Cisco Security Cloud Control: Mesh Policy Engine

Cisco Security Cloud Control
Updated NaN,

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

1 Mesh Policy Engine Overview.....5

Introduction to Mesh Policy Engine.....6
Why use Mesh Policy Engine.....6
Supported enforcers.....6
How Mesh Policy Engine policies work.....7
Getting started with Mesh Policy Engine.....7
Claim a Mesh Policy Engine subscription.....7
Assign a Mesh Policy Engine admin role.....12
Mesh Policy Engine Dashboard.....15

2 Enforcers.....17

About enforcers.....18
Prerequisites for enforcers.....18
Add credentials for third-party enforcers and managers.....18
Add a management connection for third-party enforcers.....21
Add a third-party enforcer.....26
Manage enforcers.....29

3 Policies.....33

About policies.....34
Fixed-assignment policies.....34
Policy hierarchy.....35
How Mesh Policy Engine works with existing policy.....35
How the policy works with a default action.....36
Supported rule parameters.....36
Global policy.....36
Guidelines for policies.....37
Create a fixed-assignment policy.....37
Create a fixed-assignment ruleset.....41
Create a fixed-assignment rule.....45
Import a policy.....51
View policies.....64

4 Changesets.....67

About Changesets.....68
Changeset workflow.....68
Create and use a changeset.....69
Update the changeset to the latest policy.....71

Resolve conflicts....72
Commit a changeset....81

5 Deployments....85
About deployments....86
Deploy policy changes to enforcers....86
View deployments....89

1 Mesh Policy Engine Overview

Topics:

- Introduction to Mesh Policy Engine
- Why use Mesh Policy Engine
- Supported enforcers
- How Mesh Policy Engine policies work
- Getting started with Mesh Policy Engine

Find an overview of Mesh Policy Engine and the main tasks for managing security policies across security devices from multiple vendors.

Mesh Policy Engine helps you orchestrate and manage security policies across security devices from multiple vendors in one dashboard. It simplifies policy updates, tracks ownership and version history, and ensures consistent policy deployment. This approach makes policy management easier and strengthens network security as your organization grows.

Introduction to Mesh Policy Engine

Learn what Mesh Policy Engine offers for managing security policies across multiple vendors. Understand the problems it addresses before you start configuring policies.

Managing network security policies can be challenging when your organization has complex, enterprise-level, multivendor networks and needs to move to large-scale multicloud architectures. Your network operators or application development team often creates or edits security policies to support increased connectivity and access for product teams and developers across your organization. These frequent changes can clutter policy management and make it hard to scale your enterprise network as your organization grows.

In addition, because there are a large number of rules in the policy, it becomes even harder to manage and keep track of the policies' versions, changes, and ownership history. If you do not manage these complex and changing security policies carefully, your organization's network security could weaken and become more vulnerable to malicious threats.

To address these needs, you can use Mesh Policy Engine in Security Cloud Control, which helps you orchestrate and manage security policies across security devices from multiple vendors. With Mesh Policy Engine, you can track policy ownership, policy change history, and version control. Mesh Policy Engine makes policy management easier and helps keep your network security strong.

Using Mesh Policy Engine, you can view all your security policies on one dashboard, create new policies, update existing ones, and deploy them to enforcers. With common objects in Security Cloud Control, your network changes can be easily deployed across Security Cloud Control products, including Mesh Policy Engine policies.

Why use Mesh Policy Engine

Learn why organizations use Mesh Policy Engine to manage policies across vendors, speed up updates, and keep security practices consistent as networks grow.

Implementing Mesh Policy Engine in your enterprise environment delivers these key business outcomes:

- Reduced operational complexity—Eliminate the need for specialized expertise in each vendor's CLI or management console. Managing all enforcers from a single location reduces the overhead of maintaining a multi-vendor environment.
- Accelerated agility—Policy updates that traditionally took weeks to coordinate across different teams and vendors can be implemented consistently across the entire infrastructure in minutes.
- Enhanced device performance—Placing only relevant rules on specific enforcers reduces the size of policy documents, which improves performance and makes troubleshooting easier.
- Improved security posture—Using Mesh Policy Engine as the "source of truth" for all workload access strengthens your security posture. Mapping each policy rule to your original request or intent simplifies annual audits and ensures your security intent remains clear during translation.
- Automated policy consistency—Your defined security intent is maintained across the network. If someone makes a manual change directly on a device, Mesh Policy Engine restores your intended policy during the next deployment.
- Scalability—Built on an elastic cloud architecture, Mesh Policy Engine automatically scales to handle large enterprise environments with high request volumes and complex, dynamic policy requirements.

Supported enforcers

Check which Cisco and third-party security devices Mesh Policy Engine supports. Review device and software prerequisites before you add enforcers.

For software and hardware prerequisites, see Prerequisites for enforcers on page 18.

Supported Cisco enforcers

Mesh Policy Engine supports the following security devices that have been onboarded to Security Cloud Control:

- Secure Access
- Secure Firewall Threat Defense

Supported third-party enforcers

Mesh Policy Engine supports the following third-party enforcers:

- Fortinet FortiGate
- Juniper
- Palo Alto Networks

Supported managers for policy import

Mesh Policy Engine supports the following managers for policy import:

- Panorama–Palo Alto Networks policies

How Mesh Policy Engine policies work

Learn how Mesh Policy Engine policies are structured and assigned to enforcers. Understand fixed-assignment and dynamic-assignment policy types before creating rules.

Mesh Policy Engine supports fixed-assignment policies. You can manually assign a single child policy to an enforcer that includes its parent policies. The fixed-assignment policy includes Mandatory and Default sections that are grouped with like sections in the policy hierarchy.

Mesh Policy Engine creates global policies that apply to all zones or interfaces. For Secure Access, the mesh policy is part of the access policy.

Getting started with Mesh Policy Engine

Learn the setup tasks for Mesh Policy Engine in Security Cloud Control, from subscription and access to the dashboard and policy management.

Set up Mesh Policy Engine in Security Cloud Control to manage policies across multi-vendor enforcers.

Claim a Mesh Policy Engine subscription

Learn which Mesh Policy Engine subscription options are available and when you need a claim code or included service. Choose the option that matches your entitlement.

Security Cloud Control supports several types of subscriptions and services:

- Paid subscription–A paid subscription provides the full-functionality Mesh Policy Engine. This type of subscription requires a claim code that you can activate for a product instance. Refer to Claim a paid or trial Mesh Policy Engine subscription on page 8.
- Trial subscription–A trial subscription provides the full-functionality Mesh Policy Engine. This type of subscription requires a claim code that you can activate for a product instance. Trials can be stacked with paid subscriptions to extend the subscription period. Refer to Claim a paid or trial Mesh Policy Engine subscription on page 8.

- Platform-enabled service—A platform-enabled service may be available for your organization by default with Security Cloud Control, or it may come with a paid or trial subscription for another product such as Firewall Management. The platform-enabled service supports a basic-functionality version of Mesh Policy Engine.

> **Note**
>
> The platform-enabled service version of Mesh Policy Engine does not include support for third-party devices.
>
> If you have a platform-enabled service version of a product such as Firewall Management, it doesn't also have a platform-enabled service version of Mesh Policy Engine; only the paid or trial subscription of Firewall Management has a platform-enabled service version of Mesh Policy Engine.

For more information about subscriptions, see *Security Cloud Control Administration Guide*.

Claim a paid or trial Mesh Policy Engine subscription

Claim a paid or trial Mesh Policy Engine subscription with the claim code from your welcome email. Add the entitlement to your organization.

Using the claim code from your welcome email, claim the Mesh Policy Engine subscription within your organization.

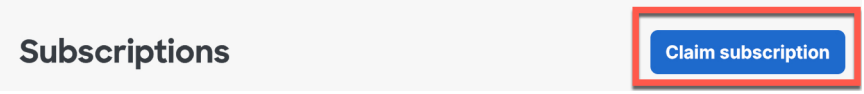
Before you begin

Set up your Security Cloud Sign On account and sign in. Use the Account Sign Up page to set up a Security Cloud Sign On account or to sign in to your existing account.

Procedure

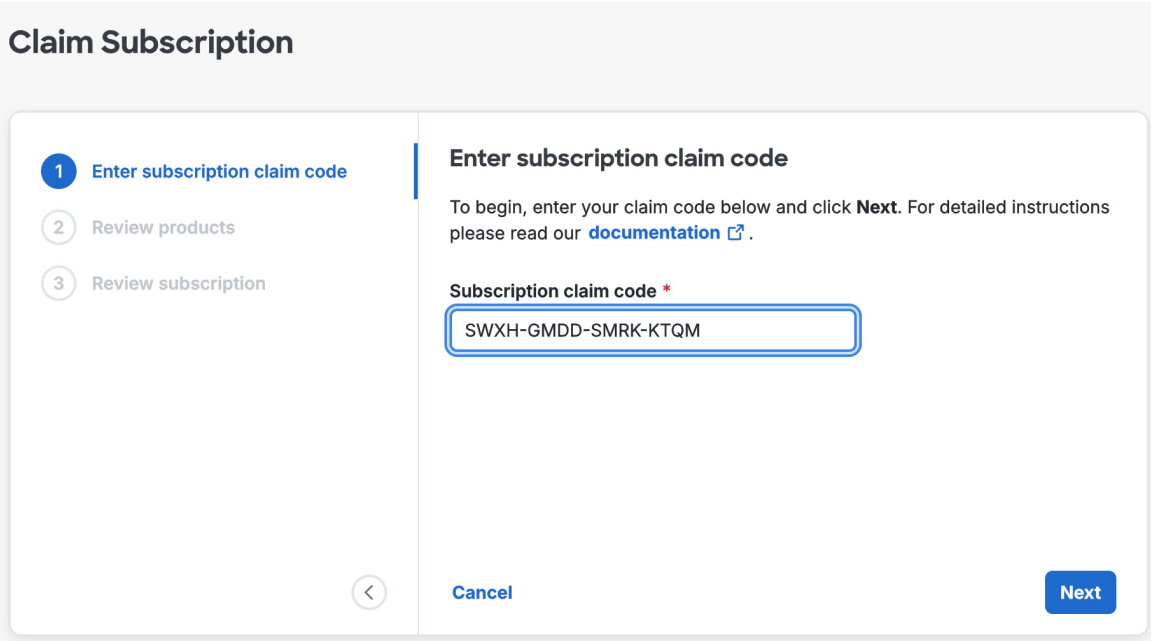
1. From the Security Cloud Control Home page, choose **Product Management >Platform Management** > **Product Subscriptions** > **Subscriptions & Service Management**.
2. Click **Claim subscription**.

   Figure 1: Claim subscription

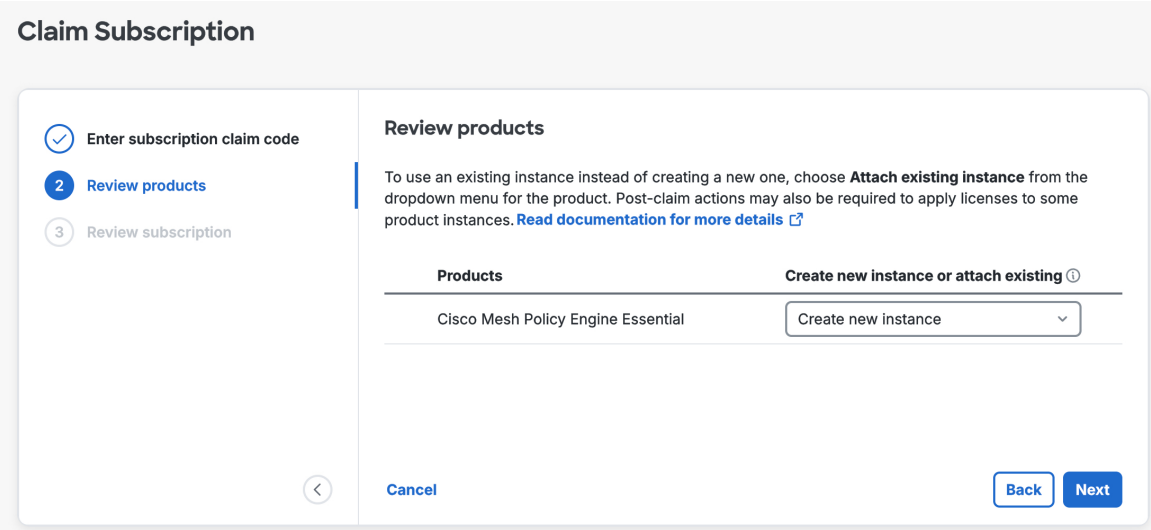
3. Enter the claim code and click **Next**.

   Figure 2: Subscription claim code



4. For Cisco Mesh Policy Engine Essential, choose **Create new instance** from the drop-down list.

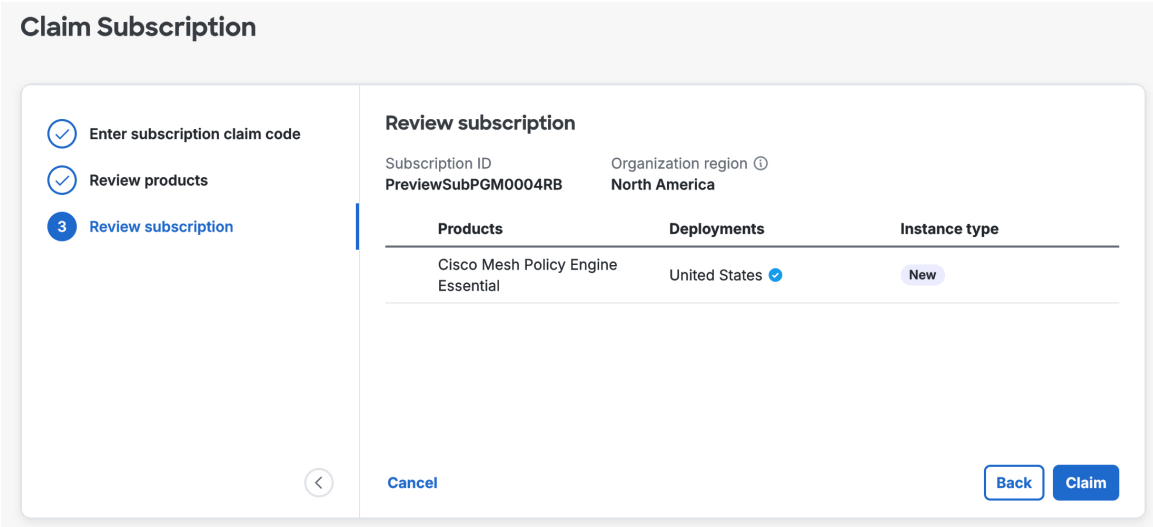
Figure 3: Create new instance



For trial subscriptions only–if you already have a Mesh Policy Engine instance and are applying a paid subscription to replace an existing trial subscription or are stacking a trial subscription on top of an existing paid subscription, choose **Attach existing instance**.

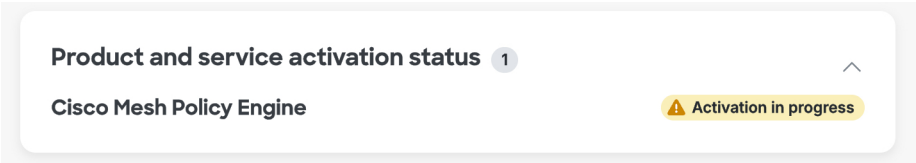
5. If you have any other products on this claim code, make your selections, and then click **Claim**.

Figure 4: Claim



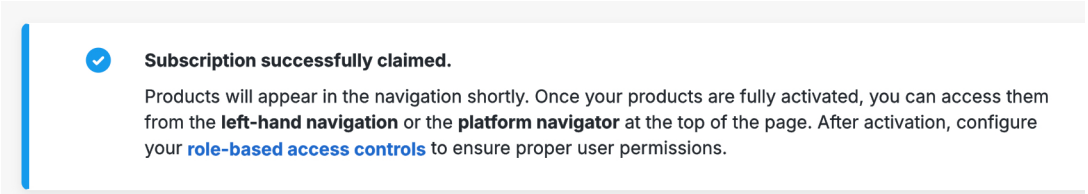
You may see this message during activation:

Figure 5: Activation in progress



You will see a message at the top of the page showing success.

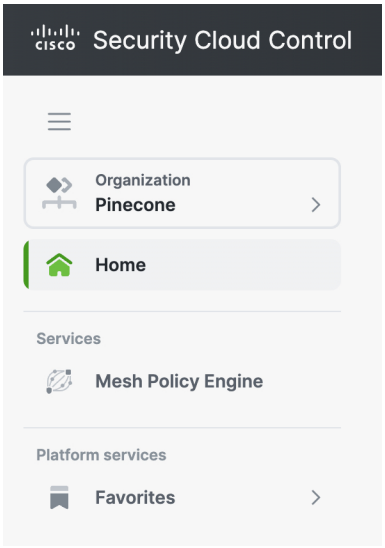
Figure 6: Product successfully claimed



6. Add a Mesh Policy Engine role for other users before they can use Mesh Policy Engine.

   Mesh Policy Engine only appears in the Security Cloud Control menu under **Services** for users or groups that have an assigned Mesh Policy Engine role. As the organization administrator, you are probably a member of the All Products Administrator group, so you are assigned the Mesh Policy Engine admin role automatically. Refer to Assign a Mesh Policy Engine admin role on page 12.

   Figure 7: Services menu



Enable a platform-enabled service version of Mesh Policy Engine

Enable the included Mesh Policy Engine service for your organization. Complete the setup steps so authorized users can begin managing policies.

If you have a platform-enabled service version of Mesh Policy Engine, follow these steps.

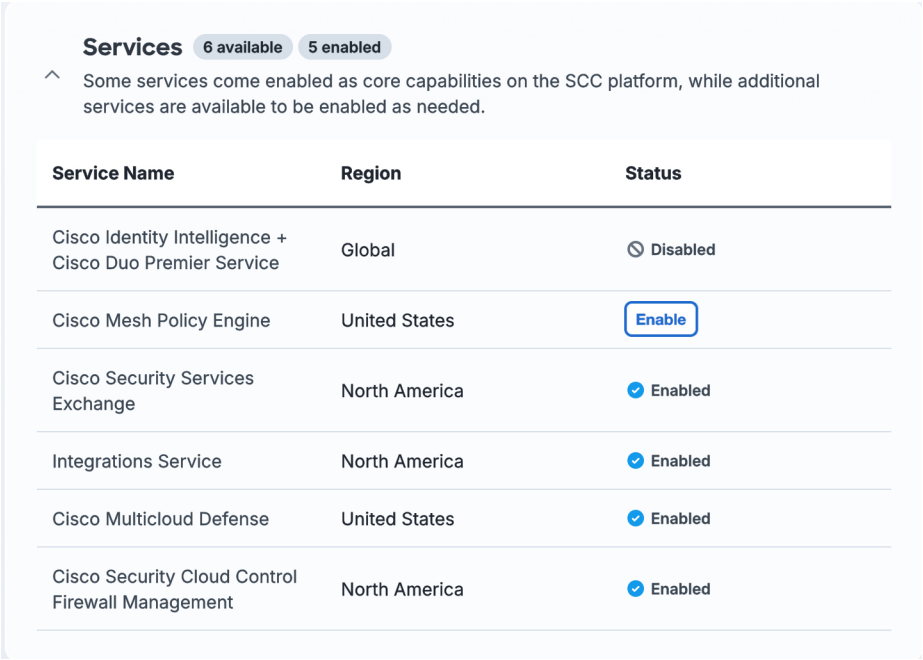
Before you begin

Set up your Security Cloud Sign On account and sign in. Use the Account Sign Up page to set up a Security Cloud Sign On account or to sign in to your existing account.

Procedure

1. From the Security Cloud Control Home page, choose **Product Management >Platform Management** > **Product Subscriptions** > **Subscriptions & Service Management**.
2. In the **Services** area next to **Cisco Mesh Policy Engine**, click **Enable**.

Figure 8: Enable the Mesh Policy Engine service

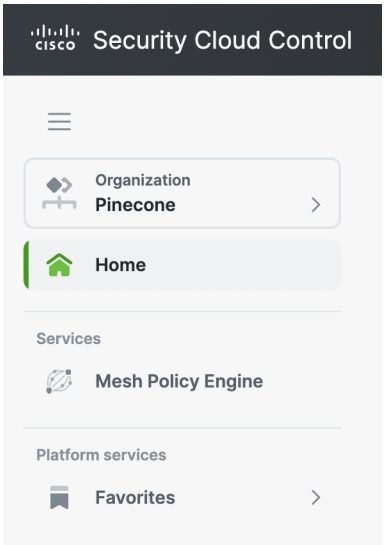


You may see the message **Activation in progress**. Eventually, you will see a message showing success.

3. Add a Mesh Policy Engine role for other users before they can use Mesh Policy Engine.

   Mesh Policy Engine only appears in the Security Cloud Control menu under **Services** for users or groups that have an assigned Mesh Policy Engine role. As the organization administrator, you are probably a member of the All Products Administrator group, so you are assigned the Mesh Policy Engine admin role automatically. Refer to Assign a Mesh Policy Engine admin role on page 12.

Figure 9: Services menu



Assign a Mesh Policy Engine admin role

Assign an admin role so a user can access Mesh Policy Engine. Review the available assignment options before granting access to users or groups.

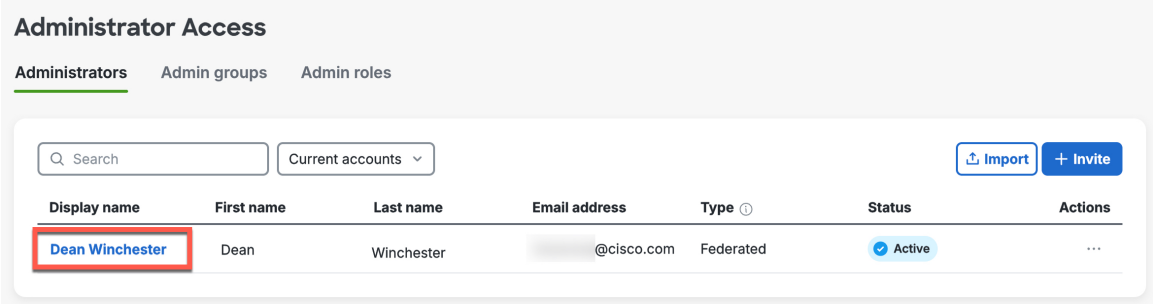
Users can't access Mesh Policy Engine until you assign a Mesh Policy Engine admin role. This procedure describes how to assign a role to each user separately.

You can alternatively choose the role and then assign users to the role (Assign Roles to Existing Users), or you can assign roles to groups (Assign Roles to Groups).

Procedure

1. From the Security Cloud Control Home page, choose **Platform Management** > **Access Management** > **Administrator Access**.
2. On the **Administrators** page, with **Current Accounts** selected in the drop-down list, click the **Display Name** of the user.

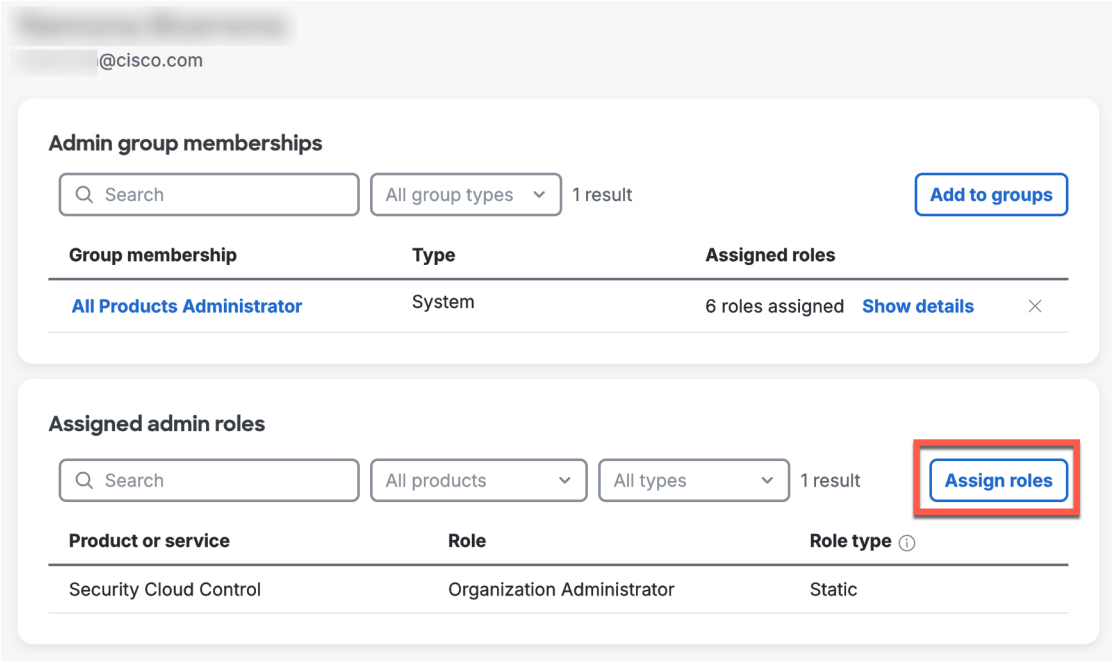
   Figure 10: Display name



   The resulting page displays user details such as assigned admin roles and admin groups.

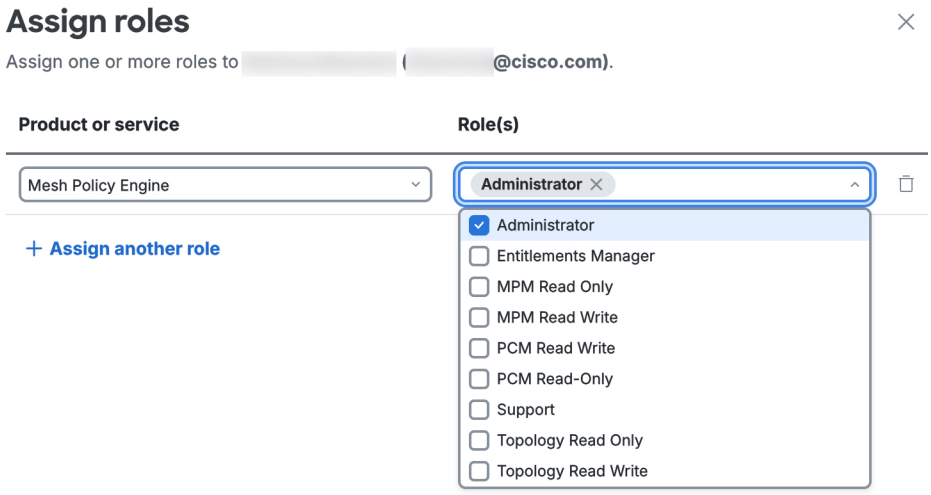
3. Click **Assign roles**.

   Figure 11: Assign roles



4. In the **Assign Roles** slide-in pane, assign roles to products.

   Figure 12: Assign roles per product



a) From the **Product or service** drop-down list, choose a product.
b) From the **Roles** drop-down list, choose one or more roles to assign.

Mesh Policy Engine supports static roles.

Here is a list of static roles and their level of access to APIs.

Table 1: Mesh Policy Engine Static Roles

Role	Description
Administrator	Provides full platform authority with access to all API operations.
Entitlements Manager	Provides limited authority for managing client credentials. Does not provide full platform access.
Support	Provides access to a broad set of API operations for support and operational tasks.
PCM Read-Only	Provides read-only access to Persisted Connection Management (PCM) API operations.
PCM Read Write	Provides read and write access to PCM API operations.
Topology Read Only	Provides read-only access to Topology API operations. (performed by network operators).
Topology Read Write	Provides read and write access to Topology API operations. (performed by network operators).
MPM Read Only	Provides read-only access to Manual Policy Manager (MPM) API operations.
MPM Read Write	Provides read and write access to MPM API operations.

c) Click **+Assign another role** to add more products for the user.
d) Click **Assign roles**.

The selected product roles are assigned to the user.

Mesh Policy Engine Dashboard

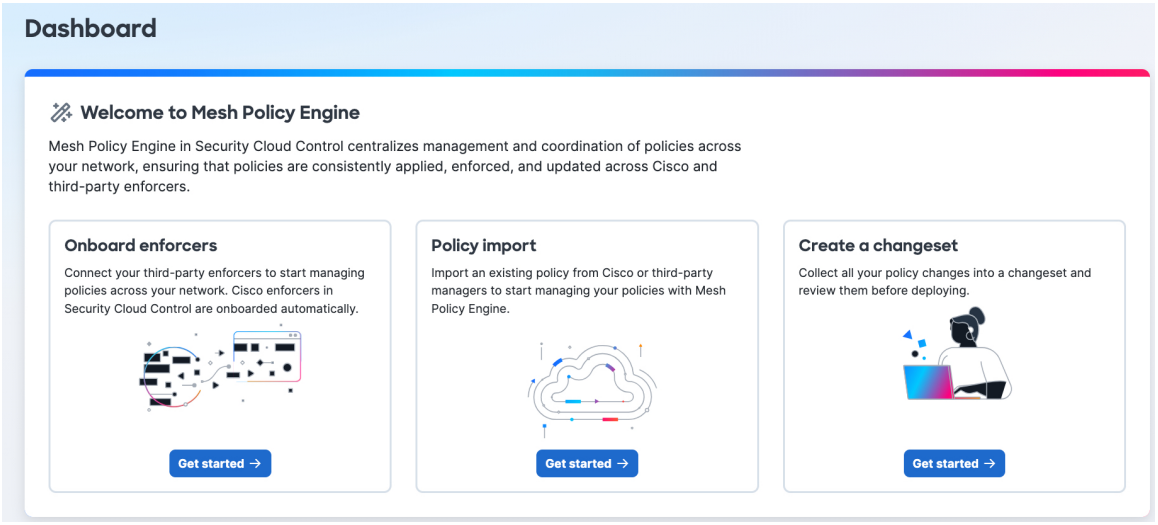
Learn how to use the Mesh Policy Engine dashboard to check policy, enforcer, and topology status and open the areas where you manage changes.

The Mesh Policy Engine dashboard is the starting point for configuring centralized policy management.

Dashboard areas

The dashboard contains the following quick access areas:

Figure 13: Dashboard welcome and getting started cards



2 Enforcers

Topics:

- About enforcers
- Prerequisites for enforcers
- Add credentials for third-party enforcers and managers
- Add a management connection for third-party enforcers
- Add a third-party enforcer
- Manage enforcers

Find a definition of enforcers and learn which security devices or device groups share a policy in Mesh Policy Engine.

An enforcer is a security device or group of devices, like a high-availability pair or cluster, that shares the same security policy.

About enforcers

Learn what enforcers are and how Cisco and third-party security devices appear in Mesh Policy Engine. Use this overview before adding or managing devices.

When you onboard a security device to Security Cloud Control that Mesh Policy Engine supports, it is automatically listed as an enforcer in Mesh Policy Engine.

You can also add third-party devices as enforcers by providing connection details.

Prerequisites for enforcers

Check supported enforcer types and their prerequisites before adding devices to Mesh Policy Engine. Review the required software, management mode, and connectivity for each type.

Supported Cisco enforcers

Mesh Policy Engine supports the following security devices that have been onboarded to Security Cloud Control:

- Secure Access
- Secure Firewall Threat Defense

All versions and modes supported by Security Cloud Control are supported in Mesh Policy Engine.

Supported third-party enforcers

Device or Manager	Software Version	Mode
Fortinet FortiGate	7.4.3	Standalone
Juniper	22.4R3.25	Multinode high-availability mode
Juniper	22.4R3.25	Cluster mode
Palo Alto Networks	PAN-OS 11.1.4-h7	Active/passive mode Active/active mode

Add credentials for third-party enforcers and managers

Add credentials for third-party enforcers or managers that Mesh Policy Engine needs to connect to. Reuse saved credentials when you add more devices.

To securely connect to third-party enforcers and managers (for policy import), Mesh Policy Engine must authenticate with the device using their credentials. Each credential is a reusable object that you can use for one or more devices by name.

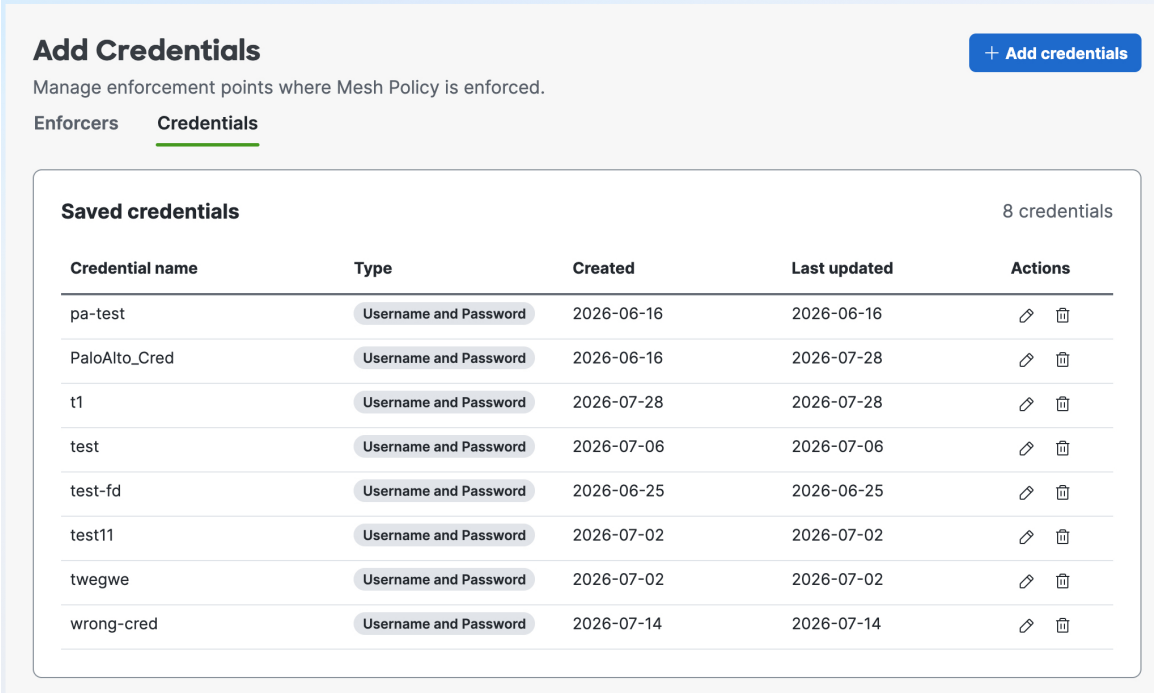
Note

You don't need to add Cisco credentials unless devices are not reachable directly in Security Cloud Control.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Choose **Enforcers** > **Credentials**.

Figure 14: Credentials

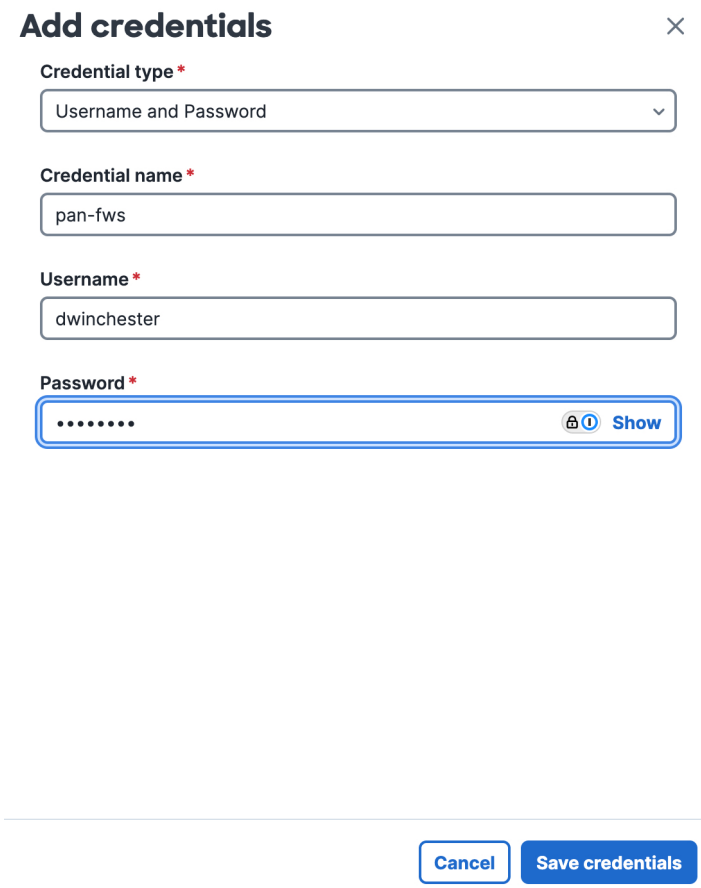


Existing credentials are listed on this page.

3. Click **Add credentials**.
4. Set the credential type: **Username and Password**, **Token**, or **Cisco Multicloud Defense**.

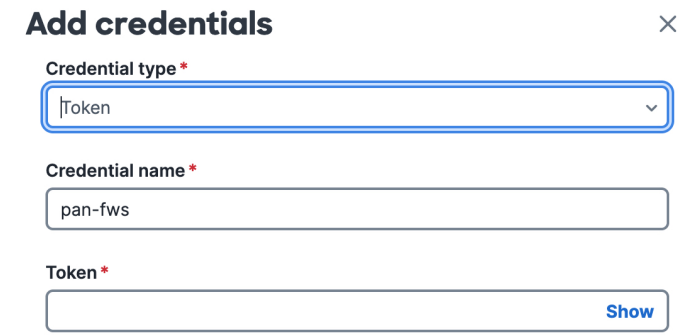
   The fields depend on the credential type.

Figure 15: Username and Password



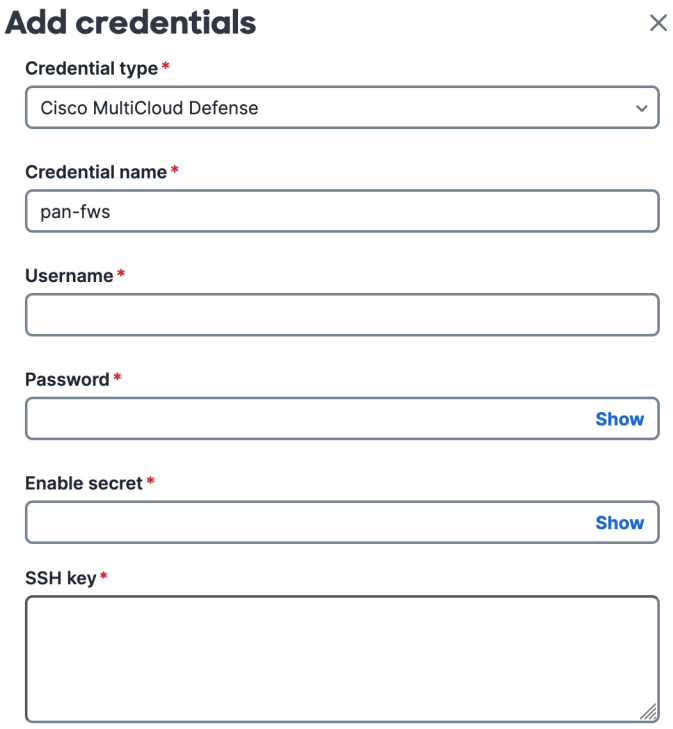
- **Credential name**–Name for this credential object.
- **Username**–The username to log into the device.
- **Password**–The password to log into the device.

Figure 16: Token



- **Credential name**–Name for this credential object.
- **Token**–Paste in the token used for login.

Figure 17: Cisco Multicloud Defense



- **Credential name**–Name for this credential object.
- **Username**–The username to log into the device.
- **Password**–The password to log into the device.
- **Enable secret**–The privileged mode (enable) password.
- **SSH key**–Paste in the SSH key used for authentication.

5. Click **Save credentials**.

   You can now use these credentials in Add a third-party enforcer on page 26 and Import a policy on page 51.

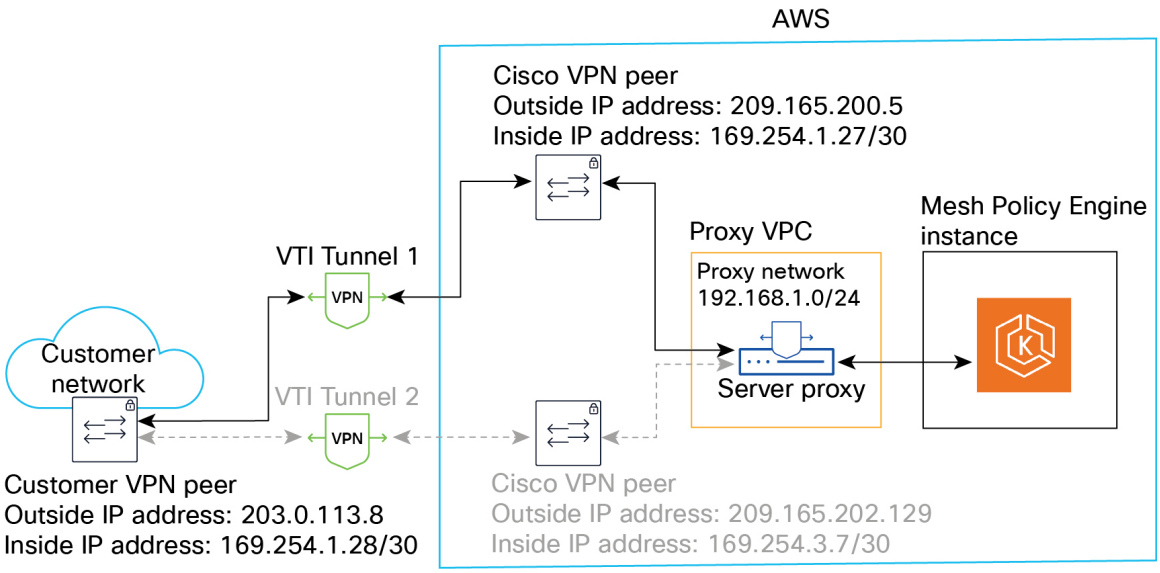
Add a management connection for third-party enforcers

Add a management connection so Mesh Policy Engine can reach third-party enforcers on private networks. Use the connection details to complete setup for policy deployment.

For third-party enforcers with management interfaces that do not have internet-reachable IP addresses, you need to establish a route-based site-to-site VPN connection using a Virtual Tunnel Interface (VTI) from the customer VPN peer to Cisco so that Mesh Policy Engine can access and update policies directly on your enforcers. You will have your own Cisco AWS VPC on a private network to terminate the connection on the Cisco end.

The VPN connection includes an active and a standby tunnel for redundancy; however, only one tunnel can be active. You can configure the other tunnel and manually bring it up in case of failure.

Figure 18: Management connection to Cisco



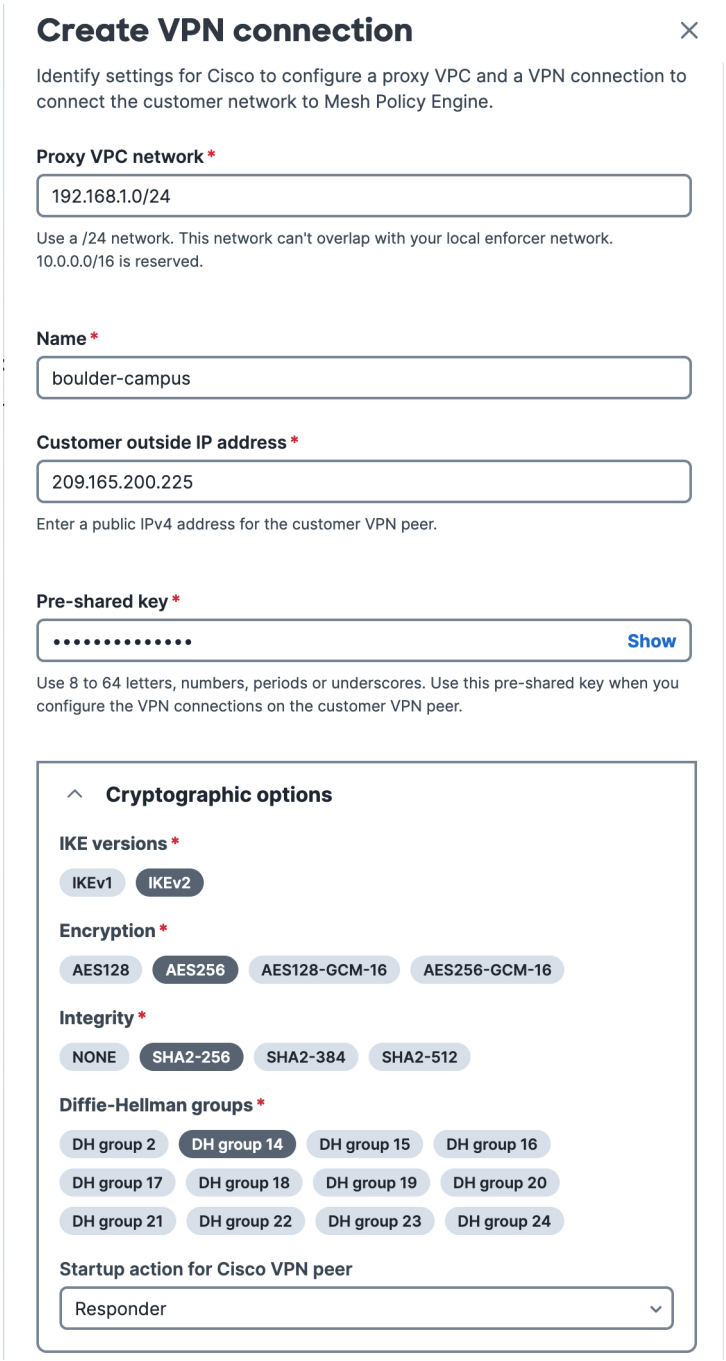
If you use active/standy failover for the customer VPN peers, you can add two VPN connections. Only one tunnel can be active, so be sure to enable only one tunnel for each connection.

For Cisco enforcers, a separate proxy connection is not required. If your third-party enforcer has a management interface with a routable IPv4 address, you don't need a VPN connection; Mesh Policy Engine can access your enforcer directly over the internet using the standard encrypted connection supported by your platform for management.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Choose **Enforcers** > **Management connections** > **VPN connections**.
3. Click **Create VPN connection**.

Figure 19: Create VPN connection



a) Enter the **Proxy VPC network**.

   For your initial VPN connection, provide the private network for the VPC. Subsequent connections, if any, will use the same network.

   Use a /24 network with the last octet a multiple of 16, between 0 and 208. This network can't overlap with your local enforcer network. If you have multiple Security Cloud Control organizations in the same region, make sure this network does not overlap with any other organization proxy VPC network. 10.0.0.0/16 is reserved. Cisco splits the subnet into three /28 subnets–one per AWS Availability Zone–for the proxy instances and load balancer, with headroom for future expansion.

   If you want to change the VPC network, you need to delete all VPN connections and start over.

b) Enter a **Name** for this connection.
c) Enter the **Customer outside IP address**.

Identify the public outside IPv4 address of your VPN peer. This address is your VTI's tunnel source interface IP address.

d) Enter a **Pre-shared key** of your choice, between 8 to 64 characters of letters, digits, period (.), and underscore (_) only.

Cisco stores the pre-shared key in the AWS Secrets Manager.

e) Optional: In **Cryptographic options**, change the cryptographic settings for the connection.

See the following defaults:

- **IKE versions–IKEv2**
- **Encryption–AES256, AES256-GCM-16**
- **Integrity–SHA2-256, SHA2-384, SHA2-512**. If you use GCM encryption, they provide built-in integrity.
- **DH groups–14, 15, 16, 19, 20, 21**
- **Startup action–Responder**. Sets if the Cisco VPN peer responds to tunnel initiation or initiates the tunnel.

f) Click **Submit**.

The request appears in the **Request status** tab with status `IN_PROGRESS`.

g) Refresh the **Request status** page to track status.

First-time provisioning of the VPC takes approximately 30 minutes. You can leave the page and return later. When the request reaches `COMPLETED`, the new connection appears on the main table with two tunnel endpoints–the **Cisco outside IP address**–for each tunnel.

> **Note**
>
> The Cisco outside IP addresses are not known in advance. AWS allocates them dynamically when the VPN connection is created, so you must submit the connection in Mesh Policy Engine before you can add the customer peer connection.

Adding additional connections reuses the existing Proxy VPC and takes approximately 10 minutes per connection.

Table 2: Request status

State	Meaning
`SUBMITTED`	The request is accepted and waiting to start. You can reject it from this state.
`IN_PROGRESS`	The workflow is running.
`COMPLETED`	The workflow finished successfully. The connections table reflects the new state.
`FAILED`	The workflow encountered an error. Expand the row for the failure reason and request ID. Contact support with that ID.
`REJECTED`	You canceled the request before it started.

4. Configure the customer VPN peer to establish a tunnel to *one* of the Cisco outside IP addresses.

Every AWS Site-to-Site VPN connection has two tunnels that terminate in different Availability Zones. The two tunnels exist for AWS-side resilience: if one tunnel goes down because of AWS maintenance, an Availability Zone event, or an endpoint replacement, the other tunnel remains available.

On the customer side, configure only one tunnel as active at any time. Treat the second tunnel as a cold standby—fully configured on your peer, but kept administratively down until you need to fail over. The reason you can't have two active tunnels is Cisco's VPN uses static routing, not BGP. With static routing, the customer peer does not have a dynamic protocol to elect a single active path, which could cause asymmetric flows and traffic flapping.

a) View the completed connection on the **VPN connections** tab and pick one of the two Cisco outside IP addresses as the primary. Either tunnel is acceptable; the two endpoints are equivalent.
b) Configure the primary tunnel on the customer peer.

   Use the following settings:

   - Tunnel source interface—The interface that has the public outside IP address you specified.
   - Inside IP address—**Customer inside IP address**. The inside network for the VTI endpoints is a 169.254.x.x/30 network with two addresses. Cisco uses the first IP address as its inside IP address. For example, if the Cisco inside IP address is 169.254.6.7/30, the customer IP address will be 169.254.6.8/30.
   - Tunnel destination IP address—**Cisco outside IP address**.
   - Cryptographic settings—Use the same or compatible settings as the Cisco peer:
     - IKE versions
     - Encryption
     - Integrity
     - DH groups
     - Customer startup action—For example, if you set the Cisco startup action to be Responder, then you should set the customer peer to be Initiator.

c) Configure a static route on the customer peer to send enforcer traffic to the proxy VPC network over the primary tunnel.

   To simplify routing for the two tunnels, you can configure two static routes—the primary one with a higher metric—and use static route tracking such as SLA monitor. For the monitored address, you can specify the Cisco outside IP address.

Mesh Policy Engine automatically routes traffic to your enforcers through the proxy. No additional Mesh Policy Engine configuration is required.

5. Configure the second tunnel but leave it administratively down.

If the primary tunnel goes down—for AWS maintenance, endpoint replacement, or any failure—bring up the standby manually and take the primary down.

Configure a static route with a lower metric for this tunnel.

6. For active/standby high availibility for the customer VPN peer, you can add a second VPN connection.

Like the active VPN connection, you can only make one of the tunnels active. High availability will fail over automatically to the standby VPN connection. There isn't any way to fail over automatically to the standby tunnel within each VPN connection, however.

7. To delete a connection, click the Delete icon.

Deleting the last remaining connection also tears down the proxy VPC and the proxy. All private connectivity infrastructure is removed, and any subsequent setup must start over when you add a new connection.

Add a third-party enforcer

Add a third-party enforcer to Mesh Policy Engine so you can manage its policies. Provide the connection details required for the device type you choose.

Before you begin

- Add credentials for third-party enforcers and managers on page 18
- Might be required: Add a management connection for third-party enforcers on page 21

Add a third-party enforcer that supports direct deployment. These enforcer types are supported for this procedure:

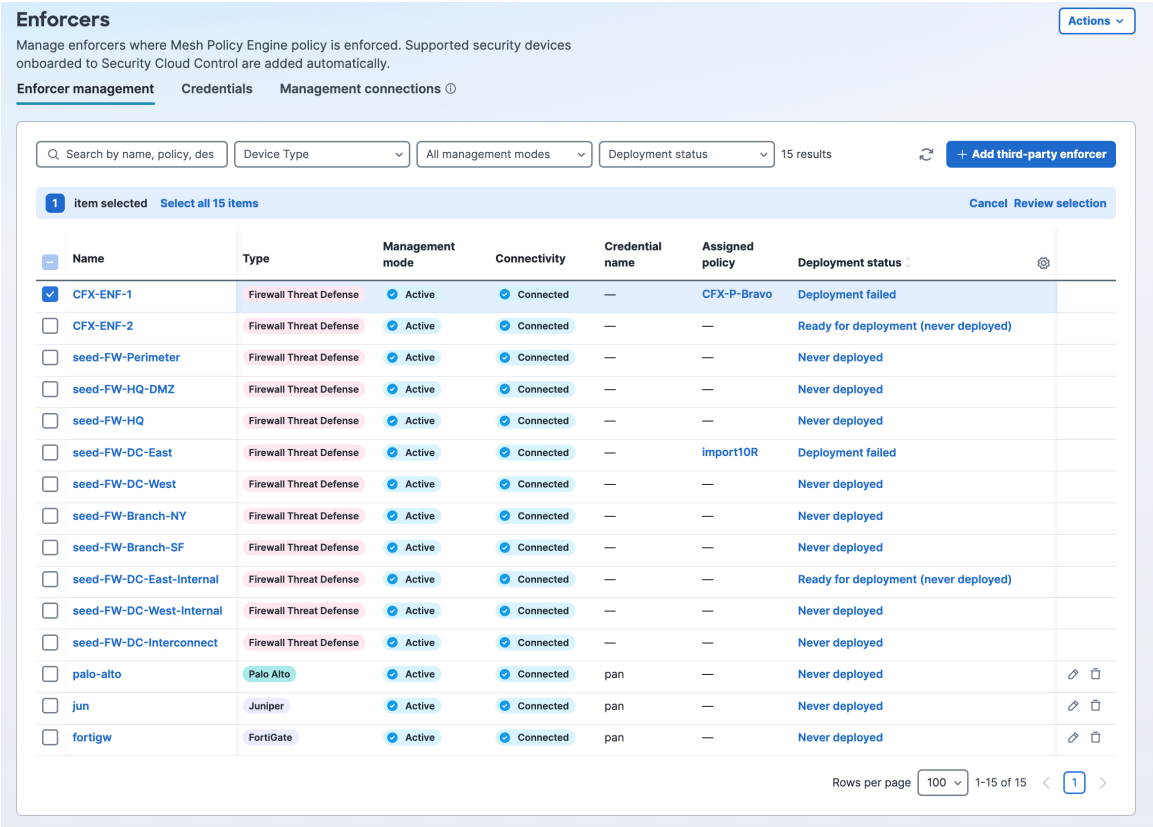
- FortiGate
- Palo Alto Networks
- Juniper

Cisco enforcers in Security Cloud Control are added automatically to the **Enforcer management** table.

Procedure

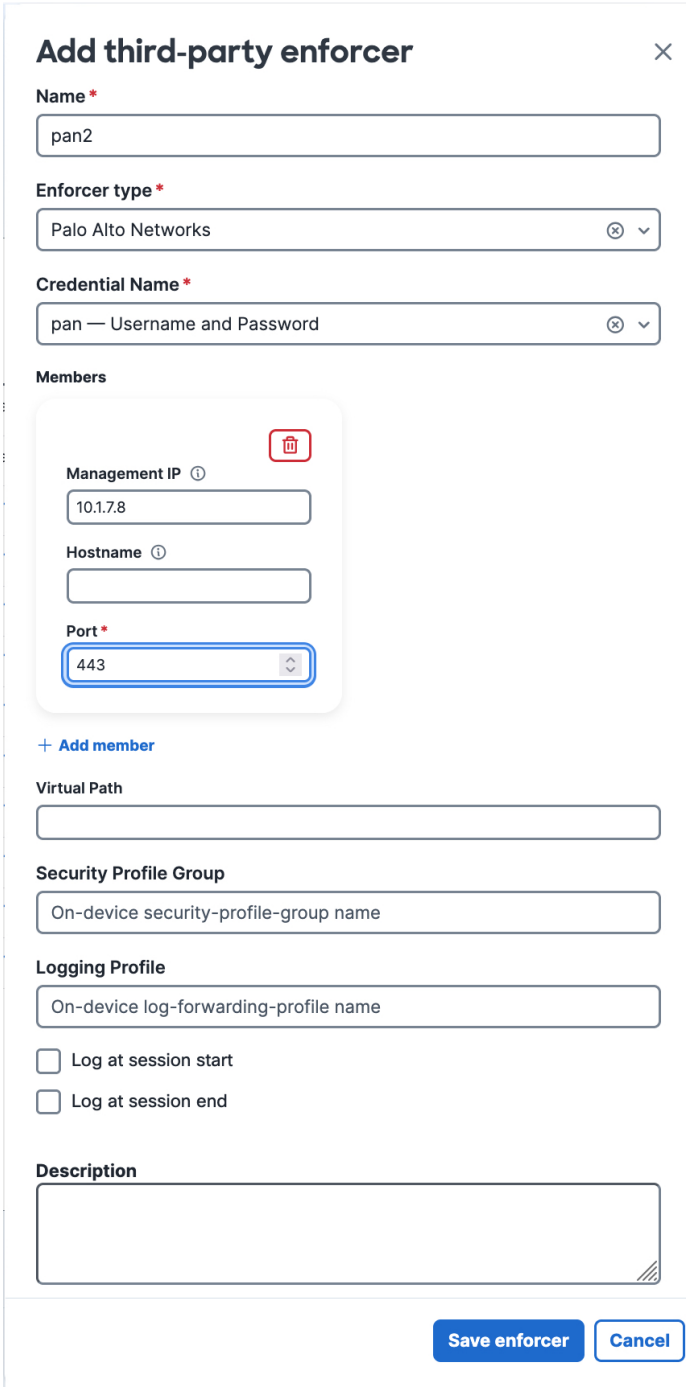
1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Choose **Enforcers** > **Enforcer management**.

Figure 20: Enforcer management



3. Click **Add third-party enforcer** and configure communication settings.

Figure 21: Add third-party enforcer



a) Enter a **Name** for the enforcer.
b) Select the enforcer type: **FortiGate**, **Juniper**, or **Palo Alto Networks**.
c) Select a **Credential name** you defined in Add credentials for third-party enforcers and managers on page 18.
d) Set the **Management IP** or **Hostname**, as well as the **Port** number for Mesh Policy Engine to manage the enforcer.

   If you added a management VPN connection, Mesh Policy Engine will reach the enforcer over the VPN tunnel.

   If your enforcer is part of a high-availability pair or cluster, you can add more members by clicking **Add member**.

e) Other settings depend on the enforcer type. For example, if your enforcer has a named profile that should be associated with the policy, you can specify it by name. Make sure the name matches exactly with the name present on the enforcer.

4. Click **Save enforcer**.

   You see the enforcer on the **Enforcer management** tab.

Manage enforcers

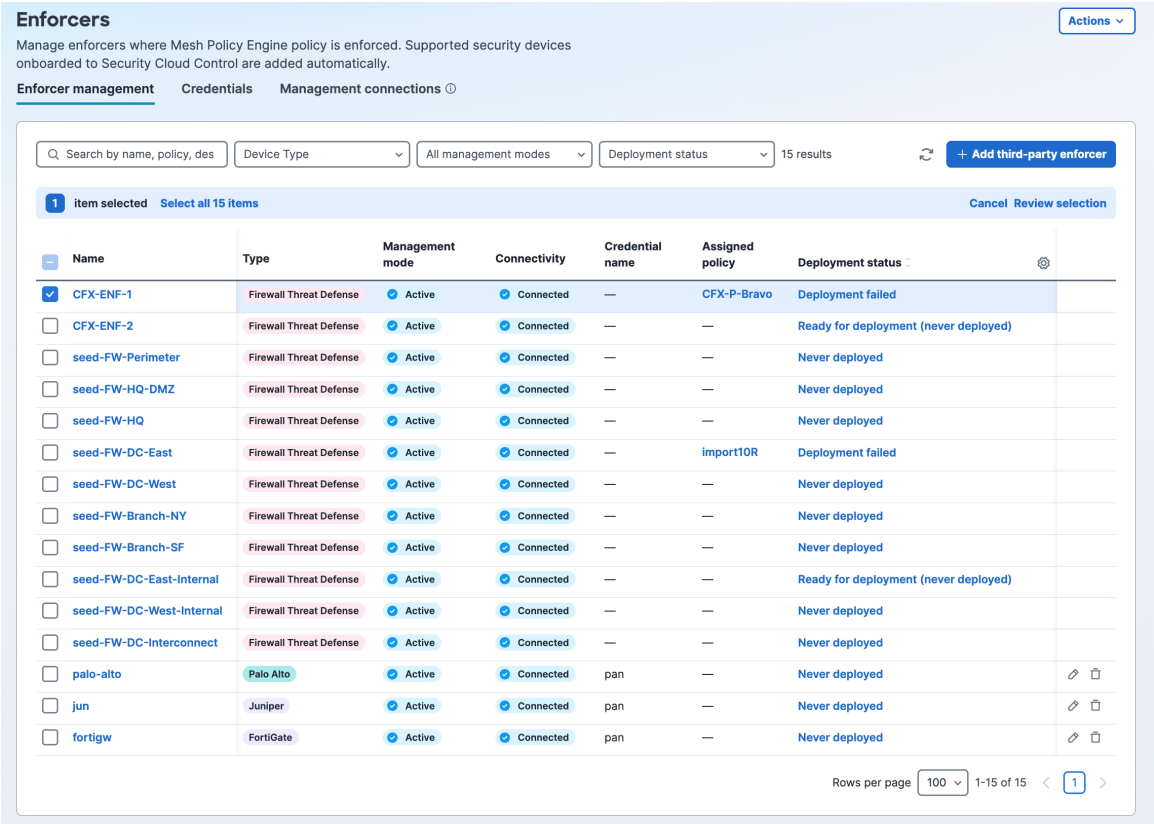
Manage the enforcers listed in Mesh Policy Engine. View device details, adjust settings, and check which devices are ready for policy deployment.

All enforcers, both Cisco and third-party, are listed on the **Enforcer management** tab. You can refresh the list, view details, set global defaults, and deploy the policy to enforcers.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Choose **Enforcers** > **Enforcer management**.

   Figure 22: Enforcer management



   You can use the filters at the top to view devices by name, policy, description, type, or management mode.

3. Click the Edit icon (✎) to change the enforcer settings.

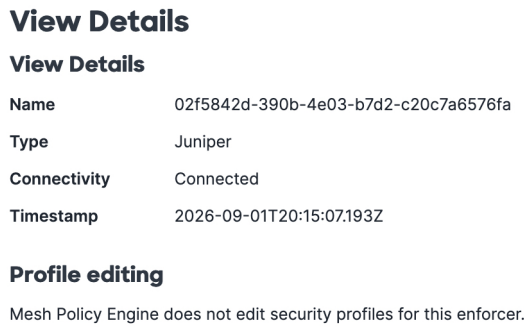
   You can only edit enforcers without pending deployments.

4. Click the Delete icon (Delete 🗑) to delete the enforcer.

   You can only delete enforcers without pending deployments.

5. Click the enforcer **Name** to view details.

Figure 23: Enforcer details



6. Click the **Assigned policy** name to go to that policy.
7. Click **Refresh** to update the list.
8. Select one or more enforcers and click **Actions** to perform the following actions:
   - **Deploy**–See Deploy policy changes to enforcers on page 86 for more information.
   - **Force refresh**–Forces a refresh for only the selected enforcers.
9. Choose **Actions** > **Global defaults** to set default profiles and other settings for policies for each enforcer type. Select the **Device type**, set the defaults, and click **Save**.

   This screen lets you set the logging actions for all Firewall Threat Defenses; third-party enforcers have logging settings per enforcer.

Figure 24: Global defaults


Global Defaults
Device type
FortiGate
FortiGate profile defaults
Antivirus Profile
On-device profile name (blank to inherit / clear)
Application Control List
On-device profile name (blank to inherit / clear)
DLP Profile
On-device profile name (blank to inherit / clear)
DNS Filter Profile
On-device profile name (blank to inherit / clear)
Email Filter Profile
On-device profile name (blank to inherit / clear)
File Filter Profile
On-device profile name (blank to inherit / clear)
IPS Sensor
On-device profile name (blank to inherit / clear)
SSL/SSH Inspection Profile
On-device profile name (blank to inherit / clear)
Web Filter Profile
On-device profile name (blank to inherit / clear)
Save

3 Policies

Topics:

- About policies
- Guidelines for policies
- Create a fixed-assignment policy
- Import a policy
- View policies

Find an overview of policies in Mesh Policy Engine, including policy types, hierarchy, rulesets, and the tasks for creating and viewing policies.

Configure all your shared policies on this page.

About policies

Learn about policy types in Mesh Policy Engine and how policies relate to enforcers. Use this overview to understand the policy structure before creating rules.

Mesh Policy Engine supports fixed-assignment policies. You can manually assign a single child policy and its inherited parent policies to an enforcer.

Fixed-assignment policies

Learn how fixed-assignment policies organize ordered allow and block rules in Mandatory and Default sections. Understand where these policies fit in a hierarchy.

Fixed-assignment policies consist of one or more rulesets that include allow and block rules, in order, that you can place in the following sections:

- Mandatory
- Default

The policy types and rule sections become important when you use policy hierarchy: parent and child policies. With hierarchy:

1. The Mandatory sections are evaluated in order from parent to child.
2. The Default sections are evaluated in reverse order, from child to parent.

See Policy hierarchy on page 35 for more information.

Rulesets

Learn how rulesets group rules in a fixed-assignment policy and which enforcer types they support. Use rulesets to keep related rules together.

Within a fixed-assignment policy, you can add rules to one or more rulesets. Rulesets let you categorize a set of rules, which makes it easy to move or clone a group of rules in the policy. In addition, you must choose one or more enforcer types for the rulesets; the rules will only let you set parameters that are common to all of the chosen types. For example, if one type supports a source service and another doesn't, source service won't be available for that rule.

When you have mixed rulesets in a policy—some rulesets for Firewall Threat Defense and Palo Alto Networks, others for Juniper, say—when you deploy the policy to the enforcer, only the applicable rulesets are included.

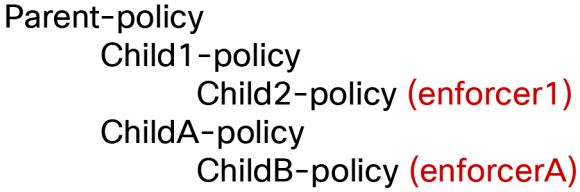
Rulesets are not reusable between policies, but you can clone a ruleset to a different policy.

How to assign fixed-assignment policies

Learn which child policies in a fixed-assignment policy hierarchy you can assign to enforcers. Understand when adding a lower-level child requires reassignment.

You can assign a policy to enforcers at the lowest-level child of a branch. You can also create sibling child policies, with some enforcers using one sibling and others using another:

Figure 25: Enforcers at the lowest level



If you later add a lower-level child policy, you will have to reassign your enforcers.

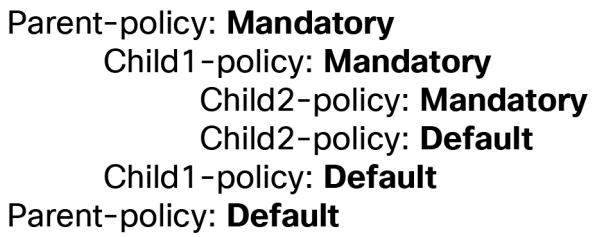
Policy hierarchy

Learn how parent and child policies organize Mandatory and Default sections. Understand the policy order that applies to an enforcer before assigning child policies.

The policy rule sections become important when you use policy hierarchy: parent and child policies. With hierarchy:

1. The Mandatory sections are evaluated in order from parent to child.
2. The Default sections are evaluated in reverse order, from child to parent.

Figure 26: Mandatory and Default section evaluation order



Mesh Policy Engine supports only one top-level fixed-assignment policy parent, but you can create multiple child branches.

How Mesh Policy Engine works with existing policy

Learn how Mesh Policy Engine policy relates to policies already on an enforcer. Understand when the existing policy remains in place before planning changes.

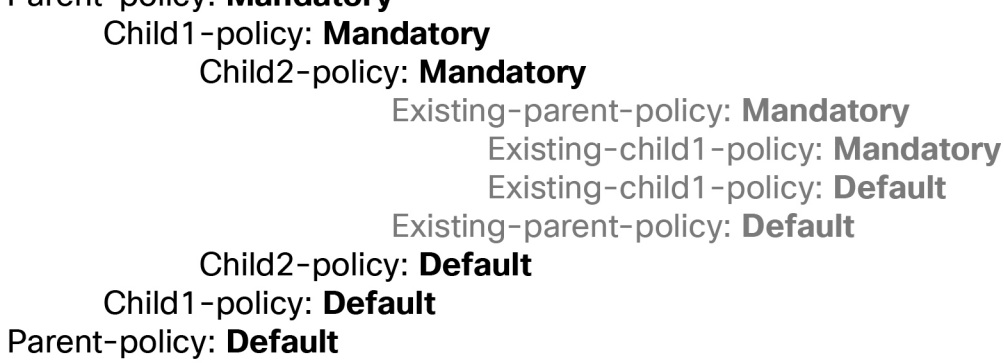
Most enforcers have their policy replaced by Mesh Policy Engine.

However, the following platforms have their existing policy maintained:

- Firewall Threat Defense
- Secure Access

In this case, the Mesh Policy Engine policy is added as a parent policy. For example, Firewall Threat Defense also uses hierarchical policies, so the resulting policy on the device looks like this:

Figure 27: Hierarchical existing policy



For Secure Access, the resulting policy is similar, but without an existing hierarchical policy. The hierarchy is maintained in Mesh Policy Engine only.

Figure 28: Non-hierarchical existing policy

Parent-policy: **Mandatory**
Child1-policy: **Mandatory**
Child2-policy: **Mandatory**
Existing-policy: **All**
Child2-policy: **Default**
Child1-policy: **Default**
Parent-policy: **Default**

How the policy works with a default action

Learn where the default action comes from when Mesh Policy Engine policies interact with an enforcer's existing policy. Use this information when reviewing traffic behavior.

If existing policy is maintained, the default action comes from the enforcer's configuration. For example, for Firewall Threat Defense, the default action of the lowest-level child on the enforcer is applied at the end:

Figure 29: Default action in a fixed-assignment policy hierarchy

Parent-policy: **Mandatory**
Child1-policy: **Mandatory**
Child2-policy: **Mandatory**
Existing-parent-policy: **Mandatory**
Existing-child1-policy: **Mandatory**
Existing-child1-policy: **Default**
Existing-parent-policy: **Default**
Child2-policy: **Default**
Child1-policy: **Default**
Parent-policy: **Default**
Existing-child1-policy: **Default action**

For enforcers where the entire policy is owned by Mesh Policy Engine, the policy uses whatever implicit policy is on the enforcer, if any. For example, the ASA has an implicit deny all for anything not explicitly allowed in the policy. Mesh Policy Engine does not have any implicit default action as part of its policy.

Supported rule parameters

Learn which networks, services, and security group tags policy rules can use. Compare the parameters for fixed-assignment and dynamic-assignment policies.

For fixed-assignment policies, you can include the following parameters in allow and block rules, depending on the enforcer limitations for a given ruleset:

- Source network–Host, network, range, FQDN, or group
- Source port–ICMP, TCP, UDP, ICMPv6, Other, or group
- Destination network–Host, network, range, or FQDN, or group
- Destination port–ICMP, TCP, UDP, ICMPv6, Other, or group

Global policy

Learn when policies apply globally or to individual interfaces on supported enforcers. Understand the policy placement choices before configuring access rules.

Mesh Policy Engine creates global policies that apply to all zones or interfaces.

For Secure Access, the mesh policy is part of the access policy.

Guidelines for policies

Check policy guidelines for supported enforcers and rule objects before deploying changes. Use these requirements to avoid unsupported settings in policy rules.

Deployment guidelines

- FortiGate—Mesh Policy Engine does not validate the staged configuration and only performs postcommit validation. Any inconsistencies discovered during this validation, however unlikely, will raise an error, but the device configuration will not be rolled back.

SGT in a network object guidelines

- Secure Access—Only Secure Access supports SGT objects.

General service object guidelines

- All—Mesh Policy Engine doesn't support AppIDs in service objects; it always uses the protocol and port numbers. For example, FTP is represented by protocol 6 and port 21.

ICMP in a service object guidelines

- Firewall Threat Defense—Doesn't support rules with ICMP type 30 in them.
- Palo Alto Networks—Doesn't support ICMP without any type (null type).
- Palo Alto Networks—Mesh Policy Engine lets you create ICMP services with the same type and code but a different timeout. Palo Alto Networks doesn't support ICMP services that only differ by timeout.

Timeouts in a service object guidelines

- Firewall Threat Defense—Doesn't support timeouts in service objects, so they are ignored.
- FortiGate—If you specify a timeout less than 300 seconds, the timeout in the rule will be changed to 300 seconds.
- Palo Alto Networks—Mesh Policy Engine lets you create ICMP services with the same type and code but a different timeout. Palo Alto Networks doesn't support ICMP services that only differ by timeout.

Create a fixed-assignment policy

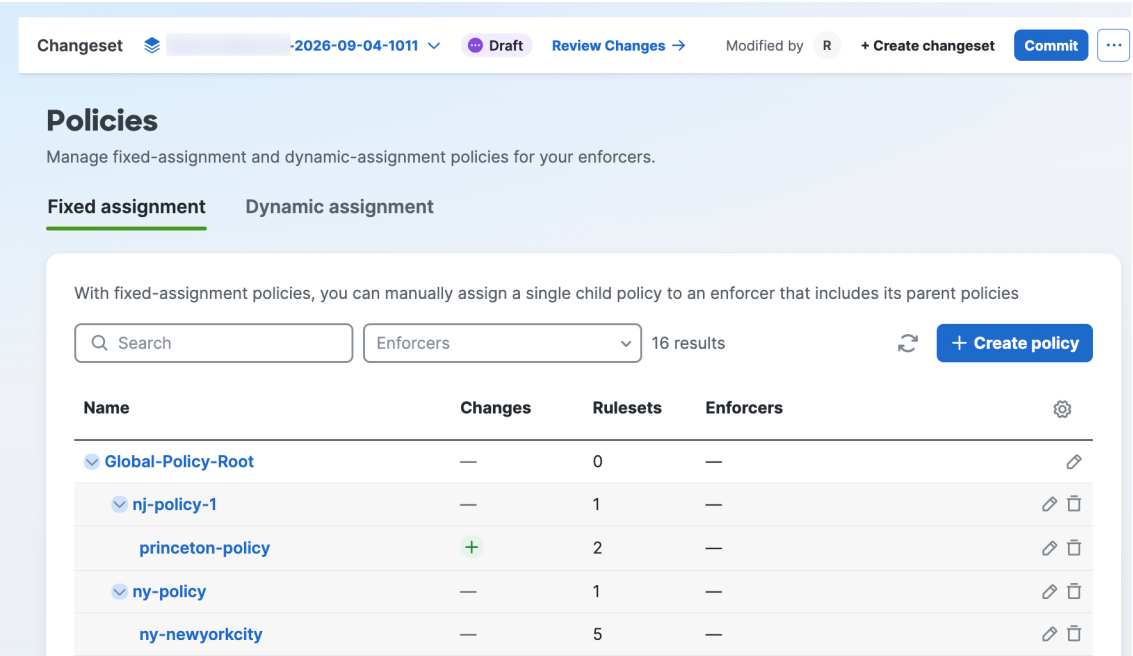
Create a fixed-assignment policy in the policy hierarchy and assign it to enforcers. Save your changes in a changeset before committing the policy.

Create a fixed-assignment policy in your policy hierarchy. Collect all policy changes in a changeset and then commit them as a group. You also assign enforcers to the lowest-level child policies.

Procedure

1. Navigate to the **Policies** page and select a changeset to gather your policy changes.
   a) From the Security Cloud Control Home page, click **Mesh Policy Engine**.
   b) Choose **Policies** > **Fixed assignment**.

   Figure 30: Policies



c) At the top of the screen, select a changeset.

Figure 31: Select a changeset



2. Click **Create policy** and set the following parameters.

Figure 32: Create policy



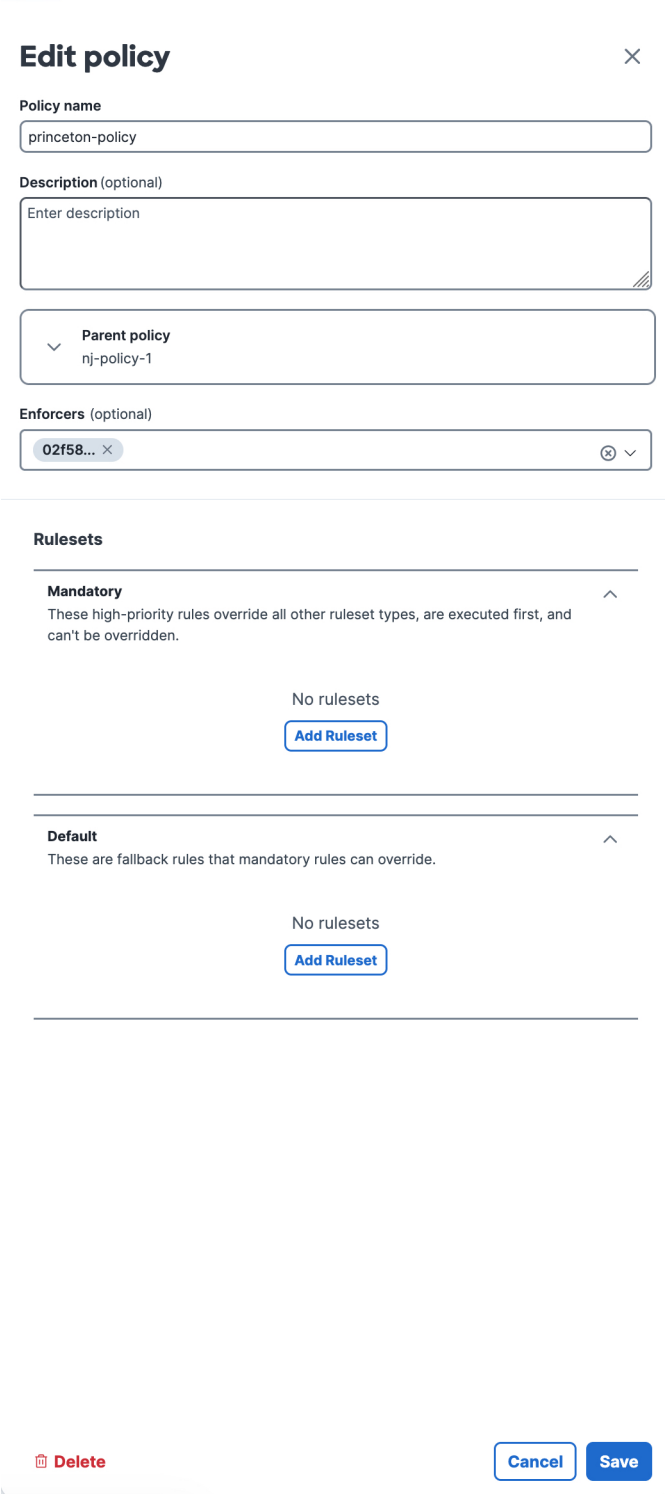
a) Enter a unique **Name** for the policy.
b) Optional: Enter a **Description**.
c) Choose the **Parent policy**.

   If this is the first policy that you add, don't choose a parent policy. If you choose a parent policy with assigned enforcers, the enforcers will automatically be reassigned to this new policy since this policy is now the lowest-level child.

d) Click **Create**.

3. After you create a policy or when you edit an existing policy, the **Edit policy** drawer opens. You can perform only one action at a time. **Save** the policy before you perform another action.

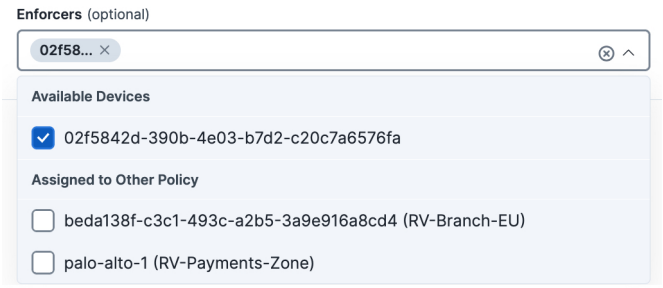
Figure 33: Edit policy drawer



- Assign **Enforcers** to the policy by checking one or more available enforcers from the drop-down list.

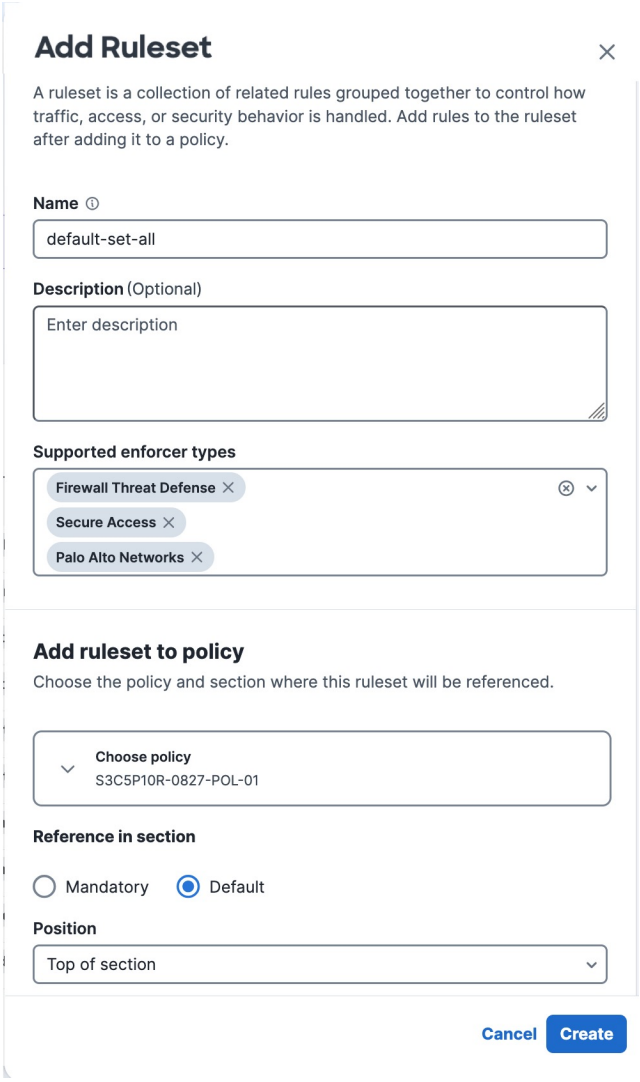
  You can assign enforcers only to a lowest-level child policy.

Figure 34: Assign enforcers



- Add a ruleset to the policy.

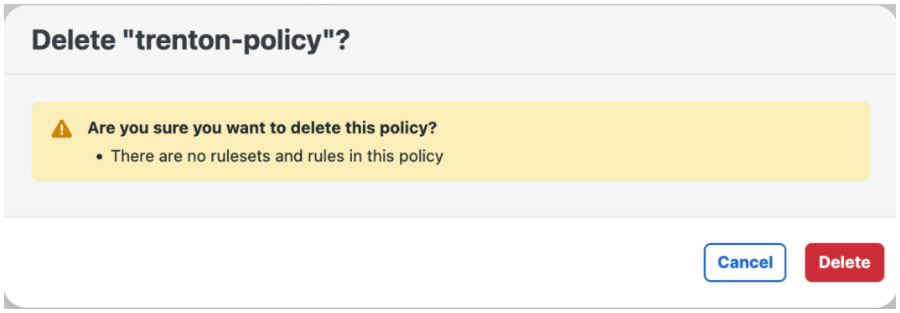
Figure 35: Add a ruleset



For information about adding rulesets and rules, see Create a fixed-assignment ruleset on page 41.

4. To delete a policy, click the Delete icon (Delete).

Figure 36: Delete a policy



Note

You cannot delete a policy that is assigned to any enforcers. Unassign all enforcers before you delete the policy.

Create a fixed-assignment ruleset

Create a ruleset in a fixed-assignment policy and choose its section, enforcer types, and position. Use it to organize rules for deployment.

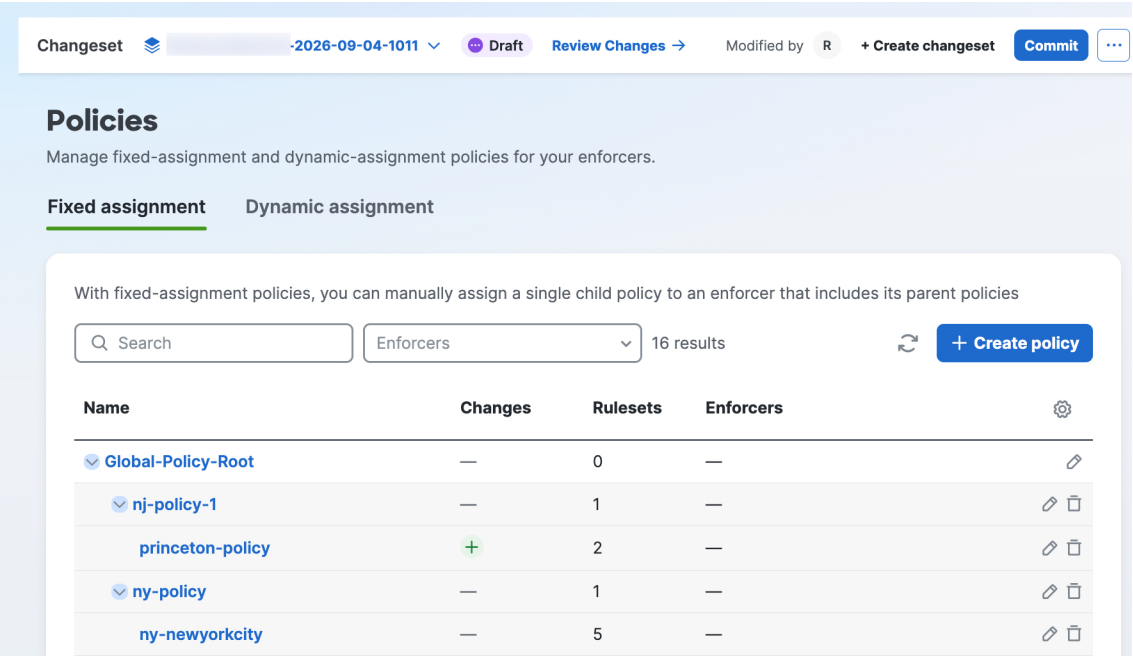
Configure rulesets in a fixed-assignment policy.

Rulesets organize ordered allow and block rules in the Mandatory or Default section. For each ruleset, you choose one or more enforcer types, and the rules support only parameters that are common to all the chosen types. When you deploy the policy, each enforcer receives only the applicable rulesets.

Procedure

1. Navigate to the **Policies** page and select a changeset to gather your policy changes.
   a) From the Security Cloud Control Home page, click **Mesh Policy Engine**.
   b) Choose **Policies** > **Fixed assignment**.

   Figure 37: Policies



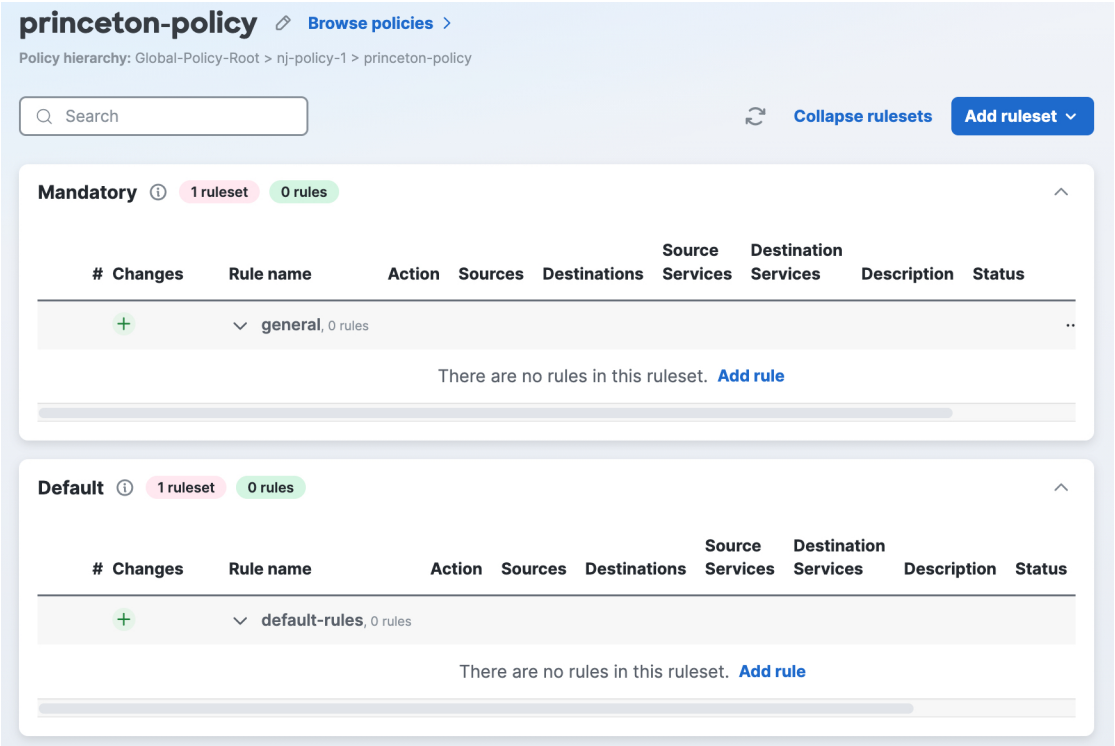
c) At the top of the screen, select a changeset.

Figure 38: Select a changeset



2. Click the policy name to edit the policy.

Figure 39: Policy rulesets and rules



3. Add a ruleset.

To edit an existing ruleset, click the More icon (•••) and select **Edit**.

a) Click **Add ruleset** and select either **Mandatory** or **Default**.

Figure 40: Select a ruleset section

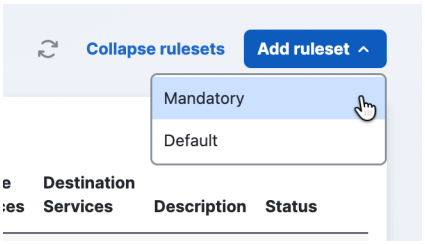
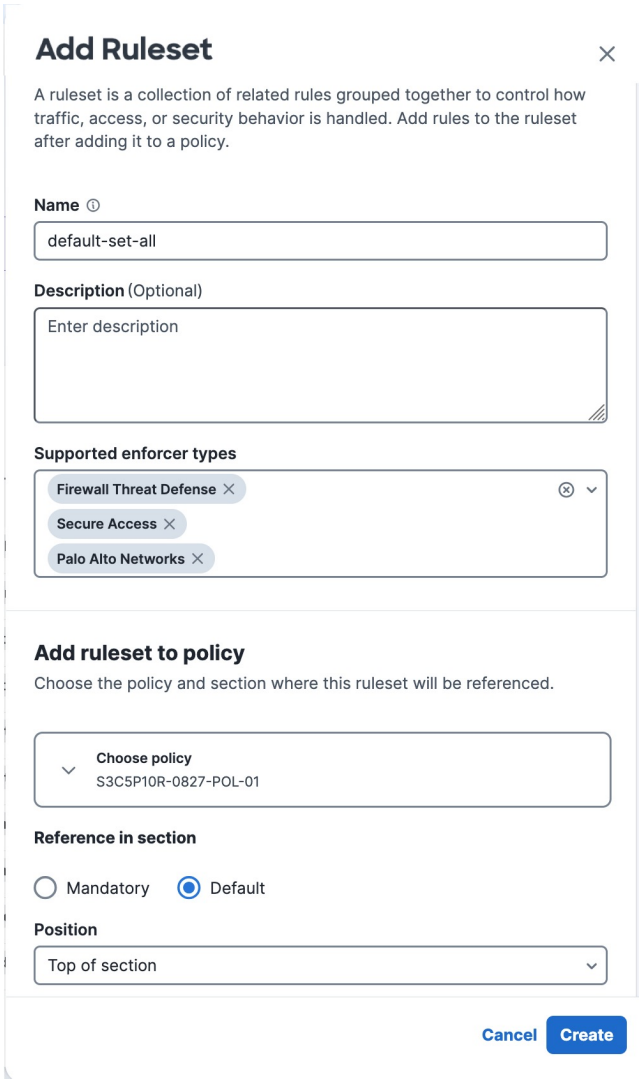


Figure 41: Add a ruleset



b) Enter a **Name** for the ruleset.

c) Optional: Enter a **Description**.

d) Under **Supported enforcer types**, select one or more enforcer types.

Don't add enforcer types that you don't have support for in your organization; you won't be able to add rules to the ruleset. For example, make sure you have an active instance of Firewall Management if you want to add rulesets

for Firewall Threat Defense. If you later add or delete enforcer types, some fields may be added or disallowed. If you have a value in an unsupported field for a new enforcer type, you can't add that enforcer type to the ruleset.

e) Under **Choose policy**, the current policy is selected. If you want to add this ruleset to a different policy, you can choose it here.
f) **Reference in section** shows the section to which you are adding the ruleset; you can change it if needed.
g) For **Position**, select **Top of section**, **Above ruleset**, **Below ruleset**, or **Bottom of section**.

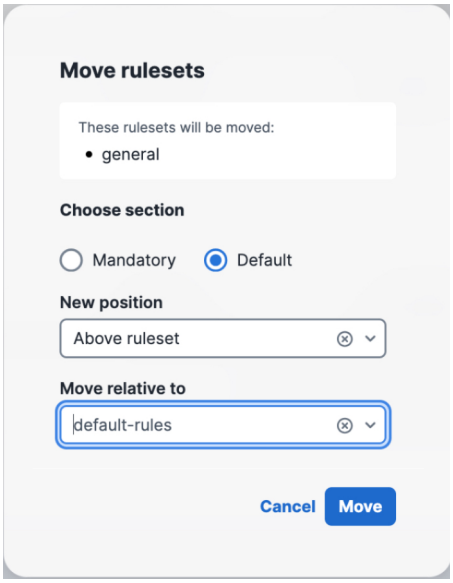
   If you select **Above ruleset** or **Below ruleset**, select a ruleset from **Move relative to**.

h) Click **Create**.

4. To move a ruleset, click the More icon (•••) next to the ruleset and select **Move**.

   Alternatively, use the Drag icon (⠿) to move a ruleset within its current section. You cannot drag a ruleset between the Mandatory and Default sections. You cannot move a ruleset to a different policy, but you can clone the ruleset to another policy.

Figure 42: Move rulesets



a) Under **Choose section**, select **Mandatory** or **Default**.
b) For **New position**, select **Top of section**, **Above ruleset**, **Below ruleset**, or **Bottom of section**.

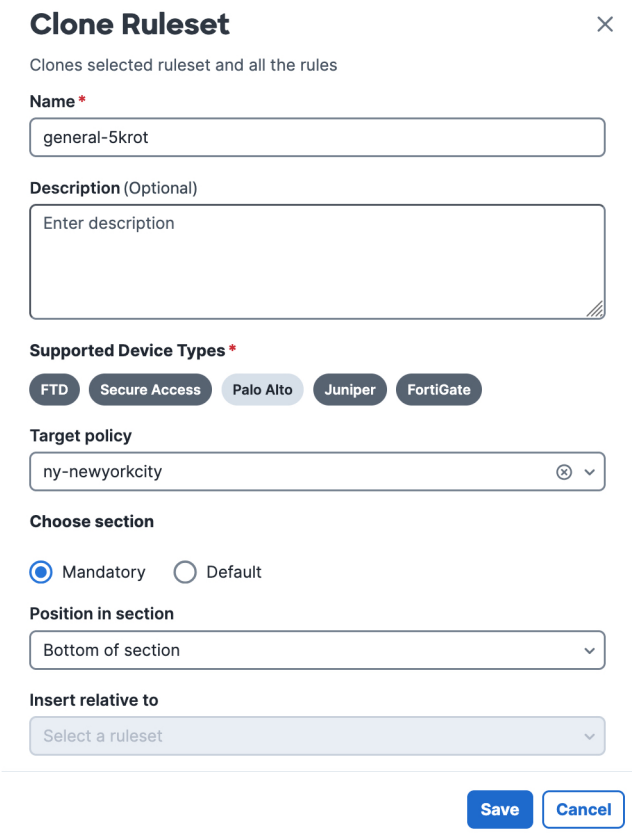
   If you select **Above ruleset** or **Below ruleset**, select a ruleset from **Move relative to**.

c) Click **Move**.

5. To clone a ruleset, click the More icon (•••) next to the ruleset and select **Clone**.

   Cloning copies the selected ruleset and all its rules.

Figure 43: Clone a ruleset



a) Enter a **Name** for the cloned ruleset.
b) Optional: Enter a **Description**.
c) Under **Supported Device Types**, select one or more enforcer types.
d) Select the **Target policy**.
e) Under **Choose section**, select **Mandatory** or **Default**.
f) For **Position in section**, select **Top of section**, **Above ruleset**, **Below ruleset**, or **Bottom of section**.

   If you select **Above ruleset** or **Below ruleset**, select a ruleset from **Insert relative to**.

g) Click **Save**.

6. To delete a ruleset, click the More icon (•••) next to the ruleset and select **Delete**. Click **Delete** on the confirmation dialog box.

Create a fixed-assignment rule

Create a rule in a fixed-assignment policy to allow or block traffic. Choose the networks, services, and other supported criteria for its ruleset.

Create rules in a fixed-assignment policy. The available rule fields depend on the enforcer types selected for the ruleset.

For multiple values of the same type for source or destination, the values are ORed: 10.1.10.0/24 OR 192.168.1.0/24.

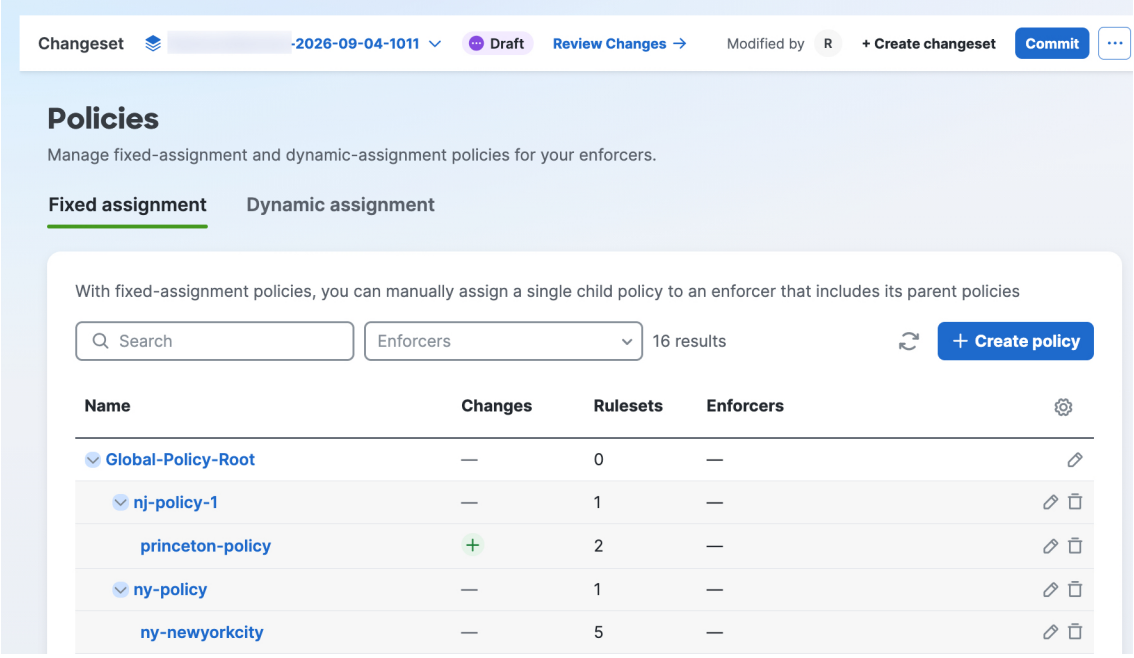
For dissimilar types, values are ANDed: 10.1.10.0/24 AND TCP:443

Secure Access allows ORs between dissimilar values, but those rules aren't supported in Mesh Policy Engine. You can make multiple rules to accomplish the same outcome.

Procedure

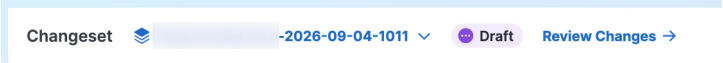
1. Navigate to the **Policies** page and select a changeset to gather your policy changes.
   a) From the Security Cloud Control Home page, click **Mesh Policy Engine**.
   b) Choose **Policies** > **Fixed assignment**.

   Figure 44: Policies



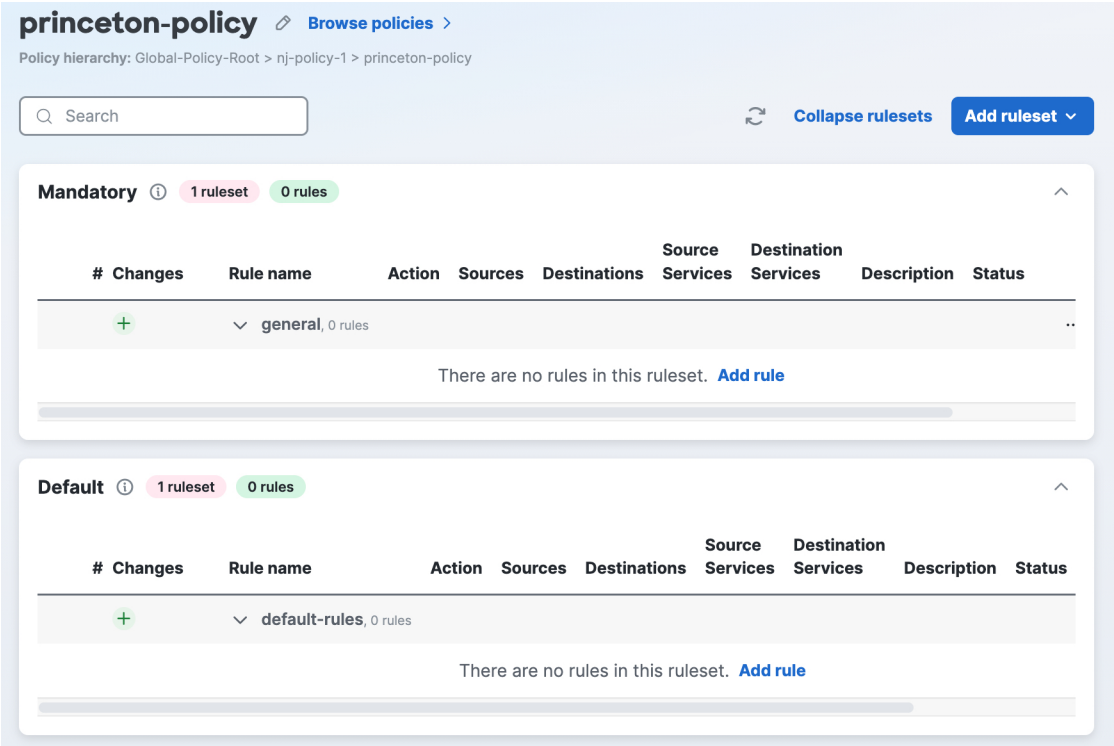
   c) At the top of the screen, select a changeset.

   Figure 45: Select a changeset



2. Click the policy name to edit the policy.

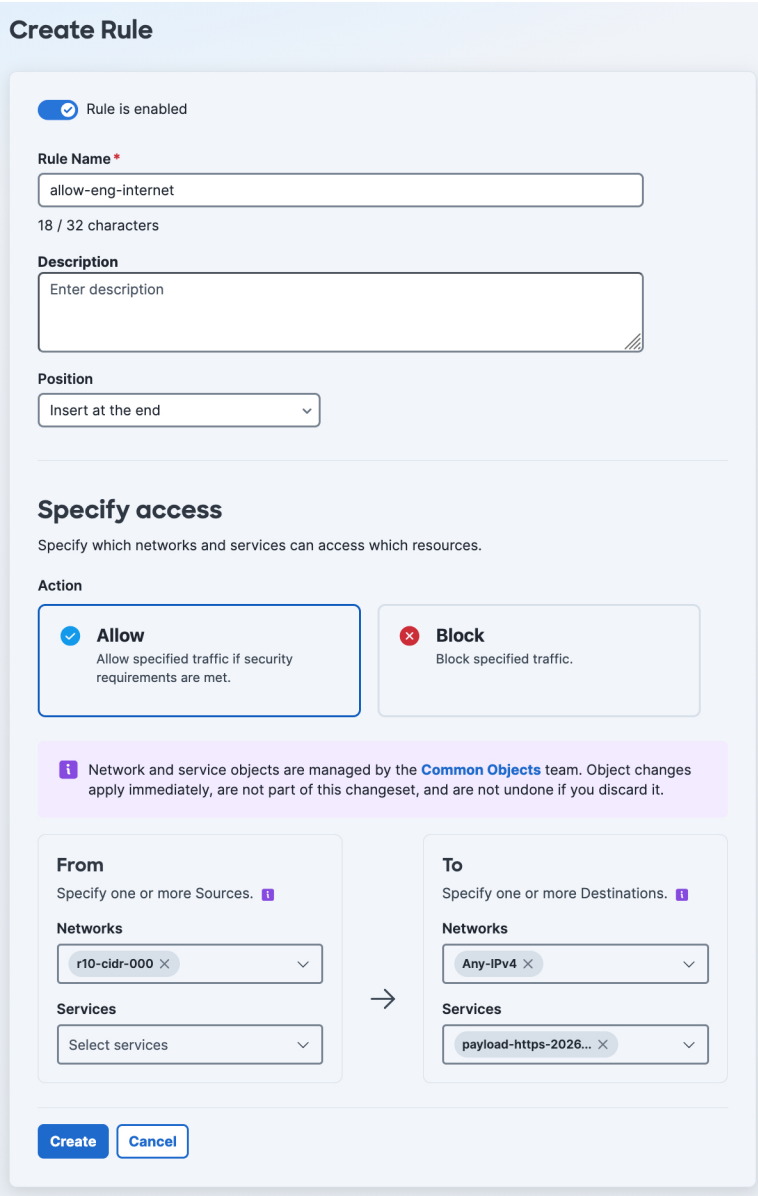
   Figure 46: Policy rulesets and rules



3. Add a rule to a ruleset.
   a) Click the More icon (...) next to the ruleset and select **Add rule**.

      To edit an existing rule, click the More icon (...) next to the rule and select **Edit**.

      Figure 47: Create Rule



The available rule fields depend on the enforcer types selected for the ruleset.

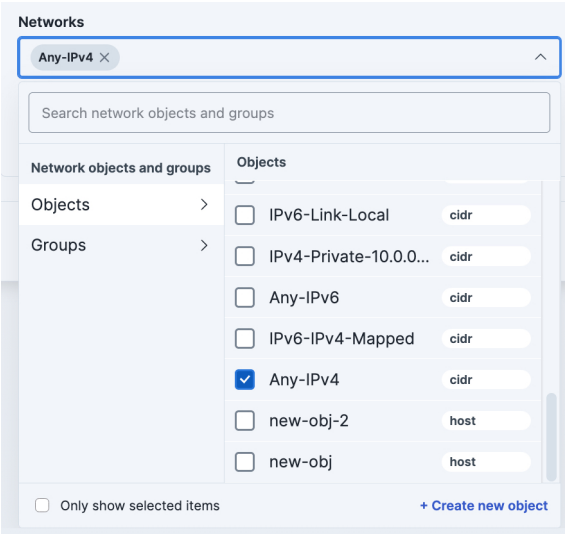
b) Enter a **Rule Name**.
c) Optional: Enter a **Description**.
d) Choose where to add this rule in the ruleset by selecting a **Position**: **Insert at the end**, **Insert at the beginning**, **Insert before a rule**, or **Insert after a rule**.

   When you choose before or after a rule, select the rule in **Relative to rule**.

e) For **Action**, select **Allow** or **Block**.
f) In the **From** and **To** areas, select source and destination **Networks**.

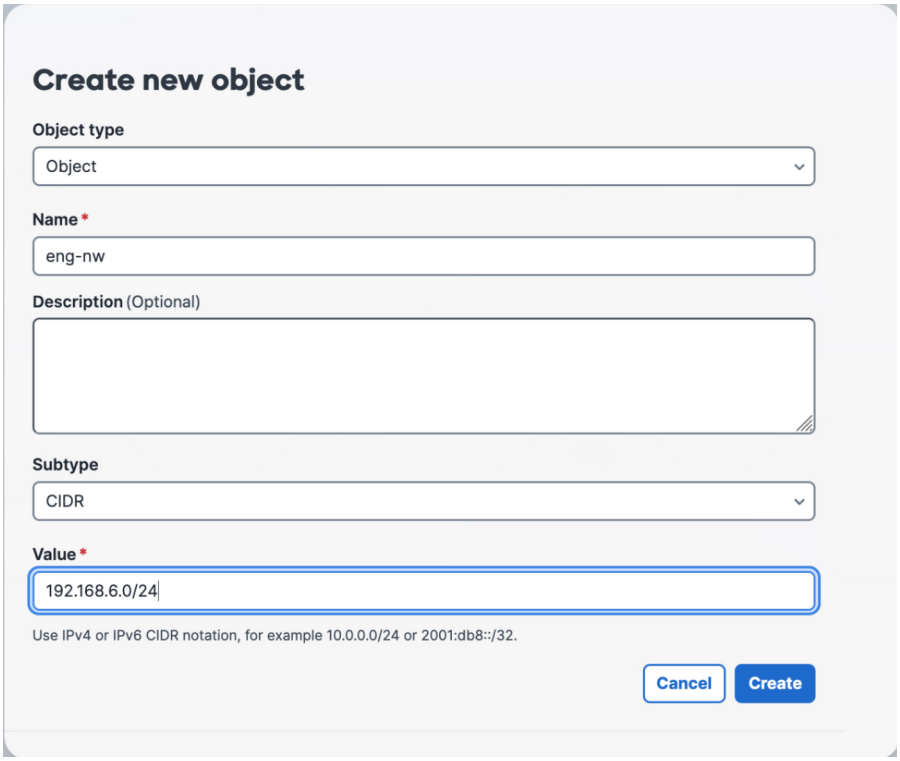
   For each field, select an existing common object or click **Create new object**. If you leave a field empty, the value defaults to Any network.

Figure 48: Select network objects and groups



To create an object, select the **Object type**, enter a **Name** and an optional **Description**, select the **Subtype**, enter the **Value**, and click **Create**. New objects are added to **Common Objects** for Security Cloud Control.

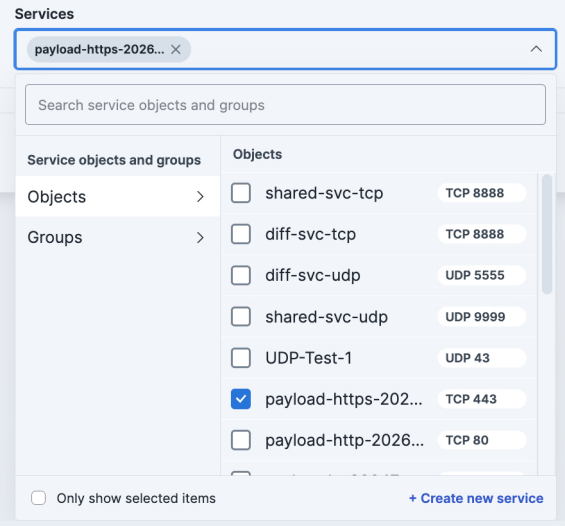
Figure 49: Create a network object



g) In the **From** and **To** areas, select source and destination **Services**.

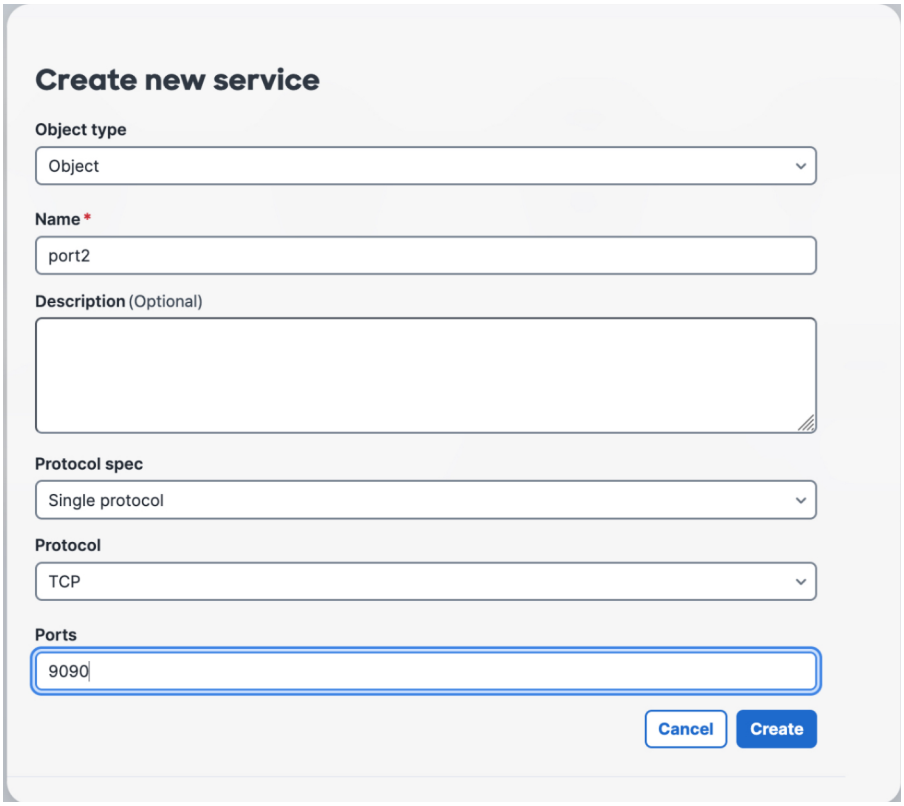
For each field, select an existing service or click **Create new service**. If you leave a field empty, the value defaults to Any service.

Figure 50: Select service objects and groups



To create a service, select the **Object type**, enter a **Name** and an optional **Description**, configure the **Protocol spec**, **Protocol**, and **Ports**, and click **Create**. New objects are added to **Common Objects** for Security Cloud Control.

Figure 51: Create a service



h) Click **Create**.

The new rule is added at the end of the ruleset. You can then use the Drag icon (⠿) to drag the rule to a new location within the ruleset.

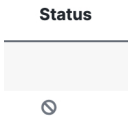
4. To reorder rules within a ruleset, click the Drag icon (⠿) and drag the rule to a new location.

You can't move a rule between rulesets.

5. To disable a rule, click the More icon (•••) next to the rule and select **Disable**.

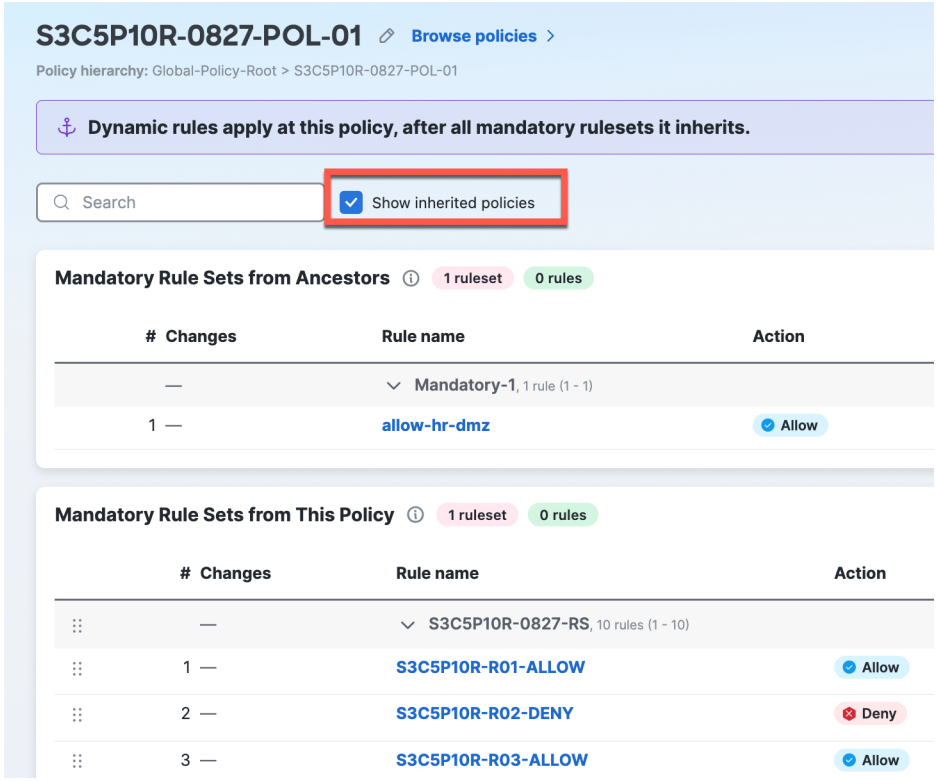
   The **Status** column shows a disabled icon instead of the enabled icon.

   Figure 52: Status



6. To delete a rule, click the More icon (•••) next to the rule and select **Delete**. Click **Delete** on the confirmation dialog box.
7. To view rules from parent policies, click **Show inherited policies**.

   Figure 53: Show inherited policies



Import a policy

Import a policy from a supported manager into Mesh Policy Engine so you can review and manage it alongside other policies.

You can import fixed-assignment policies from supported managers, or you can paste in a formatted policy. You can perform one policy import at a time. All policy changes are gathered into a custom changeset created just for the import. This procedure supports the following managers:

- Panorama–Palo Alto Networks policies

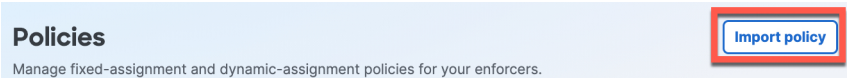
Note

For imported network or service objects, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane.

Procedure

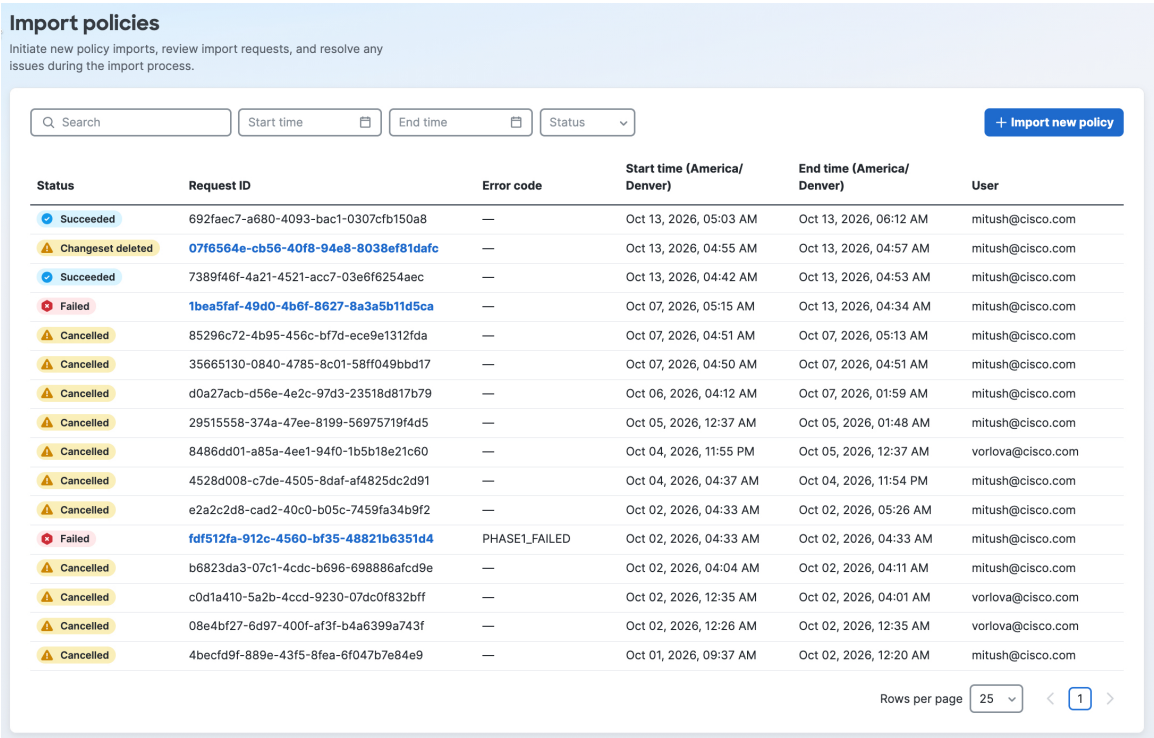
1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Select **Policies** and click **Import policy**.

   Figure 54: Import policy button on the Policies page

   You can view past imports on this page.

   Figure 55: Import policies page

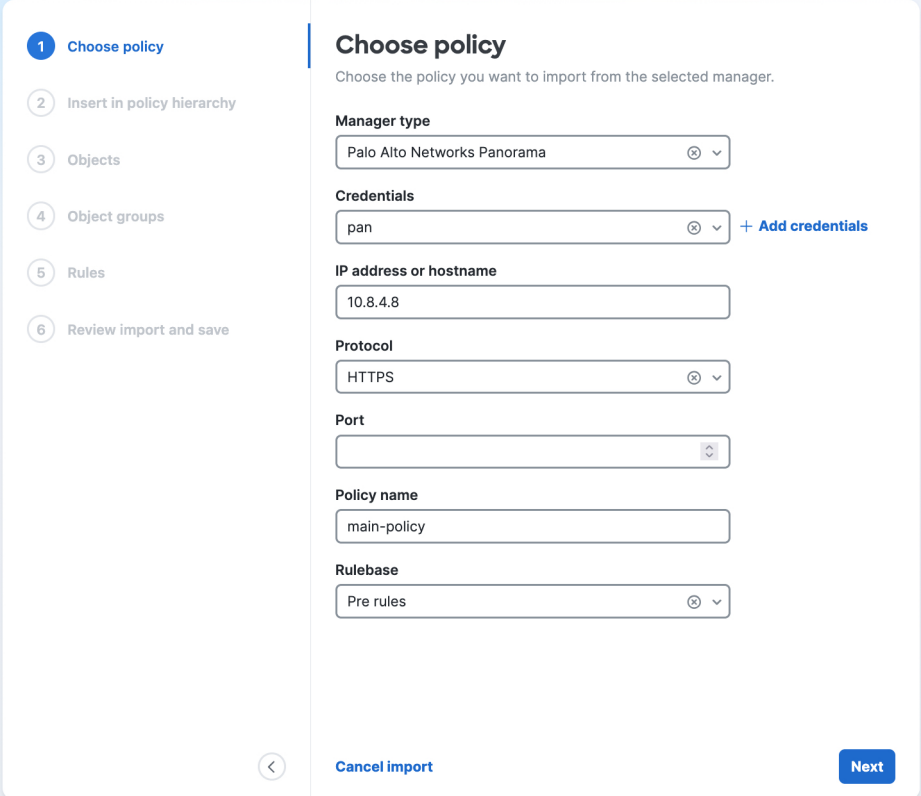
3. Click **Import new policy** and select the **Manager type**.

   The button will be disabled if you have an in-progress import. Wait until the import finishes before starting a new import.

   The fields vary depending on the **Manager type**.

   a) For **Palo Alto Networks Panorama**, configure these settings.

   Figure 56: Palo Alto Networks Panorama policy import

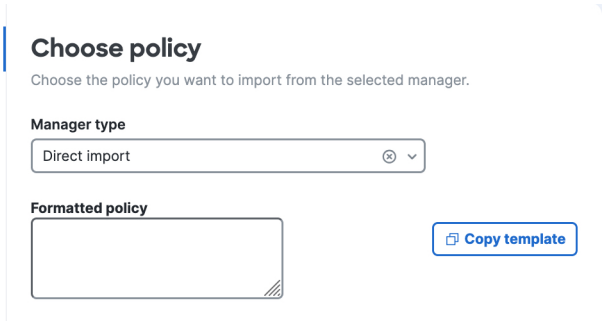


- **IP address or hostname**–The IP address or hostname of the manager. If you added a management VPN connection, Mesh Policy Engine will reach the manager over the VPN tunnel.
- **Credentials**–The credential name that you specified in Add credentials for third-party enforcers and managers on page 18.
- **Protocol**–**https** or **http**
- **Port**–The port to reach the manager on.
- **Policy name**–Enter the exact name of the policy on the manager.
- **Rulebase**–**Pre rules** or **Post rules**.

b) For Direct import, paste the properly formatted policy into the **Formatted policy** box.

You can click **Copy template** and paste into a text editor to get started.

Figure 57: Direct import



Example


```
{
  "targetRulesetName": "imported-scale-10",
  "networkObjects": [
    {
      "foreignId": "net-h-000",
      "name": "s10-host-000",
      "description": "Scale host 0",
      "type": "host",
      "value": "10.210.0.1"
    },
    {
      "foreignId": "net-h-001",
      "name": "s10-host-001",
      "description": "Scale host 1",
      "type": "host",
      "value": "10.210.0.2"
    },
    {
      "foreignId": "net-h-002",
      "name": "s10-host-002",
      "description": "Scale host 2",
      "type": "host",
      "value": "10.210.0.3"
    },
    {
      "foreignId": "net-h-003",
      "name": "s10-host-003",
      "description": "Scale host 3",
      "type": "host",
      "value": "10.210.0.4"
    },
    {
      "foreignId": "net-c-000",
      "name": "s10-cidr-000",
      "description": "Scale subnet 0",
      "type": "cidr",
      "value": "10.211.0.0/24"
    }
  ],
  "networkGroups": [
    {
      "foreignId": "ng-000",
      "name": "s10-netgrp-000",
      "description": "Hosts 0-3",
      "memberForeignIds": [
        "net-h-000",
        "net-h-001",
        "net-h-002",
        "net-h-003"
      ],
      "memberGroupForeignIds": []
    }
  ],
  "serviceObjects": [
    {
      "foreignId": "svc-tcp-000",
      "name": "s10-tcp-21001",
      "description": "TCP 21001",
      "type": "port",
      "value": "21001",
```

```
                  "ports": [
                    "21001"
                  ],
                  "protocol": "tcp",
                  "protocolSpec": "single"
                },
                {
                  "foreignId": "svc-udp-000",
                  "name": "s10-udp-31001",
                  "description": "UDP 31001",
                  "type": "port",
                  "value": "31001",
                  "ports": [
                    "31001"
                  ],
                  "protocol": "udp",
                  "protocolSpec": "single"
                },
                {
                  "foreignId": "svc-icmp-3-9",
                  "name": "s10-icmp-t3-c9",
                  "description": "ICMP type 3 code 9",
                  "type": "icmp",
                  "value": "icmp/type=3/code=9",
                  "protocol": "icmp",
                  "protocolSpec": "type=3/code=9"
                }
              ],
              "serviceGroups": [
                {
                  "foreignId": "sg-000",
                  "name": "s10-svcgrp-000",
                  "description": "Services s10-tcp-21001, s10-udp-31001,
s10-icmp-t3-c9",
                  "memberForeignIds": [
                    "svc-tcp-000",
                    "svc-udp-000",
                    "svc-icmp-3-9"
                  ],
                  "memberGroupForeignIds": []
                }
              ],
              "rules": [
                {
                  "foreignId": "r-0001",
                  "name": "s10-allow-0001",
                  "ruleNumber": 10,
                  "action": "ALLOW",
                  "sources": [
                    "net-h-000"
                  ],
                  "destinations": [
                    "net-h-003"
                  ],
                  "services": [
                    "svc-tcp-000"
                  ],
                  "description": "net-h-000 -> net-h-003 on svc-tcp-000",
                  "enabled": true
                },
                {
                  "foreignId": "r-0002",
```

```
    "name": "s10-allow-0002",
    "ruleNumber": 20,
    "action": "ALLOW",
    "sources": [
      "net-h-001"
    ],
    "destinations": [
      "net-c-000"
    ],
    "services": [
      "svc-udp-000"
    ],
    "description": "net-h-001 -> net-c-000 on svc-udp-000",
    "enabled": true
  },
  {
    "foreignId": "r-0003",
    "name": "s10-allow-0003",
    "ruleNumber": 30,
    "action": "ALLOW",
    "sources": [
      "net-h-002"
    ],
    "destinations": [
      "net-h-000"
    ],
    "services": [
      "svc-icmp-3-9"
    ],
   "description": "net-h-002 -> net-h-000 on svc-icmp-3-9",

    "enabled": true
  },
  {
    "foreignId": "r-0004",
    "name": "s10-allow-0004",
    "ruleNumber": 40,
    "action": "ALLOW",
    "sources": [
      "net-h-003"
    ],
    "destinations": [
      "net-h-000"
    ],
    "services": [
      "sg-000"
    ],
    "description": "net-h-003 -> net-h-000 on sg-000",
    "enabled": true
  },
  {
    "foreignId": "r-0005",
    "name": "s10-allow-0005",
    "ruleNumber": 50,
    "action": "ALLOW",
    "sources": [
      "net-c-000"
    ],
    "destinations": [
      "net-h-001"
    ],
    "services": [
```

```
        "svc-tcp-000"
      ],
      "description": "net-c-000 -> net-h-001 on svc-tcp-000",
      "enabled": true
    },
    {
      "foreignId": "r-0006",
      "name": "s10-allow-0006",
      "ruleNumber": 60,
      "action": "ALLOW",
      "sources": [
        "ng-000"
      ],
      "destinations": [
        "net-c-000"
      ],
      "services": [
        "svc-udp-000"
      ],
      "description": "ng-000 -> net-c-000 on svc-udp-000",
      "enabled": true
    },
    {
      "foreignId": "r-0007",
      "name": "s10-allow-0007",
      "ruleNumber": 70,
      "action": "ALLOW",
      "sources": [
        "net-h-000"
      ],
      "destinations": [
        "net-h-003"
      ],
      "services": [
        "svc-icmp-3-9"
      ],
     "description": "net-h-000 -> net-h-003 on svc-icmp-3-9",

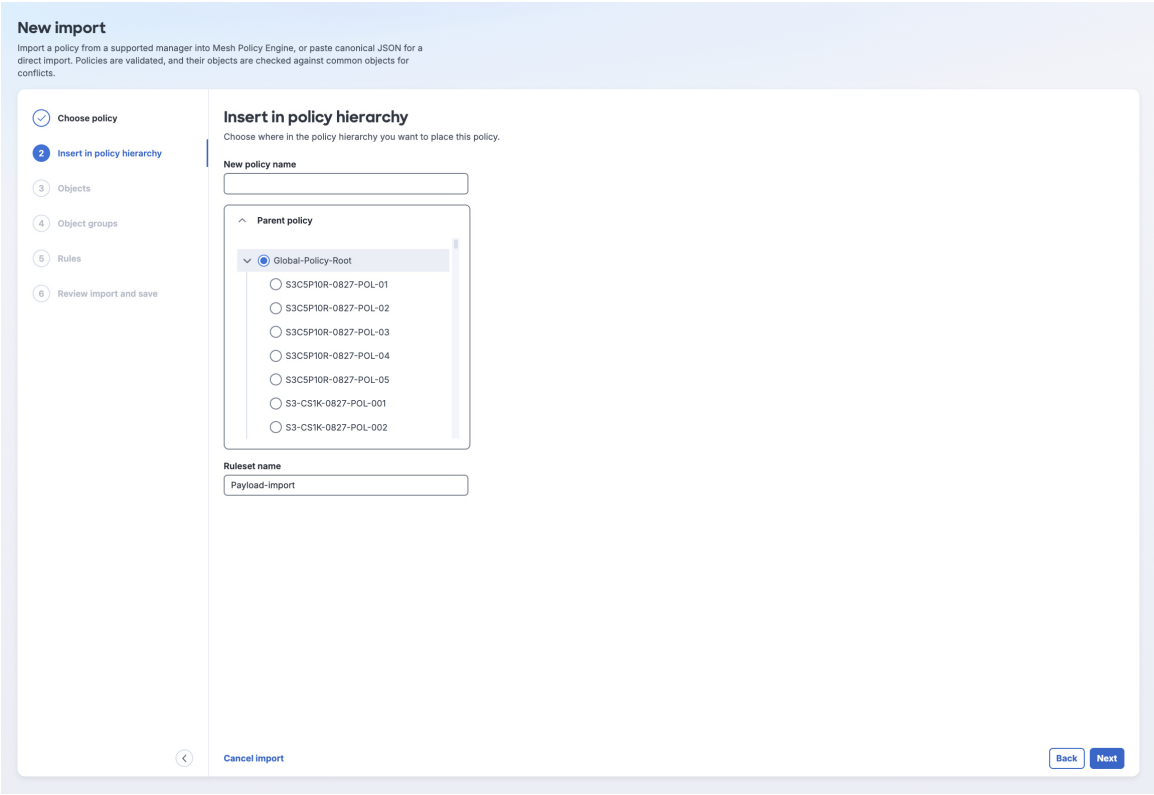
      "enabled": true
    },
    {
      "foreignId": "r-0008",
      "name": "s10-allow-0008",
      "ruleNumber": 80,
      "action": "ALLOW",
      "sources": [
        "net-h-001"
      ],
      "destinations": [
        "net-c-000"
      ],
      "services": [
        "sg-000"
      ],
      "description": "net-h-001 -> net-c-000 on sg-000",
      "enabled": true
    },
    {
      "foreignId": "r-0009",
      "name": "s10-allow-0009",
      "ruleNumber": 90,
      "action": "ALLOW",
```

```
                "sources": [
                  "net-h-002"
                ],
                "destinations": [
                  "net-h-000"
                ],
                "services": [
                  "svc-tcp-000"
                ],
                "description": "net-h-002 -> net-h-000 on svc-tcp-000",
                "enabled": true
              },
              {
                "foreignId": "r-0010",
                "name": "s10-deny-0010",
                "ruleNumber": 100,
                "action": "DENY",
                "sources": [
                  "net-h-003"
                ],
                "destinations": [
                  "net-h-000"
                ],
                "services": [
                  "svc-udp-000"
                ],
                "description": "net-h-003 -> net-h-000 on svc-udp-000",
                "enabled": true
              }
            ]
          }
```


c) Click **Next**.

4. Place the imported policy in the policy hierarchy and name its ruleset.

Figure 58: Insert in policy hierarchy



a) Optional: Enter a name in **New policy name**.

   If you leave this field blank, the import uses the policy name you specified in the **Choose policy** step.

b) Optional: Under **Parent policy**, select the policy under which you want to place the imported policy.

   If this is your first policy, don't select a parent policy.

c) Review **Ruleset name** and change it if needed.

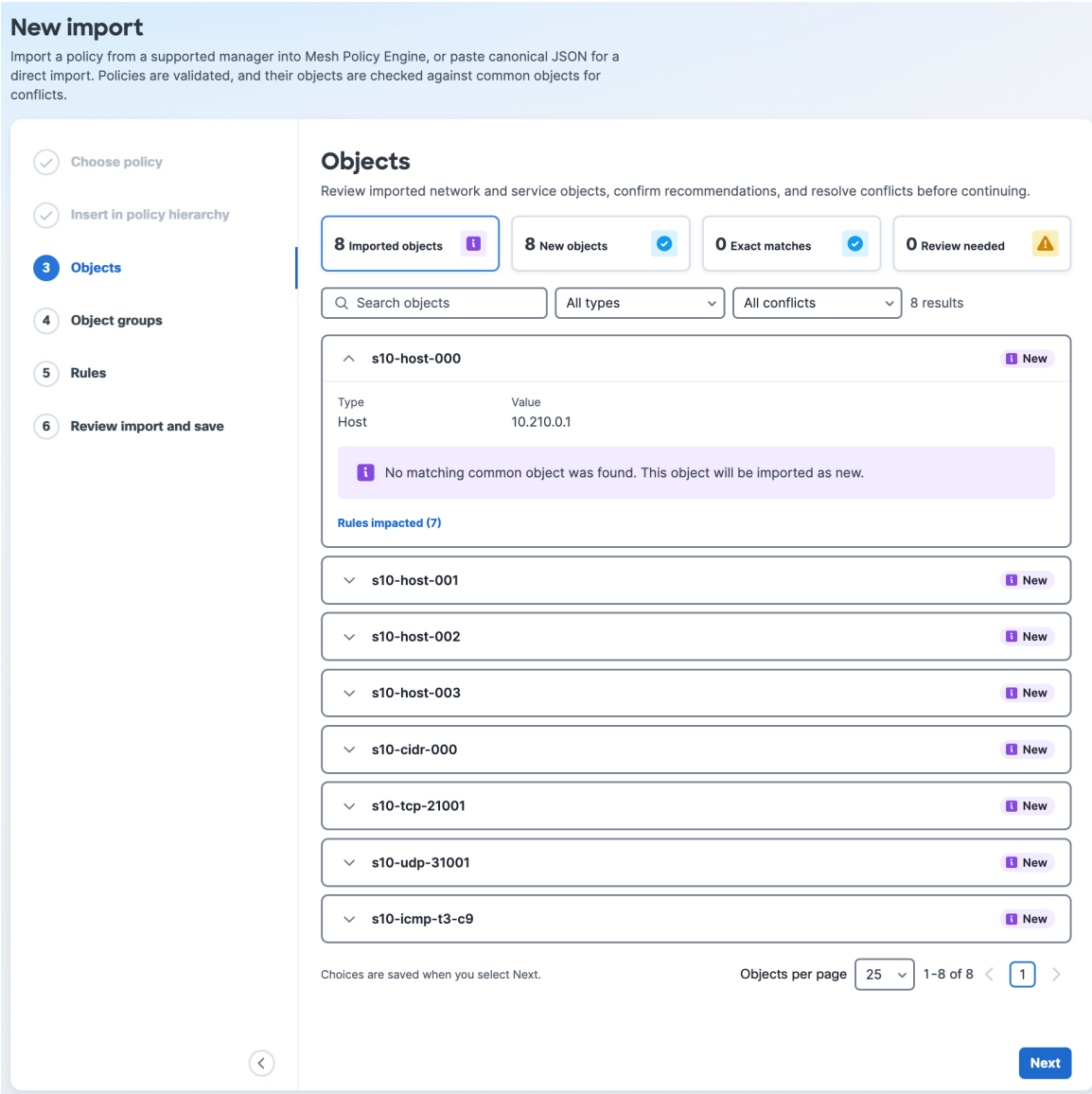
   The import creates a ruleset with this name for the imported rules.

d) Click **Next**.

5. On the **Objects** page, review each imported network or service object, resolve any conflicts, and click **Next**.

   Expand an object to see its details and the rules it affects. Use the summary cards and filters to find objects that need review.

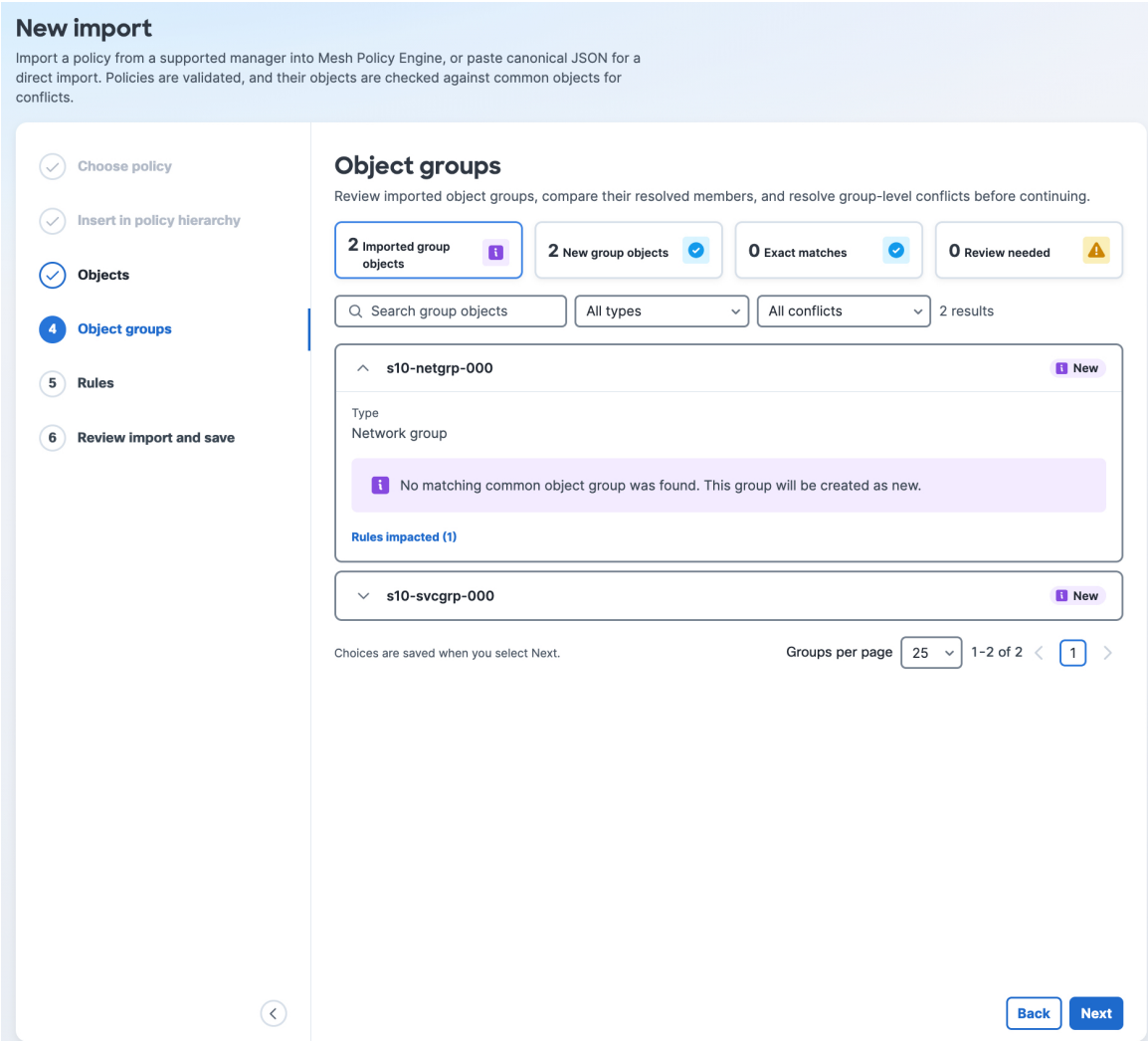
Figure 59: Review imported objects



6. On the **Object groups** page, review the imported groups, resolve any conflicts, and click **Next**.

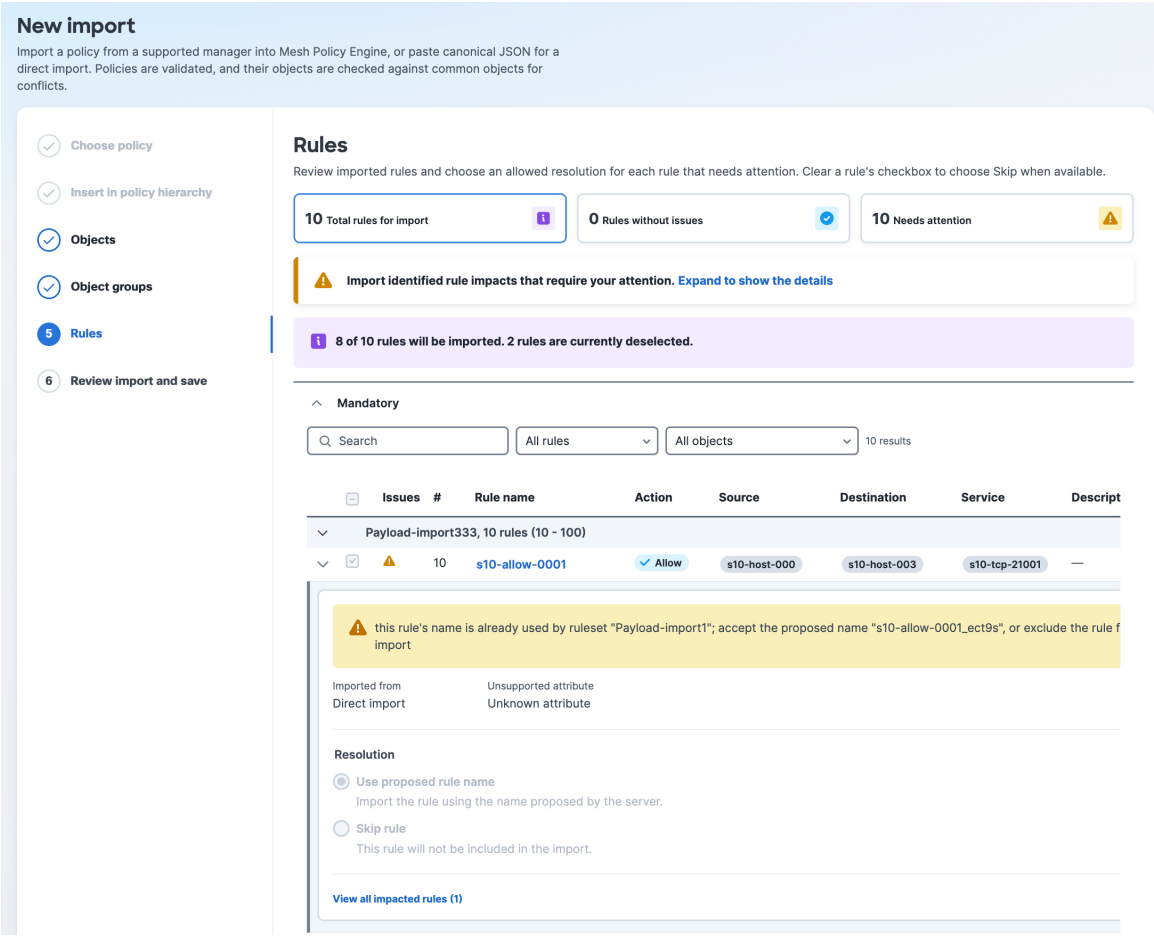
   Expand a group to review its members and the rules it affects. Compare it with any matching common object group before you continue.

Figure 60: Review imported object groups



7. On the **Rules** page, review the imported rules, choose a resolution for each rule that needs attention, and click **Next**. Expand a rule to see its issues and available resolutions. To skip a rule, clear its checkbox when the option is available.

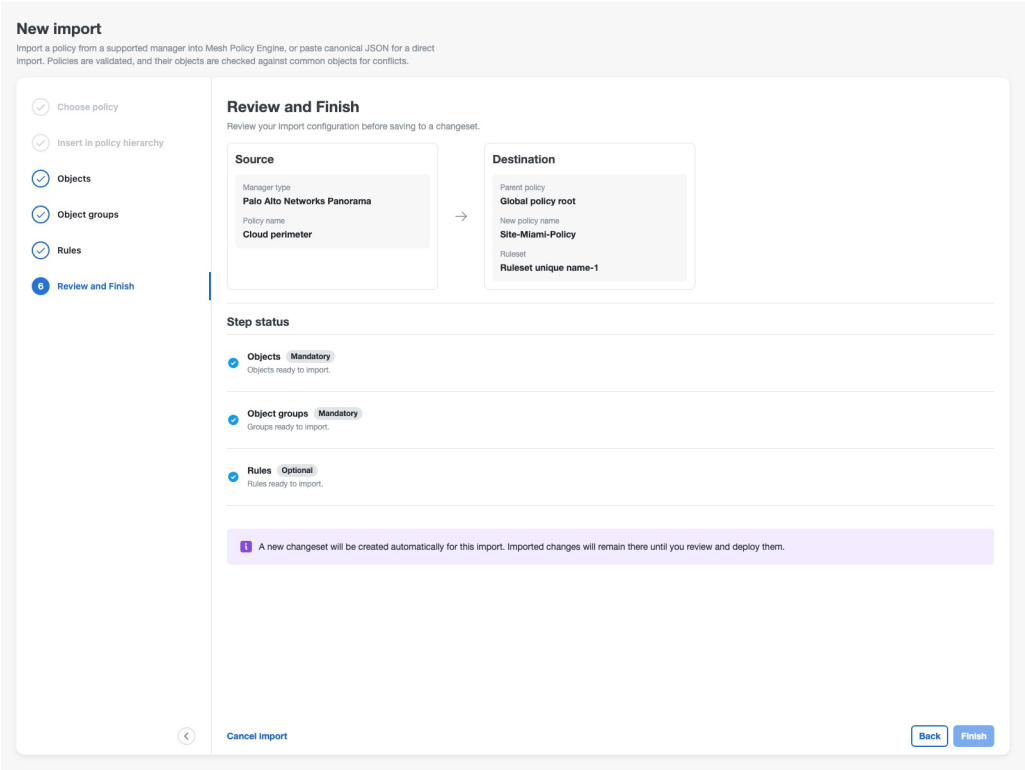
Figure 61: Review imported rules



8. On the **Review and finish** page, review the details and click **Finish**.

   You can't finish the import if you haven't resolved all your conflicts. If you have unresolved issues, go back to previous steps to finish the tasks.

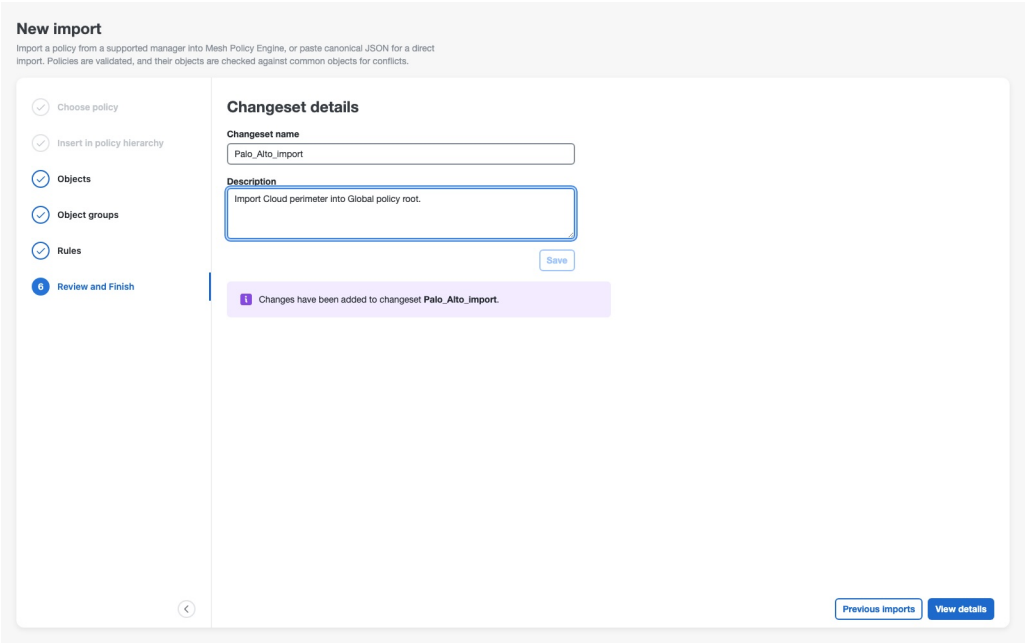
Figure 62: Review and finish the policy import



After you click **Finish**, you are shown the changeset created for your import. Either accept the default name or enter a new name. If you add a **Description**, click **Save**.

To view the changeset, click **View details**. **Previous imports** takes you back to the import list.

Figure 63: Changeset details for an imported policy



View policies

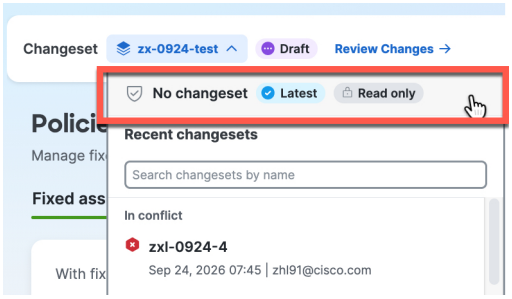
View the latest committed policy and inspect its rulesets and rules. Show inherited rules to understand the complete policy for a child.

View the latest committed policy and inspect its rulesets and rules. Show inherited rules to understand the complete policy for a child.

Procedure

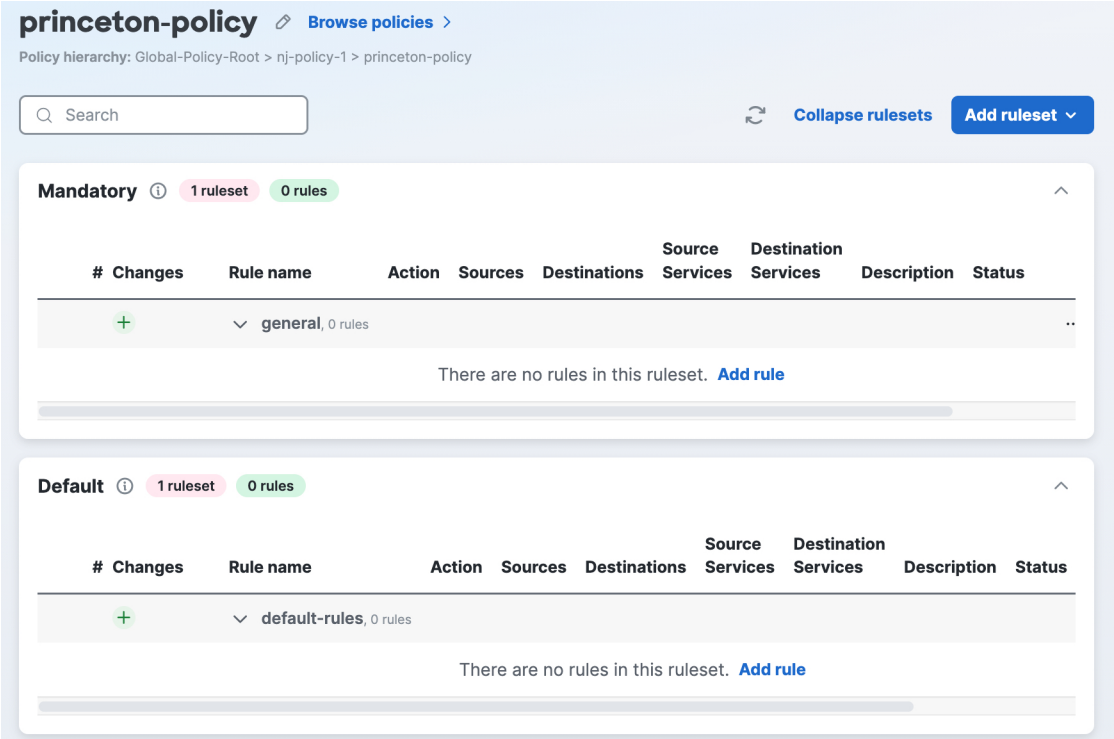
1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. View the latest committed policy.
   a) Select **Policies**.
   b) At the top of the screen, select **No changeset**.

   Figure 64: Select No changeset



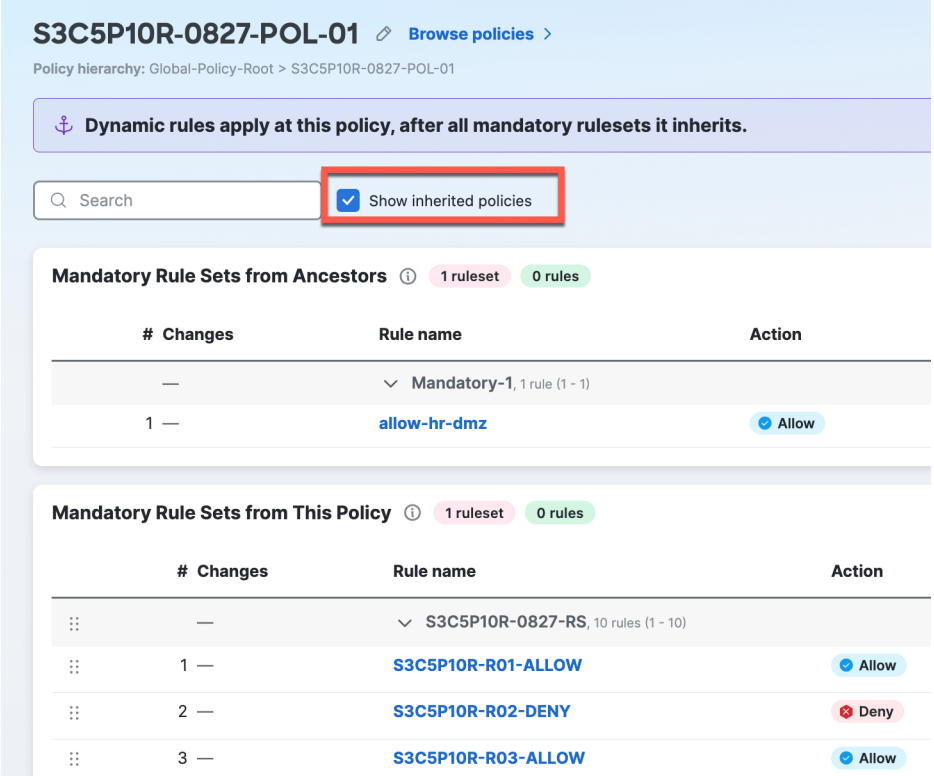
3. Click the policy name to view the policy.

   Figure 65: Policy rulesets and rules



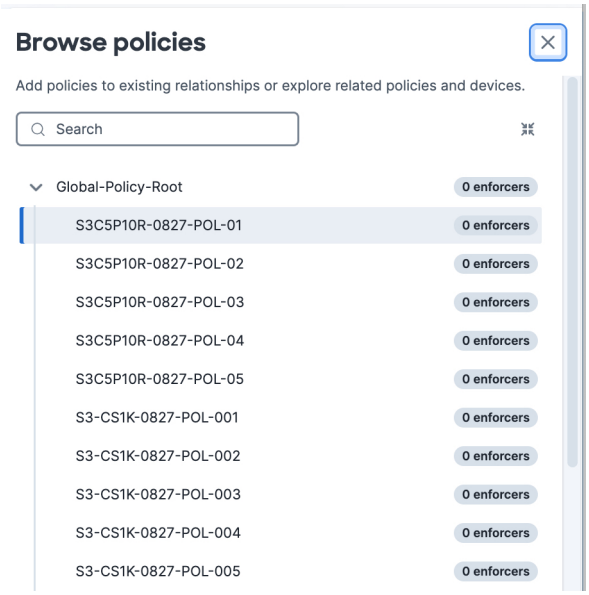
4. To view rules from parent policies, click **Show inherited policies**.

Figure 66: Show inherited policies



5. Click **Browse policies** to view this policy in the hierarchy and quickly select another policy.

Figure 67: Browse policies drawer



4 Changesets

Topics:

- About Changesets
- Changeset workflow
- Create and use a changeset
- Update the changeset to the latest policy
- Resolve conflicts
- Commit a changeset

Find a brief definition of changesets and their role in collecting policy edits before you commit those edits to the latest policy.

A changeset is a formal collection of changes or change commits made to a policy.

About Changesets

Learn how changesets help you collect and review policy edits before you commit them. Understand how concurrent edits can affect the latest policy.

A changeset is a formal collection of changes made to a policy. You must select a changeset before making any changes. When you're ready, you can commit the changeset; after resolving any conflicts created by concurrent changeset commitments, your changeset is merged into the policy. You can then deploy the latest policy to enforcers.

When you add or make changes to network or service objects as part of a rule change, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane. Object changes will be included in a deployment even if you don't have any committed changesets.

Changeset workflow

Find details about the changeset workflow, from collecting policy edits through updating and committing them. Use it to understand when conflicts require attention.

You must use a changeset to collect one or more changes you want to make to a policy.

> **Note**
>
> When you add or make changes to network or service objects as part of a rule change, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane. Object changes will be included in a deployment even if you don't have any committed changesets.

1. **Create and use a changeset on page 69**.

   You will add all policy changes to the changeset.

   a. Create a new changeset.

      You can only create a changeset from the latest committed policy. By default, the name is prefilled with *your_name-date*.

   b. Create additional changesets.

      You can create multiple changesets. However, after you commit a changeset, other changesets are now based on a previous revision of the policy unless you update to the latest.

   c. Make a changeset active to gather policy changes.

2. (Optional) **Update the changeset to the latest policy on page 71**.

   If previous changesets were committed, but you need to make more changes, we recommend that you manually update your changeset to the latest policy so that you can have an accurate base to work on.

> **Note**
>
> If your changeset shows conflicts, you must resolve the conflicts before you can view the latest policy.

3. **Resolve conflicts on page 72**.

   If there are conflicts due to earlier changeset commits, you need to resolve them before trying to commit.

4. **Commit a changeset on page 81**.

   When you commit a changeset, the changeset is merged to create the latest revision.

Create and use a changeset

Create a changeset to collect policy edits, then select it when you work on policies. Review or remove changesets as needed.

Create or select a changeset to gather all policy edits. You can make up to 2500 changes per changeset.

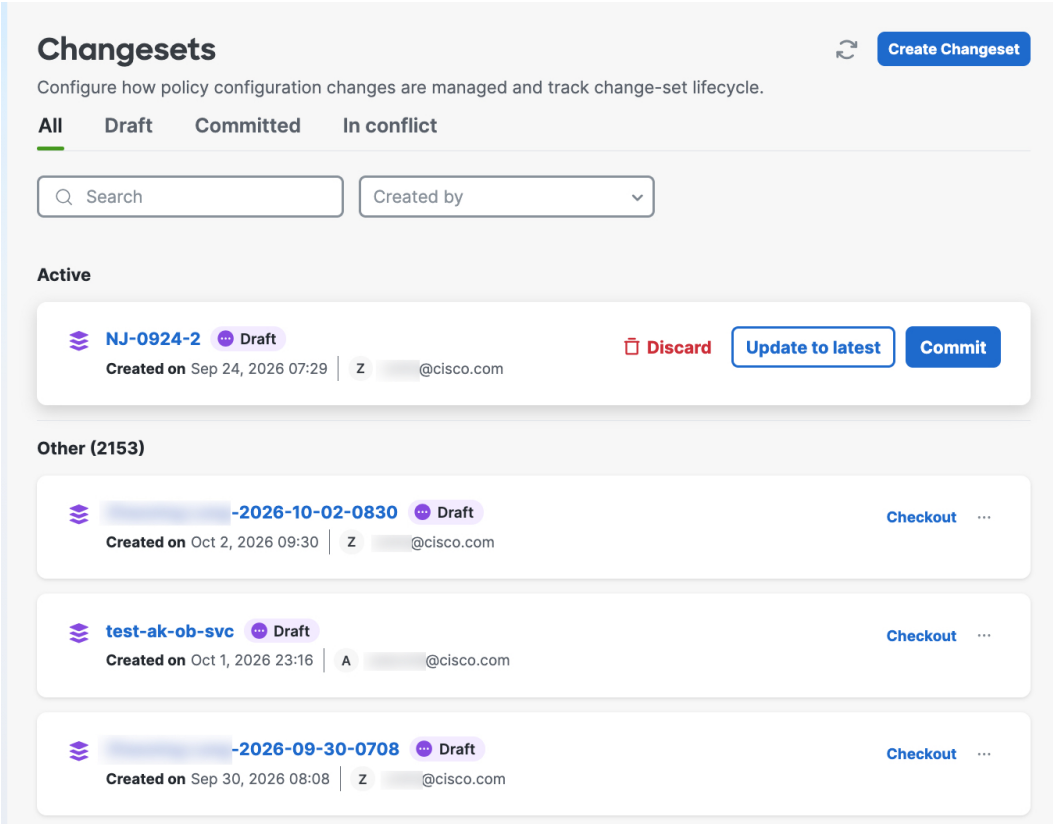
> **Note**
>
> When you add or make changes to network or service objects as part of a rule change, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane. Object changes will be included in a deployment even if you don't have any committed changesets.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Select **Changesets**.

   If you have an active changeset selected, it will show at the top.

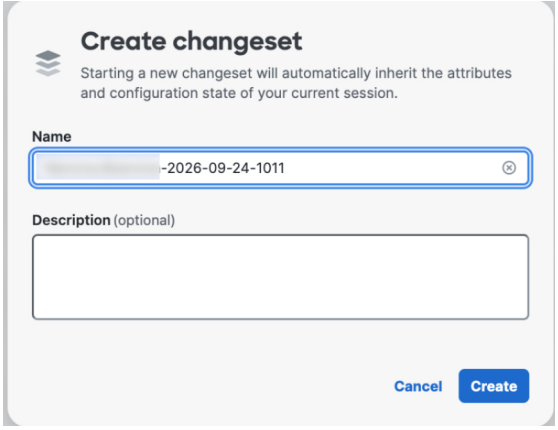
   Figure 68: Changesets



3. Click **Create Changeset**, either accept the default **Name** or enter your own name and optional **Description**, and then click **Create**.

   Alternatively, you can create a changeset from the drop-down list at the top of the **Policies** page.

   Figure 69: Create changeset

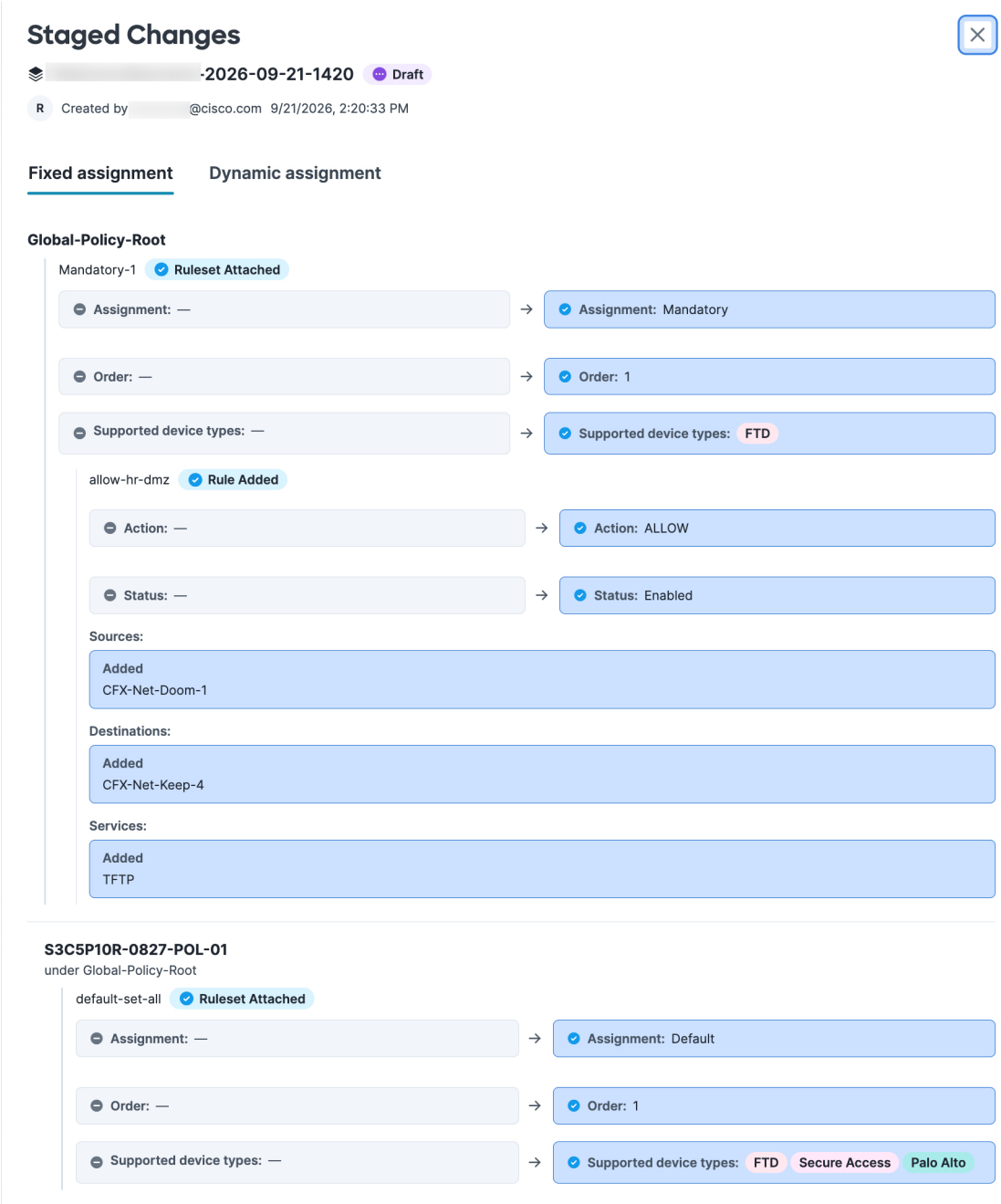


4. To select the changeset for policy changes, click **Checkout** to the right of the policy name.

   Alternatively, you can select a changeset at the top of the **Policies** page. If you try to make changes to a policy, you will be prompted to select or create a changeset.

5. Click the changeset name to view an overview of in-progress changes.

   Figure 70: Staged changes



6. To delete a changeset, click the More icon (•••) and click **Delete**.

Update the changeset to the latest policy

Update an existing changeset to the latest committed policy before continuing your edits.

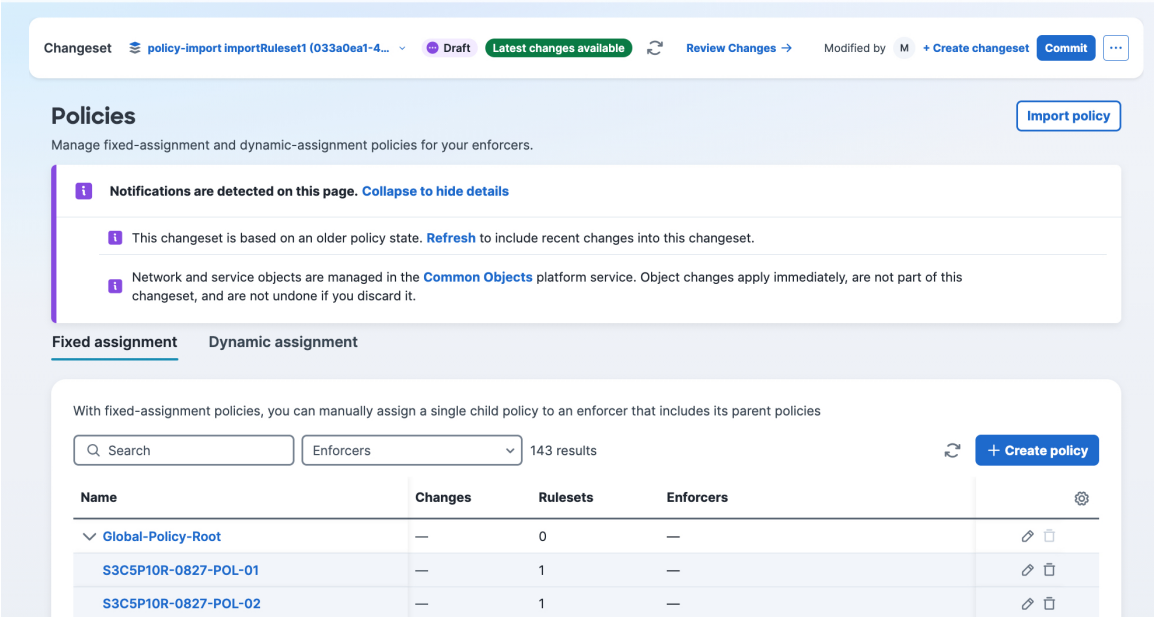
After someone commits another changeset, your changeset will be based on an older policy revision. You should update the changeset to the latest before you continue making changes to avoid creating additional conflicts.

> **Note**
>
> If your changeset shows conflicts, you must resolve the conflicts before you can view the latest policy.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Select **Policies**.
3. At the top of the screen, select the Draft changeset that you want to update.
4. Click the Refresh icon ( ).

   Figure 71: Refresh a changeset based on an older policy state



5. If the update reveals conflicts, review and resolve them before you commit the changeset.

Resolve conflicts

Resolve changeset conflicts before you commit policy updates. Review competing edits and choose the changes you want to keep.

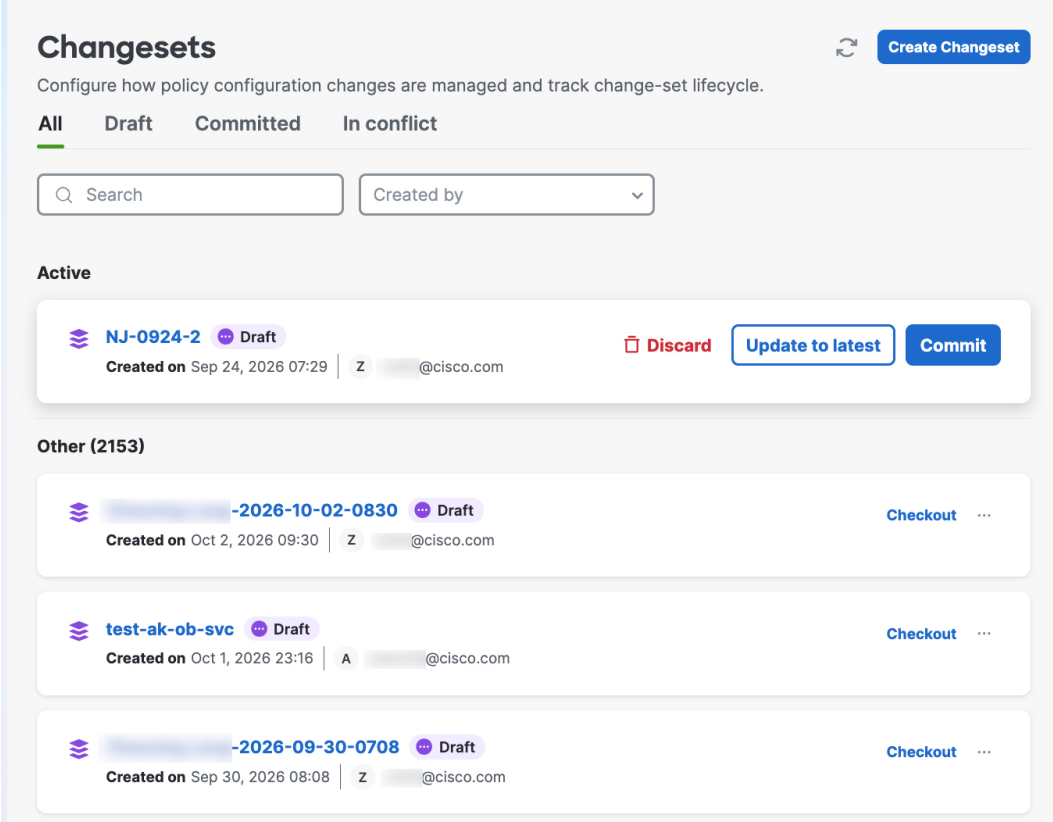
A conflict can occur when the same item is edited by two different users, and they both commit their edits; whichever commit occurs second will have to resolve the conflict by either reverting the edit, enforcing its edit, or making a different edit. You must resolve all conflicts before you commit the changeset.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Select **Changesets**.

If you have an active changeset selected, it will show at the top.

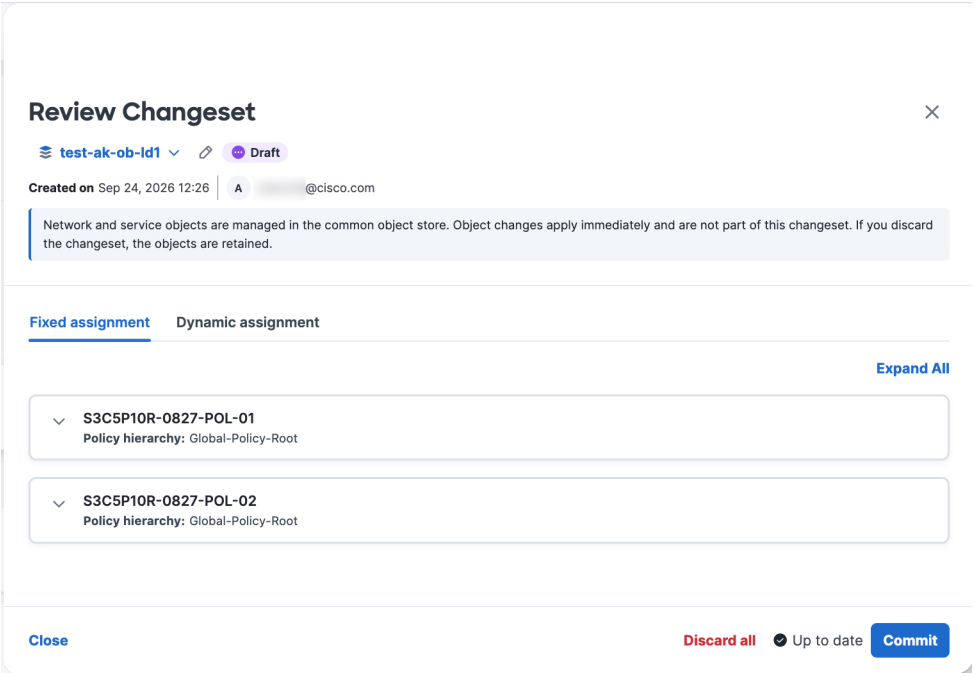
Figure 72: Changesets



3. Click the changeset name, and if the changeset isn't active, click **Checkout**.

   After the changeset is checked out, it lets you perform actions such as resolving conflicts, committing, or discarding changes.

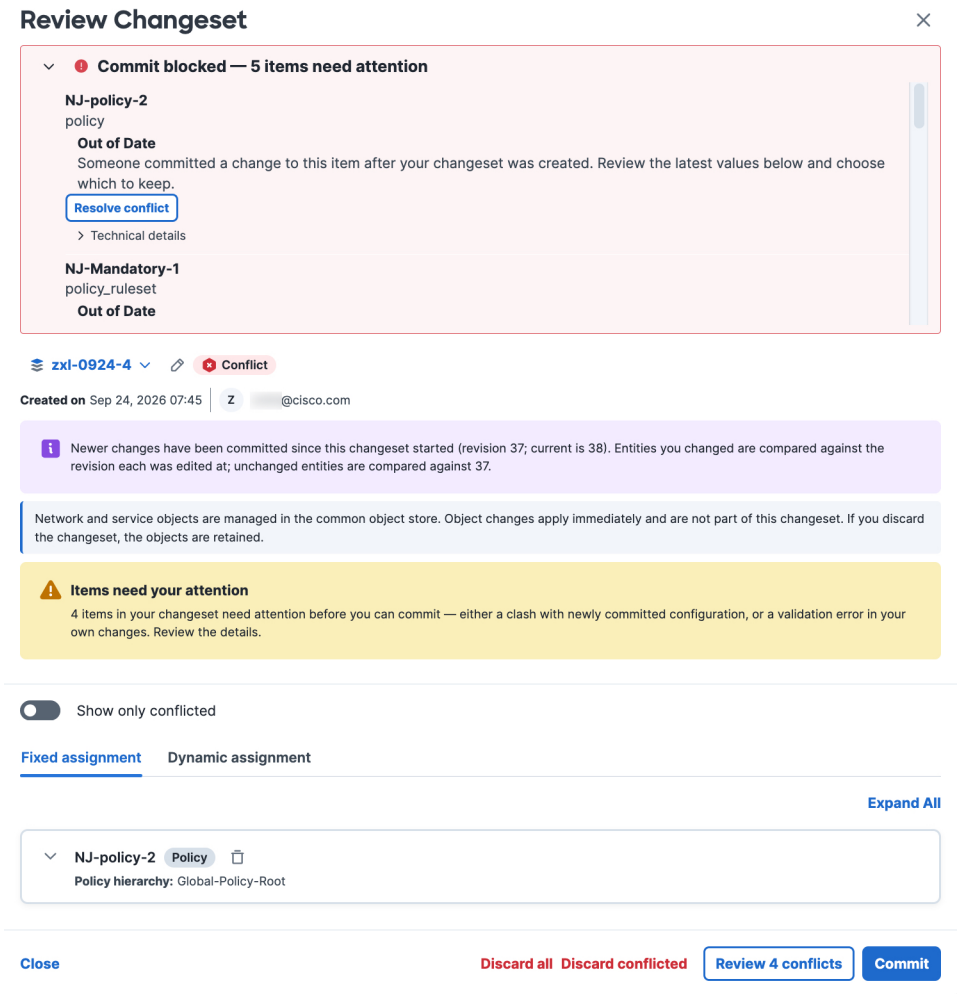
Figure 73: Review changeset



4. Click **Review** *x* **conflicts**.

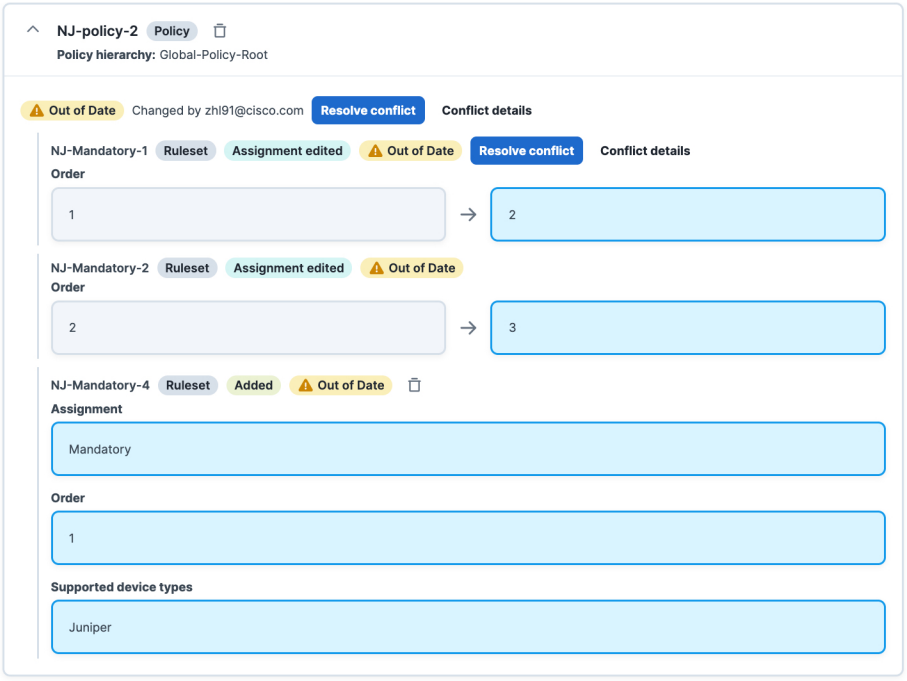
   Each conflict is listed at the top.

Figure 74: Review changeset conflicts



You can also view conflict details within the hierarchy at the bottom:

Figure 75: Review changeset conflicts



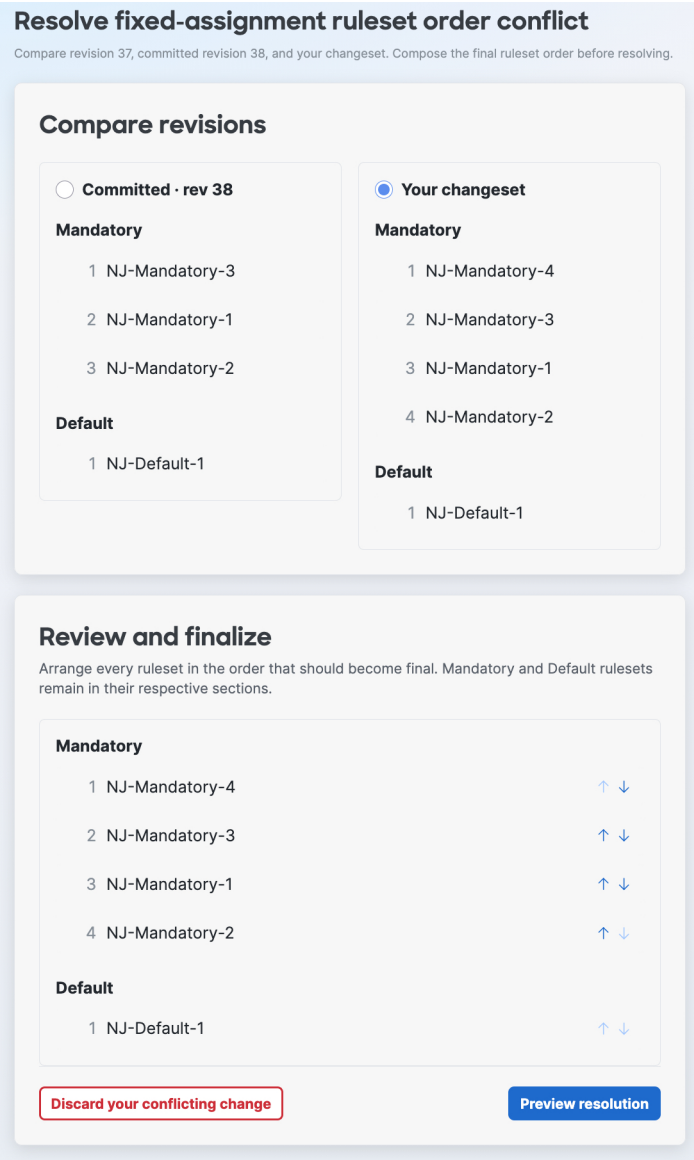
5. Resolve each conflict.

   The exact resolution depends on the type of conflict.

   a) Click **Resolve conflict**.

      In this example, the conflict that is being detected is a new ruleset that was placed in position 1, which changes the position of the existing rulesets.

      Figure 76: Resolve ruleset order conflict



b) If you want to revert to the committed version, click **Discard your conflicting change**.

   Otherwise, continue to the next step.

c) If you still want to make a change, choose either the **Committed** version or **Your changeset** version as your starting point.

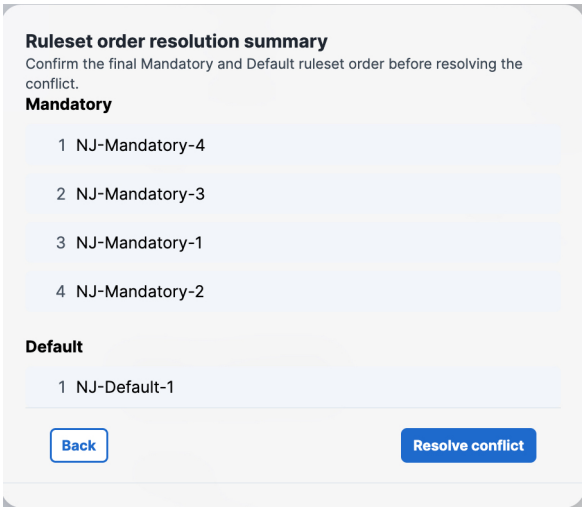
   In this example, the committed version is missing the NJ-Mandatory-4 ruleset, so if you want to include that ruleset, you need to start from **Your changeset**.

d) Make any additional changes in the **Review and finalize** area.

   In this example, you can change the order of the rulesets.

e) Click **Preview resolution**.

Figure 77: Ruleset order resolution summary

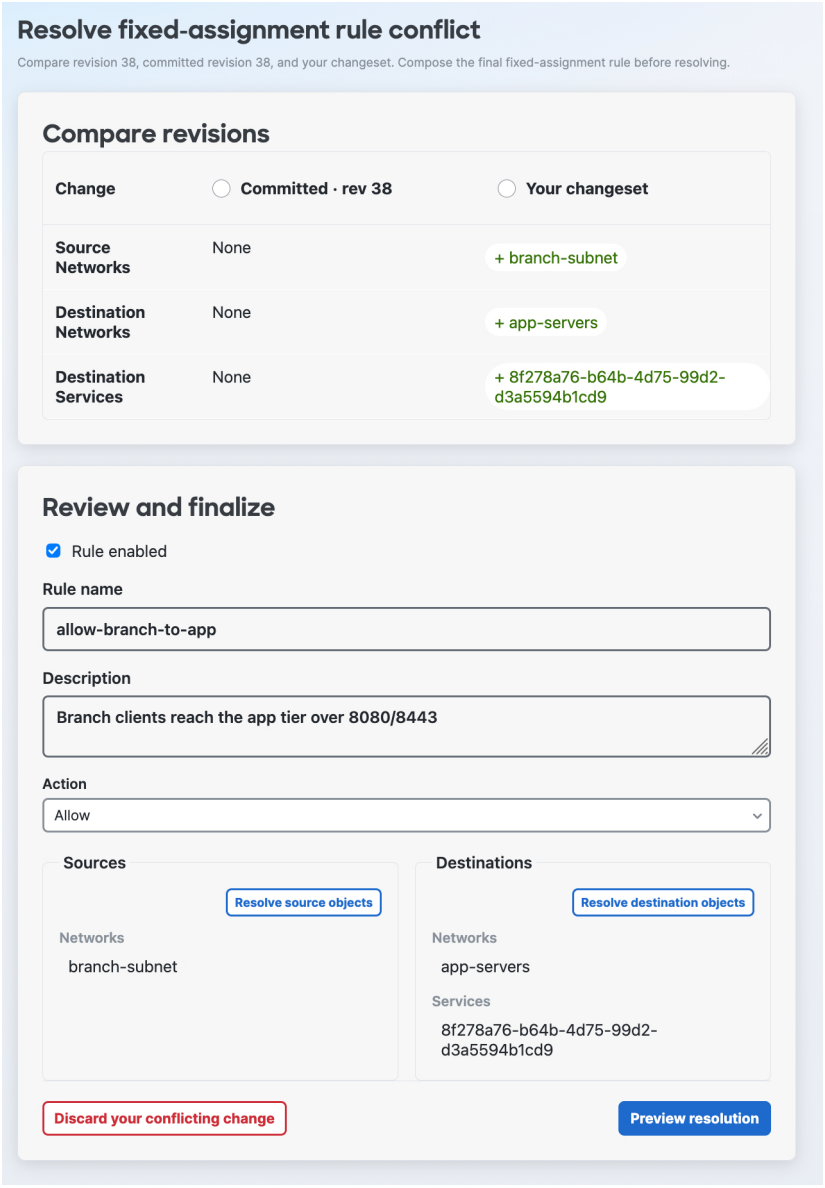


f) Click **Resolve conflict** to accept the solution.

Rule conflict example

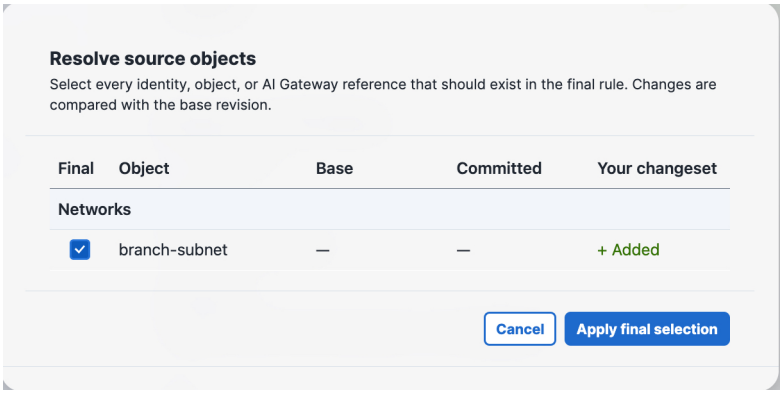
In this example, a rule had new source and destination networks and ports added. You can see that the rule didn't yet have any networks or services defined. In addition to the changed fields, you can change basic settings like whether the rule is enabled, the name, the description, and the action.

Figure 78: Resolve rule conflict



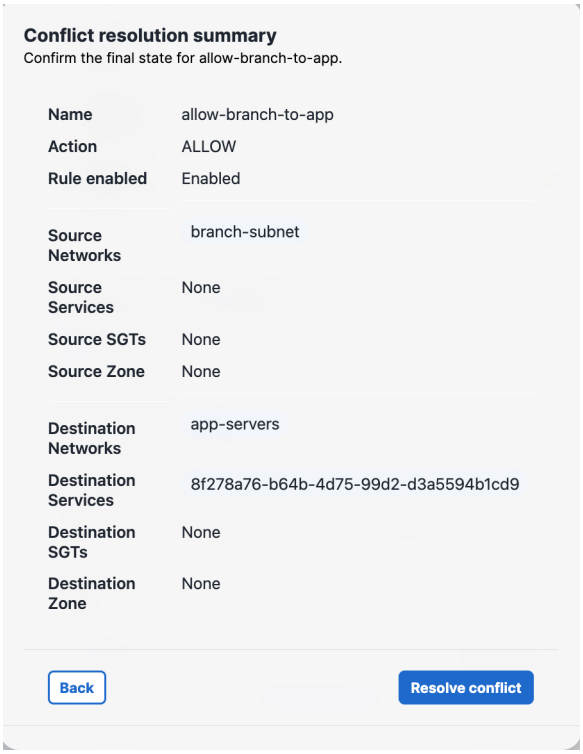
For each changed field, you can accept the new value or you can revert to the original value. You can't choose a new value altogether from the common object store.

Figure 79: Resolve source objects



The summary shows the final values.

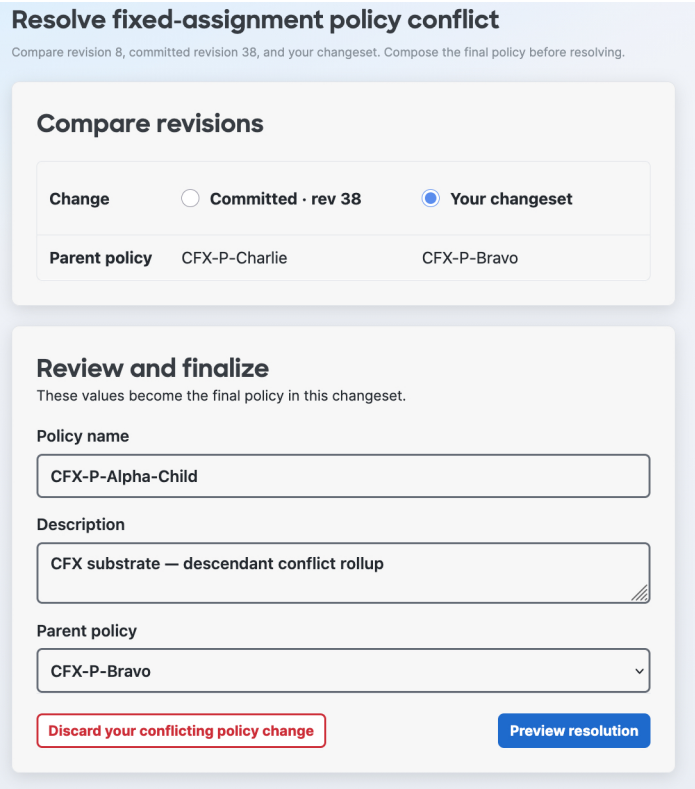
Figure 80: Conflict resolution summary



Parent policy conflict example

In this case, a different parent policy was chosen. You can choose any new parent policy to resolve the conflict, including the committed one or the new one. You can also change the policy name and description.

Figure 81: Resolve policy conflict



Commit a changeset

If your changeset doesn't have any conflicts, you can commit the changes.

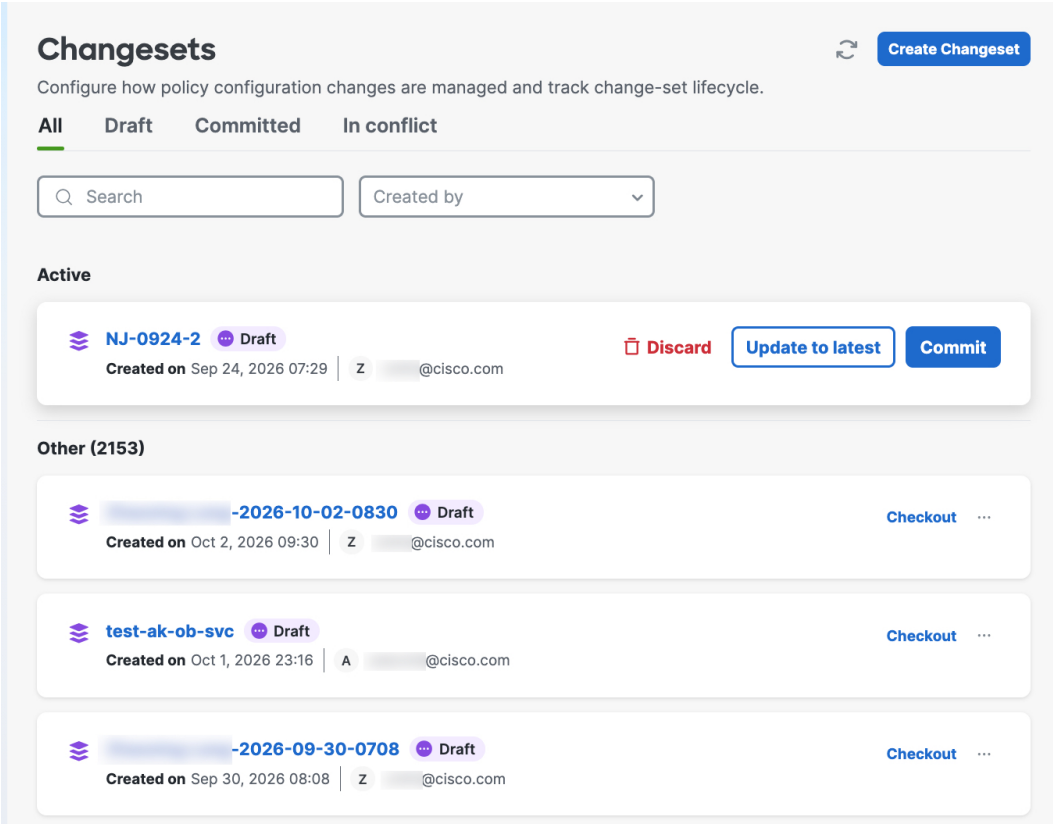
Commit your changeset to merge your changes into the policy.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Select **Changesets**.

   If you have an active changeset selected, it will show at the top.

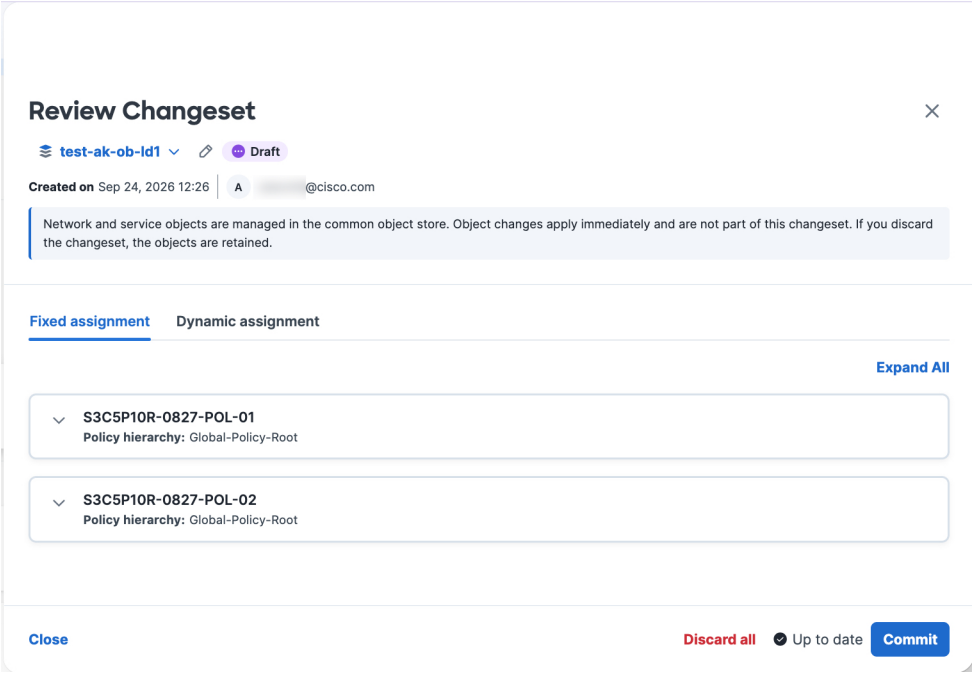
   Figure 82: Changesets



3. Click the changeset name, and if the changeset isn't active, click **Checkout**.

   After the changeset is checked out, it lets you perform actions such as resolving conflicts, committing, or discarding changes.

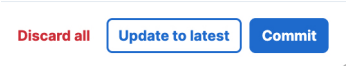
Figure 83: Review changeset



4. If there are conflicts, see Resolve conflicts on page 72 before continuing. You can't commit a changeset with any conflicts or validation errors.

5. If you see **Update to latest** at the bottom, click the button. This state means that other changesets were committed since you created your changeset. This action lets you see the latest policy.

   Figure 84: Changesets



6. Click **Commit**.

   When you add or make changes to network or service objects as part of a rule change, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane. Object changes will be included in a deployment even if you don't have any committed changesets.

5 Deployments

Topics:

- About deployments
- Deploy policy changes to enforcers
- View deployments

Find an overview of how to deploy committed policy changes to enforcers and where to review the results of each deployment.

Deploy the policy to your enforcers.

About deployments

Learn what a policy deployment includes and how to review past deployment results for enforcers, including failures that need your attention.

You can choose one or more enforcers and deploy the committed policy. Each enforcer receives the applicable parts of the policy depending on its type. For example, a Palo Alto Networks enforcer will receive the rulesets of its assigned policy and its parent policies that have Palo Alto Networks specified; it won't receive any rulesets that aren't tagged for Palo Alto Networks.

When you add or make changes to network or service objects as part of a rule change, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane. Object changes will be included in a deployment even if you don't have any committed changesets.

You can also view past deployments and any reasons why they might have failed.

Deploy policy changes to enforcers

Deploy committed policy changes to selected enforcers and review the changes before starting deployment. Check that each enforcer receives the intended policy.

Deploy the policy to your enforcers.

Before you begin

- Commit the changeset that includes the policy changes you want to deploy. Commit a changeset on page 81.

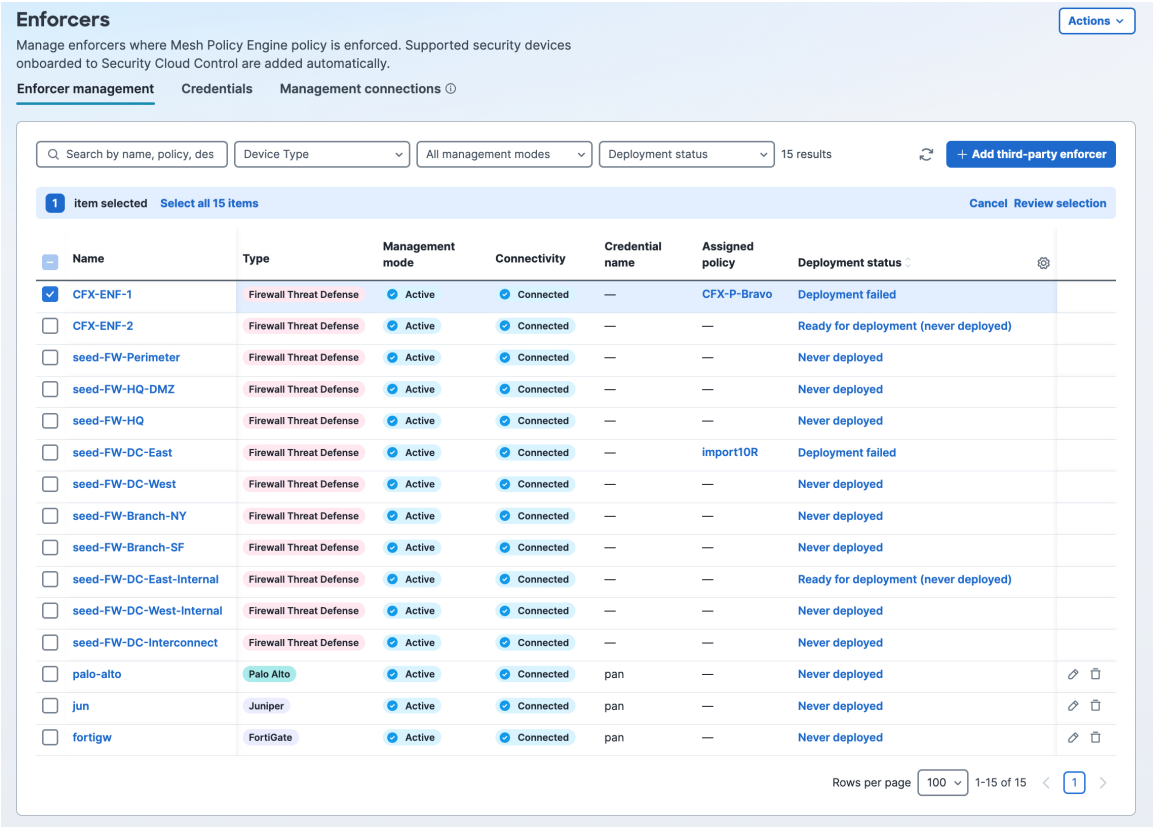
> **Note**
>
> When you add or make changes to network or service objects as part of a rule change, the objects are saved immediately and not collected with the changeset. Objects are managed as part of the common object store, accessible by selecting **Common Objects** in the left pane. Object changes will be included in a deployment even if you don't have any committed changesets.

- Assign each enforcer to a fixed-assignment policy. Create a fixed-assignment policy on page 37.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Choose **Enforcers** > **Enforcer management**.

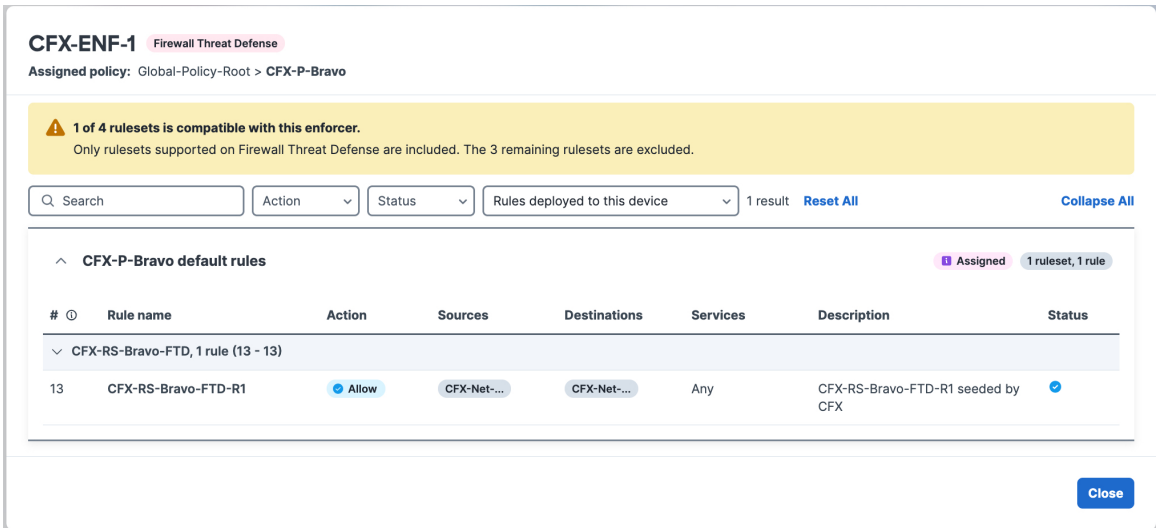
Figure 85: Enforcer management



You can use the filters at the top to view devices by name, policy, description, type, management mode, or deployment status.

3. To view the entire policy to be deployed to a given enforcer, click the **Assigned policy** name.

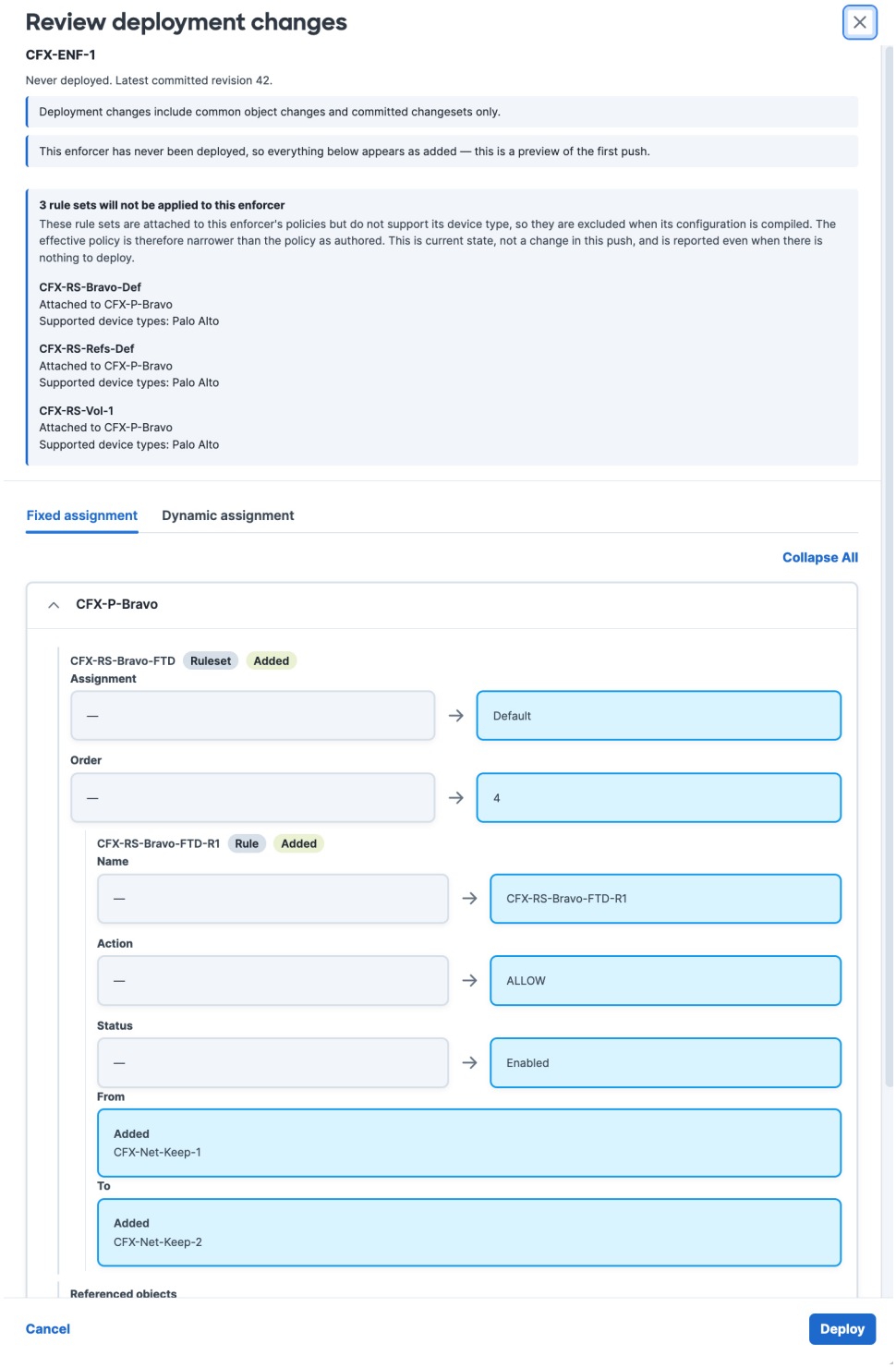
Figure 86: Rulesets and rules deployed to an enforcer



The **Rules deployed to this device** option is selected. You can see the full policy, including rulesets that don't apply to this enforcer, by selecting **All rules across policies**.

4. Optional: In the **Last deployment** column, click **Ready for deployment** to see the pending changes for each enforcer.

Figure 87: Review deployment changes

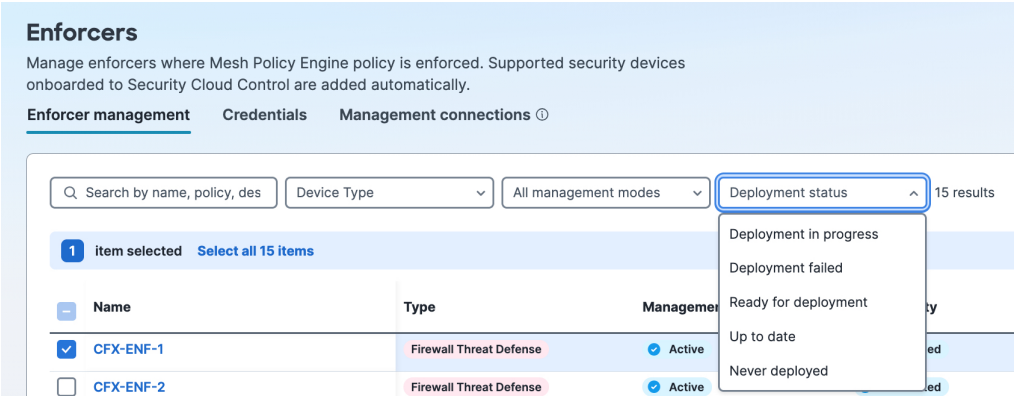


Fixed-assignment rulesets that will not be applied to this enforcer are listed at the top.

5. Click the checkbox next to the enforcers you want to deploy to.

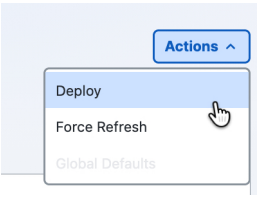
   You can filter on **Deployment status >** > **Pending deployment** to see all of the enforcers that you can deploy to.

Figure 88: Filter enforcers by deployment status



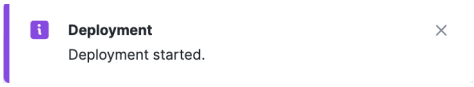
6. Choose **Actions** > > **Deploy**.

Figure 89: Actions menu



You see a message that deployment has started.

Figure 90: Deployment started



7. Go to the **Deployment Logs** page to check the status of the deployment. If a deployment succeeds, you will see the **Last deployment** column updated. Otherwise, check other statuses on the **Deployment Logs** page: View deployments on page 89.

View deployments

View deployment history to check policy status, affected enforcers, and details of failed deployments. Use the results to investigate problems.

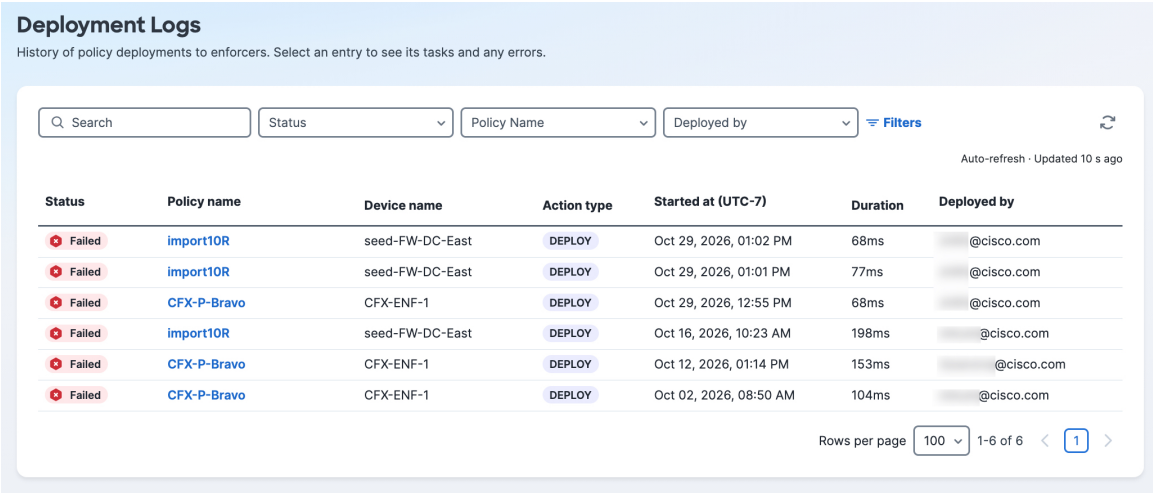
The **Deployment Logs** page shows each lowest-level child policy that was deployed to one or more enforcers. You can review the deployment status and the reasons for any failures.

Procedure

1. From the Security Cloud Control Home page, click **Mesh Policy Engine**.
2. Select **Deployment Logs**.

   Each enforcer and its policy is listed along with other details.

Figure 91: Deployment Logs



3. Click the policy name to view details.

Figure 92: Deployment Details

