p> <p>For AWS, provide the following configuration parameters:</p> <ul style="list-style-type: none"> • SRX username—Specify the username of the vSRX device that you have instantiated for a VPC. • SRX identifier tag—Specify the tag name of the vSRX device, if the recommended vSRX name was not used. If you do not specify any value for this field, Policy Enforcer uses vSRX as a default tag name to identify the device. <p>This enables discovery of this particular vSRX device in Junos Space. This vSRX device is also added to a specific secure fabric site.</p> <ul style="list-style-type: none"> • Infected Host Security Group—Specify the security group name that you would want to tag an infected workload for threat remediation. • SRX authentication key—Specify the authentication key file to access the vSRX device. Editing this in the grid prompts you to either upload the authentication key file or view an already existing uploaded authentication key. <p>For Contrail, provide the following configuration parameters:</p> <ul style="list-style-type: none"> • SRX username • SRX password • Infected host security group

**NOTE:**

- For AWS and Contrail connectors, the site association is achieved in the Connectors page itself.
- When a connector is added to the site, Policy Enforcer discovers the vSRX Series associated with the connector and assigns it to the site. Hover over the connector name to view the corresponding vSRX with its IP address as a tool tip.
- If the mode in PE Setting page is SDSN with SKYATP, then you must create a SkyATP realm and assign the sites associated with the VPC or Project to the realm. Otherwise the vSRX instances in the VPC or Project does not download the dynamic address group objects, that is the list of workloads in the VPC or Project that match a policy metadata expression.

Threat Remediation Workflow

Once you create an AWS or a Contrail connector with Threat Remediation option, a site is created in the Secure Fabric page.

Perform the following actions for threat remediation:

1. Select **Configure > Threat Prevention > Sky ATP Realms**.

Select the associated Secure Fabric sites to the respective VPC or Project that is successfully added. Add the secure fabric site to a Sky ATP realm and enrol the vSRX devices to the Sky ATP. Enroll devices by clicking **Add Devices** in the list view once the realm is created.

2. Select **Configure > Shared Objects > Policy Enforcement Groups**.

Click the add icon to create a new policy enforcement group. You will see a list of all subnets that you have created in a VPC. Select the required subnets for this VPC and create a policy enforcement group. Associate this policy enforcement group to threat remediation policy.

3. Select **Configure > Threat Prevention > Policies**.

Click the add icon to create a new threat prevention policy. Add the threat prevention policy, including profiles for one or more threat types. The security group that you had selected during connector configuration is used when the host gets infected within a corresponding VPC.

Next Generation Firewall Workflow

When you create an AWS or a contrail connector with Next Generation Firewall option, it means that for a particular VPC, Layer 7 firewall policy is enabled. Perform the following actions to enable next generation firewall:

1. Select **Configure > Firewall Policy**.

2. Select the policy for which you want to define rules and click **Add Rule**.

The Create Rules page appears.

3. In the General tab, enter the name of the rule and description of the rule

4. In the Source tab, click **Select** for the Address(es) field to select the source address.

The Source Address page appears.

- In the Address Selection field, click **By Metadata Filter** option.
- In the Metadata Provider field, select **PE** as a provider from the list.
- In the Metadata Filter field, all the generated metadatas during the connector configuration are listed. Using these metadatas, create a required metadata expression. For example, Application = Web and Tier = App.

- In the Matched Addresses field, addresses matching the selected metadata are listed. This address is used as a source address. For every metadata expression, a unique dynamic address group (DAG) is created.
- Click **Ok** and complete configuring other parameters for the rule.
- Publish and update the configuration immediately or schedule it later.

Related Documentation

- [Policy Enforcer Connector Overview on page 6](#)
- [Editing and Deleting a Connector on page 18](#)
- [Viewing VPC or Projects Details on page 20](#)

Creating a Policy Enforcer Connector for Third-Party Switches

To access this page, select **Administration > Policy Enforcer > Connectors**.

Before You Begin

- Have your ClearPass, Cisco ISE, and , ForeScout server information available.
- To obtain an evaluation copy of ForeScout CounterACT to use with Policy Enforcer, click [here](#).
- Once configure, you select the Connector as an Enforcement Point in your Secure Fabric.
- Review the “[Policy Enforcer Connector Overview](#)” on [page 6](#) topic.
- To create a connector for a public or a private cloud, see “[Creating a Policy Enforcer Connector for Public and Private Clouds](#)” on [page 7](#).

To configure threat remediation for third-party devices, you must install and register the threat remediation plug-in with Policy Enforcer as follows:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Click the create icon (+).

The Create Connector page appears.

3. Complete the configuration using the information in [Table 3 on page 16](#).

4. Click **OK**.



NOTE: Once configured, you select the connector name as an Enforcement Point in your Secure Fabric.

Table 3: Fields on the Create Connector Page

Field	Description
<i>General</i>	
Name	Enter a unique string that must begin with an alphanumeric character and can include underscores; no spaces allowed; 63 characters maximum.
Description	Enter a description; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Connector Type	Select the required third-party network of devices to connect to your secure fabric and create policies for this network. The available connectors are Cisco ISE, HP ClearPass, and ForeScout CounterACT.
IP Address/URL	Enter the IP (IPv4 or IPv6) address of the product management server.
Port	Select the port to be used from the list. When this is left blank, port 443 is used as the default.
Username	<p>Enter the username of the server for the selected connector type.</p> <ul style="list-style-type: none"> • ClearPass—Enter the Client ID created while setting up the ClearPass API client. See “ClearPass Configuration for Third-Party Plug-in” on page 30 for details. • Cisco ISE—Enter the username you used when you created the API Client in the Cisco ISE UI. See “Cisco ISE Configuration for Third-Party Plug-in” on page 37. • ForeScout—Enter the username of your DEX plugin. See “Integrating ForeScout CounterACT with Juniper Networks SDSN” on page 22.
Password	<p>Enter the password of the server for the selected connector type.</p> <ul style="list-style-type: none"> • ClearPass—Enter the Client Secret string created while setting up the ClearPass API client. See “ClearPass Configuration for Third-Party Plug-in” on page 30 for details. <p>WARNING: When the Access Token Lifetime expires, you must generate a new Client Secret in ClearPass and update it here too.</p> <ul style="list-style-type: none"> • Cisco ISE—Enter the password you used when you created the API Client in the Cisco ISE UI. See “Cisco ISE Configuration for Third-Party Plug-in” on page 37. • ForeScout—Enter the password of your DEX plugin. See “Integrating ForeScout CounterACT with Juniper Networks SDSN” on page 22.

Table 3: Fields on the Create Connector Page (continued)

Field	Description
DEX User Role (For ForeScout connector type only)	Enter the Data Exchange (DEX) user role information to authenticate and connect to the ForeScout connector. See "Integrating ForeScout CounterACT with Juniper Networks SDSN" on page 22.
<i>Network Details</i>	
Subnets	<p>Connector Type: ClearPass, ForeScout CounterACT, and Cisco ISE</p> <p>Add subnet information to the connector configuration so you can include those subnets in groups and then apply policies to the groups. When using Junos Space, Policy Enforcer is able to dynamically discover subnets configured on Juniper switches. Policy Enforcer does not have the same insight with third-party devices.</p> <p>When you add subnets as part of the connector configuration, those subnets become selectable in Policy Enforcement Groups.</p> <p>To add subnet information, do one of the following:</p> <ul style="list-style-type: none"> Click Upload File to upload a text file with an IP address list. Note that the file you upload must contain only one item per line (no commas or semi colons). All items are validated before being added to the list. OR Manually enter the IP addresses. For example: 192.168.0.1/24. Click the add icon (+) to add more IP addresses. <p>NOTE: It is mandatory to add at least one IP subnet to a connector. You cannot proceed to next step without adding a subnet.</p>
<i>Configuration</i>	
Configuration	<p>Provide any additional information required for this particular connector connection. After the successful completion, the subnet you have created is mapped to that particular connector instance.</p> <p>NOTE: For ClearPass and Cisco ISE connectors no additional configuration information are required.</p>

**NOTE:**

- You can associate ClearPass, Cisco ISE, or Forescout connector to a site only in your Secure Fabric.
- When a connector is added to the site, Policy Enforcer discovers the vSRX Series associated with the connector and assigns it to the site. Hover over the connector name to view the corresponding vSRX with its IP address as a tool tip.



WARNING: Ensure that the correct credentials are provided for the ClearPass, Cisco ISE, and ForeScout identity servers. If the initial connection fails, an error message is shown only at that time. Once that message disappears, the status of connectivity to the identity server is not shown in Policy Enforcer. Note that the identity servers are only queried on-demand.

Related Documentation

- [Policy Enforcer Connector Overview on page 6](#)
- [ClearPass Configuration for Third-Party Plug-in on page 30](#)
- [Cisco ISE Configuration for Third-Party Plug-in on page 37](#)
- [Editing and Deleting a Connector on page 18](#)
- [Viewing VPC or Projects Details on page 20](#)

Editing and Deleting a Connector

You can edit or delete a connector from the Connector page.

- [Editing a Connector on page 18](#)
- [Deleting a Connector on page 19](#)

Editing a Connector

To edit a connector:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Select the connector you want to edit , and then click the pencil icon.

The Edit Connector page appears displaying the same options that were used to create a new connector. Note that you cannot edit the Name and IP Address/URL fields.

For the AWS connector, when you select a new region, you must enter the configuration parameters for the VPCs in that region. This enables you to maintain different vSRX authentication keys across different regions.

For AWS and Contrail connectors, you can enable or disable the threat remediation and next generation firewall features. If you disable the next generation firewall feature from a project or VPC, that particular project or VPC connector instance will be deleted. The VPCs are deleted from the corresponding regions.

A warning message is shown if you edit the existing generated metadata name. If you edit the existing metadata name, duplicate metadata objects are created that are associated to a firewall policy. To edit the metadata name, select **Configure > Shared Objects > Object Metadata** and edit the required metadata name. Also if the firewall policies are associated with this metadata, select **Configure > Firewall Policy > Policies** and edit the corresponding metadata expression.

To delete the mapping of the tag name with the generated metadata, disable the Map option for the corresponding project or VPC. A warning message is shown that there could be a firewall policy associated with this metadata. Select **Configure > Firewall Policy > Policies** and edit the corresponding metadata expression. The mapping is deleted at the end of the edit workflow. You can also enable the Import option for the tags that were not mapped to the generated metadata while creating the connector.

3. Modify the required field values and click **Save** to save your changes.

If you discover a new connector instance, you can enable the threat remediation or next generation firewall option. A new site is created when you enable one of these options. You must add these new sites to a realm to perform the threat remediation. At the end of the edit connector workflow, a reminder message is shown to add the sites to a realm.



NOTE:

- During the AWS connector editing, if you change the region, changes that you have made in the current session are discarded. An alert message is shown when you change the region.
- During the ClearPass or Cisco ISE connector editing, you cannot delete subnets that are already assigned to a policy enforcement group. However, you can add of any new subnets and edit their descriptions.

Deleting a Connector

To delete a connector:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

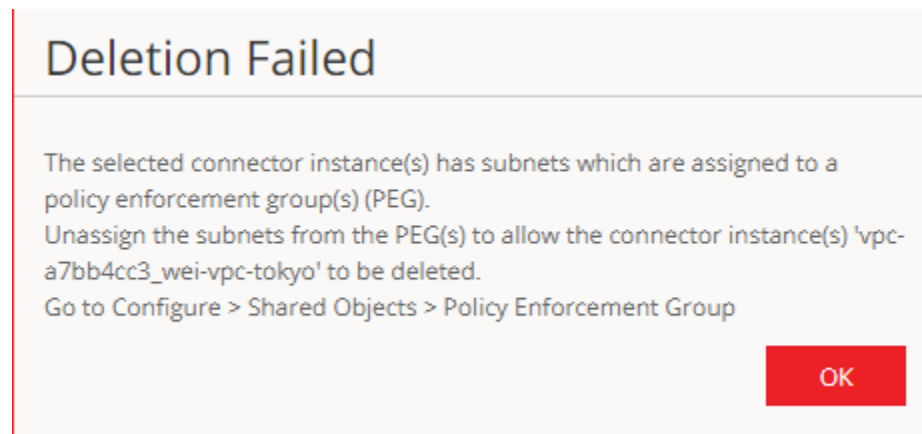
2. Select the connector that you want to delete, and select the delete icon (X).

Deleting a connector deletes the connector instances and its references as well. A warning message is shown listing all the connector instances that will be deleted, before deleting the connector.

3. Click **Delete** to delete your selection.

If the connector instances that you want to delete has PEG assigned, a warning message is shown to unassign the subnets from PEG first and then delete the connector, as shown in [Figure 1 on page 20](#).

Figure 1: Deletion Failed Warning



For AWS and Contrail connectors, if there are connector instances with PEG assigned, only those connector instances are not deleted. However, other connector instances without PEG assigned are deleted.



NOTE:

- You cannot delete the ClearPass or Cisco ISE connector if its subnets are assigned to a policy enforcement group. You must unassign those subnets from that particular policy enforcement group and then delete the connector.
 - You cannot delete a connector if it is assigned as an enforcement point to a site. Before deleting a connector, you must unassign it from the site on Secure Fabric.
-

**Related
Documentation**

- [Policy Enforcer Connector Overview on page 6](#)
- [Creating a Policy Enforcer Connector for Third-Party Switches on page 15](#)

Viewing VPC or Projects Details

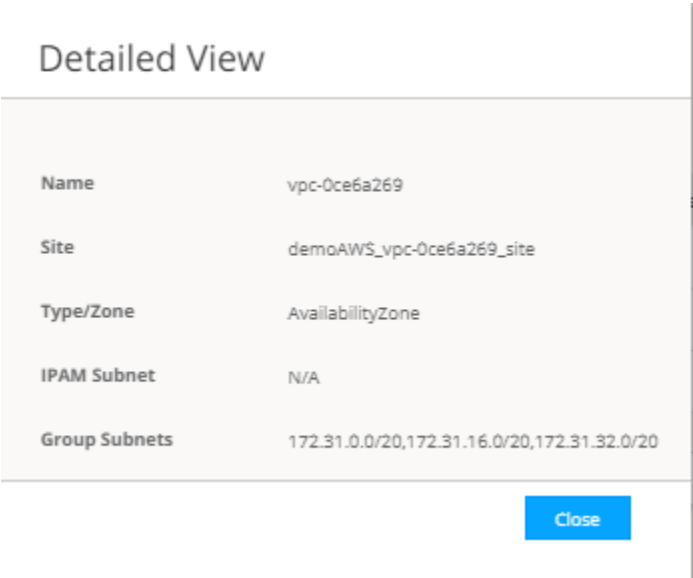
To view the complete details of a VPC or a project:

1. Select **Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Select the connector you want to edit , and then click the pencil icon.
- The Edit Connector page appears displaying the same options that were used to create a new connector.
3. In the Network Details section, get a detailed view by hovering over the VPC or project name and click the Detailed View icon before the VPC or project name.
- The Detailed View page appears, as shown in [Figure 2 on page 21](#).

Figure 2: Detailed View Page



[Table 4 on page 21](#) explains fields on the Detailed View page.

Table 4: Fields on the Detailed View Page

Field	Description
Name	Specifies name of a VPC or project.
Secure Fabric	Specifies the site to which the VPC or project s allocated.
Type/Zone	Specifies the connector type. For example, virtual network for Contrails and AvailabilityZone for AWS.
IPAM Subnet	Specifies the IP Address Management (IPAM) subnets allocated to the respective VPC or project.
Group Subnets	<div>Specifies the group of subnets allocated to the VPC or project.</div> <div>For Contrail, you will see a key value of Tier. For example, the group is called web and assigned subnet is x.x.x.x/xx. For AWS, you will see only the group of subnets.</div> <div>For Contrail, they are still group of subnets. However, each of the subnets are allocated to a tag, for example, database, tier, application, and so on.</div>

**Related
Documentation**

- [Creating a Policy Enforcer Connector for Third-Party Switches on page 15](#)
- [Editing and Deleting a Connector on page 18](#)

Integrating ForeScout CounterACT with Juniper Networks SDSN

This topic provides instructions on how to integrate the third-party device ForeScout CounterACT with Juniper Networks Software-Defined Secure Networks (SDSN) solution to remediate threats from infected hosts for enterprises. ForeScout CounterACT is an agentless security appliance that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. CounterACT applies an agentless approach and integrates with SDSN to block or quarantine infected hosts on Juniper Networks' devices, third-party switches, and wireless access controllers with or without 802.1x protocol integration.

To integrate ForeScout CounterACT with SDSN, you must create a connector in Policy Enforcer that enables CounterACT to connect to your secure fabric and create policies for CounterACT. Before you configure the ForeScout CounterACT connector, you must ensure that ForeScout CounterACT is installed and running with the Open Integration Module (OIM). The ForeScout OIM consists of two plug-ins: Data Exchange (DEX) and Web API. Install both the plug-ins and ensure that they are running. You must configure these plug-ins before you create a connector in Policy Enforcer.

If you do not have ForeScout CounterACT installed in your network, obtain an evaluation copy from [here](#).

This topic includes the following sections:

- [Configuring the DEX Plug-in on page 22](#)
- [Configuring the Web API Plug-in on page 25](#)
- [Creating ForeScout CounterACT Connector in Security Director on page 27](#)

Configuring the DEX Plug-in

The DEX plug-in receives API information about infected hosts from the ForeScout CounterACT connector. Messages from infected hosts are either blocked or quarantined.

When you configure the DEX plug-in, you also configure a new property, Test, for DEX. When configured, this property ensures that Web services are available for Policy Enforcer, monitors the network status, and validates usernames and passwords.

To configure the DEX plug-in:

1. Select **Tools > Options > Data Exchange (DEX)** in the CounterACT UI.

The Data Exchange configuration page appears.

2. On the Data Exchange (DEX) page, select the **CounterACT Web Services > Accounts** tab, as shown in [Figure 3 on page 23](#).

The DEX Accounts page appears.

Figure 3: DEX Accounts Page

Data Exchange (DEX)
Use DEX to exchange data with external sources.
Define external databases and web services, and map data to custom endpoint properties.

CounterACT Web Service | General Settings

Accounts | Properties | Security Settings

Define account credentials to log in to the CounterACT Web Service.
Requests sent to the web service must include account credentials.
Host properties defined in the CounterACT Web Service Properties tab are associated with an account defined here.

Search

Name	Description	User Name
Administrator	Policy Enforcer	admin

3. Select **Add**.

The Add page appears.

4. In the Name field, enter the name for the CounterACT Web service account.

Enter this name in the DEX User Role field (see Step 3) while configuring the ForeScout connector in Security Director.

5. In the Description field, enter a brief description of the purpose of the Web service account.

6. In the Username field, enter the username that will be used to authorize CounterACT to access the Web service account.

7. In the Password field, enter the password that will be used to authorize CounterACT to access this Web service account.

8. Click **OK**.9. In the Properties tab, click **Add**.

The General pane of the Add Property from CounterACT Web Service wizard opens, as shown in [Figure 4 on page 24](#).

Figure 4: Add Property-General Pane Page

Add Property from CounterACT Web Service

General

Define a host property that is set via the CounterACT Web Service. Associate the property with a CounterACT web service account. Only requests submitted to the web service using this account can set the property.

Property Name

Property Tag (ASCII only)

Description

Account

Help Previous Next Finish Cancel

10. Add properties such as block, quarantine, and Test, as shown in Figure 5 on page 24.

You must include the Test property. Otherwise, you cannot add CounterACT as a third-party connector to Policy Enforcer successfully.

Figure 5: DEX Properties Page

Data Exchange (DEX)

Use DEX to exchange data with external sources.
Define external databases and web services, and map data to custom endpoint properties.

SQL/LDAP External Web Services **CounterACT Web Service** General Settings

Accounts **Properties** Security Settings

Define host properties that are set by the CounterACT Web Service.
Each host property defined in this tab is associated with one of the accounts in the CounterACT Web Service Accounts tab.
To set a property, a client must send a request that uses the account credentials of the associated account for authentication.

Search

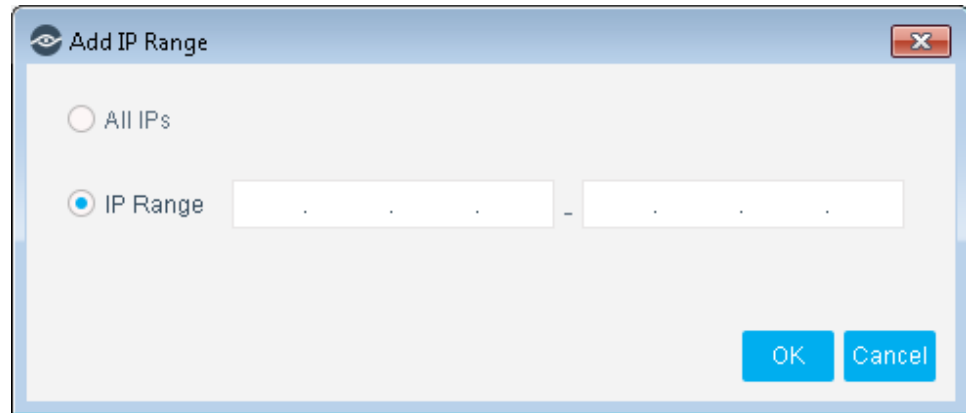
Name	Description	Type	Account
block	Policy Enforcer Block Action	Boolean	Administrator
quarantine	Policy Enforcer Quarantine Action	Boolean	Administrator
Test		Boolean	Administrator

Add... Edit... Remove Import... Export...

Help Apply Cancel

11. In the Security Settings tab, click **Add** and add the IP address range from where communication is expected, as shown in Figure 6 on page 25.

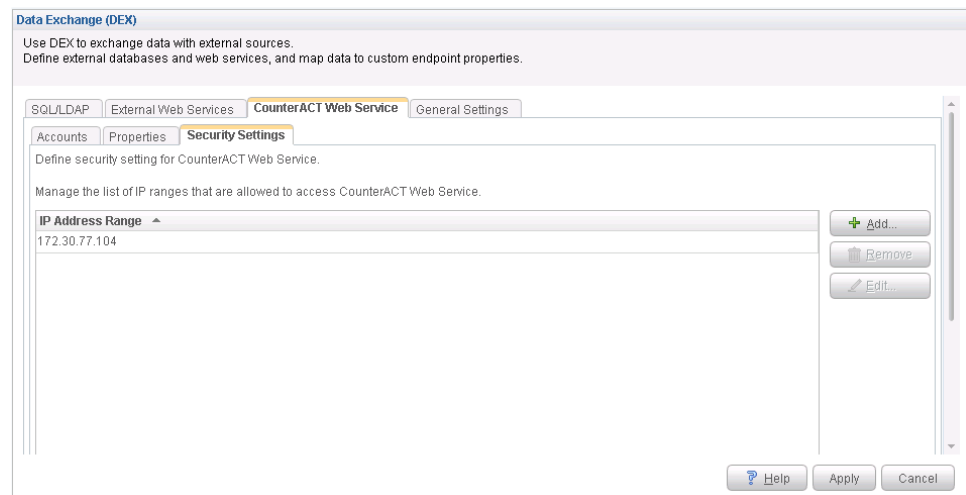
Figure 6: Add IP Range Page



The dialog box titled "Add IP Range" has a close button (X) in the top right corner. It contains two radio buttons: "All IPs" and "IP Range". The "IP Range" radio button is selected. To the right of the "IP Range" radio button is a text input field for an IP range, currently showing ". . . - . . .". At the bottom right, there are two buttons: "OK" and "Cancel".

Click **OK**. The IP address appears in the IP Address Range list, as shown in Figure 7 on page 25.

Figure 7: DEX Security Settings Page



The "Data Exchange (DEX)" page shows the "CounterACT Web Service" tab selected. Under the "Security Settings" sub-tab, there is a section titled "Manage the list of IP ranges that are allowed to access CounterACT Web Service." Below this is a table with the header "IP Address Range" and one entry: "172.30.77.104". To the right of the table are three buttons: "Add...", "Remove", and "Edit...". At the bottom right of the page are buttons for "Help", "Apply", and "Cancel".

12. On the Data Exchange (DEX) page, click **Apply**.

The configuration is saved and the configuration settings are applied.

Configuring the Web API Plug-in

The Web API plug-in enables external entities to communicate with CounterACT by using simple, yet powerful Web service requests based on HTTP interaction. You configure the Web API plug-in to create an account for Policy Enforcer integration.

To configure the Web API plug-in:

1. Select **Tools > Options > Web API** in the CounterACT UI.

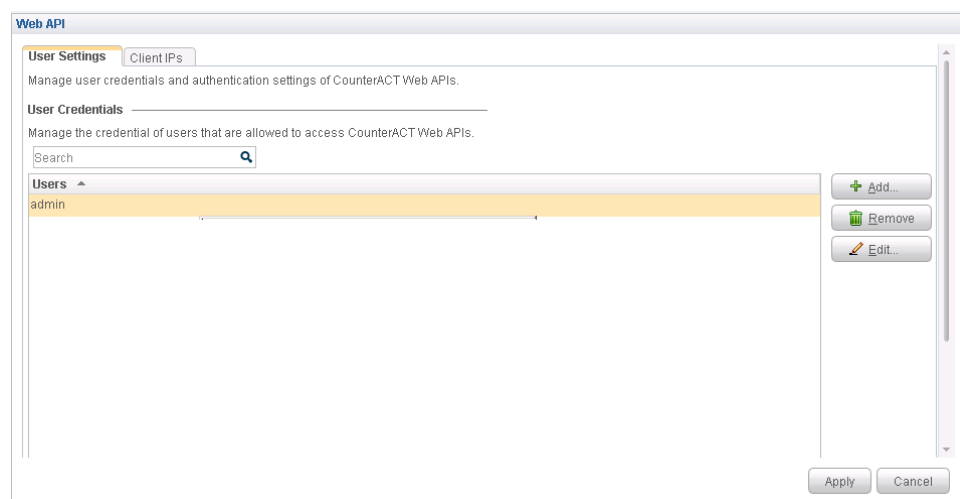
The Web API page appears.

2. In the User Settings tab, select **Add**.

The Add Credentials page appears.

3. Use the same username and password that you created for the DEX configuration (see Step 6 and Step 7) and click **OK**, as shown in [Figure 8 on page 26](#).

Figure 8: Web API User Settings Page

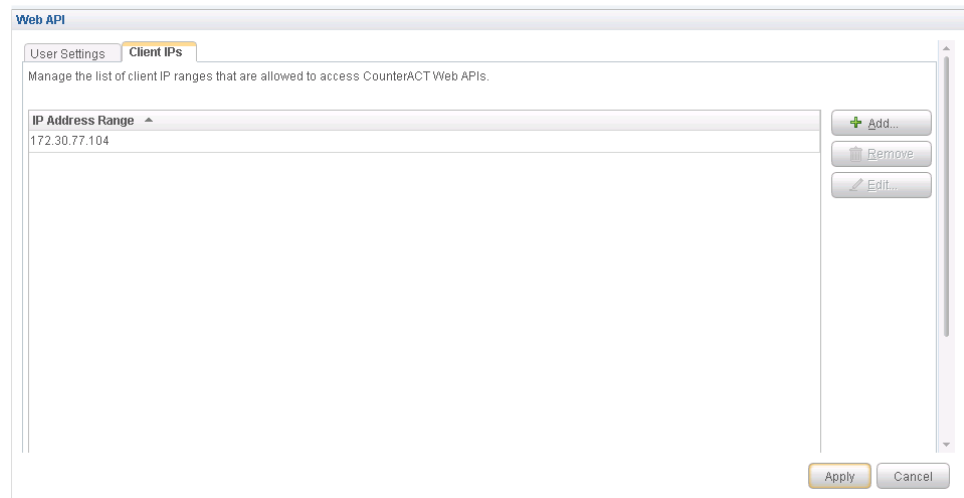


4. Select the **Client IPs** tab and click **Add**.

Add the Policy Enforcer IP address into the access list.

5. Click **OK**.

The IP address appears in the IP Address Range list, as shown in [Figure 9 on page 27](#).

Figure 9: Web API Client IPs Page

6. Click **Apply** to save and apply your configuration.

Creating ForeScout CounterACT Connector in Security Director

After you configure the DEX and Web API plug-ins, you need to create a connector for ForeScout CounterACT in Policy Enforcer.

To create a ForeScout CounterACT connector in Junos Space Security Director:

1. Select **Security Director > Administration > Policy Enforcer > Connectors**.

The Connectors page appears.

2. Click the create icon (+).

The Create Connector page appears.

3. In the General tab, select ForeScout CounterACT as the connector type and provide the username, DEX user role, and password, as shown in [Figure 10 on page 28](#). (The DEX user role is the one that you created in Step 4).

Specify 443 as the port number for communication.

Figure 10: Edit Connector Page

Administration / Policy Enforcer / Connectors

Connectors

1 selected

Name	Type
forescoutconnector	Fore Scout

1 items

Edit Connector

General Network Details Configuration

General

Name * forescoutconnector

Description fs

ConnectorType * Fore ScoutCounterACT

Primary Identity Server

IP Address * 10.92.82.139

Port * 443

Username * admin

Password *

Dex User Role * Administrator

4. In the Network Details tab, configure the IP subnets, as shown in [Figure 11 on page 28](#).
CounterACT treats the IP subnets as endpoints and takes action.

Figure 11: Edit Connector - Network Details Page

Administration / Policy Enforcer / Connectors

Connectors

1 selected

Name	Type
forescoutconnector	Fore Scout

1 items

Edit Connector

General Network Details Configuration

Network Details

Subnets

Click on the field to create subnets or click Upload file to import subnets from a file stored in your local system.

Upload file + ✕

Subnet	Description
192.168.199.254/24	fs subnet1
192.168.202.254/24	fs subnet2

2 items

5. In the Configuration tab, specify the Web API username and password, as shown in [Figure 12 on page 29](#).

Figure 12: ForeScout Connector - Configuration Tab

Edit Connector ?

1 General 2 Network Details 3 Configuration

Configuration

Configuration

Enter configuration values for the configuration keys.

Configuration Key	Configuration Value
User ID of CounterACT web application	admin
Password of CounterACT web application	****

Cancel Back Finish

6. Click **Finish**.

A new ForeScout CounterACT connector is created.

7. Verify that the communication between Policy Enforcer and CounterACT is working.

After installing ForeScout CounterACT and configuring a connector, in the CounterACT UI, create policies for CounterACT to take the necessary action on the infected hosts. The Hosts page lists compromised hosts and their associated threat levels, as shown in Figure 13 on page 29.

Figure 13: Host Information

Host Name	IP Address	Subnet	MAC Address	Threat Level	Actions
ENGLABSDSN-WINDO...	10.92.83.154	Subnet_101	005056bb37b6		
ENGLABSDSN-WINDO...	10.92.83.153	Subnet_101	005056bb754f		
ENGLABSDSN-WINDO...	10.92.83.144	Subnet_101	005056bb2326		
ENGLABSDSN-WINDO...	10.92.83.155	Subnet_101	005056bb46c0		
ENGLABSDSN-WINDO...	10.92.83.143	Subnet_101	005056bb2dbf		
192.168.199.9	192.168.199.9	Subnet_101	005056b3c442		
192.168.199.5	192.168.199.5	Subnet_101	7819f77096e8		
192.168.199.3	192.168.199.3	Subnet_101	d067e5468910		
192.168.199.25	192.168.199.25	Subnet_101	005056bb0eab	10.92.81.115:ge-0/0/4	ge-0/0/4 (missing alias)
192.168.199.22	192.168.199.22	Subnet_101	005056bb667f	10.92.81.115:ge-0/0/2	ge-0/0/2 (missing alias)
192.168.199.21	192.168.199.21	Subnet_101	005056bb72b9		
192.168.199.20	192.168.199.20	Subnet_101	005056bb5e1b	10.92.81.115:ge-0/0/2	ge-0/0/2 (missing alias)

Profile Compliance All policies

IP Address: 192.168.199.25 Connectivity: Internal
MAC Address: 005056bb0eab

Host Information

IP Address: 192.168.199.25
MAC Address: 005056bb0eab
NIC Vendor: VMware, INC.
Block: Yes 1/31/18 12:11:58 PM

Switch IP: 10.92.81.115
Switch Hostname: js-ex42k-01
Switch Port Name: ge-0/0/2
Switch Port Alias: ge-0/0/2 (missing alias)
Switch IP and Port Name: 10.92.81.115:ge-0/0/2
Switch Port VLAN: 999
Switch Port ACL:
Switch Port VLAN Name: quarantine
Switch Port Voice Device: No

[Table 5 on page 30](#) shows the recommended actions performed by CounterACT on the infected hosts that are blocked or quarantined.

Table 5: Recommended Action to Be Performed on the Infected Hosts

Infected Host Policy Enforcer Action	Connection State	Action Performed by CounterACT
Blocked	Wired	Apply access control list (ACL) to block inbound and outbound traffic for a specific MAC address.
	Wireless	Apply WLAN block on the endpoint, which will block the traffic based on the wireless MAC address.
	Dot1x	Apply CoA.
Quarantined	Wired	Apply VLAN. This action is specified by Policy Enforcer.
	Wireless	Apply VLAN. This action is specified by Policy Enforcer.

Related Documentation

- [Policy Enforcer Connector Overview on page 6](#)
- [Creating a Policy Enforcer Connector for Third-Party Switches on page 15](#)

ClearPass Configuration for Third-Party Plug-in

Policy Enforcer's ClearPass Connector communicates with the Clearpass Radius server using the Clearpass API. As part of threat remediation, Policy Enforcer's Clearpass Connector uses enforcement profiles. This section provides information for configuring Clearpass so that Policy Enforcer can invoke the appropriate enforcement profiles.

As part of the configuration, on ClearPass you will create two enforcement profiles, one for quarantine and one for terminate. Then you will use them in the ClearPass enforcement policy. Once ClearPass is configured, you will configure a ClearPass Connector on Policy Enforcer.



NOTE:

- Always use a third-party switch that supports 802.1x, Radius CoA, Radius Accounting, and DHCP snooping features. Enabling DHCP snooping is important which configures the Radius attribute, Framed-IP-Address. Only after configuring Framed-IP-Address, Policy Enforcer can detect the session related to the infected-host IP addresses and terminate the session.
- The stale sessions in ClearPass cannot be terminated and therefore, the actual East-West traffic block will not be active until you reauthenticate the session. You must ensure to clear the stale sessions in ClearPass frequently.

On ClearPass you will configure the following:

- API Client
- Custom Attribute
- Enforcement Profiles
- Enforcement Policy

To configure the API Client:

1. In ClearPass, navigate to **Administration > API Services > API Clients** and create a client with the following attributes:



NOTE: You must login as ClearPass Guest to see the API services menu.

- Client ID: sdsncient
- Enabled: Select the check box for **Enable API client**
- Operator Profile: Create a profile from **Administrator > Operator Logins > Profiles** for the API client with minimum access privileges as shown in [Figure 14 on page 31](#).

Figure 14: ClearPass API Client Operator Profile Minimum Privileges

Operator Profile	
Name:	sdsnop
Description:	
Operator logins:	Enabled
Privileges:	<div> API Services Custom <ul style="list-style-type: none"> Allow API Access Allow Access </div> <div> Guest Manager Custom <ul style="list-style-type: none"> Active Sessions Full Access Active Sessions History Read Only </div> <div> Policy Manager Custom <ul style="list-style-type: none"> Identity - Endpoints Read and Write Insight - Endpoints Read and Write </div>
Skin:	
Start Page:	(Default)
Language:	(Default)
Time Zone:	(GMT-08:00) America/Los Angeles; Pacific Time

- Grant Type: Select **Client credentials** (`grant_type = client_credentials`)
- Client Secret: Copy and save this. It will not be shown again.
- Access Token Lifetime: Enter 5 minutes as a time-frame.

Figure 15: ClearPass Edit API Client

ClearPass Guest

Home » Administration » API Services » API Clients

Edit API Client (sdsncient)

Use this form to edit the API client 'sdsncient'.

Changing properties other than the description will invalidate any existing access tokens.

Edit API Client	
* Client ID:	sdsncient <small>The unique string identifying this API client. Use this value in the OAuth2 "client_id" parameter.</small>
Description:	<input type="text"/> <small>Use this field to store comments or notes about this API client.</small>
Enabled:	<input checked="" type="checkbox"/> Enable API client
* Operator Profile:	sdsnop <small>The operator profile applies role-based access control to authorized OAuth2 clients. This determines what API objects and methods are available for use.</small>
* Grant Type:	Client credentials (grant_type=client_credentials) <small>Only the selected authentication method will be permitted for use with this client ID.</small>
Client Secret:	Encrypted, not shown <input type="checkbox"/> Generate a new client secret
Access Token Lifetime:	5 minutes <small>Specify the lifetime of an OAuth2 access token.</small>

Save Changes **Cancel**

* required field

2. Click **Save Changes**.

To configure a Custom Attribute:

1. Select ClearPass Policy Manager and navigate to **Administration > Dictionaries > Attributes** to create a custom attribute. Then add it into the Dictionary: sdsnEpStatus. Enter the following:
 - Entity Type: **Endpoint**
 - Name: sdsnEpStatus (Note that you must use this name - sdsnEpStatus)
 - Data Type: **List**
 - Is Mandatory: **Yes**
 - Allowed Values: **healthy, blocked, quarantine**
 - Default Value: **healthy**

Figure 16: ClearPass Edit Attribute

Administration » Dictionaries » Attributes
Attributes

Filter: Name contains sdsnEp

#	Name	Entity	Data Type
1.	sdsnEpStatus	Endpoint	List

Showing 1-1 of 1

Edit Attribute

Entity	EndPoint
Name	sdsnEpStatus
Data Type	List
Is Mandatory	Yes
Allowed Value	healthy, blocked, quarantine (e.g., example1,example2,example3)
Default Value (optional)	healthy Select from the list

2. Click **Save**.

To configure Enforcement Profiles:

1. In ClearPass, navigate to **Configuration > Enforcement > Profiles** and create two enforcement profiles.
2. Profile 1: Create the following profile to quarantine infected endpoints:
 - Name: **JNPR SDSN Quarantine**
 - Description: **Quarantine profile for SDSN**
 - Type: **RADIUS**
 - Action: **Accept**

Figure 17: ClearPass Enforcement Profile: Quarantine

Support | Help | Logout
admin (Super Administrator)

Configuration » Enforcement » Profiles » Edit Enforcement Profile - JNPR SDSN Quarantine

Enforcement Profiles - JNPR SDSN Quarantine

Summary Profile Attributes

Profile:

Name:	JNPR SDSN Quarantine
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:IETF	Tunnel-Private-Group-Id	= v100
2. Radius:IETF	Tunnel-Type	= VLAN (13)
3. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
4. Radius:IETF	Acct-Interim-Interval	= 60

Back to Enforcement Profiles Copy Save Cancel



NOTE: The data displayed at the bottom of the screen is for example and not for configuration purposes. Note that the 4th attribute can be set for the accounting packets to be sent by the NAS device to the Clearpass Radius server.

3. Profile 2: Create the following profile to block infected endpoints:



NOTE: To configure this profile, copy the default system profile Juniper Terminate Session and edit the profile name and attributes.

- Name: JNPR SDSN Terminate Session
- Description: Block profile for SDSN
- Type: RADIUS_CoA
- Action: Disconnect



NOTE: If there are any vendor-specific additional attributes required for the Terminate COA, those needs to be added here. For example, in the case of Juniper Networks Trapeze Wireless Clients, the JNPR SDSN Terminate Session profile requires two additional attributes: NAS-IP-Address and User-Name.

Figure 18: ClearPass Enforcement Profile: Terminate

ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#)
admin (Super Administrator)

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Juniper SDSN Terminate Session

Enforcement Profiles - Juniper SDSN Terminate Session

Summary Profile Attributes

Profile:

Name:	Juniper SDSN Terminate Session
Description:	System-defined profile to disconnect user (Juniper)
Type:	RADIUS_CoA
Action:	Disconnect
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:IETF	Calling-Station-Id	= %{Radius:IETF:Calling-Station-Id}
2. Radius:IETF	Acct-Session-Id	= %{Radius:IETF:Acct-Session-Id}

[Back to Enforcement Profiles](#) [Copy](#) [Save](#) [Cancel](#)

Configure an Enforcement Policy:

In ClearPass, navigate to **Configuration > Enforcement > Policies**. Both profiles you created must be added to all the enforcement policies for endpoints addressed by Policy Enforcer.

Figure 19: ClearPass Enforcement Policy

ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#)
admin (Super Administrator)

Configuration » Enforcement » Policies » Edit - HR Windows Policy

Enforcement Policies - HR Windows Policy

Enforcement policy has not been saved

Summary Enforcement Rules

Enforcement:

Name:	HR Windows Policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	HR Windows Profile

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Endpoint:sdsnEpStatus EQUALS blocked)	Juniper SDSN Terminate Session
2. (Endpoint:sdsnEpStatus EQUALS quarantine)	JNPR SDSN Quarantine
3. (LocalUser:Department EQUALS HR)	[RADIUS] HR Windows Profile

[Back to Enforcement Policies](#) [Copy](#) [Save](#) [Cancel](#)



NOTE: Rules Evaluation should be set to "First applicable."



NOTE: Make sure the default termination enforcement profile for each of the supported vendors is not superseded by any of its enforcement profile copies. Also make sure that all the attributes required for termination are set in the profile. (As in the previous Juniper Networks Trapeze Wireless Clients example.)

Enable Insight:

1. In ClearPass, navigate to **Administration > Server Manager > Server Configuration** for the server in use.
2. Enable Insight in the **System** tab.

Set the Log accounting Interim-update Packets as TRUE:

1. In ClearPass, navigate to **Administration > Server Manager > Server Configuration** for the server in use.
2. Select the **Service Parameters** tab.
3. In the **Select Service** drop down list, select **Radius Server** and set the Log accounting Interim-update Packets as **TRUE**.
4. Proceed to [“Creating a Policy Enforcer Connector for Third-Party Switches” on page 15](#) to finish the configuration with Policy Enforcer.

**Related
Documentation**

- [Creating a Policy Enforcer Connector for Third-Party Switches on page 15](#)
- [Policy Enforcer Connector Overview on page 6](#)

Cisco ISE Configuration for Third-Party Plug-in

Policy Enforcer's Cisco ISE Connector communicates with the Cisco Identity Services Engine server using the Cisco ISE API. As part of threat remediation, Policy Enforcer's Connector uses enforcement profiles. This section provides information for configuring Cisco ISE so that Policy Enforcer can invoke the appropriate enforcement profiles.

As part of the configuration, on Cisco ISE you will create two enforcement profiles, one for quarantine and one for terminate. Then you will use them in the Cisco ISE enforcement policy. Once Cisco ISE is configured, you will configure a Cisco ISE Connector on Policy Enforcer.



NOTE: Always use a third-party switch that supports 802.1x, Radius CoA, Radius Accounting, and DHCP snooping features. Enabling DHCP snooping is important which configures the Radius attribute, Framed-IP-Address. Only after configuring Framed-IP-Address, Policy Enforcer can detect the session related to the infected-host IP addresses and terminate the session.

On Cisco ISE you will configure the following:

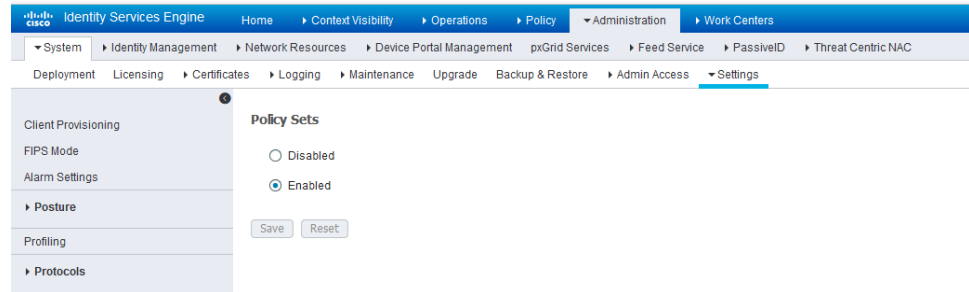
- Change policy modes
- Create an API client
- Configure network profiles
- Add a custom attribute
- Configure authorization profiles
- Set an authorization policy

On Cisco ISE, the Simple Mode policy model is selected by default. For creating an API client, Policy Sets should be enabled.

- Navigate to **Administration > System > Settings > Policy Sets** and Enable **Policy Sets** mode.

You are prompted to login again after changing the mode.

Figure 20: Cisco ISE: Enable Policy Sets Mode

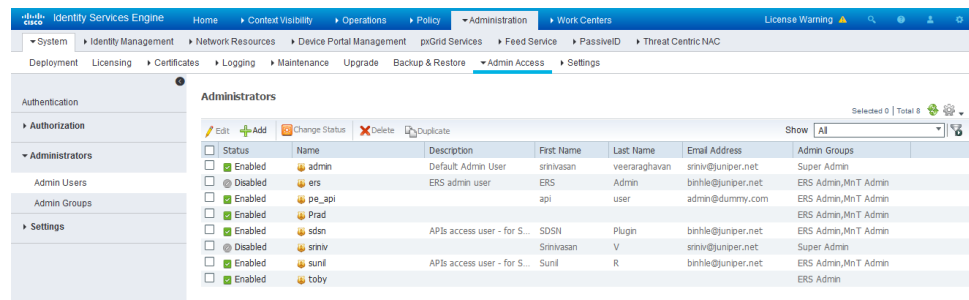


Create an API Client:

1. Using the Cisco ISE web UI, create an Admin User by navigating to **Administration > System > Admin Access > Administrator > Admin User**.
2. Create an Admin User and assign it to the following Admin Groups: **ERS Admin, MnT Admin**.

Make note of the username and password. You will need them when you configure the connector portion in Policy Enforcer later on.

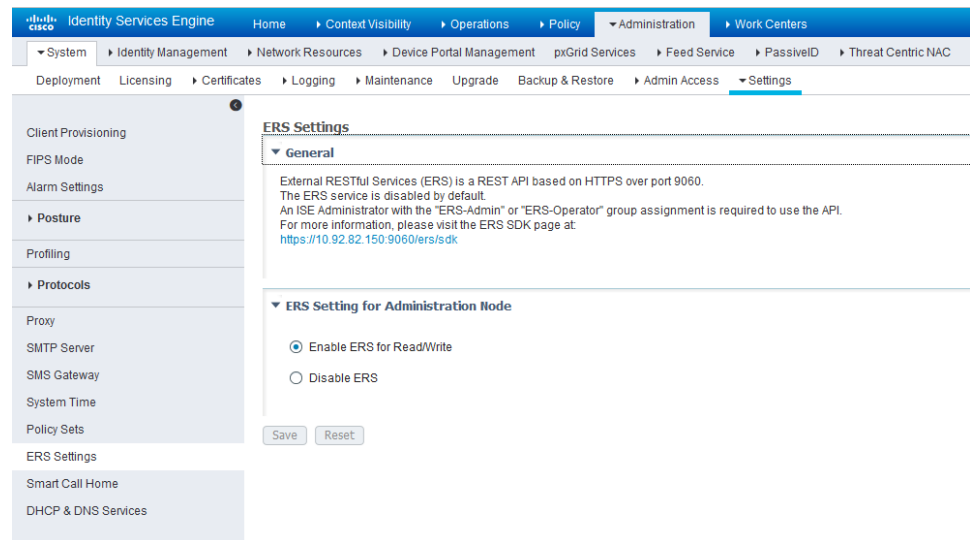
Figure 21: Cisco ISE: Create Admin User and Assign to Admin Groups



Enable the External RESTful Services API (ERS) for the Administration Node:

1. Navigate to **Administration > System > Settings > ERS Settings** and select **Enable ERS for Read/Write**.
2. Click **Save**.

Figure 22: Cisco ISE: Enable ERS



Configure network profiles:

Devices managed by ISE must support RADIUS CoA and have the proper network profiles assigned to handle the CoA commands sent by the ISE server:

1. Navigate to **Administration > Network Resources > Network Device Profiles** and verify the existing network device profile list.

If you are creating a new profile, proceed to the next step for information.

Figure 23: Cisco ISE: Network Device Profiles List

The screenshot shows the 'Network Device Profiles' page in the Cisco ISE Administration console. The page has a table with columns: Name, Description, Vendor, and Source. The table lists several profiles, including AlcatelWired, ArubaWireless, BrocadeWired, Cisco, Prad, HPWired, HPWired_SNMP_CoA, HPWireless, Juniper, MotorolaWireless, and RuckusWireless. The 'Source' column indicates whether the profile is 'Cisco Provided' or 'User Defined'.

Name	Description	Vendor	Source
AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided
Prad		Cisco	User Defined
HPWired	Profile for HP switches	HP	Cisco Provided
HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP	Cisco Provided
HPWireless	Profile for HP wireless network access devices	HP	Cisco Provided
Juniper	Profile for Juniper Switches - created by Binh.	Juniper	User Defined
MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

2. If you are configuring a new profile, you must minimally set the following:
 - Enable RADIUS and add a corresponding dictionary in the supported protocol list.

Figure 24: Cisco ISE: Network Device Profile, Enable RADIUS

Network Device Profile List > **New Network Device Profile**

Network Device Profile Submit Cancel

* Name

Description

Icon Change Icon... Set To Default i

Vendor

Supported Protocols

RADIUS ☒

TACACS+ ☐

TrustSec ☐

RADIUS Dictionaries

- Enable and configure the Change of Authorization (CoA) according to the figure below.

Figure 25: Cisco ISE: Configure Change of Authorization (CoA)

Change of Authorization (CoA)

CoA by

* Default CoA Port i

* Timeout Interval seconds i

* Retry Count i

Send Message-Authenticator ☐

- Configure the Disconnection and Re-authenticate operation with the proper RADIUS attributes and vendor specific VSA to handle the standard disconnect and reauthenticate operations. Below is the sample configuration for Juniper's EX devices.

Figure 26: Sample Configuration for Juniper EX

Disconnect

☒ RFC 5176

Radius:Acct-Session-Id = 0

Radius:Event-Timestamp = 0

Radius:User-Name = 0

☐ Port Bounce

Radius:VendorSpecific = "Port-Bounce"

☐ Port Shutdown

Radius:Acct-Session-Id = Radius:Acct-Session-Id

Re-authenticate

☒ Basic

Radius:Calling-Station-ID = 0

Radius:User-Name = 0

☐ Rerun

Select an item =

☐ Last

Select an item =

CoA Push

☐ RFC 5176

Configure a custom attribute.

1. Navigate to **Administration > Identity Management > Settings > Endpoint Custom Attribute** and add attribute `sdsnEpStatus` with type string.

Figure 27: Cisco ISE: Add Attribute `sdsnEpStatus`

Identity Services Engine | Home | Context Visibility | Operations | Policy | **Administration** | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | PassiveID | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | **Settings**

User Custom Attributes

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Endpoint Custom Attributes

Endpoint Attributes (for reference)

Required	Attribute Name	Data Type
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

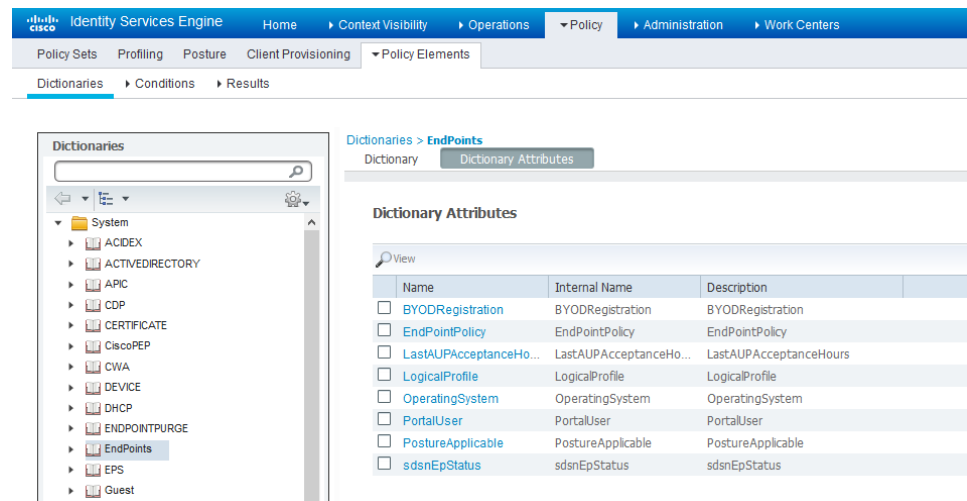
Endpoint Custom Attributes

Attribute name:

Type: − +

2. Verify the attribute under **Policy > Policy Elements > Dictionaries > System > Endpoints**.

Figure 28: Cisco ISE: Verify Attribute



3. Navigate to **Policy > Policy Elements > Conditions > Authorization > Simple Conditions**. Add there authorization simple conditions using the **sdsnEpStatus** attribute you created.

In the screen below,, there are three conditions created using sdsnEpStatus attribute. The condition names do not need to be the same as in the screen here, but the expressions must be matched. These conditions will be used in Policy Sets to handle the threat remediation for managed endpoints as described later in the Policy Sets setting section. Only the sdsnEpStatus-blocked and sdsnEpStatus-quarantine conditions will be used there. sdsnEpStatus-healthy is created for fulfillment purpose and can be ignored for now.

Figure 29: Cisco ISE: Configure Simple Conditions, Match Expression

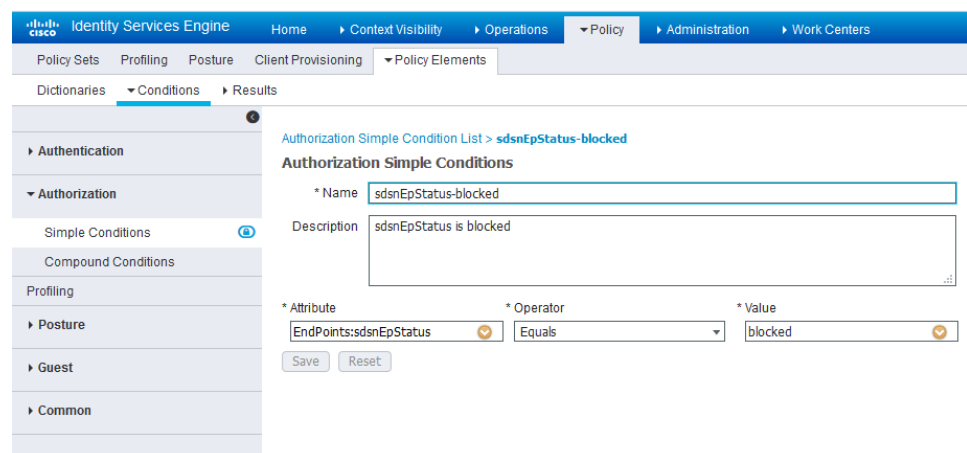


Figure 30: Cisco ISE: Configure Simple Conditions, Match Expression

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows a tree view with categories like Authentication, Authorization, Simple Conditions, Compound Conditions, Profiling, Posture, Guest, and Common. The 'Simple Conditions' option is selected, and a new condition named 'sdsnEpStatus-quarantine' is being configured.

Authorization Simple Condition List > sdsnEpStatus-quarantine

Authorization Simple Conditions

* Name:

Description:

* Attribute	* Operator	* Value
<input type="text" value="EndPoints:sdsnEpStatus"/>	<input type="text" value="Equals"/>	<input type="text" value="quarantine"/>

Configure permission/authorization profiles.

You can create the authorization profiles corresponding to “block” and “quarantine” actions as fits your needs. In the sample configuration provided here, the block action will result as total denial access to the network, and the quarantine profile will move the endpoint to another designated VLAN.

1. Navigate to From **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Refer to the figures below for sample configurations.

Figure 31: Cisco ISE: Configure Authorization Profiles

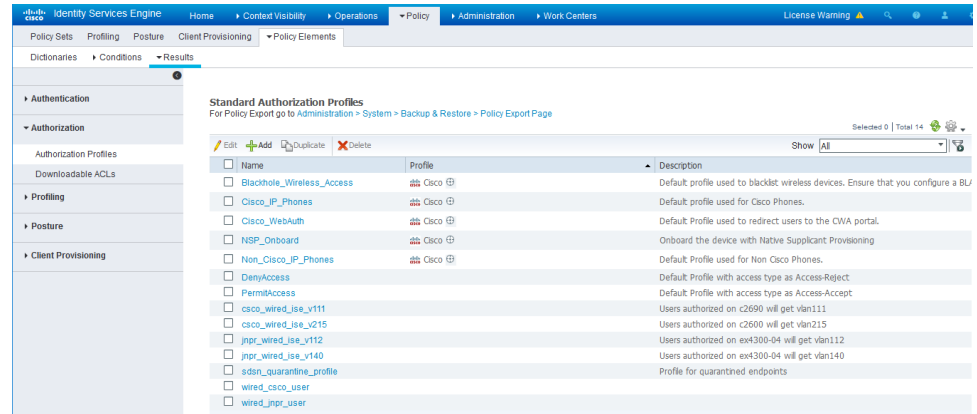
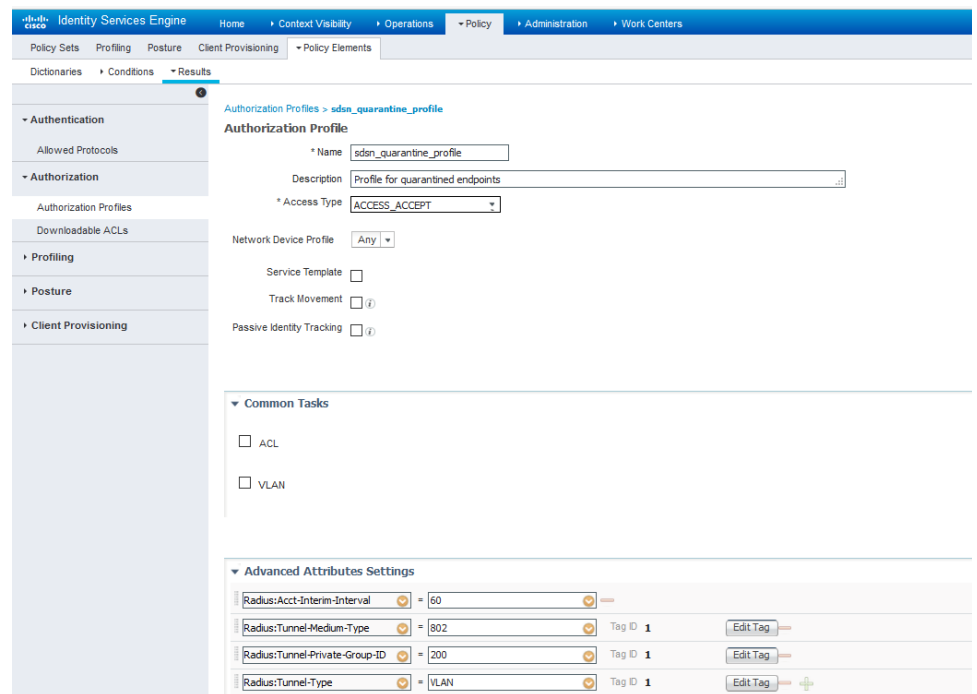


Figure 32: Cisco ISE: Configure Authorization Profiles



NOTE: For blocking a host, the default 'DenyAccess' profile is used.

Set the authorization policy:

1. Create two rules as Local Exceptions, applying the conditions and

authorization/permission profiles we created in the previous step. Names may be different, but these two rules must be at the top of the Exception list.

Refer to the figure below for a sample configuration.

Figure 33: Cisco ISE: Local Exception Rules, Example

The screenshot shows the Cisco ISE Policy Sets configuration page. On the left, the 'Policy Sets' sidebar is visible, showing a search bar and a list of policy sets including 'Summary of Policies', 'Global Exceptions', and 'Default'. The main area displays the 'Authorization Policy' configuration. It includes a table of exceptions with columns for Status, Rule Name, Conditions, and Permissions. The table lists 11 exceptions, including 'Wireless Black List Default', 'Profiled Cisco IP Phones', 'Profiled Non Cisco IP Phones', 'Compliant_Devices_Access', 'Employee_EAP-TLS', 'Employee_Onboarding', 'Wi-Fi_Guest_Access', 'Wi-Fi_Redirect_to_Guest_Log in', 'Basic_Authenticated_Access', and 'Default'.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco_IP_Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	if Network_Access_Authentication_Passed AND Compliant_Devices	then PermitAccess
<input checked="" type="checkbox"/>	Employee_EAP-TLS	if Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN	then PermitAccess AND BYOD
<input checked="" type="checkbox"/>	Employee_Onboarding	if Wireless_802.1X AND EAP-MSCHAPV2	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if Guest_Flow AND Wireless_MAB	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Log in	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess



NOTE: Find this under Policy > Policy Sets > Authorization Policy.

- Proceed to “Creating a Policy Enforcer Connector for Third-Party Switches” on page 15 to finish the configuration with Policy Enforcer.

Related Documentation

- Creating a Policy Enforcer Connector for Third-Party Switches on page 15
- Policy Enforcer Connector Overview on page 6