Juniper Networks | Engineering Simplicity

Policy Enforcer

Policy Enforcer Connectors Guide

Published
2022-12-21

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

Policy Enforcer Policy Enforcer Connectors Guide

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://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

1

CHAPTER

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

Policy Enforcer Settings

To configure your Policy Enforcer, perform the following actions.

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 Enforcer 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 the new root password 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: *Juniper ATP Cloud Configuration Type Overview* before you make a Juniper ATP Cloud or Juniper Advanced Threat Prevention (JATP) Configuration Type selection on the Policy Enforcer Settings page.

- If you are using Juniper ATP Cloud or JATP without Juniper Connected Security or Cloud Feeds only, you must still download Policy Enforcer and create a policy enforcer virtual machine.

- Juniper ATP Cloud license and account are needed for three of the configuration types (Juniper ATP Cloud or JATP with Juniper Connected Security, Juniper ATP Cloud or JATP, and Cloud Feeds only), but not for the default mode (No Selection). If you do not have a Juniper ATP Cloud license, contact your local sales office or Juniper Networks partner to place an order for a Juniper ATP Cloud premium license. If you do not have a Juniper ATP Cloud account, when you configure Juniper ATP Cloud, you are redirected to the Juniper ATP Cloud server to create one. Please obtain a license before you try to create a Juniper ATP Cloud account. Refer to *Policy Enforcer Installation Overview* for instructions on obtaining a Juniper ATP Cloud premium license.

To set up ATP Cloud or JATP Configuration Type, you must do the following:

1. Select **Security Director**>**Administration**>**Policy enforcer**>**Settings**.

2. 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.)

3. 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.

4. If you want to use certificate based authentication, enable the **Certificate Based Authentication** option.

   Browse the X509 certificate file and X509 certificate Key file.

5. Select ATP Cloud Configuration Type. If you do not select a type, Policy Enforcer works in *default mode*. (See *Juniper ATP Cloud Configuration Type Overview* for more information.)

   Refer Table 1 on page 6 to understand the supported threat prevention types for different Policy Enforcer modes:

   Table 1: Supported Threat Prevention Types for Different PE Modes

Threat Prevention Type	No Selection (Default)	Cloud Feeds Only	ATP Cloud or JATP	ATP Cloud or JATP with Juniper Connected Security
Custom feeds	Yes	Yes	Yes	Yes
Command and Control (C&C) feeds	Yes	Yes	Yes	Yes
Infected Host feed	-	Yes	Yes	Yes
Malware inspection	-	-	Yes	Yes
Enforcement on EX Series and QFX Series switches or using 3rd party Connectors	-	-	-	Yes

   You cannot change or modify a higher configuration to a basic mode. For example, you cannot change:

   - Juniper ATP Cloud or JATP ->Cloud feeds only

- Juniper ATP Cloud or JATP with Juniper Connected Security ->Cloud feeds only
- Juniper ATP Cloud or JATP ->No Selection (Default)

WARNING: If you change to a lower mode, you must reinstall Security Director and Policy Enforcer.

However, you can change or modify your configuration to a higher mode. For example you can change:

- Cloud feeds only-> Juniper ATP Cloud or JATP
- Cloud feeds only ->Juniper ATP Cloud with Juniper Connected Security
- Juniper ATP Cloud or JATP -> Juniper ATP Cloud with Juniper Connected Security

6. 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.
7. Click **Enable Feeds Purge** to enable the purge option. You can purge the feeds that are older than a specified number of days.
8. The Purge History determines the number of days you can preserve the history of the feeds in Policy Enforcer. You can set a range between 300 to 600 days. The default is 365 days.

   The purge job runs every day at 12:00 PM and makes sure that the data set on the purge history is maintained.
9. 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 Juniper Connected Security and non-Juniper Connected Security Configuration Steps
Using Guided Setup for Juniper ATP Cloud with Juniper Connected Security
Using Guided Setup for Juniper ATP Cloud
Configuring Cloud Feeds Only

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 2: 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.

Table 2: Connectors Information- Main Page *(continued)*

Field	Description
Status	The current status of the connector. (Active or Inactive.) Hover over the status to see more details of connector instances and their respective status. The following statuses are shown: • 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.
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 | 41

Cisco ISE Configuration for Third-Party Plug-in | 48

Creating a Policy Enforcer Connector for Third-Party Switches | 21

Creating a Policy Enforcer Connector for Public and Private Clouds

Perform the following actions to configure connectors for the public and private clouds.

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.
- For Microsoft Azure connector:
  - Get started with Microsoft Azure. See Getting Started With Microsoft Azure.
  - Create tenant ID for you Azure account. See Managing Access Keys for Your Microsoft Azure Account.

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 3 on page 11.

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 for AWS and Contrail

Field	Description
General	
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, Contrail, or Microsoft Azure 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, Contrail, or Microsoft Azure. 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. For Microsoft Azure, this field is set to management.azure.com, by default. This is where all virtual networks are located. You cannot edit this field.
Port	For AWS and Microsoft Azure connectors, the port is set to 443 by default and you cannot edit this field. For Contrail connector, provide the port number as 8081.
Username	Enter the username of the server for the selected connector type. For AWS, enter the generated access key for your Amazon account. This is not same as your Amazon account username.

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Password	Enter the password for the selected connector type. For AWS, enter your secret password generated along with your access key. This is not same password as your amazon account.
Subscription ID *(only for Microsoft Azure connector)*	Enter the Azure subscription ID available per tenant basis.
Tenant ID *(only for Microsoft Azure connector)*	Enter the Microsoft Azure tenant ID.
Network Details	

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Connector Type: AWS Virtual Private Clouds	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. Security Director suggests a default Secure Fabric site name for the VPC, in the <*connector name*>_<*vpc name*>_site 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. 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. 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 28. **NOTE:** You can perform search on VPCs. Search is not supported for the site names.

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Connector Type: Microsoft Azure Virtual Networks	One or more virtual networks under the Microsoft Azure account are discovered. These virtual networks are based on the Azure subscription per tenant basis. A tenant can have more than one subscription and a single subscription can contain one or more virtual networks. Security Director suggests a default site name for the project, in the <*connector name*>_<*virtual network name*>_site 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. 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. You can get a detailed view of the virtual network by hovering over the name and clicking the Detailed View icon.

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Connector Type: Contrail Project	Tenant information determined from the Contrail connector is listed. Security Director suggests a default site name for the project, in the <*connector name*>_<*project name*>_site 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. 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. 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 28. **NOTE:** You can perform search on Project names. Search is not supported for the site names.
Subnets	The subnet information for Contrail, Microsoft Azure, and AWS is determined from the respective systems. For AWS and Microsoft Azure, 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. Subnets for AWS, Microsoft Azure, and Contrail are allocated to be within the tenant IP Address Management (IPAM) scheme.
Configuration	

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
Configuration	

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
	Metadata 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. For AWS and Microsoft Azure connector, the resource tag values are fetched from AWS and Microsoft Azure for all the endpoints and then mapped them to the Security Director generated metadata names. 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. However, in the Generated MetaData Name column, you cannot use the following predefined metadata names: • Tenant • Provider • Controller If you provide these names, an appropriate error message is shown to choose a different name. 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. Mapping of Contrail, Microsoft Azure, and AWS connector resource tags to Security Director metadata enables you to create the next generation firewall policy definitions

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
	for the source and destination rules, based on the metadata expressions. Policy Enforcer dynamically determines the matching VM instances in AWS, Microsoft Azure, 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. 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. After the successful completion, the subnet you have created is mapped to that particular connector instance. For AWS and Microsoft Azure, provide the following configuration parameters: • SRX username—Specify the username of the vSRX device that you have instantiated for a VPC or a virtual network. • 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. This enables discovery of this particular vSRX device in Junos Space. This vSRX device is also added to a specific secure fabric site. • 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.

Table 3: Fields on the Create Connector Page for AWS and Contrail *(continued)*

Field	Description
	For Contrail, provide the following configuration parameters: • SRX username • SRX password • Infected host security group

NOTE:

- For AWS, Microsoft Azure, 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 Juniper Connected Security with ATP Cloud, then you must create ATP Cloud 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, Microsoft Azure, 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** > **ATP Cloud Realms**.

   Select the associated Secure Fabric sites to the respective VPC, virtual networks, or Project that is successfully added. Add the secure fabric site to a Juniper ATP Cloud realm and enrol the vSRX devices to the Juniper ATP Cloud. 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 or virtual network. Select the required subnets for this VPC or a virtual network 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 or a virtual network.

Next Generation Firewall Workflow

When you create an AWS, Microsoft Azure, or a contrail connector with Next Generation Firewall option, it means that for a particular VPC or a virtual network, 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 | 8

Editing and Deleting a Connector | 25

Viewing VPC or Projects Details | 28

Creating a Policy Enforcer Connector for Third-Party Switches

Perform the following actions to create connectors for the third-party switches.

Before You Begin

- Have your ClearPass, Cisco ISE, ForeScout, Pulse Secure 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 8 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 10.

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 4 on page 21.

4. Click **OK**.

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

Table 4: Fields on the Create Connector Page

Field	Description
General	

Table 4: Fields on the Create Connector Page *(continued)*

Field	Description
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, Pulse Secure, 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	Enter the username of the server for the selected connector type. • ClearPass—Enter the Client ID created while setting up the ClearPass API client. See "ClearPass Configuration for Third-Party Plug-in" on page 41 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 48. • ForeScout—Enter the username of your DEX plugin. See "Integrating ForeScout CounterACT with Juniper Networks Connected Security" on page 30.

Table 4: Fields on the Create Connector Page *(continued)*

Field	Description
Password	Enter the password of the server for the selected connector type. • ClearPass—Enter the Client Secret string created while setting up the ClearPass API client. See "ClearPass Configuration for Third-Party Plug-in" on page 41 for details. **WARNING:** When the Access Token Lifetime expires, you must generate a new Client Secret in ClearPass and update it here too. • 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 48. • ForeScout—Enter the password of your DEX plugin. See "Integrating ForeScout CounterACT with Juniper Networks Connected Security" on page 30.
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 Connected Security" on page 30.
Network Details	

Table 4: Fields on the Create Connector Page *(continued)*

Field	Description
Subnets	**Connector Type: ClearPass, ForeScout CounterACT, Pulse Secure, and Cisco ISE** 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. When you add subnets as part of the connector configuration, those subnets become selectable in Policy Enforcement Groups. To add subnet information, do one of the following: • 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. **NOTE:** It is mandatory to add at least one IP subnet to a connector. You cannot proceed to next step without adding a subnet.
Configuration	
Configuration	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. **NOTE:** For ClearPass and Cisco ISE connectors no additional configuration information are required.

NOTE:

- You can associate ClearPass, Cisco ISE, Pulse Secure, 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, Pulse Secure, 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 | 8

ClearPass Configuration for Third-Party Plug-in | 41

Cisco ISE Configuration for Third-Party Plug-in | 48

Editing and Deleting a Connector | 25

Viewing VPC or Projects Details | 28

Editing and Deleting a Connector

IN THIS SECTION

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

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.

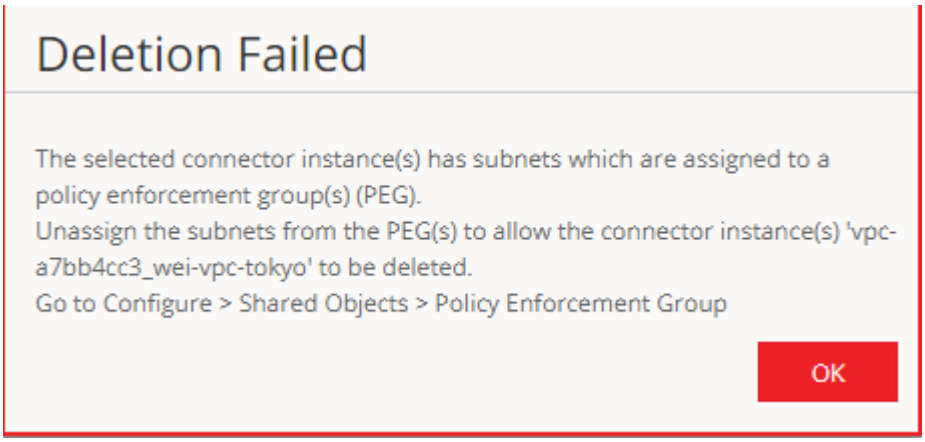
2. Select the connector that you want to delete, and select the delete icon (X).

   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 27.

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 | 8

Creating a Policy Enforcer Connector for Third-Party Switches | 21

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 29.

Figure 2: Detailed View Page

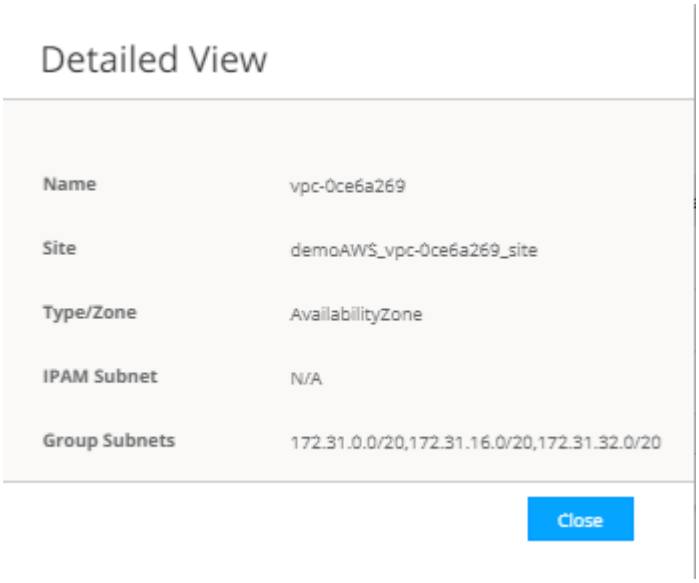


Table 5 on page 29 explains fields on the Detailed View page.

Table 5: 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	Specifies the group of subnets allocated to the VPC or project. 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. 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.

RELATED DOCUMENTATION

Integrating ForeScout CounterACT with Juniper Networks Connected Security

IN THIS SECTION

This topic provides instructions on how to integrate the third-party device ForeScout CounterACT with Juniper Networks Connected Security 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 Juniper Connected Security 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 Juniper Connected Security, 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

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:

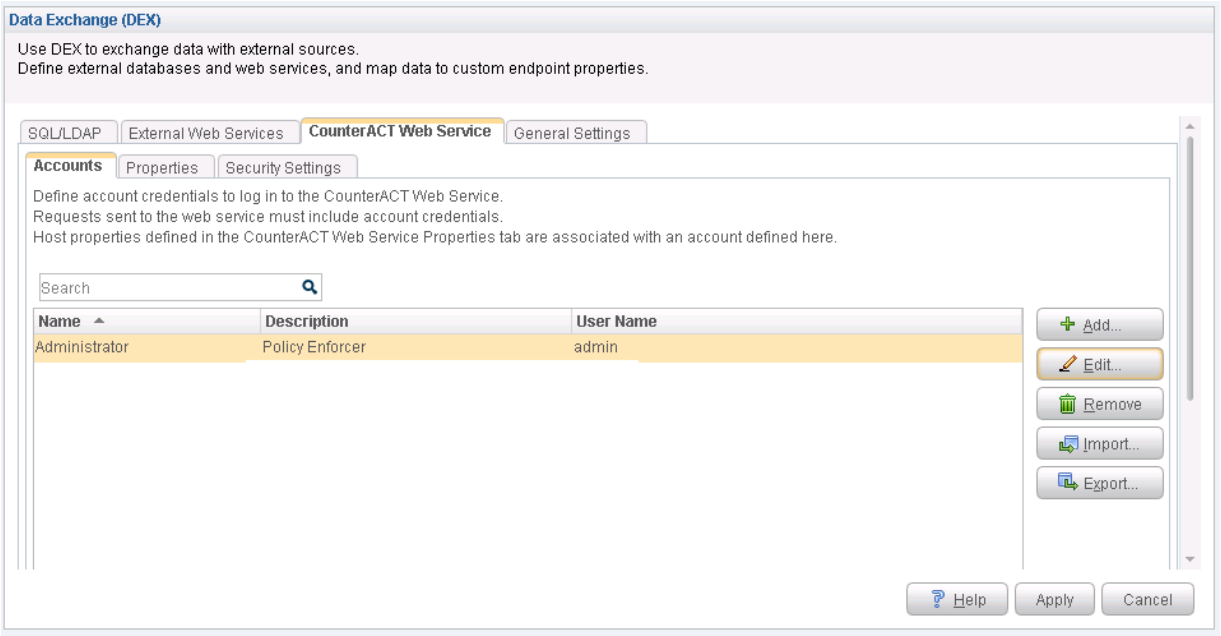
1. Select **Tools** > **Options** > **Data Exchange (DEX)** in the CounterACT UI.

   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 31.

   The DEX Accounts page appears.

Figure 3: DEX Accounts Page



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.

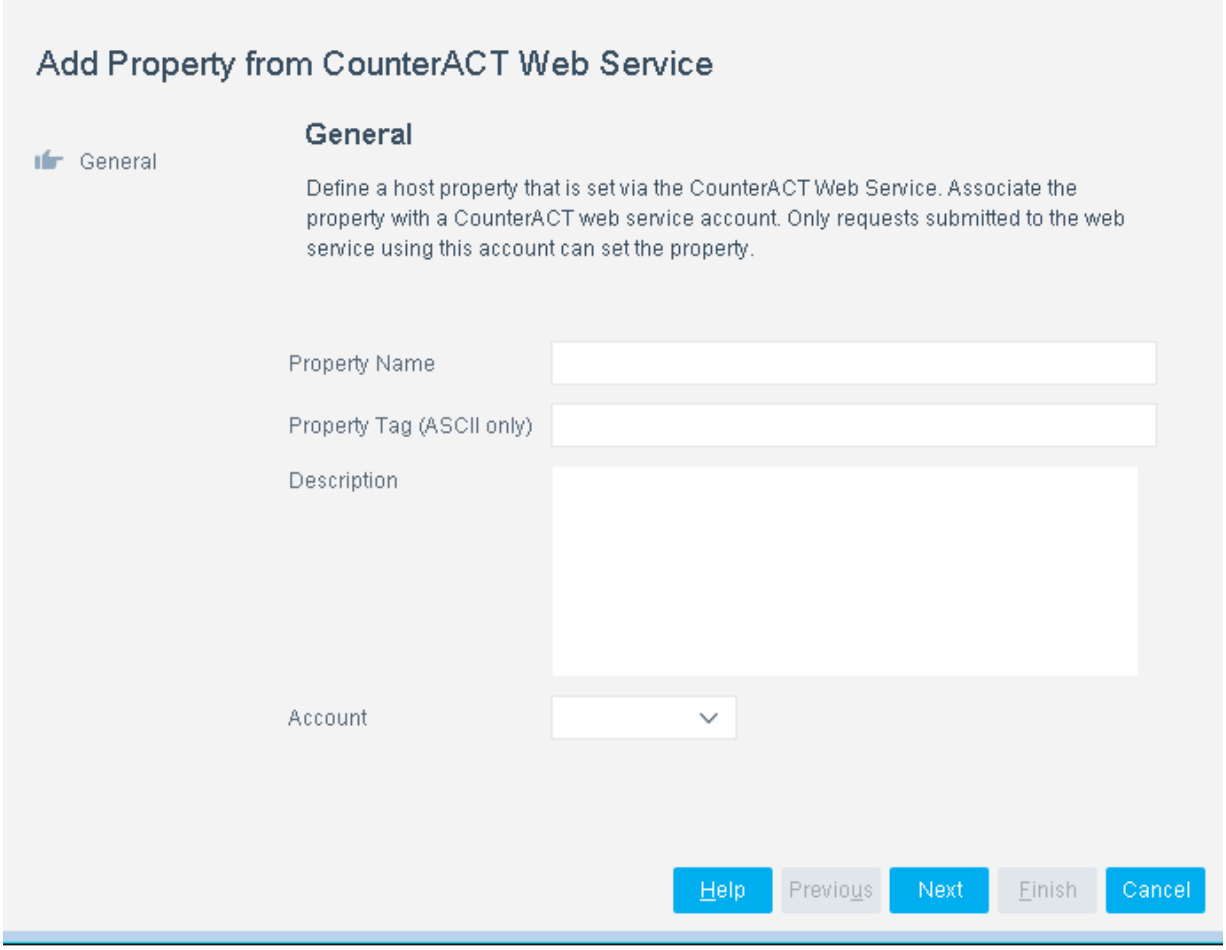
7. In the Password field, enter the password that will be used to authorize CounterACT to access this Web service account.

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 33.

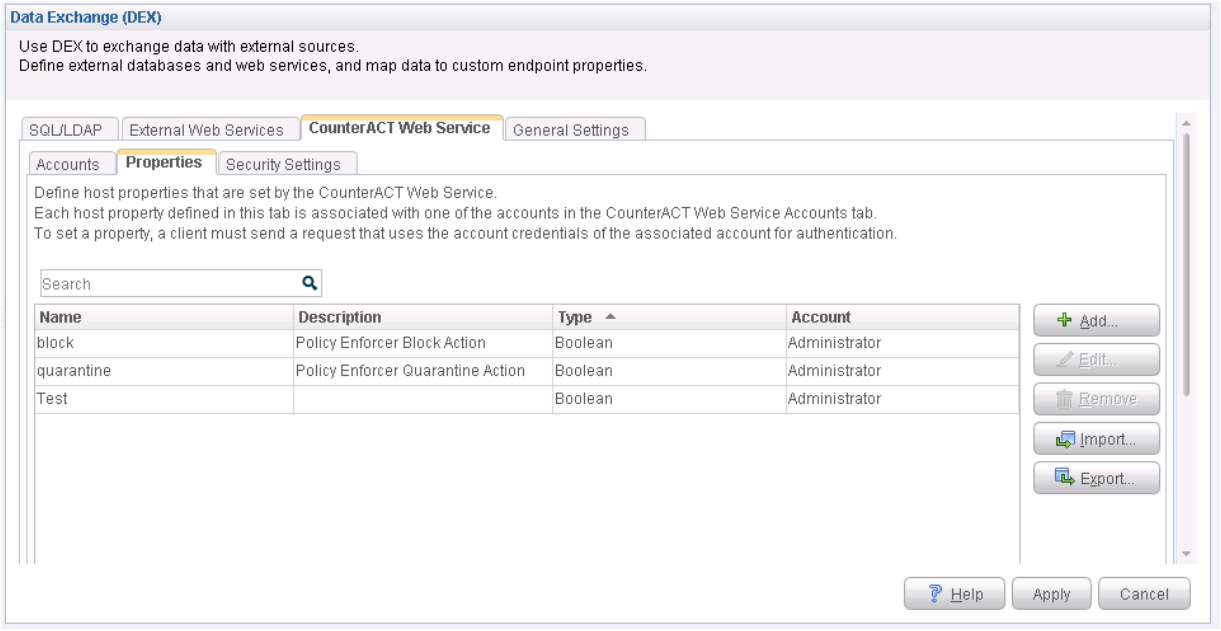
Figure 4: Add Property-General Pane Page



10. Add properties such as block, quarantine, and Test, as shown in Figure 5 on page 34.

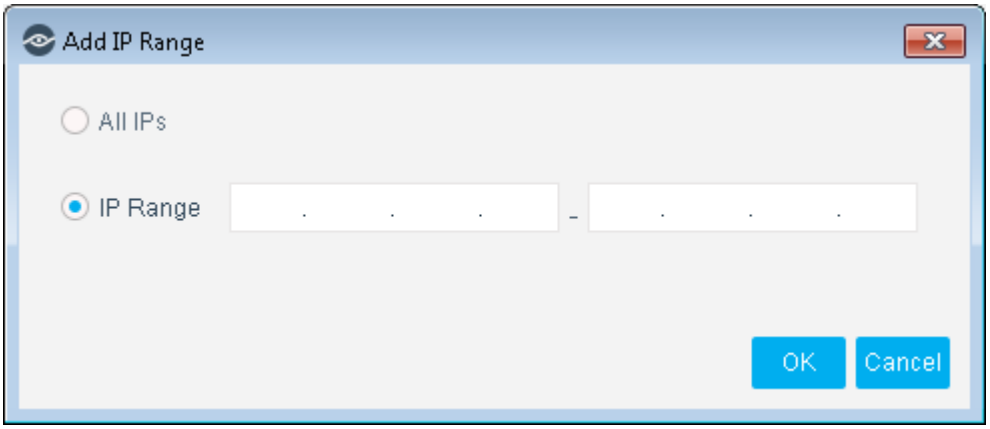
    You must include the Test property. Otherwise, you cannot add CounterACT as a third-party connector to Policy Enforcer successfully.

Figure 5: DEX Properties Page



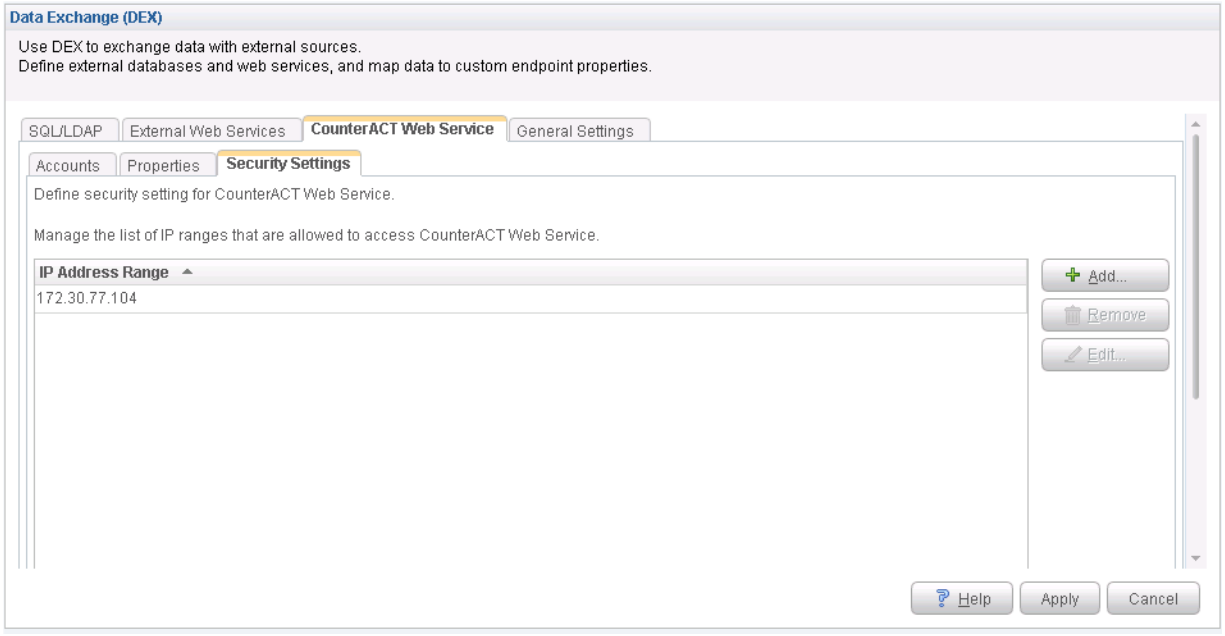
11. In the Security Settings tab, click **Add** and add the IP address range from where communication is expected, as shown in Figure 6 on page 34.

Figure 6: Add IP Range Page



Click **OK**. The IP address appears in the IP Address Range list, as shown in Figure 7 on page 35.

Figure 7: DEX Security Settings Page



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.

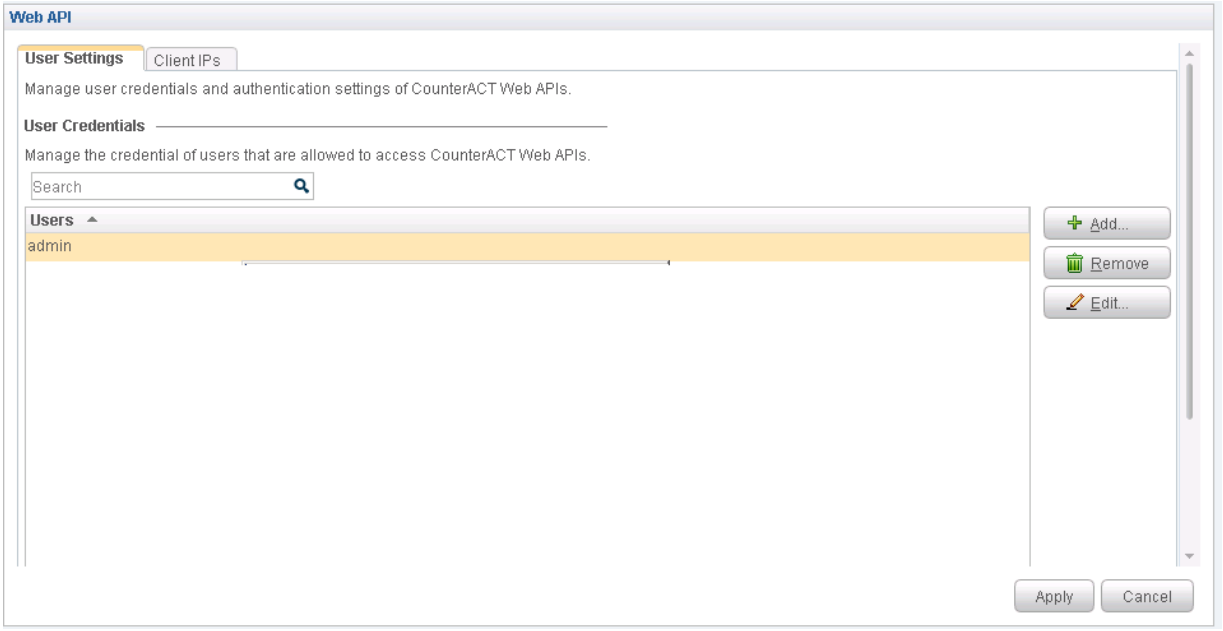
   The Web API page appears.

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 36.

Figure 8: Web API User Settings Page



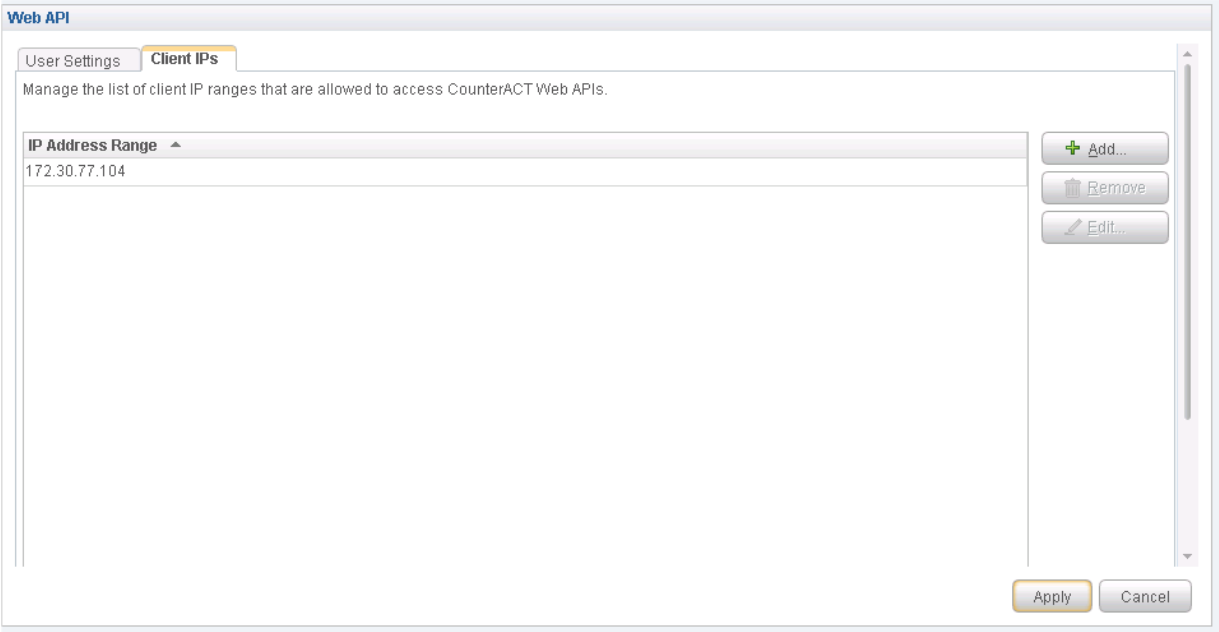
4. Select the **Client IPs** tab and click **Add**.

   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 37.

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.

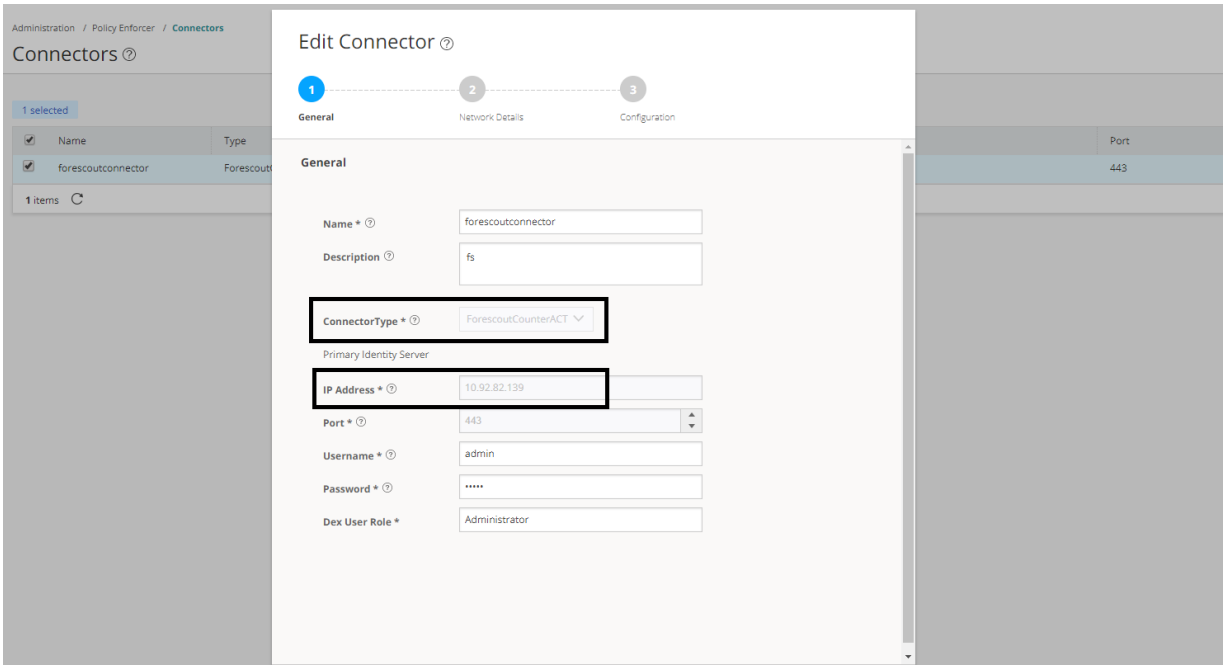
2. Click the create icon (+).

   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 38. (The DEX user role is the one that you created in Step 4).

   Specify 443 as the port number for communication.

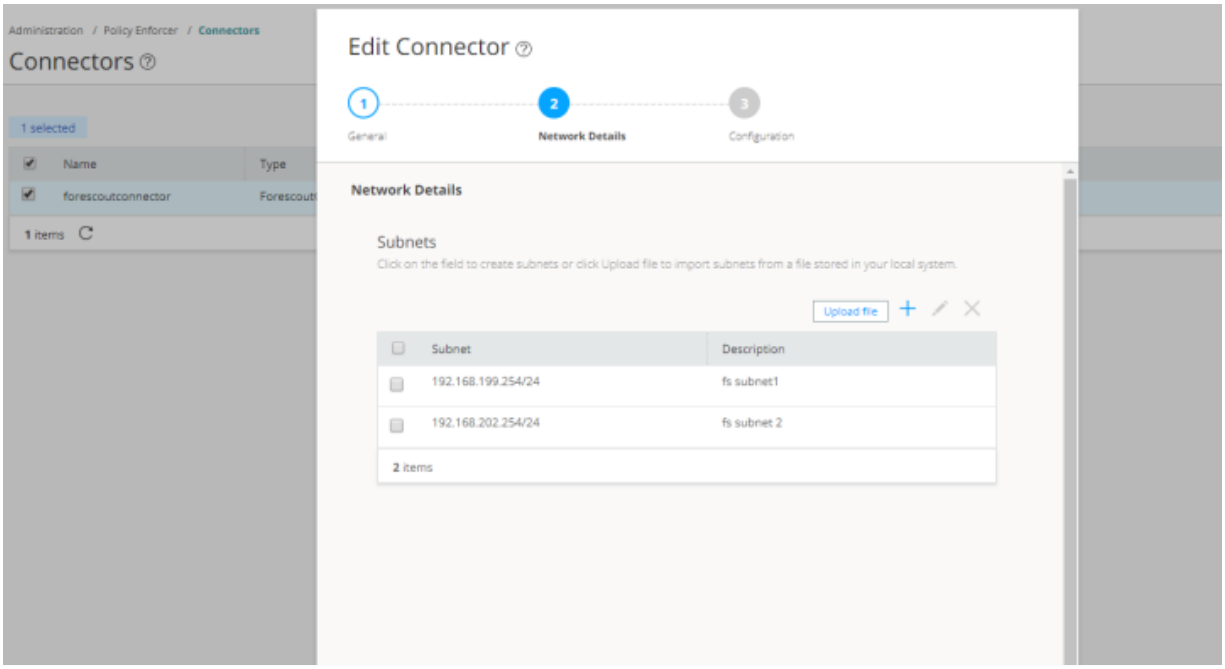
Figure 10: Edit Connector Page



4. In the Network Details tab, configure the IP subnets, as shown in Figure 11 on page 38.

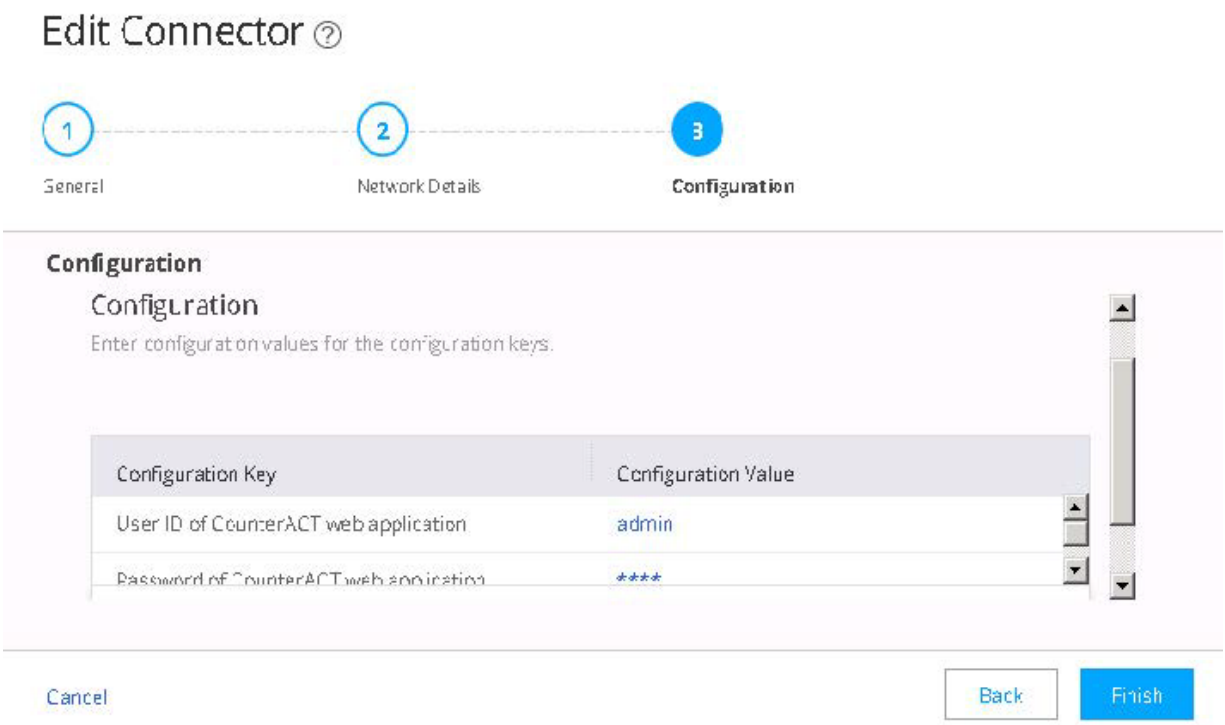
   CounterACT treats the IP subnets as endpoints and takes action.

Figure 11: Edit Connector - Network Details Page



5. In the Configuration tab, specify the Web API username and password, as shown in Figure 12 on page 39.

Figure 12: ForeScout Connector - Configuration Tab



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 40.

Figure 13: Host Information

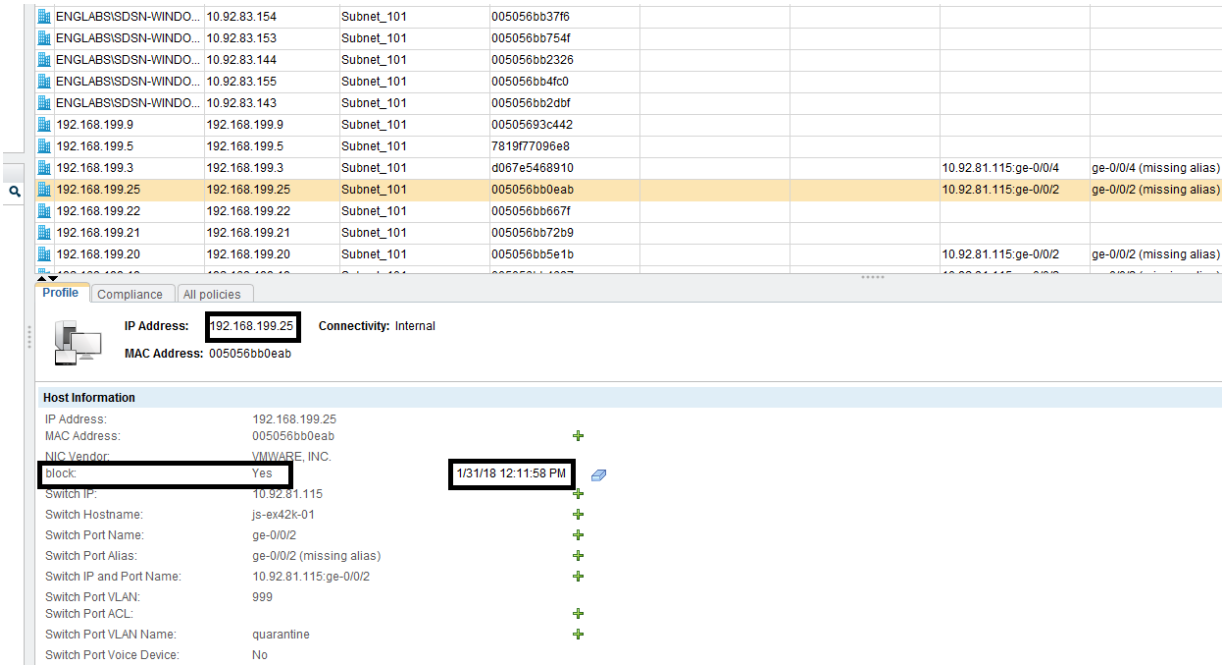


Table 6 on page 40 shows the recommended actions performed by CounterACT on the infected hosts that are blocked or quarantined.

Table 6: 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 | 8

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

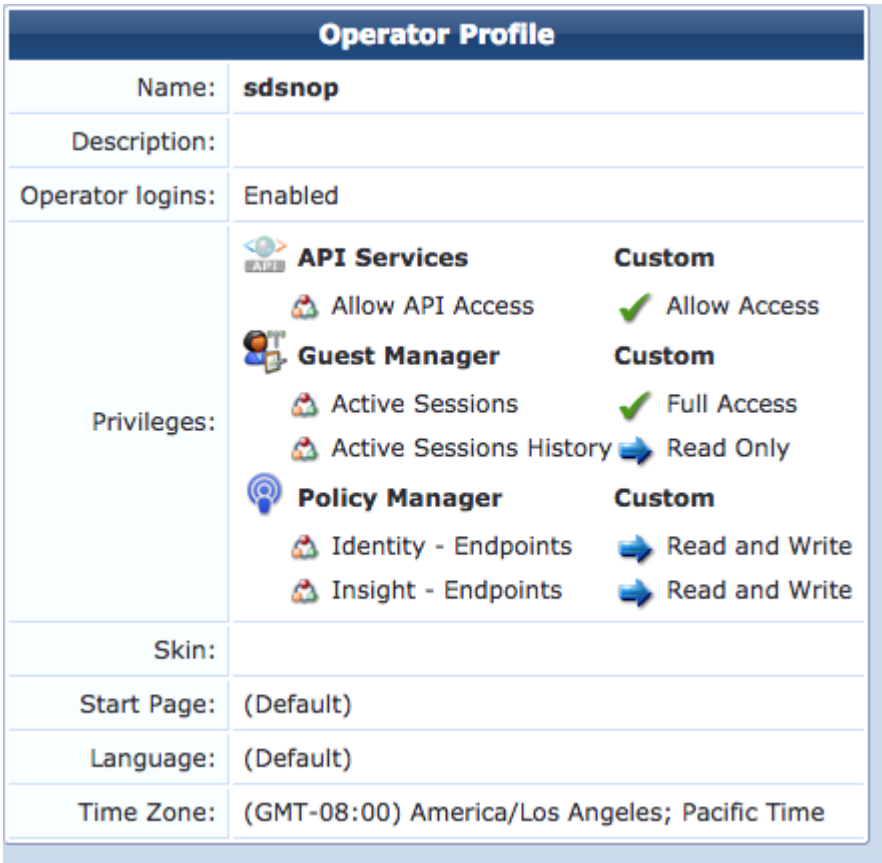
To configure the API Client:

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.

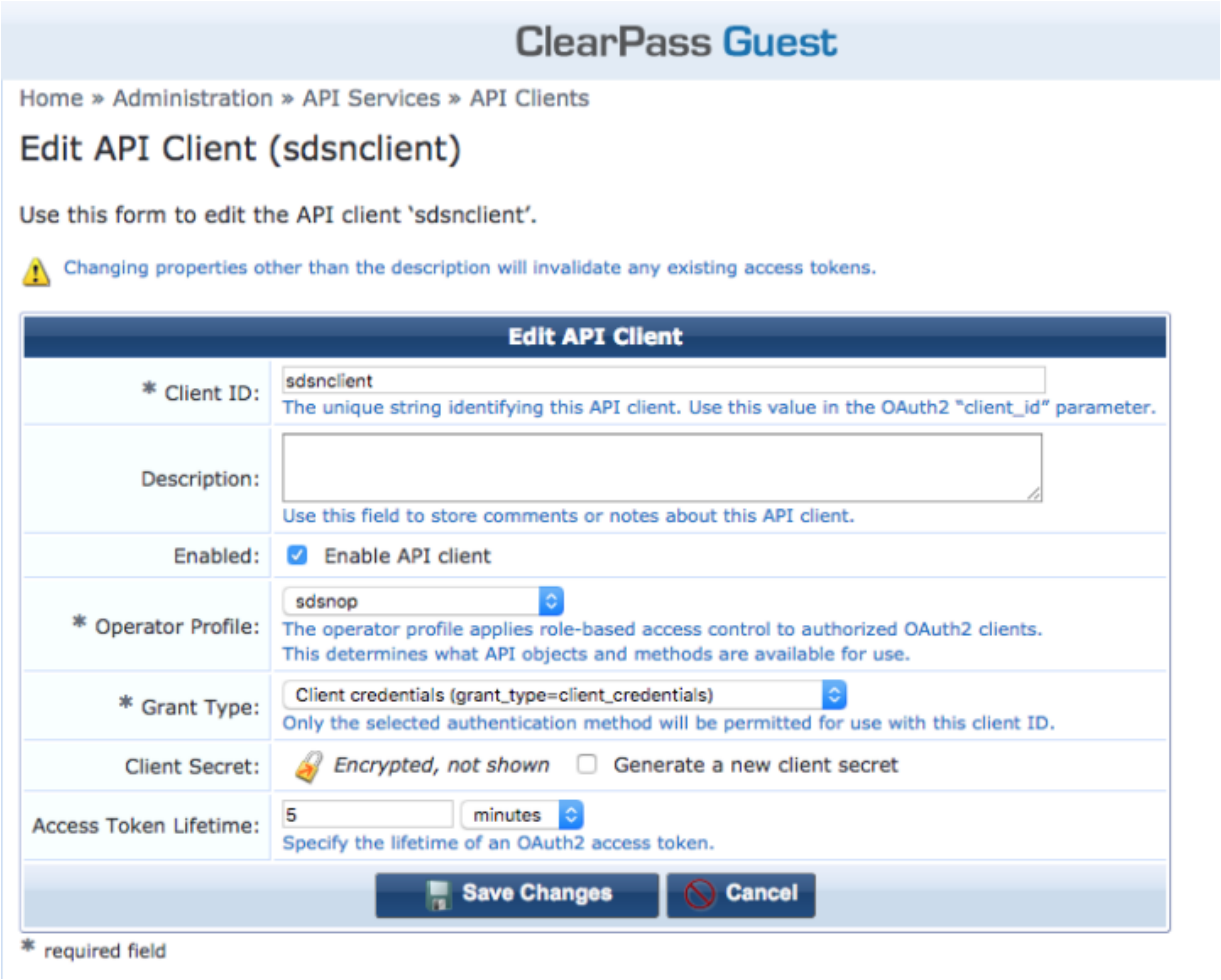
- Client ID: sdsnclient
- Enabled: Select the check box for **Enable API client**
- Operator Profile: Create a profile from Administrator > Operator Logins > Profiles for the API client with minimum access privileges as shown in Figure 14 on page 42.

Figure 14: ClearPass API Client Operator Profile Minimum Privileges



- 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

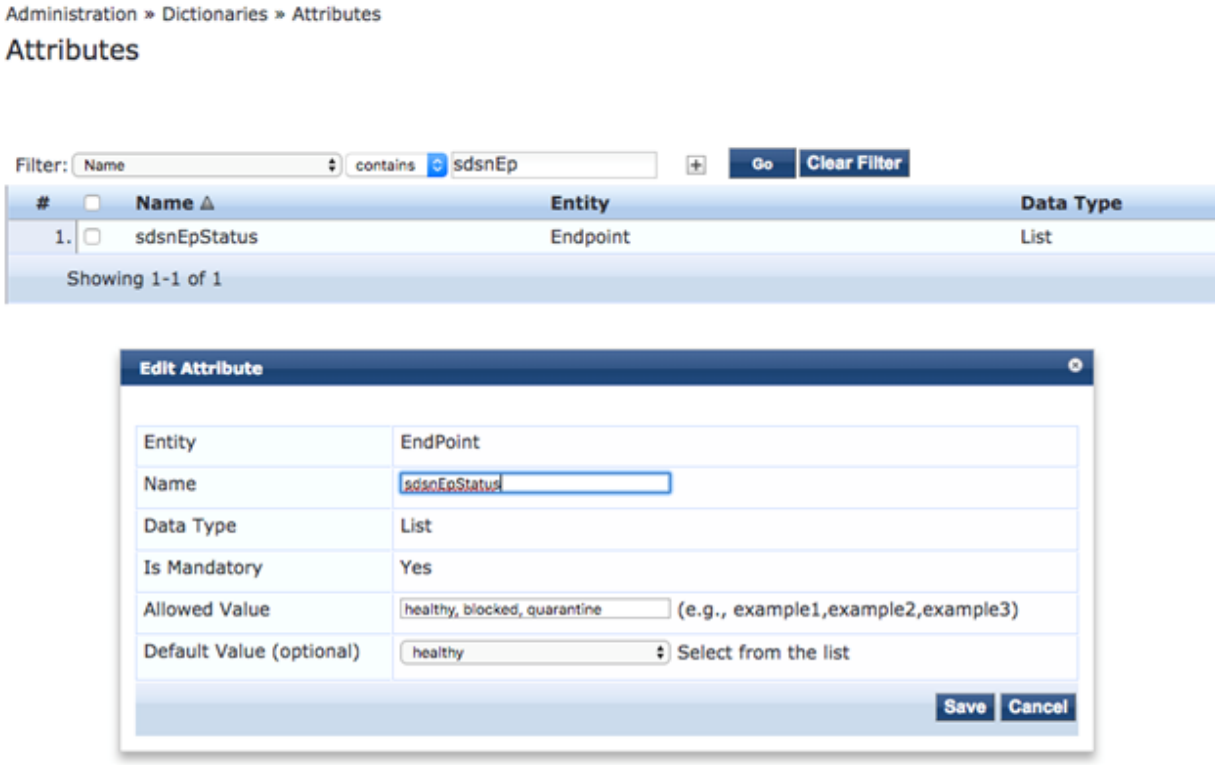


2. Click **Save Changes**.

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



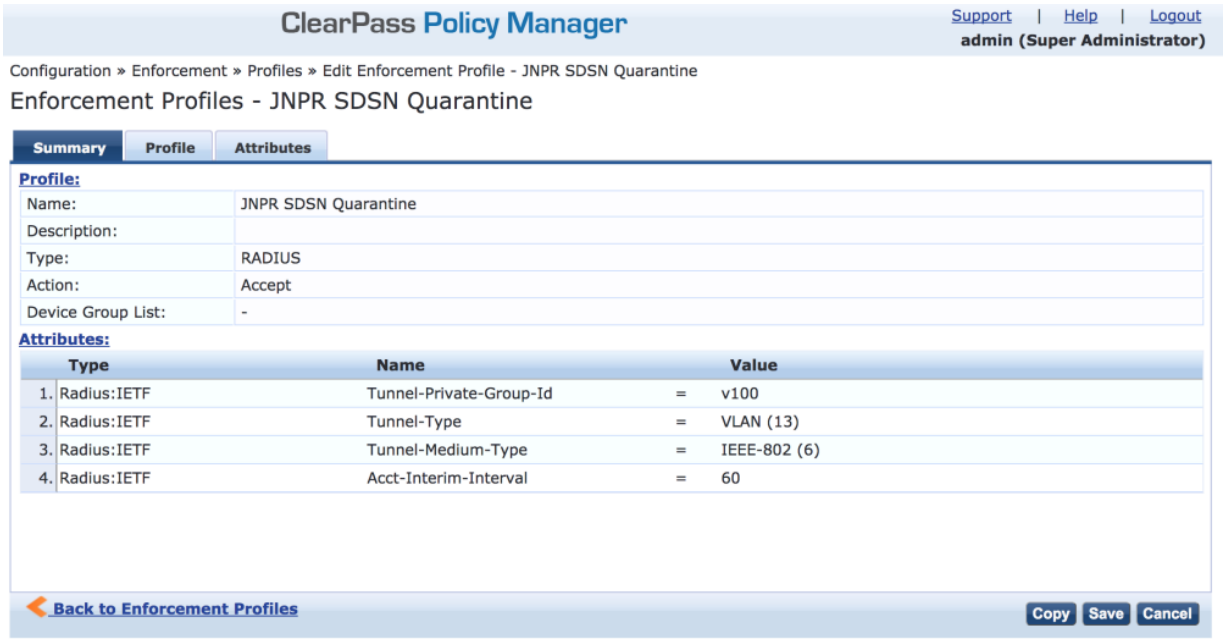
2. Click **Save**.

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: **Name of the enforcement profile**
   - Description: **Quarantine profile for Juniper Connected Security**
   - Type: **RADIUS**
   - Action: **Accept**

Figure 17: ClearPass Enforcement Profile: Quarantine



> **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.

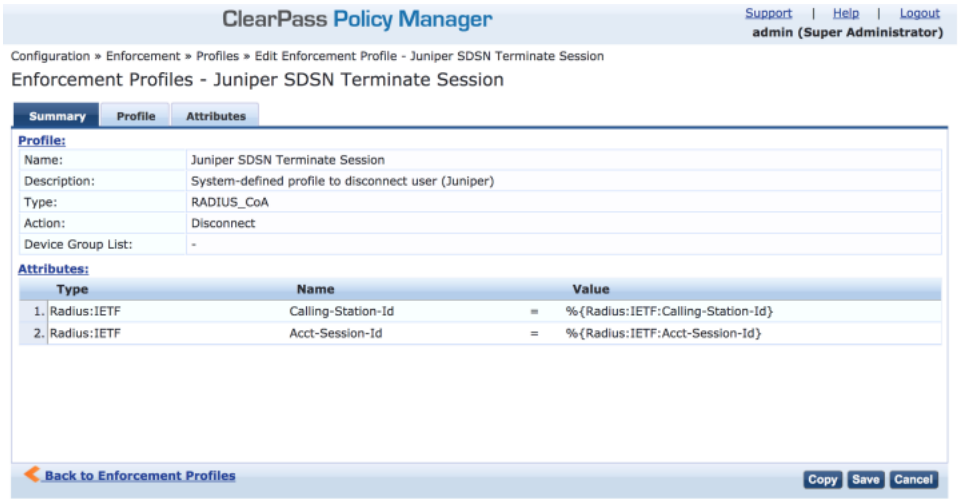
3. Profile 2: Create the following profile to block infected endpoints:

> **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.

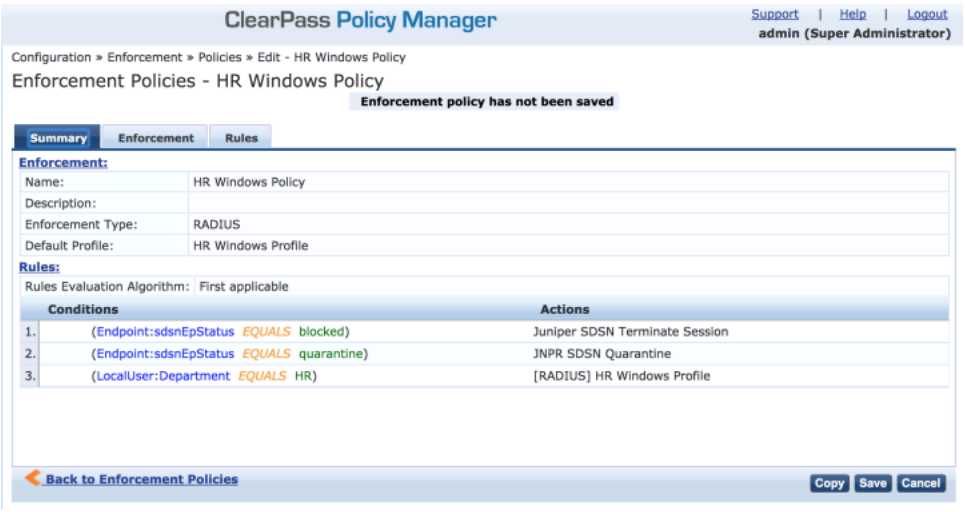
Figure 18: ClearPass Enforcement Profile: Terminate



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



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 21 to finish the configuration with Policy Enforcer.

RELATED DOCUMENTATION

Creating a Policy Enforcer Connector for Third-Party Switches | 21

Policy Enforcer Connector Overview | 8

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.

On Cisco ISE you will configure the following:

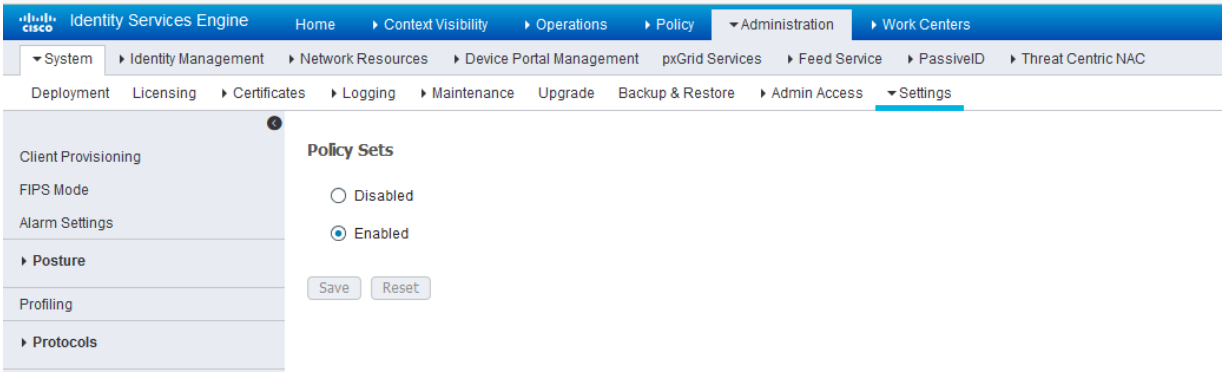
- Change policy modes
- Create an API client
- Configure network profiles
- Add a custom attribute
- Configure authorization profiles
- Set an authorization policy

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



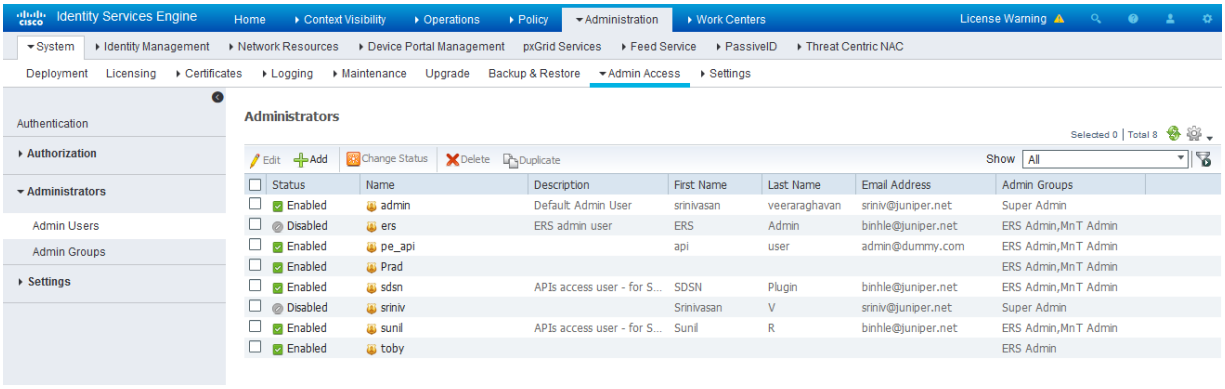
Create an API Client:

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

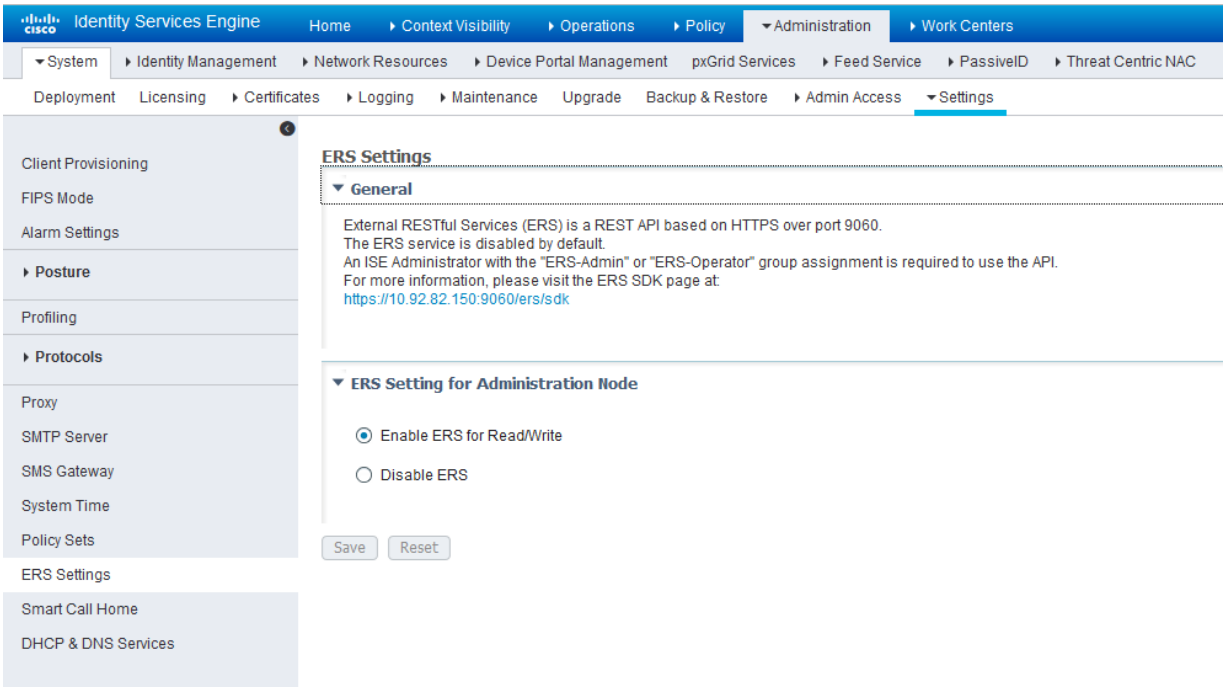


Enable the External RESTful Services API (ERS) for the Administration Node:

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

2. Click **Save**.

Figure 22: Cisco ISE: Enable ERS



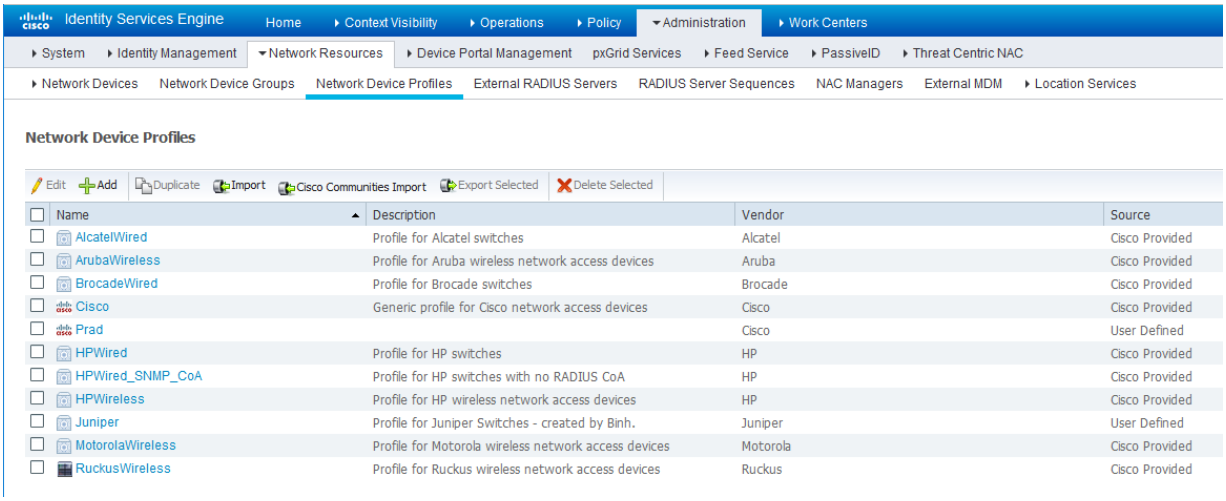
Configure network profiles:

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.

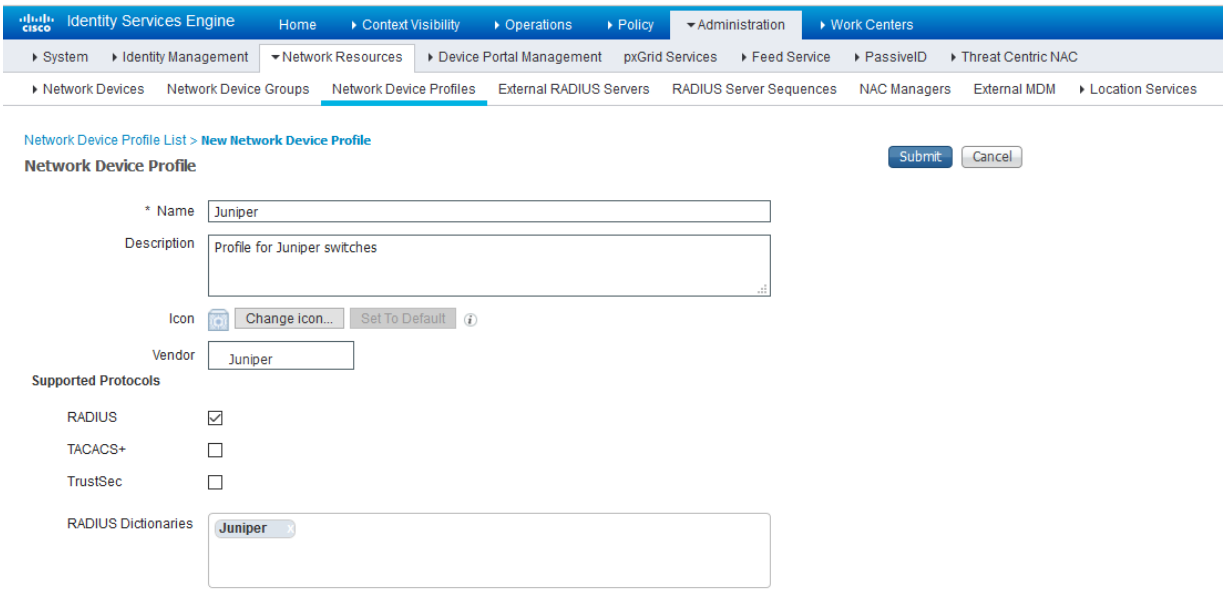
Figure 23: Cisco ISE: Network Device Profiles List



2. If you are configuring a new profile, you must minimally set the following:

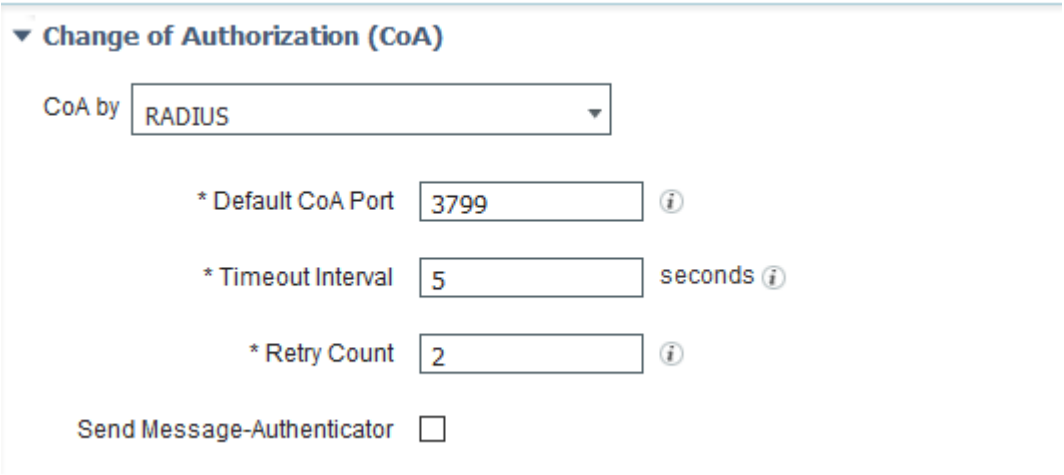
   - Enable RADIUS and add a corresponding dictionary in the supported protocol list.

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



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

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



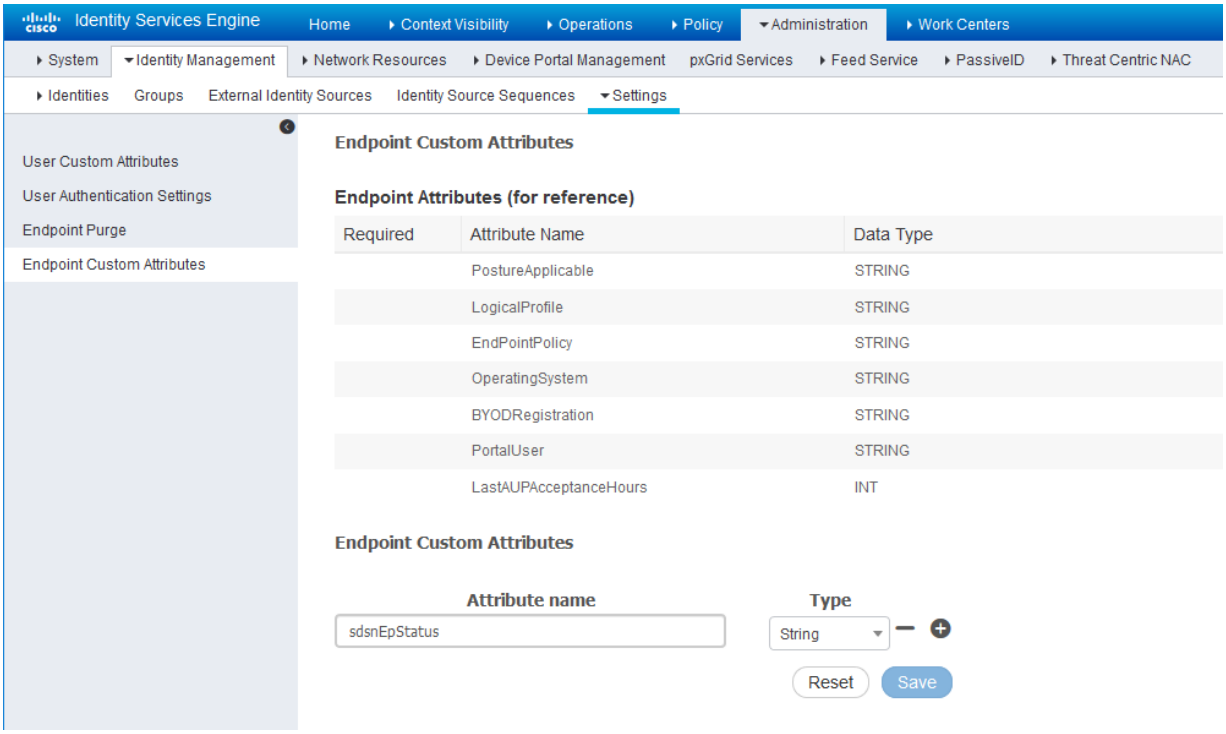
- Configure the Disconnection and Re-authenticate operation with the proper RADIUS attributes and vendor specific VSA to handle the standard disconnect and reauthenticate operations. Below is the sample configuration for Juniper's EX devices.

Figure 26: Sample Configuration for Juniper EX

Configure a custom attribute.

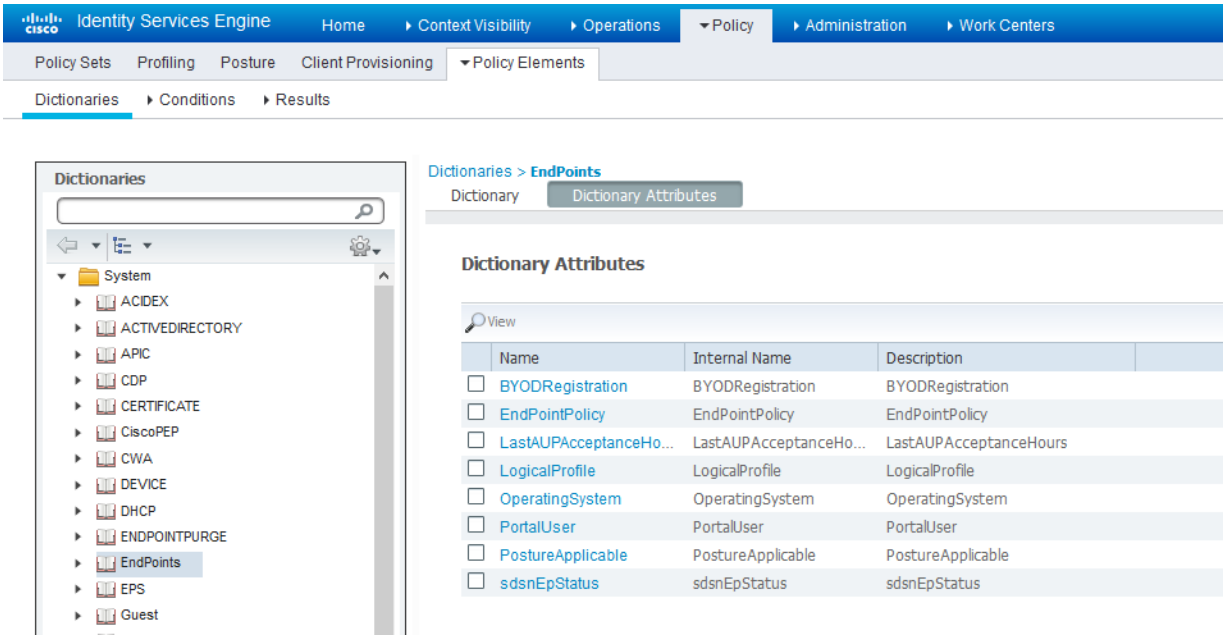
1. Navigate to **Administration** > **Identity Management** > **Settings** > **Endpoint Custom Attribute** and add attribute **sdsnEpStatus** with type string.

Figure 27: Cisco ISE: Add Attribute sdsnEpStatus



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

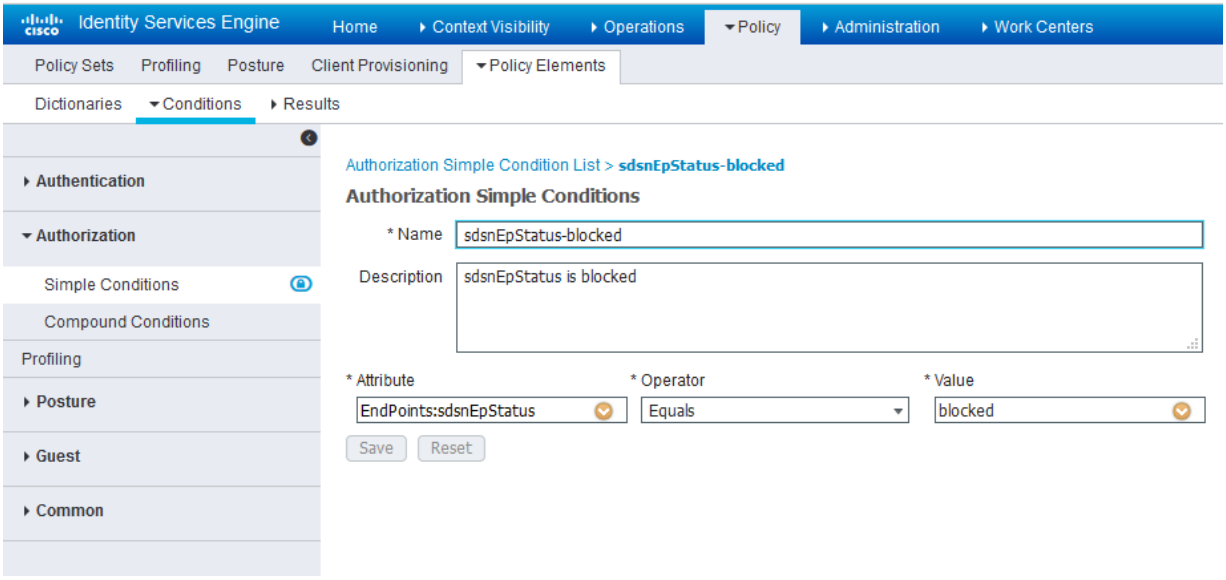
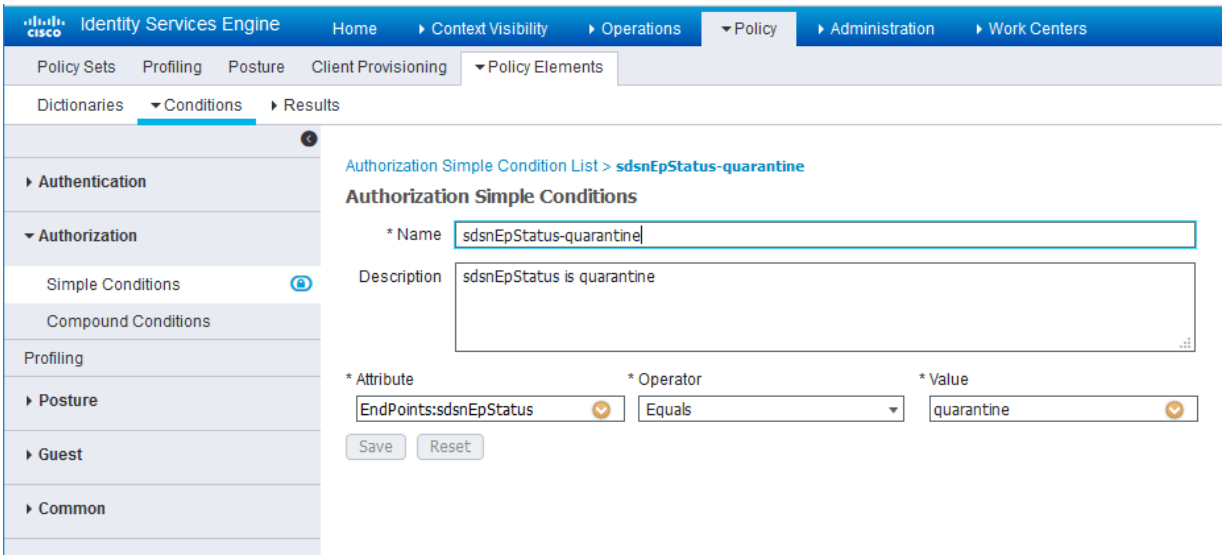


Figure 30: Cisco ISE: Configure Simple Conditions, Match Expression



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

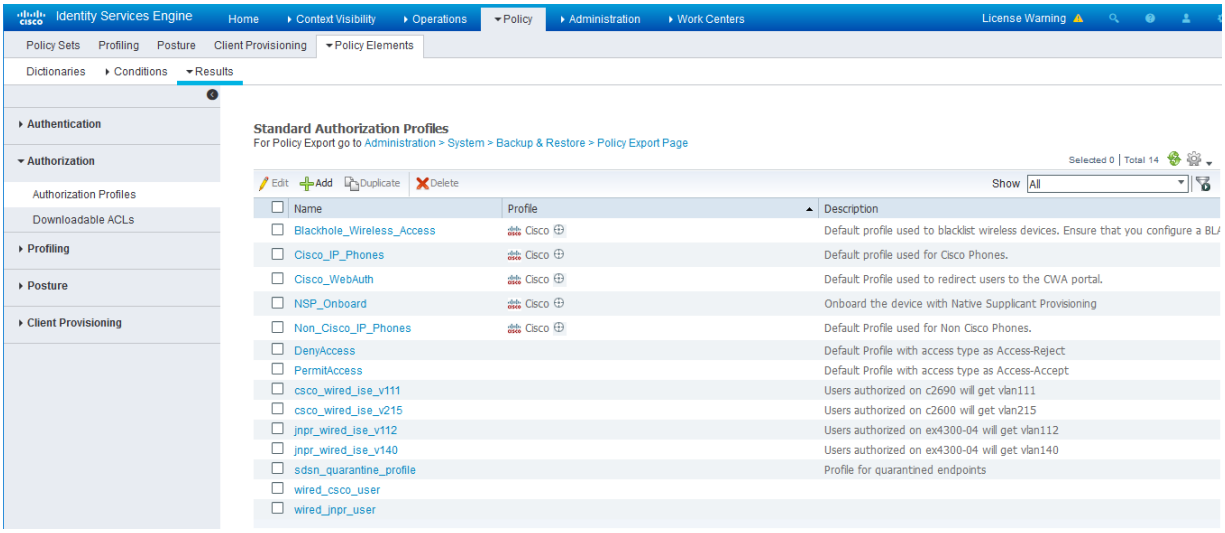
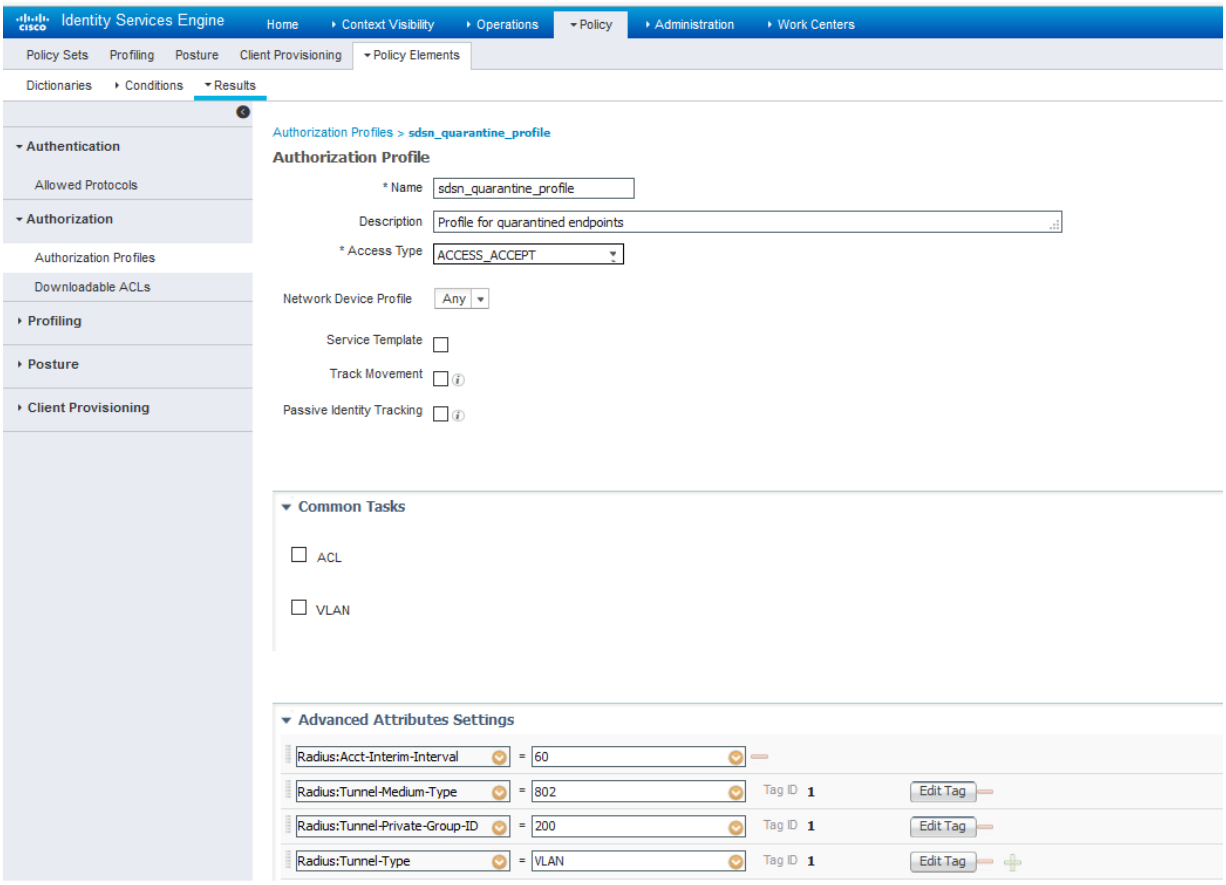


Figure 32: Cisco ISE: Configure Authorization Profiles



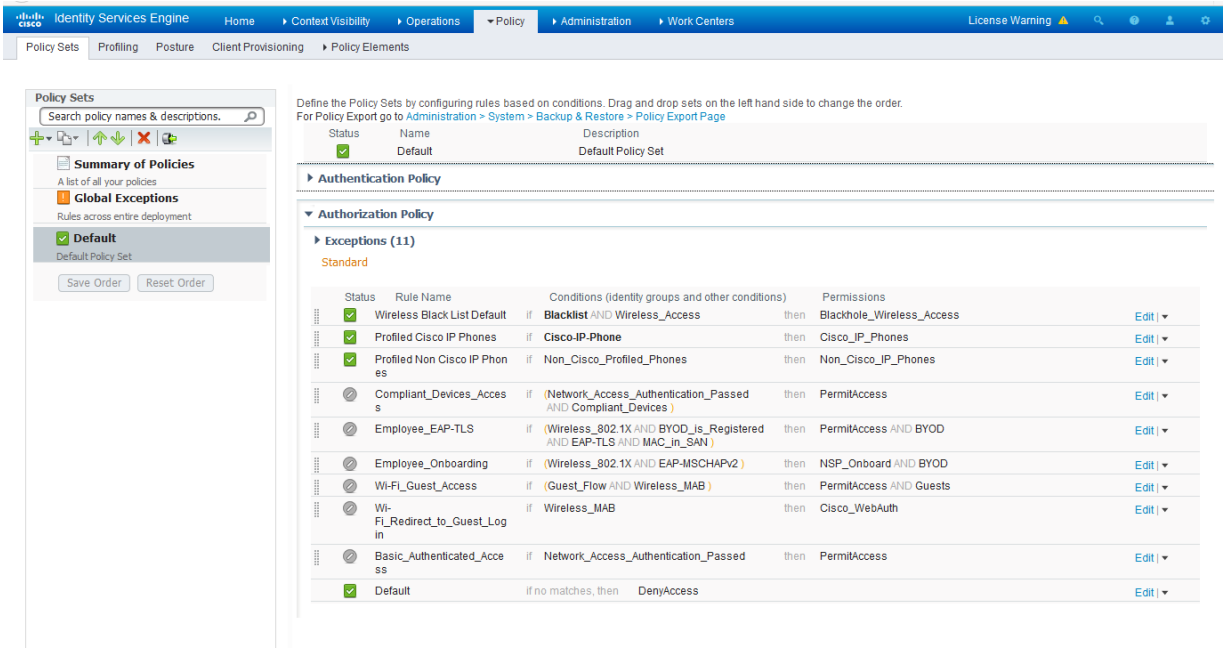
NOTE: For blocking a host, the default 'DenyAccess' profile is used.

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



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

2. Proceed to "Creating a Policy Enforcer Connector for Third-Party Switches" on page 21 to finish the configuration with Policy Enforcer.

RELATED DOCUMENTATION

Creating a Policy Enforcer Connector for Third-Party Switches | **21**

Policy Enforcer Connector Overview | **8**

Integrating Pulse Policy Secure with Juniper Networks Connected Security

IN THIS SECTION

Overview

This topic provides instructions on how to integrate the third-party device Pulse Policy Secure (PPS) with Juniper Networks Connected Security solution to remediate threats from infected hosts for enterprises. The Juniper Connected Security solution provides end-to-end network visibility that enables enterprises to secure their entire physical and virtual networks. PPS provides visibility into the network by detecting and continuously monitoring the network. Using the threat detection and policy enforcement, the PPS and Juniper Connected Security solution automates the network security and supports centralised management, in a multi-vendor environment.

PPS integrates with Juniper Networks Connected Security solution through RESTful APIs and takes appropriate action based on the admission control policies. The PPS integration with Juniper Connected Security solution detects and enforces threat prevention policies and provides a collaborative and comprehensive approach towards complete network security. It enables users to leverage the existing trusted threat feed sources to provide a consistent and automated defense across diverse environments.

Benefits of the Pulse Policy Secure Integration with Juniper Connected Security

- PPS has more visibility of endpoints connected to the network.
- Based on the threat alerts received from Juniper Connected Security, PPS enhances the security by isolating or acting at the endpoint level.

Deployment of Pulse Policy Secure with Juniper Connected Security

The following high level workflow describes the deployment of PPS with Juniper Connected Security. PPS receives the threat alert information from Juniper Connected Security solution and takes an action on the endpoint based on the admission control policies.

1. User successfully authenticates with the PPS server.
2. User downloads a file from the Internet. The perimeter firewall (SRX Series device) scans the file and based on the user-defined policies, sends the scanned file to Juniper ATP Cloud for analysis.
3. Juniper ATP Cloud detects that the file contains malware, identifies the endpoint as an infected host, and notifies the SRX Series device and Policy Enforcer.
4. Policy Enforcer downloads the infected host feed and sends a threat action to PPS.
5. The PPS server quarantines or blocks the endpoint.

   PPS tracks the infected host and does not allow the infected host to acquire full access until the endpoint is disinfected. When the host is disinfected and cleared from Juniper ATP Cloud or Policy Enforcer, PPS receives a *clear* event from the Policy Enforcer connector. After receiving the *clear* event, PPS removes the infected host. The host is now authenticated and an appropriate role is assigned to it.

Configuring Pulse Policy Secure with Juniper Connected Security

IN THIS SECTION

The network security devices are configured with PPS for admission access control.

A high-level overview of the configuration steps required to set up and run the integration is described below:

1. The administrator configures the basic PPS configurations such as creating an authentication server, authenticating realm, user roles, and role mapping rules. To know more about configuring your PPS, see Pulse Policy Secure Administration Guide.

2. Configure Policy Enforcer as a client in PPS. PPS acts as a RESTful API server for Policy Enforcer.

   The RESTful API access for the admin user must be enabled by accessing the serial console or alternatively from the PPS admin user interface (UI). Select **Authentication**>**Auth Server**>**Administrators**>**Users**. Click **Admin** and enable the **Allow access to REST APIs** option.

3. Configure PPS to block or quarantine the endpoint based on the threat prevention policy.

   You must configure the admission control client to obtain the Policy Enforcer IP address that sends events to PPS and admission control policy to understand the PPS event types such as, events-block-endpoint, quarantine-endpoint, clear-blocked-endpoint, and clear-quarantine-endpoint.

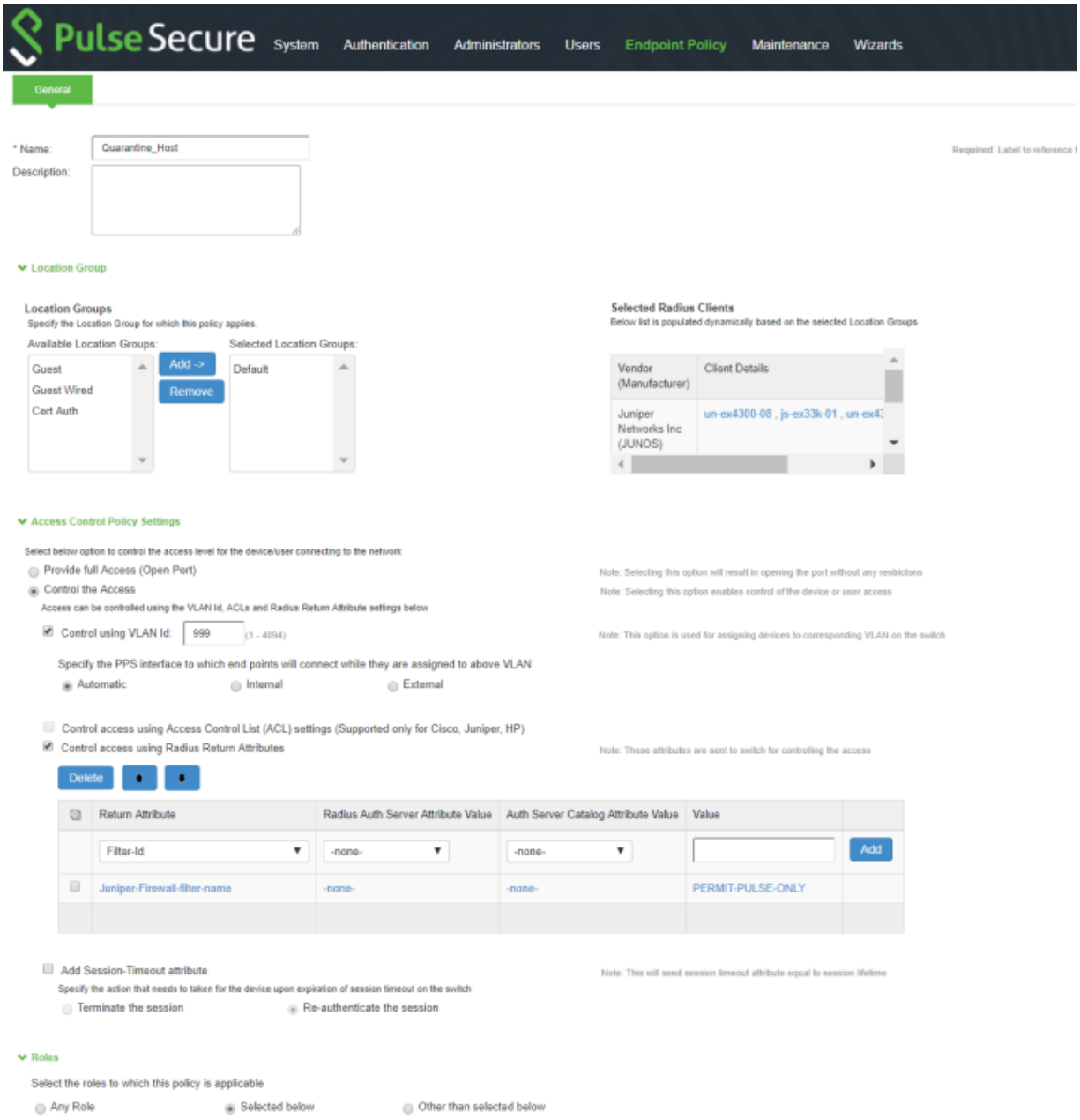
4. Configure the Switches or WLC as RADIUS Client in PPS by selecting **Endpoint Policy**>**Network Access**>**Radius Clients**>**New Radius Client**. The switch is configured with PPS as a RADIUS server.

5. Configure RADIUS return attribute policies, to define the action upon receiving the quarantine event.

   - Quarantine using VLANs:

     The PPS determines which quarantine VLAN to send to RADIUS Client when a quarantine-endpoint event is received, as shown in Figure 34 on page 63.

Figure 34: RADIUS Return Attributes for Quarantine-Host



- Quarantine using ACLs:

  For environments that has flat VLAN, the PPS provides the ability to quarantine users by applying a preconfigured firewall filter. Also, this is a preferred method in environments that use static IP address assignment for end devices.

  The following example shows the firewall filter configuration on the switch. The firewall filter name is then passed on as RADIUS return attribute, as shown in Figure 35 on page 65.

Configure the PERMIT-PULSE-ONLY and PERMIT-ALL firewall filters on the switch using the following commands:

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term pps from destination-address 10.92.81.113/32

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term pps then accept

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term dhcp_allow from destination-port 67

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term dhcp_allow then accept

set firewall family ethernet-switching filter PERMIT-PULSE-ONLY term pps-discard then discard

deactivate firewall family ethernet-switching filter PERMIT-PULSE-ONLY

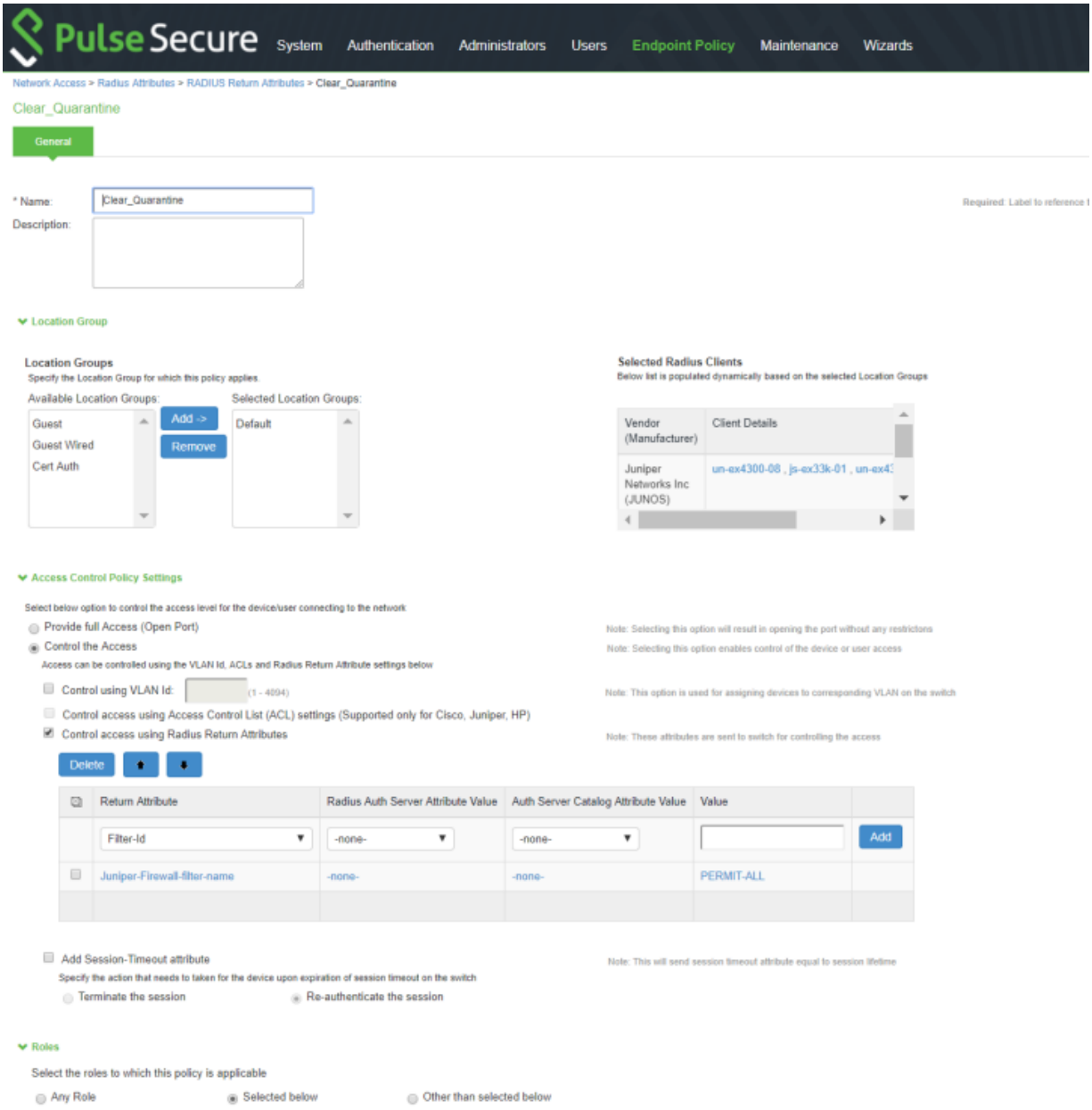
set firewall family ethernet-switching filter PERMIT-ALL term ALLOW-ALL from destination-address 0.0.0.0/0

set firewall family ethernet-switching filter PERMIT-ALL term ALLOW-ALL then accept

deactivate firewall family ethernet-switching filter PERMIT-ALL

To assign these filters in PPS, select **Endpoint Policy**>**Network Access**>**Radius Attributes**>**Return Attributes**.

Figure 35: RADIUS Return Attributes for Clear-Quarantine



NOTE:

- Ensure that PPS has the endpoint IP address for the enforcement to work correctly.
- Since the endpoint IP address is mandatory, deployments where the user is behind a NAT might not work as expected. This is because PPS might have the actual IP address, and Juniper Connected Security might send the NATed IP address.
- To receive the endpoint IP address (accounting information) by PPS, you must use the Pulse Secure client on endpoints when they are connected to EX4300 Series switches.

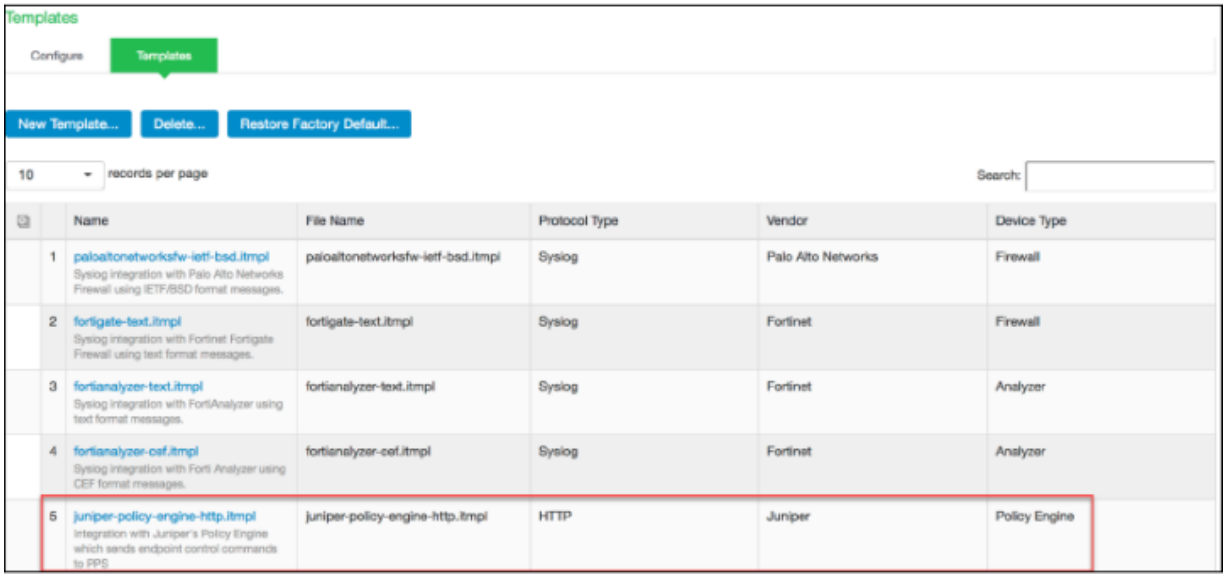
Admission Control Template

The admission control template provides a list of possible events that can be received from the network security device along with the regular expression to parse the message. The template also provides possible actions that can be taken for an event.

PPS is loaded with default templates for Policy Enforcer. The administrators can create templates for other security devices and upload those templates.

To view the admission control templates, select **Endpoint Policy**>**Admission Control**>**Templates**, as shown in Figure 36 on page 66. You can view the list of configured integration templates with the list of network security devices and the supported protocol types.

Figure 36: Pulse Secure Templates Page



Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity of the information received from the network security device.

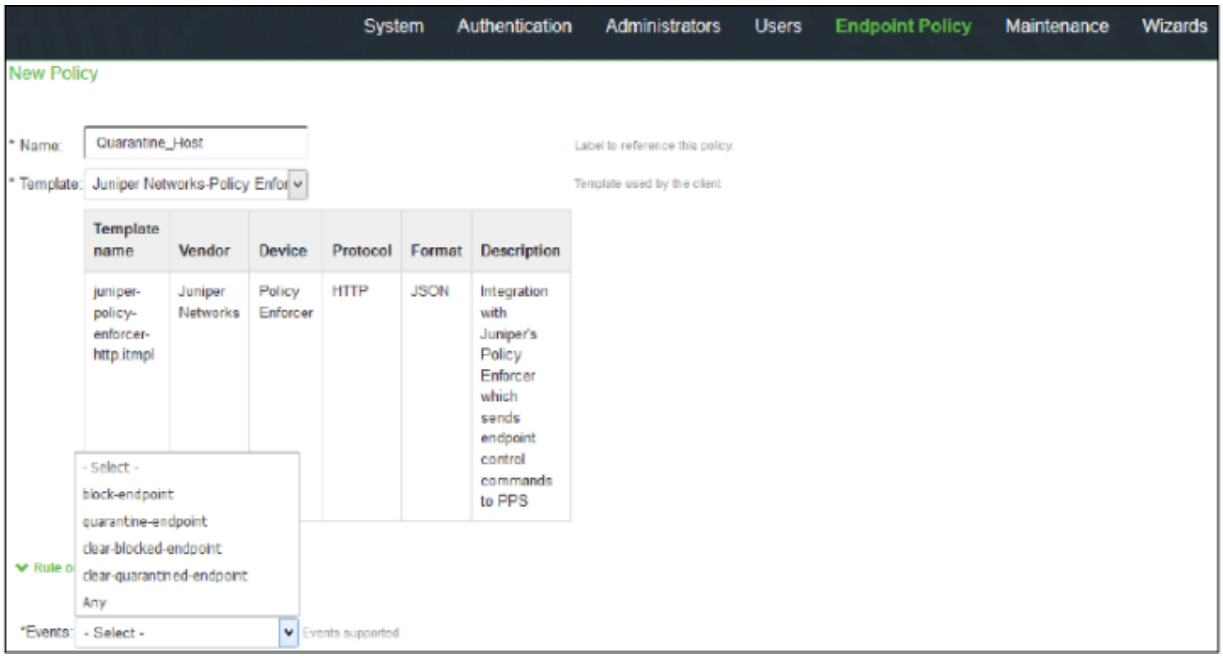
To view and add the new integration policy:

1. Select **Endpoint Policy**>**Admission Control**>**Policies**.

2. Click **New Policy**.

   The New Policy page appears, as shown in Figure 37 on page 67.

Figure 37: Pulse Secure - New Policy Page



3. Enter the policy name.

4. Select **Juniper Networks Policy Enforcer** as a template.

5. In the Rule on receiving section, select one of the following event types and the severity level. The event types and the severity level are based on the selected template.

The following event types are supported on sessions:

- Block-endpoint—Blocks the host MAC Address on the PPS permanently. If the administrator chooses to clear the blocked endpoint, it can be cleared either by using the Junos Space Security Director application or by using the PPS Administration UI.
- Quarantine-endpoint (Change user roles)—Changes the roles assigned to the user on PPS so that restrictions or privileges for the user can be changed. The administrator can choose to apply these roles permanently or temporarily. If it is permanent, system is directly quarantined regardless of which network it connects to.
- Clear Blocked Endpoint—Clears a previously blocked MAC Address.
- Clear Quarantined Endpoint—Clears a previously quarantined MAC Address.

6. In the then perform this action section, select the following desired action:
   - Select a role and assign it to the endpoint to put that endpoint into a quarantine network.
   - In the Make this role assignment option, specify the following actions:
     - Permanent—To apply the role assignment permanently. This is the recommended option. Choose this option for the action to persist.
     - For this session only—To apply the role assignment only for the current session.
7. In the Roles section, specify the following options:
   - Policy applies to ALL roles—To apply the policy to all users.
   - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
   - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who are mapped to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

   NOTE: These options are applicable to both quarantine and block actions.

8. Click **Save changes**.

Once the policy is created, you can see the summary page. Figure 38 on page 69 shows the different policies created for different events with different user roles.

Figure 38: Pulse Secure - Policies Configure Page

Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

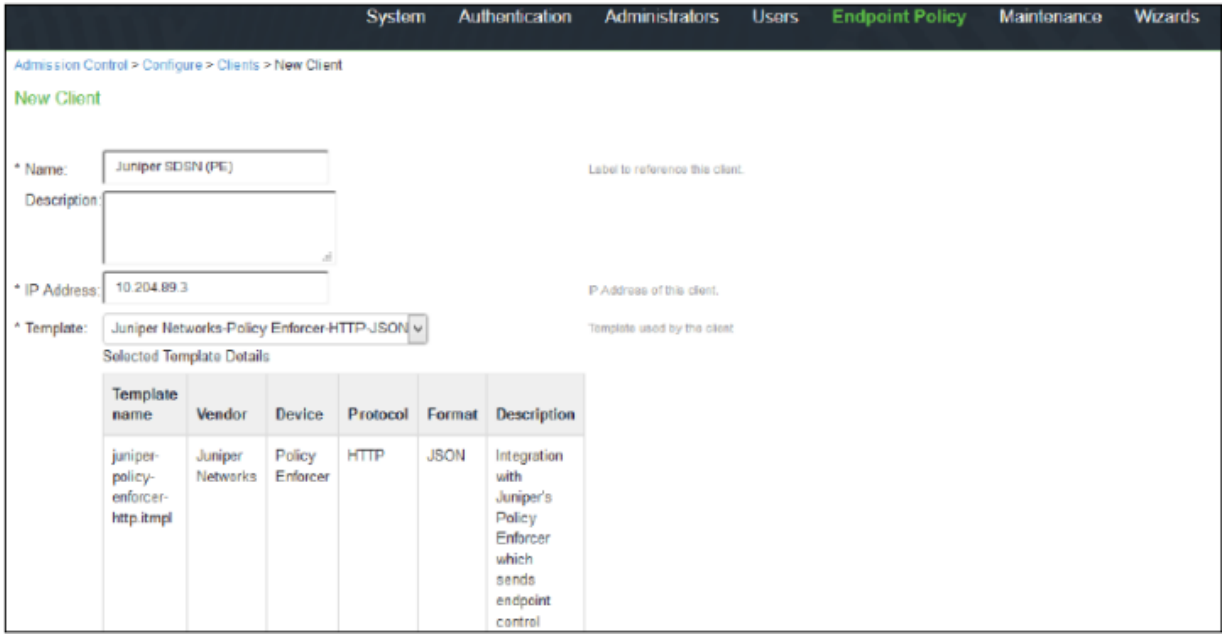
To add a client:

1. Select **Endpoint Policy**>**Admission Control**>**Clients**.

2. Click **New Client**.

   The New Client page appears, as shown in Figure 39 on page 70.

Figure 39: Pulse Secure - New Client Page



3. Enter the name of the Juniper Networks Policy Enforcer. This is added as a client in the PPS.

4. Enter the description.

5. Enter the IP address of the client.

6. Select the template used by the client: JuniperNerworks-Policy Enforcer-HTTP-JSON.

7. Click **Save Changes**.

   Policy Enforcer is added a new client in the PPS.

Creating Pulse Policy Secure Connector in Security Director

Once you add Policy Enforcer as a client in PPS, create a connector for PPS to configure the Juniper Connected Security to send the event information.

To create a connector for PPS and configure Juniper Connected Security using Security Director:

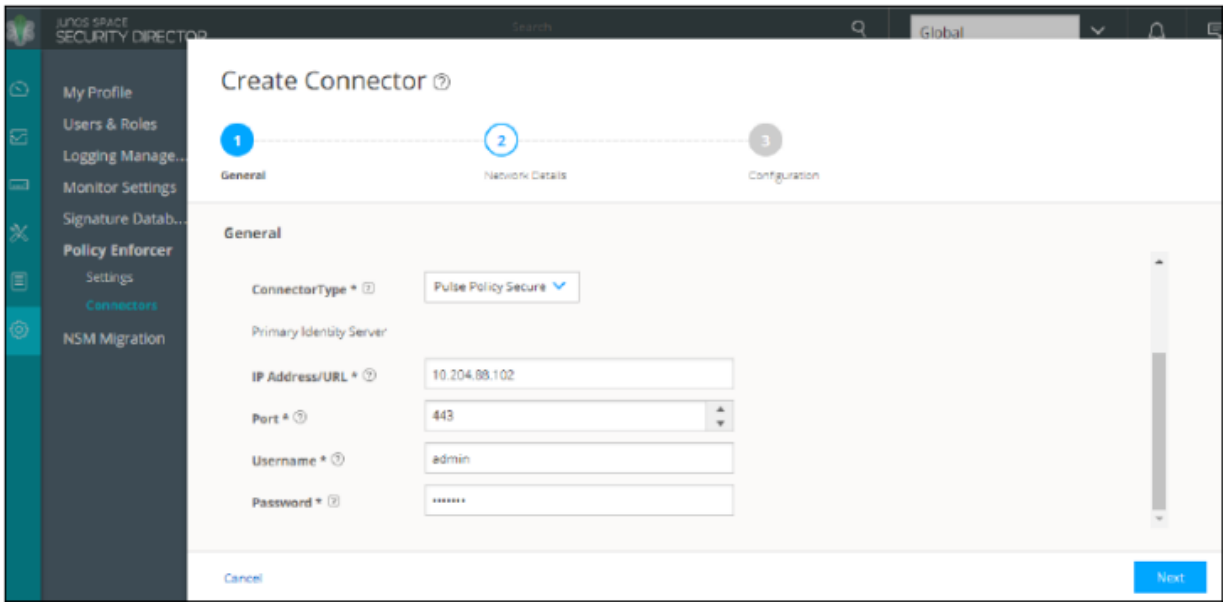
1. Select **Security Director**>**Administration**>**Policy Enforcer**>**Connectors**.

   The Connectors page appears.

2. Click the create icon (+).

   The Create Connector page appears, as shown in Figure 40 on page 71.

Figure 40: Create Connector Page



3. In the General tab, select **Pulse Policy Secure** in the ConnectorType list.

4. In the IP Address/URL field, enter the IP address of PPS.

5. Retain the default port number as 443.

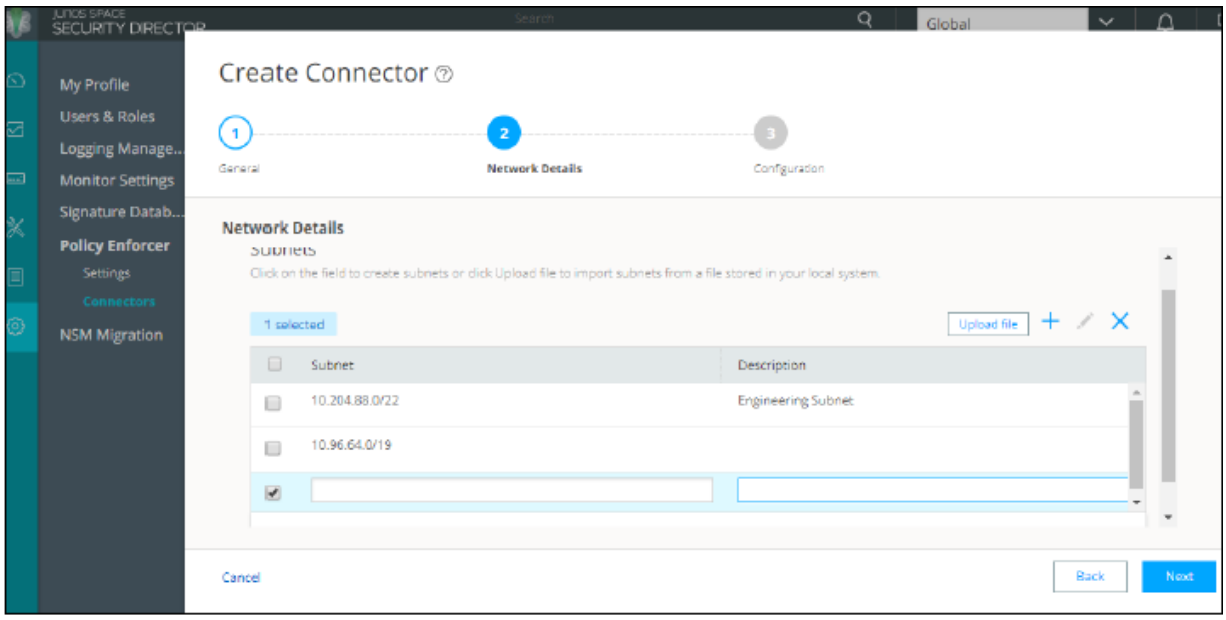
6. Enter the username and password of PPS.

   Note that you must have enabled the REST API access on PPS (Authentication > Auth Server > Administrators > Users > click “admin”, enable Allow access to REST APIs).

7. Click **Next**.

8. In the Network Details section, configure the IP subnets, as shown in Figure 41 on page 72.

Figure 41: Create Connector Network Details Page

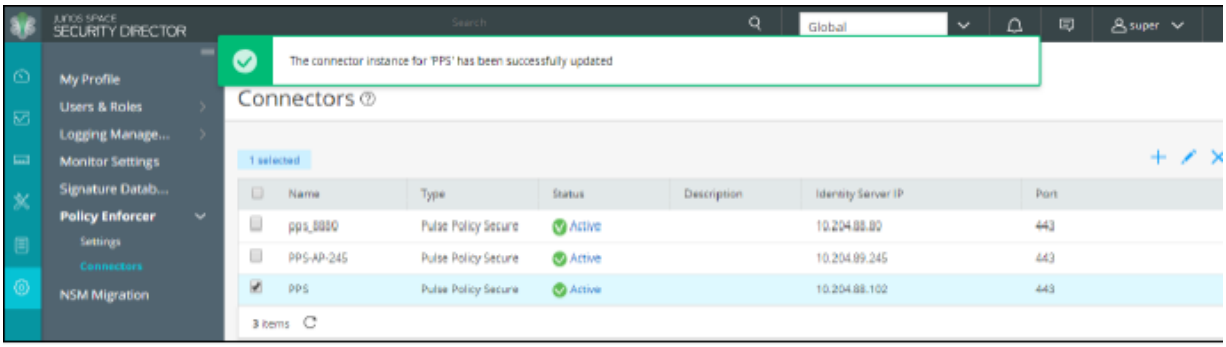


9. In the Configuration tab, provide any additional information required for this specific connector connection.

10. Click **Finish**.

    Once the configuration is successful the following page is displayed, as shown in Figure 42 on page 72.

Figure 42: Connectors Page



11. Verify that the communication between Policy Enforcer and PPS is working.

    After installing PPS and configuring a connector, in the PPS UI, create policies for PPS to take the necessary action on the infected hosts.

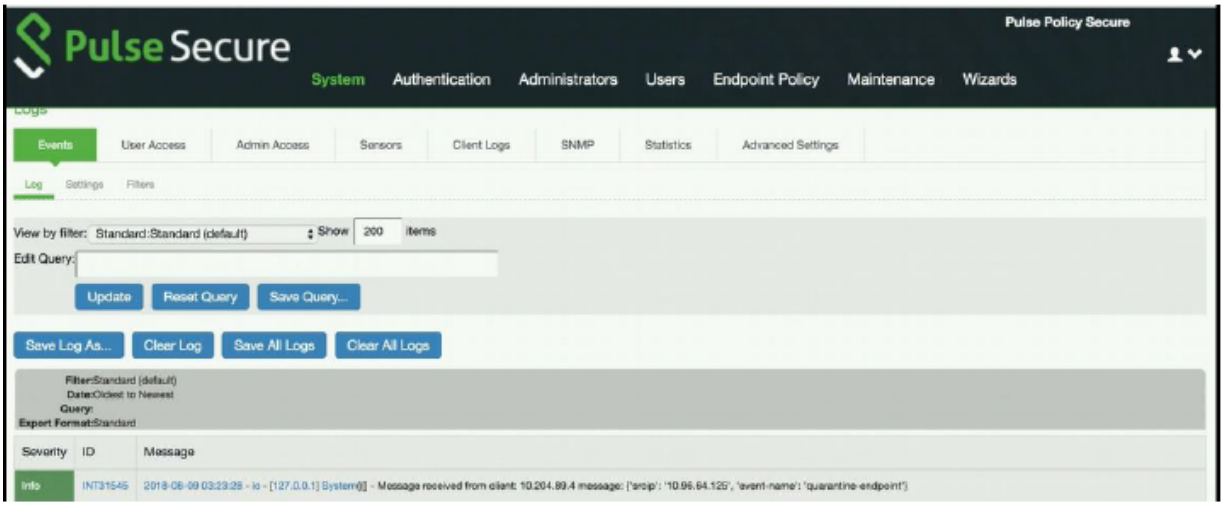
Troubleshooting

The following troubleshooting logs are available:

- To verify the event logs on PPS, select **System**>**Log/Monitoring**>**Events**.

  You can verify that the event logs are generated every time when an event is received from Policy Enforcer, as shown in Figure 43 on page 73.

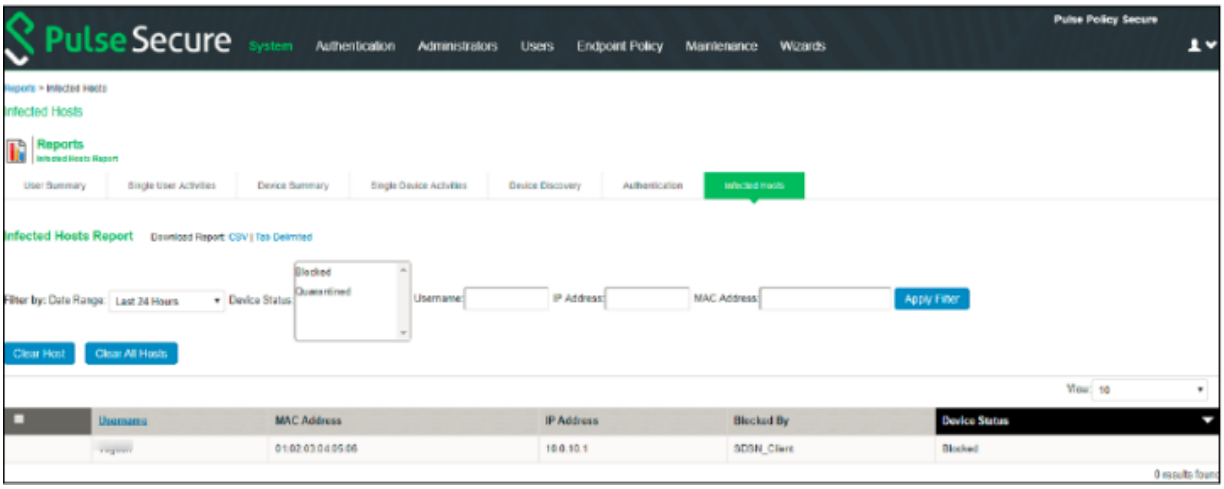
Figure 43: Pulse Secure Events Page



- To verify the user login related logs such as realm, roles, username, and IP address, select **System**>**Logs & Monitoring**>**User Access**.
- To verify the reports, select **System**>**Reports**>**Infected Hosts**.

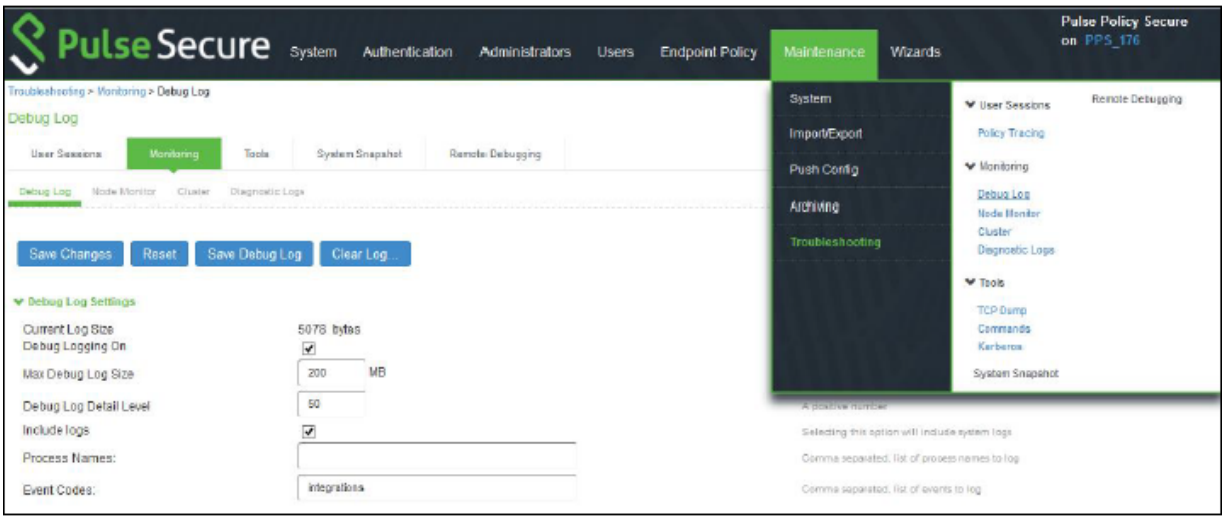
  You can verify whether the quarantined or blocked host is listed in the Infected Devices report. This report lists the MAC address, IP address, and the device status, as shown in Figure 44 on page 74.

Figure 44: Infected Hosts Reports Page



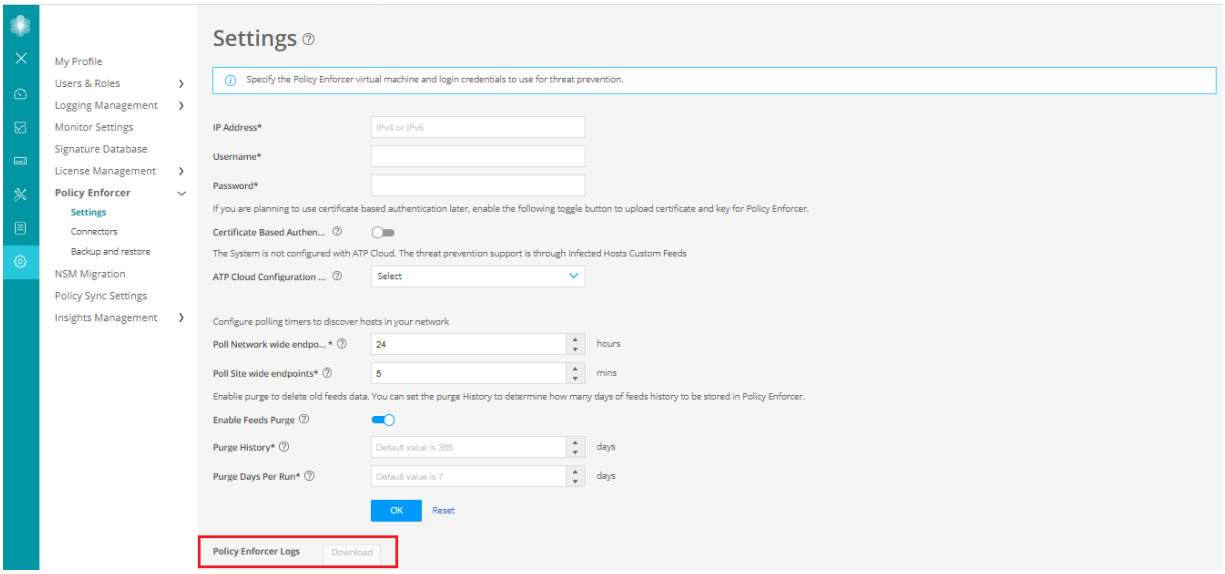
- To enable the debug logs for troubleshooting, select **Maintenance**>**Troubleshooting**>**Monitoring**>**Debug Log**, as shown in Figure 45 on page 74.

Figure 45: Debug Log Monitoring Page



- To troubleshoot any issues on the Policy Enforcer, download and verify the Policy Enforcer logs from Security Director>Administration>Policy Enforcer>Settings page, as shown in Figure 46 on page 75.

Figure 46: Policy Enforcer Settings Page



- The administrators can also verify the Hosts table from Juniper ATP Cloud to check the status of the host, as shown in Figure 47 on page 75.

  You can clear the host entry if the State Of Investigation field value is Resolved-Fixed.

Figure 47: Juniper ATP Cloud Hosts Page