Illumio Core®

Version 22.1.3

PCE Administration Guide

Legal Notices

Product Versions

PCE Version: 22.1.3 (Standard release) | Illumio Core Cloud customers only

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Resources

Legal information, see https://www.illumio.com/legal-information

Trademarks statements, see https://www.illumio.com/trademarks

Patent statements, see https://www.illumio.com/patents

License statements, see https://www.illumio.com/eula

Open source software utilized by the Illumio Core and their licenses, see Open Source Licensing Disclosures

Contact Information

To contact Illumio, go to https://www.illumio.com/contact-us

To contact the Illumio legal team, email us at legal@illumio.com

To contact the Illumio documentation team, email us at doc-feedback@illumio.com

Contents

Overview of PCE Administration

This chapter contains the following topics:

This section explains concepts that will help you with ongoing PCE operations and administration.

About This Administration Guide

The following sections give useful information to help you get the most out of this guide.

How to Use This Guide

This guide describes how to maintain and operate the Policy Compute Engine (PCE). It also includes other important tasks required to manage your PCE deployment.

Before Reading This Guide

Before attempting the procedures in this guide, you should be familiar with the following technology:

- Your organization's security goals
- Illumio Core

- General computer system administration of Linux and Windows operating systems, including startup/shutdown, common processes or services
- Linux shell (bash) and Windows PowerShell
- TCP/IP networks, including protocols and well-known ports
- PKI certificates

Notational Conventions in This Guide

- Newly introduced terminology is italicized. Example: *activation code* (also known as pairing key)
- Command-line examples are monospace. Example: `illumio-ven-ctl --activate`
- Arguments on command lines are monospace italics. Example: `illumio-ven-ctl --activate` *`activation_code`*
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row. Example:

```
...
some command or command output
...
```

PCE Architecture and Components

This section describes how the PCE functions, and provides an overview of its components and how they function together.

About the PCE Architecture

The PCE has service tiers responsible for various functions.
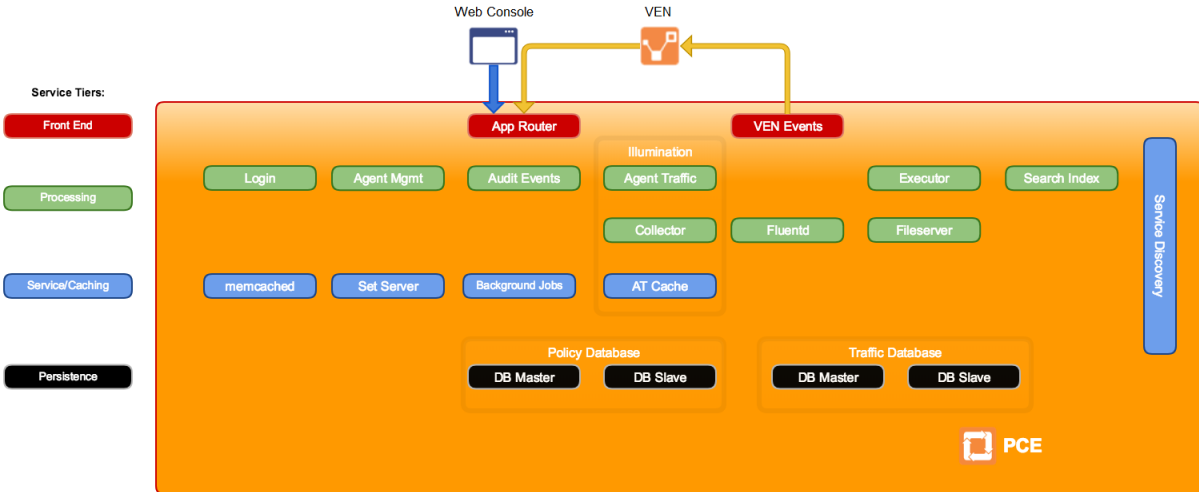
Description of PCE Components

Tier	PCE component	Description
Front-end	Management interfaces: PCE web console and VEN	Management interfaces include: • PCE web console • REST API • PCE command line • VEN command line
	VEN events	For information, see VEN Architecture and Components in the *VEN Administration Guide*.
	App Router	Directs requests to the proper service.

Tier	PCE com- ponent	Description
Processing	Login	Central server for authentication.
	Agent Man- ager	Manages data in the policy domain, such as workload context and policy definitions. Also, manages data for all user and organization authentication and author- ization, such as users, organizations, API keys, and roles.
	Agent Traffic	Provides information about traffic to and from VENs. Serves as the service underlying Illumination.
	Collector	Aggregates packet and traffic flow information sent from the VEN. Serves as the service underlying Illu- mination.
	Audit Events	Creates an overview of auditable system events across the PCE and VENs.
	Fluentd	Log forwarder service that forwards the flow log files received from VENs.
	Executor	Backbone for asynchronous job execution, such as report generation and background jobs.
	Fileserver	Central storage and retrieval for large data files.
	Search Index	Supports auto-completion in the PCE web console.
Service	memcached	Open source component: in-memory cache.
	Background Jobs	Backbone for asynchronous job execution, such as report generation and background jobs.
	Set Server	In-memory cache to aid in policy calculations.
	Agent Traffic cache	Stores the traffic flow data and graphs for Illumination. See Agent Traffic. In the PCE architecture diagram, labeled "AT Cache."
Persistence	Policy primary data- base and rep- lica	Postgres database that contains all the policy and agent related data. The primary and replica databases run on separate data nodes.
	Traffic data- base primary and replica	Postgres database that contains all the historical traffic flow data. Traffic Explorer is backed by this datastore. The primary and replica databases run on separate data nodes.

Management Interfaces for PCE and VEN

The following diagram illustrates the logical view of the management interfaces to the PCE and VEN.

PCE and VEN Management Interfaces
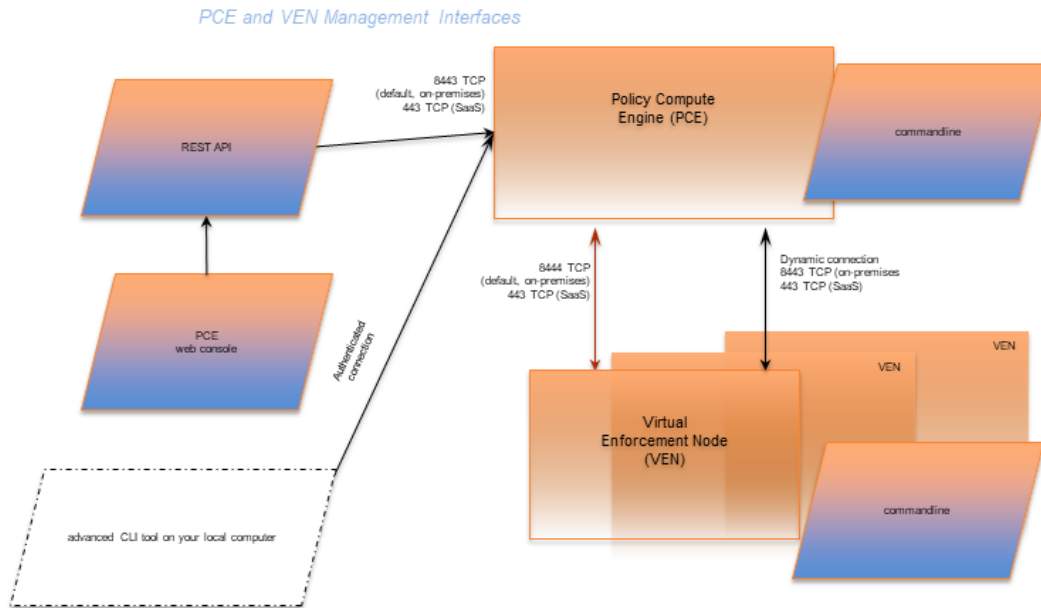
This guide focuses on the use of the `illumio-pce-ctl` control script and related administrative programs on the PCE itself.

Interface	Notes	See...
PCE web console	With the PCE web console, you can perform many common tasks for managing the Illumio Core.	*Visualization Guide*
PCE command line	Use of the command line directly on the PCE. The `illumio-pce-ctl` command-line tool is the primary management tool on the PCE. You can perform many common tasks for managing the Illumio Core, including installing and updating the VEN.	*PCE Administration Guide*
REST API	With the Illumio Core REST API, you can perform many common management tasks, such as automate the management of large groups of workloads, rather than each workload individually. The endpoint for REST API requests is the PCE itself, not the workload. The REST API does not communicate directly with the VEN.	*REST API Developer Guide*
VEN com-	The `illumio-ven-ctl` command-line tool is the	*VEN Administration*

Interface	Notes	See...
mand line	primary management tool for the VEN.	*Guide*

PCE Control Interface and Commands

The Illumio PCE control interface `illumio-pce-ctl` is a command-line tool for per-
forming key tasks for operating your PCE cluster, such as starting and stopping nodes,
setting cluster runlevels, and checking the cluster status.

> ❗ IMPORTANT:
> In this guide, all command-line examples based on an RPM installation.
> When you install the PCE using the tarball, you must modify the commands
> based on your PCE user account and the directory where you installed the
> software.

The PCE includes other command-line utilities used to set up and operate your PCE:

- `illumio-pce-env`: Verify and collect information about the PCE runtime envir-
  onment.
- `illumio-pce-db-management`: Manage the PCE database.
- `supercluster-sub-command`: Manage specific Supercluster operations.

The PCE control interface can only be executed by the PCE runtime user (`ilo-pce`),
which is created during the PCE RPM installation.

Control Command Access with `/usr/bin`

For easier command execution, PCE installation creates softlinks in `/usr/bin` by default
for the Illumio PCE control commands. The `/usr/bin` directory is usually included by
default in the `PATH` environment variable in most Linux systems. When your `PATH` does
not include `/usr/bin`, add it to your `PATH` with the following command. You might want
to add this command to your login files (`$HOME/.bashrc` or `$HOME/.cshrc`).

```
export PATH=$PATH:/usr/bin
```

Syntax of `illumio-pce-ctl`

To make it simpler to run the PCE command-line tools, you can run the following Linux
softlink commands or add them to your `PATH` environment variable.

```
$ cd /usr/bin
$ sudo ln -s /opt/illumio-pce/illumio-pce-ctl ./illumio-pce-ctl
$ sudo ln -s /opt/illumio-pce/illumio-pce-db-management ./illumio-pce-db-
management
$ sudo ln -s /opt/illumio-pce/illumio-pce-env ./illumio-pce-env
```

After these commands are executed, you can run the PCE command-line tools using the following syntax:

```
$ sudo -u ilo-pce illumio-pce-ctl sub-command --option
```

Where:

sub-command is an argument displayed by `illumio-pce-ctl --help`.

PCE Organization and Users

A PCE organization is a group of policies and users targeted toward a specific business group or unit, including all the networking security rules and people who are associated with the policy. An organization can contain any number of users, workloads, policy objects (rulesets, IP lists, services, and security settings), and labels.

Organizations are initially set up by your Illumio administrator. When an organization is created, an email is sent that contains a user login for the organization. When this user logs in, the organization is created, and users can now be invited to join.

RBAC Users Roles and Permissions

For information on creating local or external users and assigning PCE permissions to those users, see Role-based Access Control.

Invite Users to Your Organization

When you are an organization owner, you can invite other users to your organization and grant roles to specify permissions for those users.

When you invite a user to your organization, the user receives an email at the specified address that contains a link for their account setup. The link in invitation email is valid only for 7 days, after which it expires. If you invited a user who did not receive their email or did not sign up using that email, you can re-invite them.

External Users and Non-Email Usernames

When you use an external corporate Identity Provider (IdP) to authenticate users with the PCE, but your IdP usernames do not use email addresses, the PCE cannot send email invitations to those users when you add them to the PCE. When you add this type of user, send them a login URL that they can use to set up their Illumio Core accounts and log in to the PCE web console.

Invitation Emails Are Not Sent

When users you invite do not receive their invitation emails, the SMTP server might not be configured correctly with the PCE.

- Make sure that your PCE's IP address is allowed to relay messages and that its emails are not blocked by any anti-spam protection.
- Check your PCE's `runtime_env.yml` file to make sure that the `smtp_relay_address` value is correct.

Connectivity Configuration for PCE

This chapter contains the following topics:

This section describes how to configure connectivity to control access to network resources and communication between workloads.

Connectivity Settings

This section describes how to modify PCE settings that affect connectivity.

> ✅ **NOTE:**
> Permission to edit these settings is dependent on your role. See About Roles, Scopes, and Granted Access for information.

Private Data Centers

The PCE uses connectivity settings to decide whether workloads are allowed to communicate with each other in private datacenters, private clouds, and shared network environments (private datacenter and public cloud).

By default, the Private Data Center connectivity setting is set and intended for workloads that are hosted in private datacenters, which do not have duplicate IP addresses in the network. When your network environment hosts workloads in your own private datacenter and in a public cloud, and you want to change this setting, contact Illumio Support.

Offline Timers

You can configure Offline Timers in the PCE web console and choose appropriate set-tings for your workloads.

> NOTE:
> To configure Offline Timers, you must be the Global Organization Owner for your PCE or a member of the Global Administrator role. See About Roles, Scopes, and Granted Access for information.

> WARNING:
> Disabling the Offline Timer setting degrades your security posture because the PCE will not remove IP addresses that belonged to workloads that have been disconnected from those that were allowed to communicate with the disconnected workloads. You need to remove the disconnected workloads from the PCE to ensure that its IP addresses are removed from the policy.

The PCE isolates a workload from the other workloads when the workload goes off-line. The VEN sends a heartbeat message every 5 minutes and a goodbye message when it is gracefully shutdown. The PCE marks a workload offline when these con-ditions occur:

- The PCE hasn't received a heartbeat message from the VEN for 3600 seconds (1 hour).
- The PCE receives a goodbye message from the VEN.

You can change the default Offline Timer settings before putting your workloads in enforcement under the following conditions:

- The default setting might potentially disrupt your critical applications.
- Application availability is more important than security.

> NOTE:
> How you configure this setting is a tradeoff between benefiting from an increased zero-churn outage time window versus increasing the window of time where IP addresses could be reused. You should weigh the operational and security benefits and find a balance suitable for your applications.

Decommission and IP Cleanup Timer

Sets the time period to wait after a managed workload sends a goodbye message to mark it offline. By default, the *High Security* setting is *Wait 15 minutes before IP Cleanup*. This default setting has the following affect on the PCE:

1. Listens for Goodbye messages from the VEN.

> ✅ NOTE:
> The default VEN goodbye timeout was increased from zero to 15 minutes. When required, you can reset it to 0.

2. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the removed workloads.
3. Immediately cleans up those workloads IP addresses from its active policy.

Disconnect and Quarantine Timer

Sets the time period to wait with no heartbeat before a managed workload is marked offline.

By default, the *High Security* setting is *Wait One Hour before Timeout*. This default setting has the following affect on the PCE:

1. Waits for an hour for the disconnected workloads to heartbeat and then quarantine those workloads that do not respond at the end of the hour.
2. Removes the quarantined workloads IP addresses from its active policy.
3. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the quarantined workloads.

Edit Offline Timers Settings

Edit the Offline Timers setting to change the values from the default settings.

1. From the PCE web console menu, choose **Settings** > **Offline Timers**.

   The Settings page for Offline Timers appears, which displays the current settings for the timers.

2. Click **Edit** to change the settings from the default values.

3. **Disconnect and Quarantine Timer:** Select a setting from the drop-down list to change the value from the High Security (Default) setting:

- ○ *Never Timeout or Quarantine - Highest Availability*

  This setting has the following affect on the PCE:

  - ■ Never disconnects or quarantines workloads that fail to heartbeat.
  - ■ Keeps all IP addresses in policy and never automatically removes unused IP addresses.
  - ■ Requires a removal of those unused IP addresses.

- ○ *Custom Timeout - Wait a Specified Time before Quarantine*

  Enter a time period; the minimum wait time is 300 seconds.

  The PCE performs the following actions:

  a. Waits for the specified time period for the disconnected workloads to heartbeat.
  b. Quarantines those workloads that do not respond at the end of that time period.
  c. Removes the quarantined workloads IP addresses from its active policy.
  d. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the quarantined workloads.

4. **Decommission and IP Cleanup Timer:** Select a setting from the drop-down list to change the value from the Highest Security (Default) setting:

   - ○ *Never clean up - Highest Availability*

     This setting has the following affect on the PCE:

     - ■ Ignores Goodbye messages from workloads.
     - ■ Keeps all IP addresses in policy and never automatically remove unused IP addresses.
     - ■ Requires a removal of those unused IP addresses.

   - ○ *Custom Timeout - Wait a Specified Time before IP Cleanup*

     Enter a time period; the minimum wait time is 0 seconds.

     The PCE performs the following actions:

     a. Listens for Goodbye messages from the VEN.
     b. Waits for the specified time period before cleanup of those work-loads IP addresses from its active policy.

c. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the removed workloads.

5. Click **Save**.

A message appears displaying your current and new settings.

6. Click **OK** to save the new settings.

Set the IP Version for Workloads

This section describes how to enforce a preference for IPv4 over IPv6 addresses.

Change Linux Workloads to Prefer IPv4

To ensure that your paired Linux VEN workloads prefer IPv4 over IPv6 addresses in your PCE organization, edit the `/etc/gai.conf` file on the VEN by adding the following line:

```
$ precedence ::ffff:0:0/96  100
```

This change will cause `getaddrinfo` system calls to return the IPv4 addresses before IPv6 addresses.

This method works when you assign IPv4 addresses to your workloads. However, it doesn't work when your workloads only have IPv6 addresses (meaning, no IPv4 addresses for the hosts) or the software installed is hard coded to look for IPv6 addresses.

Change Windows Workloads to Prefer IPv4

When you choose to allow only IPv4 traffic for your PCE organization, the VENs on your workloads drop IPv6 traffic when they are in Enforced mode. This decision can lead to delays and communication failures in applications because applications will wait for IPv6 connection attempts to time out before attempting to connect over IPv4.

The problem occurs because, by default, the Windows OS prefers IPv6 over IPv4 and will attempt to connect over IPv6 before IPv4. As a workaround, you can change the order of connection attempts so that IPv4 is preferred over IPv6. With this change, applications will connect over IPv4 first and succeed or fail as governed by the work-load's firewall policies.

For information about changing the connection order to prefer IPv4 over IPv6, see the Microsoft KB article Guidance for configuring IPv6 in Windows for advanced users.

As explained in the KB article, run the following command and reboot the Windows workload:

```
reg add hklm\system\currentcontrolset\services\tcpip6\parameters /v
DisabledComponents /t REG_DWORD /d 0x20
```

To avoid rebooting the Windows workload, run the following commands:

```
netsh interface ipv6 delete prefixpolicy ::ffff:0:0/96
netsh interface ipv6 add prefixpolicy ::ffff:0:0/96 60 4
```

Allow or Block IPv6 Traffic

When your network environment allows IPv6 traffic, you can configure the PCE to allow or block IPv6 traffic.

By default, all IPv6 traffic is allowed.

> ✅ NOTE:
> When you want Windows workloads to use IPv4 instead of IPv6, see Set the IP Version for Workloads.

To allow or block IPv6 traffic:

1. From the PCE web console menu, choose **Settings** > **Security**.
2. Click **Edit** > **Change IPv6**.

By default, the **All Allowed** option is selected.

3. To block all IPv6 traffic, select **All Blocked**.

   The IPv6 traffic is blocked only for workloads in the Enforced policy state. IPv6 traffic is allowed for workloads in the Build and Test policy states.

4. Click **Save**.

5. To implement these changes, click the **Provision** icon at the top right of the PCE web console, and select **Pending Changes**.

   The Provision page appears.

6. Select the checkbox corresponding to the change or the **Change** checkbox to select all changes, and click **Provision** > **Confirm & Provision**.

Enable IP Forwarding

(For Linux VENs only)

In PCE versions earlier than 21.5.10, IP forwarding is automatically enabled for hosts in a container cluster that is reported by Kubelink to the PCE or hosts explicitly set to use the Containers Inherit Host Policy feature.

Starting in PCE version 21.5.10, you can enable IP forwarding on hosts without using any container segmentation features. To enable this feature, contact Illumio Support.

1. In the PCE web console, choose **Security** > **IP Forwarding**. The IP Forwarding tab appears if the feature is enabled.

2. In this tab, you can use labels and label groups to enable IP forwarding for the workloads that match the label combination. Use combinations of Role, Application, Environment, and Location labels and label groups in the same way that you would to specify workloads for any other purpose; for example, in a Rule or any of the tabs under the Security Settings page.

Workloads with IP forwarding enabled will configure the host firewall to allow all forwarded traffic without visibility, including traffic forwarded through the host.

SecureConnect Setup

Enterprises have requirements to encrypt in transit data in many environments, particularly in PCI and other regulated environments. Encrypting in transit data is straightforward for an enterprise when the data is moving between datacenters. An enterprise can deploy dedicated security appliances (such as VPN concentrators) to implement IPsec-based communication across open untrusted networks.

However, what if an enterprise needs to encrypt in transit data within a VLAN, data-center, or PCI environment, or from a cloud location to an enterprise datacenter? Deploying a dedicated security appliance to protect every workload is no longer feasible, especially in public cloud environments. Additionally, configuring and managing IPsec connections becomes more difficult as the number of hosts increases.

Features of SecureConnect

SecureConnect has the following key features.Platforms Supported by SecureConnect

SecureConnect works for connections between Linux workloads, between Windows workloads, and between Linux and Windows workloads.

IPsec Implementation

SecureConnect implements a subset of the IPsec protocol called Encapsulating Security Payload (ESP), which provides confidentiality, data-origin authentication, connectionless integrity, an anti-replay service, and limited traffic-flow confidentiality.

In its implementation of ESP, SecureConnect uses IPsec transport mode. Using transport mode, only the original payload is encrypted between the workloads. The original IP header information is unchanged so all network routing remains the same. However, the protocol being used will be changed to reflect the transport mode (ESP).

Making this change causes no underlying interfaces to change or be created or any other underlying networking infrastructure changes. Using this approach simply obfuscates the data between endpoint workloads by encrypting the data between them.

If SecureConnect is unable to secure traffic between two workloads with IPsec, it will block unencrypted traffic when the policy was configured to encrypt that traffic.

IKE Versions Used for SecureConnect

SecureConnect connections between workloads use the following versions of Internet Key Exchange (IKE) based on workload operating system:

- Linux ↔ Linux: IKEv2
- Windows ↔ Windows: IKEv1
- Windows ↔ Linux: IKEv1

For a list of supported operating systems for managed workloads, see VEN OS Support and Package Dependencies on the Illumio Support portal.

Existing IPsec Configuration on Windows Systems

Installing a VEN on a Windows system does not change the existing Windows IPsec configuration, even though SecureConnect is not enabled. The VEN still captures all logging events (`event.log`, `platform.log`) from the Windows system that relate to IPsec thereby tracking all IPsec activity.

Performance

The CPU processing power that a workload uses determines the capacity of the encryption. The packet size and throughput determine the amount of power that is required to process the encrypted traffic using this feature.

In practice, enabling SecureConnect for a workload is unlikely to cause a big spike in CPU processing or a decrease in network throughput. However, Illumio recommends benchmarking performance before enabling SecureConnect and comparing results after enabling it.

Use Pre-Shared Keys with SecureConnect

SecureConnect includes the option of using pre-shared keys (generated by the PCE) or client-side PKI certificates for IKE authentication.

You can configure SecureConnect to use pre-shared keys (PSKs) to build IPsec tunnels that are automatically generated by the PCE. SecureConnect uses one key per organization. All the workloads in that organization share the one PSK. SecureConnect uses a randomly generated 64-character alpha-numeric string, for example:

```
c4aeb6230c508063db3e3e1fac185bea9c4d17b4642a87e091d11c9564fbd075
```

When SecureConnect is enabled for a workload, you can extract the PSK from a file in the `/opt/illumio` directory, where the VEN stores it. You cannot force the PCE to regenerate and apply a new PSK. If you feel the PSK has been compromised, contact Technical Support.

> ✅ NOTE:
> Illumio customers accessing the PCE from the Illumio cloud can have multiple Organizations. However, the Illumio PCE does not support multiple Organizations when you have installed the PCE in your datacenter.

Use PKI Certificates with SecureConnect

SecureConnect allows you to use client-side PKI certificates for IKE authentication and IPsec communication between managed workloads. If you have a certificate management infrastructure in place, you can leverage it for IKE authenticate between workloads because it provides higher security compared to using pre-shared keys (PSKs).

Certificate-based SecureConnect works for connections between Linux workloads, between Windows workloads, and between Linux and Windows workloads.

The IPsec configuration uses the certificate with the distinguished name from the issuer field that you specify during PCE configuration for IKE peer authentication.

Prerequisites, Limitations, and Caveats

Before configuring your workloads to use SecureConnect, review the following prerequisites and limitations, and consider the following caveats.

PKI Certificates with SecureConnect

The following prerequisites and limitations apply when configuring SecureConnect to use certificates:

- You must have a PKI infrastructure to distribute, manage, and revoke certificates for your workloads. The PCE does not manage certificates or deliver them to your workloads.
- The PCE supports configuring only one global CA ID for your organization.
- The VEN on a workload uses a Certificate Authority ID (CA ID) to authenticate and establish a secure connection with a peer workload.

Connected workloads must have CA identity certificates signed by the same root certificate authority. When workloads on either end of a connection use different CA IDs, the IKE negotiation between the workloads will fail and the workloads will not be able to communicate with each other.

VEN Versions

To use PKI certificates with SecureConnect, your workloads must be running VEN version 17.2 or later.

Maximum Transmission Unit (MTU) Size

IPsec connections cannot assemble fragmented packets. Therefore, a high MTU size can disrupt SecureConnect for the workloads running on that host.

Illumio recommends setting the MTU size at 1400 or lower when enabling SecureCon-
nect for a workload.

Ports

Enabling SecureConnect for a workload routes all traffic for that workload through
the SecureConnect connection using ports 500/UDP and 4500/UDP for NAT tra-
versal and for environments where ESP traffic is not allowed on the network (for
example, when using Amazon Web Services). You must allow 500/UDP and
4500/UDP to traverse your network for SecureConnect.

Unsupported SecureConnect Usage

SecureConnect is not supported in the following situations:

- SecureConnect cannot be used between a workload and unmanaged entities,
  such as the label "Any (0.0.0.0/0 and ::/0" (such as, the internet).
- SecureConnect is not supported on virtual services.
- SecureConnect is not supported on workloads in the Idle policy state. If you
  enable it for a rule that applies to workloads that are in both Idle and non-Idle
  policy states, you can impact the traffic between these workloads.
- SecureConnect is not supported on AIX and Solaris platforms.

SecureConnect and Build and Test Policy States
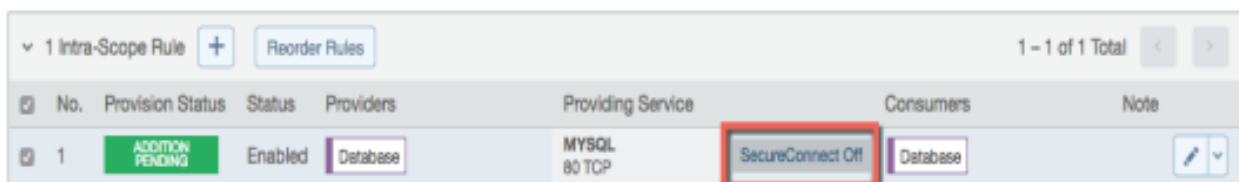
When you configure workloads to use SecureConnect be aware of the following
caveat.

SecureConnect encrypts traffic for workloads running in all policy states except Idle. If
misconfigured, you could inadvertently block traffic for workloads running in the Build
and Test policy states.

SecureConnect Host-to-Host Encryption

When you configure workloads to use SecureConnect be aware of the following
caveat.

SecureConnect encrypts traffic between workloads on a host-to-host basis. Consider
the following example.

In this example, it appears that enabling SecureConnect will only affect MySQL traffic. However, when you enable SecureConnect for a rule to encrypt traffic between a database workload and a web workload over port 3306, the traffic on all ports between the database and web workloads is protected by IPsec encryption.

Configure SecureConnect to Use Pre-Shared Keys

You can configure SecureConnect to use pre-shared keys (PSKs) for IKE authentication and IPsec communication between managed Workloads. SecureConnect uses one key per Organization. All the Workloads in that organization share the one PSK. SecureConnect generates a random 64-character alpha-numeric string for this key.

1. From the PCE navigation menu, choose **Settings** > **Security Settings**.
2. Choose **Edit** > **Configure SecureConnect**.
   The page refreshes with the settings for SecureConnect.
3. In the Default IPsec Authority field, select the **PSK** option.
4. Click **Save**.

Configure SecureConnect to Use Certificates

SecureConnect allows you to use client-side PKI certificates for IKE authentication and IPsec communication between managed Workloads. The PCE supports configuring only one global CA ID for your organization. Configuring SecureConnect to use certificates applies the setting to All Roles, All Applications, All Environments, and All Locations.

Configuring SecureConnect to use PKI certificates in the global Security Settings page does not manage certificates for your organization or deliver them to your Workloads.

> ✅ NOTE:
> You must independently set up certificates on your Windows and Linux Workloads. For information, see Requirements for Certificate Setup on Workloads.

1. From the PCE web console menu, choose **Settings** > **Security Settings**.
2. Choose **Edit** > **Configure SecureConnect**.
   The page refreshes with the settings for SecureConnect.
3. In the *Default IPsec Authority* field, select the **Certificate Authority** option.
4. In the *Global Certificate ID* field, enter the distinguished name from the Issuer field of your trusted root certificate. (This certificate is used globally for all work-

loads in your organization enabled with SecureConnect.)

5. Click **Save**.

Requirements for Certificate Setup on Workloads

To use PKI certificates with SecureConnect, you must independently set up certificates on your Windows and Linux workloads.

Generate or obtain certificates from a trusted source in your organization. You should only use certificates obtained from trusted sources.

File Requirements

File	Requirements
Issuer's certificate	The global CA certificate, either root or intermediate, in PEM or DER format ✅ NOTE: On Linux, the issuer's certificate must be readable by the Illumio user.
pkcs12 container	Archive containing the public key, private key, and identity certificate generated for the workload host. Sign the identity certificate using the global root certificate. You can password protect the container and private key but do not password protect the public key.

Installation Locations

Windows Store

Use the Windows OS, for example Microsoft Management Console (MMC), to import the files into these locations of the local machine store (not into your user store).

- Root certificate: Trusted Root Certificate Store
- pkcs12 container: Personal ("My") certificate store

Linux Directories

Copy the files into the following Linux directories. (You cannot change these directories.)

- Root certificate: `/opt/illumio_ven/etc/ipsed.d/cacert`
- pkcs12 container: `/opt/illumio_ven/etc/ipsed.d/private`

AdminConnect Setup

Relationship-based access control rules often use IP addresses to convey identity. This authentication method can be effective. However, in certain environments, using IP addresses to establish identity is not advisable.

When you enforce policy on servers for clients that change their IP addresses frequently, the policy enforcement points (PEPs) continuously need to update security rules for IP address changes. These frequent changes can cause performance and scale challenges, and the ipsets of protected workloads to churn.

Additionally, using IP addresses for authentication is vulnerable to IP address spoofing. For example, server A can connect to server B because the PEP uses IP addresses in packets to determine when connections originate from server A. However, in some environments, bad actors can spoof IP addresses and impact the PEP at server B so that it mistakes a connection as coming from server A.

Illumio designed its AdminConnect (Machine Authentication) feature with these types of environments in mind. Using AdminConnect, you can control access to network resources based on Public Key Infrastructure (PKI) certificates. Because the feature bases identity on cryptographic identity associated with the certificates and not IP addresses, mapping users to IP addresses (common for firewall configuration) is not required.

With AdminConnect, a workload can use the certificates-based identity of a client to verify its authenticity before allowing it to connect.

Features of AdminConnect

Cross Platform

Microsoft Windows provides strong support for access control based on PKI certificates assigned to Windows machines. Modern datacenters, however, must support heterogeneous environments. Consequently, Illumio designed AdminConnect to support Windows and Linux servers and Windows laptop clients.

AdminConnect and Data Encryption

When only AdminConnect is enabled, data traffic does not use ESP encryption. This ensures that data is in cleartext even though it is encapsulated in an ESP packet.

When AdminConnect and SecureConnect are enabled for a rule, the ESP packets are encrypted.

Ease of Deployment

Enabling AdminConnect for identity-based authentication is easy because it is a software solution and it does not require deploying any network choke points such as firewalls. It also does not require you to deploy expensive solutions such as Virtual Desktop Infrastructure (VDI) or bastion hosts to control access to critical systems in your datacenters.

Prerequisites and Limitations

Prerequisites

You must meet the following prerequisites to use AdminConnect:

- You must configure SecureConnect to use certificate-based authentication because both features rely on the same PKI certificate infrastructure. See the following topics for more information:
    - Configure SecureConnect to Use Certificates
    - Requirements for Certificate Setup on Workloads
    - Certificates for AdminConnect
-
    - AdminConnect must be used with VEN version 17.3 and later.
    - AdminConnect supports Linux/Windows IKE v1 (client only) with unmanaged workloads.

Limitations

You cannot enable AdminConnect for the following types of rules:

- Rules that use All services
- Rules with virtual services in providers or consumers
- Rules with IP lists as providers or consumers
- Stateless rules

AdminConnect is not supported in these situations:

- AdminConnect does not support "TCP -1" (TCP all ports) and "UDP -1" (UDP all ports) services.
- You cannot use Windows Server 2008 R2 or earlier versions as an AdminConnect server.
- Windows Server does not support more than four IKE/IPsec security associations (SAs) concurrently from the same Linux peer (IP addresses).

Certificates for AdminConnect

AdminConnect relies on PKI certificates for relationship-based access control of workloads.

The feature uses the same certificate infrastructure enabled for SecureConnect. If you have not set up certificate for SecureConnect, see Configure SecureConnect to Use Certificates and Requirements for Certificate Setup on Workloads for information.

The same prerequisites and limitations for certificate set up apply for AdminConnect. Additionally, because you can use AdminConnect to control access for laptops, certificates on laptops must meet these additional requirements:

- The certificate must have a unique Subject Name and Subject Alt Name.
- The certificate must be enabled with all extended key usage to check trust validation.

Secure Laptops with AdminConnect

You can use Illumio to authenticate laptops and grant them access to managed workloads. To manage a laptop with AdminConnect, complete the following tasks:

1. Deploy a PKI certificate on the laptop. See Certificates for AdminConnect.
2. Add the laptop to the PCE by creating an unmanaged workload and assign the appropriate labels to it to be used for rule writing
3. Create rules using those labels to grant access to the managed workloads. See Enable AdminConnect for a Rule for information.
4. Configure IPsec on a laptop.

To add a laptop to the PCE by creating an unmanaged workload:

Illumio does not support installing the VEN on laptops. Therefore, to manage a laptop with AdminConnect, add the laptop to the PCE as an unmanaged workload.

1. From the PCE web console menu, choose **Workloads** > **Add** > **Add Unmanaged Workload**.

    The Workloads – Add Unmanaged Workload page appears.
2. Complete the fields in the *General*, *Labels*, *Attributes*, and *Processes* sections. See Add an Unmanaged Workload in the *Security Policy Guide* for information.
3. In the *Machine Authentication ID* field, enter all or part of the DN string from the *Issuer* field of the end entity certificate (CA Subject Name). For example:

    CN=win2k12, O=Illumio, OU=Portal, ST=CA, C=US, L=Sunnyvale

> **TIP:**
> Enter the exact string that you get from the `openssl` command output.

4. Click **Save**.

To configure IPsec on a laptop:

To use the AdminConnect feature with laptops in your organization, you must configure IPsec for these clients.

See the Microsoft Technet article Netsh Commands for Internet Protocol Security (IPsec) for information about using netsh to configure IPsec.

See also the following examples for information about the IPsec settings required to manage laptops with the AdminConnect feature.

```
PS C:\WINDOWS\system32> netsh advfirewall show global

Global Settings:
----------------------------------------------------------------------
IPsec:
StrongCRLCheck                        0:Disabled
SAIdleTimeMin                         5min
DefaultExemptions                     NeighborDiscovery,DHCP
IPsecThroughNAT                       Server and client behind NAT
AuthzUserGrp                          None
AuthzComputerGrp                      None
AuthzUserGrpTransport                 None
AuthzComputerGrpTransport             None

StatefulFTP                           Enable
StatefulPPTP                          Enable

Main Mode:
KeyLifetime                           60min,0sess
SecMethods                            ECDHP384-AES256-SHA384
ForceDH                               Yes

Categories:
BootTimeRuleCategory                  Windows Firewall
```

```
FirewallRuleCategory                Windows Firewall
StealthRuleCategory                 Windows Firewall
ConSecRuleCategory                  Windows Firewall


Ok.



PS C:\WINDOWS\system32> netsh advfirewall consec show  rule name=all


Rule Name:                          telnet
----------------------------------------------------------------------
Enabled:                            Yes
Profiles:                           Domain,Private,Public
Type:                               Static
Mode:                               Transport
Endpoint1:                          Any
Endpoint2:                          10.6.3.189/32,10.6.4.35/32,192.168.41.163/32
Port1:                              Any
Port2:                              23
Protocol:                           TCP
Action:                             RequireInRequireOut
Auth1:                              ComputerKerb,ComputerCert
Auth1CAName:                        CN=MACA, O=Company, OU=engineering, S=CA,
C=US, L=Sunnyvale, E=user@sample.com
Auth1CertMapping:                   No
Auth1ExcludeCAName:                 No
Auth1CertType:                      Intermediate
Auth1HealthCert:                    No
MainModeSecMethods:                 ECDHP384-AES256-SHA384
QuickModeSecMethods:                ESP:SHA1-AES256+60min+100256kb
ApplyAuthorization:                 No
Ok.
```

Chapter **3**

Access Configuration for PCE

This chapter contains the following topics:

This section describes how to configure the PCE to control access.

Role-based Access Control

This section describes the concepts of role-based access control (RBAC) and how it works with the PCE.

Overview of Role-based Access Control

Security-oriented companies should grant employees the exact permissions they need based on their role. Illumio Core uses role-based access control (RBAC) to

deliver security at an enterprise scale in the following ways:

- Assign your users the least required privilege they need to perform their jobs.

  Limit access for your users to the smallest operation-set they need to perform their jobs; for example, monitor for security events.

- Implement separation of duties.

  Delegate the responsibility to manage a zone to a specific team or delegate authority to application teams; for example, delegate a team to manage security for the US-West Dev zone, or assign the DevOps team to set security policy for the HRM application they manage.

- Grant access to users based on two dimensions: roles and scopes.

  Each role grants access to a set of capabilities in Illumio Core. Scopes define the workloads in your organization that users can access and are based on three labels: Application, Environment, and Location. The scopes specify the boundaries of the sphere of influence granted to a user.

  For example, a user can be added to the Ruleset Provisioner role with the scope Application CRM, Environment Staging, and Location US. With that access, the user could provision rulesets for workloads that are part of your CRM application in the Staging environment located in the US.

- Centrally manage user authentication and authorization for Illumio Core.

  Configure single sign-on with your corporate Identity Provider (IdP) and designate which external IdP groups should have access roles. Group membership is managed by your IdP while resource authorization is configured in Illumio Core.

Use Cases

Illumio designed our RBAC feature around a set of use cases based on the way that enterprises manage the security of the computing assets in their environment. These use cases encompass common security workflows for the modern, security-conscious enterprise. The personas include different levels of security professionals.

Support the Security Workflow

Customers can configure the RBAC feature to support any type of responsibility bifurcation that they have in their workflow models. For example, the following workflows are supported:

- Architect-level professionals define all security policy for an enterprise by adding rulesets and rules in the PCE.
- Junior-level professionals provision rulesets and rules to workloads during maintenance windows. Junior personnel cannot edit any policy items in the Illumio PCE.
- Some users only view the infrastructure and alert senior team members when security issues occur.

Manage Security for Specific Workloads

When you combine Illumio Core RBAC roles with scopes, you can secure access for IT teams who support specific applications or different geographic locations. For example, customers could delegate authority for workloads in the following ways:

- To manage security for workloads around silos; for example, a particular cloud provider like AWS.
- To decentralize their security policy to specific application teams allowing them to act quickly when managing application security without waiting for the central security team.
- To bifurcate the security of their infrastructure in such a way that one user is responsible only for the West coast assets and another user is responsible for the East coast assets.

Features of Role-based Access Control

Built-in Roles

Illumio Core includes seven roles that grant users access to perform operations. Each role is matched with a scope. See About Roles, Scopes, and Granted Access for information.

Granular Permissions

You can assign multiple roles to one user and by mixing and matching the different roles, you can achieve different levels of granularity of permissions.

You can grant different permissions to different users for different resources by defining scopes. For example, you might allow some users complete access to add rulesets for all workloads in your staging environment. For other users, you might grant access to all workloads in all environments. Users can be assigned exactly one role, representing their singular job function while other users can be assigned multiple roles, representing multiple job functions.

Identity Federation Using External Users and Groups

You can connect to external LDAP directories to manage users and user groups by configuring single sign-on (SSO) for the PCE.

Using this feature, you can create and manage users locally in PCE, or use an IdP to manage users and user groups from an existing directory. External user and user groups authenticate with the external IdPs.

Custom Role Assignments

You can customize access to suit your organization by specifying specific scopes for the Ruleset Manager and Ruleset Provisioner roles.

Audit Information

You can access an audit trail of user activity through the following reports:

- The User Activity page, which displays the authentication details for each user, when they logged in, and whether they are online.
- The Organization Events page, which displays when Organization Owners granted users access, when users logged in and out, and the actions they performed.

About Roles, Scopes, and Granted Access

Illumio Core includes seven roles that grant users access to perform operations. Each role is matched with a scope. You can add users (local and external) and groups to all the roles.

Roles with Global Scopes

These Global Roles use the scope All Applications, All Environments, and All Locations. You cannot change the scope for these roles. The roles have the following capabilities in Illumio Core.

Role	Granted Access
Global Organization Owner	Perform all actions: add, edit, or delete any resource, security settings, or user account
Global Administrator	Perform all actions except user management: add, edit, or delete any resource or organization setting
Global Read Only	View any resource or organization setting They cannot perform any operations.
Global Policy Object Provisioner	Provision rules containing IP lists, services, and label groups They cannot provision rulesets, virtual services, or virtual servers, or add, modify, or delete existing policy items.

> ✅ NOTE:
> You can add, modify, and delete your API keys because you own them.

About the Read Only User Role

The Read Only User role applies to all users in your organization—local, external, and users who are members of external groups managed by your IdP. This role allows users to view resources in Illumio Core when they are not explicitly assigned to roles and scopes in the PCE.

For example, you configure single sign-on for your corporate Microsoft Active Directory Federation Services (AD FS) so that users managed by AD FS can log into the PCE by using their corporate usernames and passwords. However, you haven't added all your external users to the PCE or assigned them to roles. These users can still log into the PCE by authenticating with the corporate IdP and view resources in the PCE.

The Read Only User role is not listed in the **Role-Based Access** > **Global Roles** or **Scoped Roles** pages because it is considered a default, catchall type of role. Users have access to this role on an organization-wide basis because you either enable or disable it for your entire organization. Additionally, you do not see it in the list of a user's role assignments when you view the user's details page (**Role-Based Access** > **Users and Groups**). However, when the role is enabled for your organization, you see it listed in the **Role-Based Access** > **User Activity** details for each user.

> ✅ NOTE:
> You can enable and disable the Read Only User role from the **Role-Based Access** > **Global Roles** > **Global Read Only** page.

When the Read Only User role is disabled for your organization, users who are not assigned to roles cannot access Illumio managed resources. When attempting to log into the PCE, they are still authenticated by their corporate IdP but the PCE immediately logs them out because they do not have access (even read-only access) to any Illumio managed assets.

Roles with Custom Scopes

You can apply the following roles to specific scopes. These roles are called "Scoped Roles."

Role	Granted Access
Full Ruleset Manager	• Add, edit, and delete all rulesets within the specified scope. • Add, edit, and delete rules when the provider matches the specified

Role	Granted Access
	scope. The rule consumer can match any scope. ✅ NOTE: You can choose the All Applications, All Environments, and All Locations scope with the Full Ruleset Manager role.
Limited Ruleset Manager	• Add, edit, and delete all rulesets within the specified scope. • Add, edit, and delete rules when the provider and consumer match the specified scope. • Ruleset Managers with limited privileges cannot manage rules that use IP lists, custom iptables rules, user groups, label groups, iptables rules as consumers, or have internet connectivity. ✅ NOTE: You cannot choose the All Applications, All Environments, and All Locations scope with the Limited Ruleset Manager role.
Ruleset Provisioner	Provision rulesets within specified scope. ✅ NOTE: You can choose the All Applications, All Environments, and All Locations scope and custom scopes with the Ruleset Provisioner role.
Workload Manager	Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources. ✅ NOTE: The 19.1.0 PCE does not support unpairing multiple managed workloads via the REST API when you are logged in as a Workload Manager. You can unpair workloads using the PCE web console because it restricts selection of workloads by the user's scope. However, via the REST API, the bulk unpair operation fails when multiple workloads are selected and one or more of the workloads are out of the user's scope.

Workload Manager Role

Use Case 1

You want to use scripts in your development environment to programmatically spin up and bring down workloads; your scripts create pairing profiles and generate pairing keys without you granting elevated Admin privileges to the scripts.

Use Case 2

Your application teams are in charge of changing the security posture of workloads, such as changing the policy enforcement states. You want to allow your application teams to manage workload security without granting them broad privileges, such as All | All | All access.

Use Case 3

You want to prevent your PCE users from accidentally changing workload labels by moving the workloads in Illumination.

Solution

Users with the Workload Manager role can create, update, and delete workloads and pairing profiles. This role is a scoped role; when you assign a user to a scope, they can only manage workloads within the allocated scope. The Workload Manager can pair, unpair, and suspend VENs and change the policy state. It is an additive role; you can assign the Workload Manager role to a user and combine it with any other PCE role to provide additional privileges for that user.

Configuration

1. Create a local user with "None" or Global Read Only role.
2. Assign the Workload Manager role to the user.
3. (Optional) Provide the invitation link to the new workload manager user.
4. The workload manager can then log into the PCE and manage workloads and pairing profiles per the allocated scope.

The Workload Manager role is available under Scoped Roles. Users assigned this role can view applications that are outside their scopes but can only modify those applications that are within their scopes.

> ✅ NOTE:
> A workload manager user cannot clear traffic counters from workloads within their scope.

Example: Limited Ruleset Manager Role

A user has the role Full Ruleset Manager role and access to the following scope:

All Applications | Production Environment | All Locations

The user can create and manage:

- Any ruleset that matches the Production environment
- Intra- or extra-scope rules that match this scope:

  All Applications | Production Environment | All Locations

  Where the provider and consumer of the rule are both within the Production environment scope.

For intra-scope rules, all workloads can communicate within their group (as defined by the scope), so the rule consumer is not restricted. However, in extra-scope rules, the Environment label of the resource selected as the consumer must match the label in the scope exactly.

The user cannot create a rule with the scope "All | All | All" because that scope is broader than the user's access, which is only for the Production environment.

Because the user is a member of the Limited Ruleset Manager role, the user cannot manage custom iptables rules and the following resources cannot be selected as consumers in extra-scope rules:

- IP lists
- Label groups
- User groups
- Workloads

Combine Roles to Support Security Workflows

Illumio includes fine-grained roles to manage security policy. The roles control different aspects of the security workflow. By mixing and matching them, you can effectively control the access needed by your company.

Ruleset Only Roles

You can add users to the Full Ruleset Manager and Ruleset Provisioner roles so that they can edit the security policies on the workloads within their assigned scopes without affecting other entities, such as services, virtual services, or virtual servers.

These users can write rules for their workloads and provision them when the rules do not have dependencies on global objects, such as services or IP lists.

Ruleset Plus Global Policy Object Provisioner Roles

You can add users to the Ruleset Manager (Full or Limited) role and the Global Policy Object Provisioner role so that they can control the security policy for workloads.

These users can create rulesets within their assigned scopes and write rules that are not dependent on global objects. However, they can provision any workloads, even those containing services, IP lists, and label groups.

Global Organization Owner or Administrator Roles

You can add architect-level professionals to the Global Organization Owner or Global Administrator role so that they can define all security policy for an enterprise.

They have the capability to modify global objects, such as services and labels, add workloads, pair workloads, and change workload modes to function as a security policy administrator.

Role Access is Additive

In the following example, Joe Smith is added to two user roles and one external group and each is assigned a specific role and scope. Joe's ability to manage security for his company is a union of the roles and scopes he is assigned to.
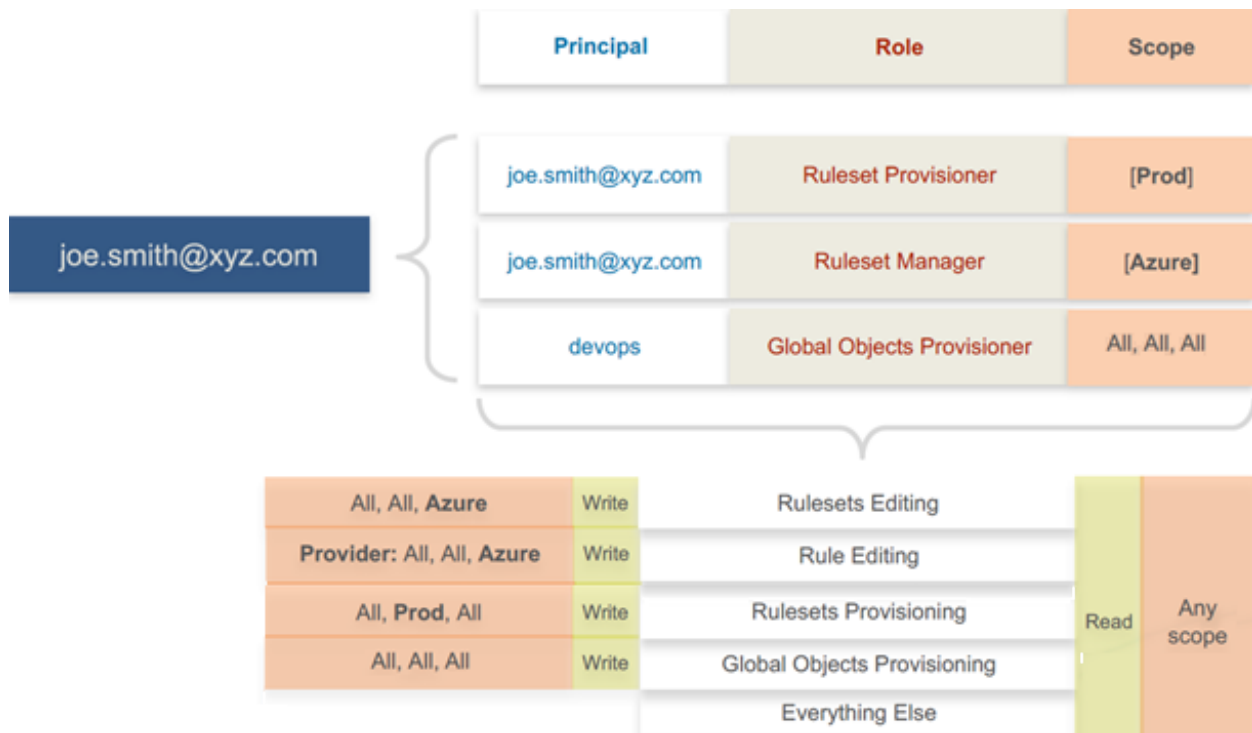
Exercise Caution when Combining Roles

Because role access is additive, some caution is advisable when assigning more than one role to a user. Be sure you do not grant permissions beyond what is intended. For example, suppose you are assigning a scoped role to a user. The user's access will be restricted to workloads within the defined scope. If you then assign the Global Read Only role to the same user, the user will be able to view all workloads, including those outside the scope that was defined in the first role.

Example Role Workflows

The following example shows the hand offs between a user who is a member of the Global Organization Owner role and a member of a Ruleset Manager role.

1. An Organization Owner grants access to one or more scopes for a Ruleset Manager by selecting specific labels, which define the permitted scopes for the Ruleset Manager.
2. The Ruleset Manager logs in and creates rules that conform to the specified scopes, as defined by the labels that are accessible to that user.
3. The Ruleset Manager has read-only access to all other PCE resources, such as services or rulesets with different scopes from the scopes that the Ruleset Manager can access.
4. The Organization Owner reviews the rules created by the Ruleset Manager and provisions them as needed.

Prerequisites and Limitations

- You must be a member of the Global Organization Owner role to manage users, roles, and scopes in the PCE.
- Configuring SSO for an Illumio supported IdP is required for using RBAC with external users and groups. See Authentication for information.

  If you have not configured SSO, you can still add external users and external groups to the PCE; however, these users will not be able to log into the PCE because they will not be able to reach the IdP or SAML server to authenticate.
- Illumio resources that are not labeled are not access restricted and are accessible by all users.
- External users who are designated by username and not an email address in your IdP will not receive an automatic invitation to access the PCE. You must send them the PCE URL so they can log in.

- You cannot change the primary designation for users and groups in the PCE; specifically, the email address for a local user, the username or email address for an external user, or the contents of the External Group field for an external group. To change these values, you must delete the users or groups and re-add them to the PCE.

- An App Owner who is in charge of the application in both production and development environments does not have permissions to write extra-scope rules between production and development.

Local users are not locked out of their accounts when they fail to log in. After 5 consecutive failures, the PCE emails the user that their account might be compromised.

Locked users retain all their granted access to scopes in the PCE; however, they cannot log into the PCE.

Setup for Role-based Access Control

This section describes how to configure role-based access control (RBAC) for the PCE. Before doing these tasks, be sure to understand the concepts in Role-Based Access Control.

> ✅ NOTE:
> Permission to configure these settings is dependent on your role. See About Roles, Scopes, and Granted Access for information.

Add a Scoped Role

Add a scoped role to create fine-grained access control to manage security policy for your workloads.

You can grant different permissions to different users for different resources by defining scopes. For example, you might allow some users complete access to add rulesets for all workloads in your staging environment. For other users, you might grant access to all workloads in all environments.

1. From the PCE web console menu, choose **Role-Based Access** > **Scoped Roles**.
2. Click **Add**.
   The Access Wizard appears.
3. Define the scope for the role by selecting labels or label groups for Applications, Environment, and Location.
4. Add a local user, external user, or user group to the role.

5. Select roles. For a description of these role, see About Roles, Scopes, and Granted Access.

6. Click **Grant Access** > **Confirm**.

    The newly-added role is displayed on the Scoped Roles page and you can select it to edit or remove access.

Manage a Local User

Local users are created in the PCE (they are not managed by an IdP). When they log into the PCE, they must enter their email addresses and passwords. The Illumio PCE encrypts and stores their passwords.

When you install the PCE, the first user account it creates is a local user. You can create additional local users as a backup in case your external IdP goes offline or the SAML server is not accessible.

To add a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **Local Users** tab.

2. Click **Add**.

3. Enter a name and an email address.
    The email address must use the format xxxx@yyyy.zzzz and be 255 characters or less. From the 20.1.0 release onwards, you can add email addresses with an apostrophe (') in them.
    In the PCE, you can have duplicate names for local users but you cannot have duplicate email addresses.
    The PCE emails the user at the address you specify an invitation with a link to create their Illumio user account. The link in invitation email is valid only for 7 days after which it expires.

4. Select a role for the user:

    ○ None

    ○ Global Organization Owner

    ○ Global Administrator

    ○ Global Read Only

    For a description of these roles, see About Roles, Scopes, and Granted Access.

You can change a user's role membership after adding them by going to the user's details page or from a role details page. From the 20.1.0 release onwards, the "My Roles" feature allows you to view the list of assigned permissions (roles).

To remove a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups**.
2. Select the user you want to remove.
3. Click **Remove**.

When you remove a local user while the user is online, the PCE logs the user out as soon as the user is removed.

The user is removed from the Local Users tab; however, the user remains in the User Activity page and is designated as offline. The user's actions remain in the Organization Events page.

You can re-add the user to the PCE as a local or external user with the same name and email address or username.

To edit a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups**.
2. Click the name of the user you want to edit.
3. Click **Edit User**.
4. Change the user's name and click **Save**.

You cannot edit a user's email address. You must remove and re-add the user with the new email address.

Changing a local user's name only changes it in the RBAC Roles pages and the Users and Groups page. The name is not changed in the user's personal profile or in the RBAC User Activity pages.

> ✅ NOTE:
> Local and external users can change their name when they create their accounts or from their profiles.

To convert a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups**.
2. Click the name of the user.
3. Click **Convert User**.

You can convert a local user to an external user so that your corporate IdP manages the user authentication credentials. When you convert a user to an external user, the user retains all their role memberships.

To invite a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups**.
2. Click the name of the user.
3. Click **Re-Invite**.

You can send a new email to a user to create their account when they haven't responded to the original email. An invitation remains valid for 7 days.

To lock or unlock a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups**.
2. Click the name of the user.
3. Click **Lock**.

Local users are locked out of their accounts when they fail to log in after 5 consecutive failures.

Locked users retain all their granted access to scopes in the PCE; however, they cannot log into the PCE. When an account is locked, the PCE web console reports that the username or password is invalid even when a user enters valid credentials. The user's account resets after 15 minutes and does not require an Illumio administrator to unlock it.

Manage a Service Account

An API key can be created by the Global Organization Owner without creating a new user account to be associated with the API key. The API key can instead be associated with a service account. The service account is a security principal, just as a user is.

- A service account can perform any API operation using its API key.
- Permissions for service accounts are specified with a combination of one or more PCE roles (Global Owner, Global Admin, etc.). You can include multiple roles for a single service account, just as you can for a user account.
- Access restrictions are supported. You can limit the use of service account API keys by IP addresses, just as you can for user API keys.

- Audit events are supported with service accounts. All audit events triggered by a service account indicate the name of the service account and ID of its API key

To create a service account:

1. Choose **Access Management** > **Service Accounts**.

2. Click Add, and give the account a unique name.

3. Set the roles and scopes that determine the permissions granted to the service account.

4. To create an API key for the service account, click Save, then click Download Credentials.

   The new credentials are saved in the API Key section of the Service Account page.

Add or Remove an External User

Using RBAC, you can control access to Illumio Core for users who are externally authenticated by a corporate IdP. Your corporate IdP manages authentication so that when these users log into the PCE, they are redirected to the IdP to authenticate. The PCE does not validate their usernames or passwords. See Authentication for more information.

Using RBAC, you control the access external users have to Illumio Core features and functionality. When you add an external user to the PCE, you specify that user's access by assigning the user to Illumio roles and scopes.

To add an external user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **External Users** tab.

2. Click **Add**.

3. Enter a name and an email address or username.
   Whether you enter an email address or username for the user depends on how you have configured your IdP to identify corporate users.
   The username can contain up to 225 alphanumeric and special characters (. @ / _ % + -).
   In the PCE, you can have duplicate names for external users but you cannot have duplicates email addresses or usernames.
   When your IdP is configured to identify users by using email addresses, the PCE emails the user at the address you specify an invitation with a link to create their

Illumio user account.

If your IdP is configured to use usernames, you must provide the user your Illu-mio PCE web console URL.

4. Select a role for the user:

- ◦ None

- ◦ Global Organization Owner

- ◦ Global Administrator

- ◦ Global Read Only

For a description of these roles, see About Roles, Scopes, and Granted Access.

Users without a role (None) can still log into the PCE to view resources when Read Only User access to the PCE is enabled. You can enable and disable Read Only User access in the Global Read Only role.

You can change a user's role membership after adding them by going to the user's details page or from a role details page.

To change an external user's name, click **Edit User** from the user's details page. You cannot edit the email address or username for an external user. You must remove and re-add the user with the new information.

To remove an external user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **External Users** tab.
2. Select the user you want to remove.
3. Click **Remove**.

Removing an external user removes the user from the External Users tab and all the user's RBAC role memberships. The user's authentication is still managed by your corporate IdP.

If Read Only User access to the PCE is enabled for your organization, the user can still log into the PCE and view resources after you remove the user.

When you remove an external user while the user is online, the PCE log the user out the next action they make after being removed.

Add or Remove an External Group

The RBAC feature in Illumio Core integrates with the user groups maintained in your corporate IdP so that you can manage user authentication centrally for the Illumio

Core. In the PCE, you assign roles and scopes to the groups managed by your IdP to control the access that Illumio users have to their Illumio managed resources.

With user groups, you can authorize your teams to manage the security for the applications they manage without waiting for a centralized security team to delegate authority.

When a user who is a member of an external group logs into the PCE, the corporate IdP authenticates the user and returns the list of groups the user belongs to. For each of those groups, the PCE determines what roles and scopes are assigned to the group. The user is granted access to the resources associated with the roles and scopes.

A user can belong to multiple external groups. When a user belongs to multiple groups, the user is granted access to Illumio resources based on the most permissive role and scopes defined for each group.

To add an external group:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **ExternalGroups** tab.
2. Click **Add**.
3. In the *Name* field, enter up to 225 alphanumeric or special characters.
4. In the *External Group* field, enter the group name as it's configured in your IdP.

In your IdP, the group is designated by a simple group name (for example "Sales") or by a group name in distinguished name (DN) format (for example "CN=Sales, OU=West"). To verify the correct format to enter in the PCE, check the memberOf attribute in the SAML assertion from your IdP.

The memberOf attribute is a multiple-value attribute that contains the list of distinguished names for groups that contain the group as a member.

5. Click **Save**.

To change an external group's name, click **Edit Group** from the group's details page. You cannot edit the External Group field. You must remove and re-add the group with the new information.

To remove an external group:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **ExternalGroups** tab.
2. Select the external group you want to remove.
3. Click **Remove**.

Removing an external group from the PCE removes all the group's RBAC role memberships and, therefore, removes access for all the group members. User authentication for the group members is still managed by your corporate IdP.

If Read Only User access to the PCE is enabled, the external group members can still log into the PCE and view resources after you remove the group. See About Roles, Scopes, and Granted Access for more information.

Change Users and Groups Added to Roles

When you change the membership for a role, the affected users must log out and log into access the new capabilities.

When you revoke a user's access to scopes or global objects while the user is online, the PCE logs the user out the next action they make after having their access revoked.

1. From the PCE web console menu, choose **Role-Based Access** > **Global Roles**.
2. Click the name of the role you want to assign users or groups to.
3. To remove a user or group from the role, select it and click **Remove**.
4. To add a user or group to a role, click **Add**.
5. From the first drop-down list, select what (Any Principal Type, Local Users, External Users, or External Groups) you want to add to the role.
   Selecting what you want to add filters the second list to display only those types of users or user groups.
6. Select the user or group to add to the role.
7. Click **Grant Access**.

Alternatively, you can select users or groups to add to roles from the **Role-Based Access** > **User and Groups** details pages, and select **Add** and follow the steps in the Access Wizard.

View User Activity

You can access a historical audit trail of user activity through the following reports:

- **User Activity:** Go to **Role-Based Access** > **User Activity**

  - Displays session details for each user, including their status, email address, when they were last logged in.
  - Click a user, to view all the roles and scopes that are assigned to that user.

  The User Activity page also displays users who were removed and are designated as offline.

  > ✅ NOTE:
  > The names that appears in the User Activity pages can be different from the **Role-Based Access** > **Users and Groups** pages when users edit their profiles or an Organization Owner changes names in the **Role-Based Access** > **Users and Groups** pages.

- **Organization Events:** Go to **Troubleshooting** > **Organization Events**

  The Organization Events page provides an ongoing log of all Organization events that occur in the PCE. For example, it captures actions, such as users logging in and logging out, and failed log in attempts; when a system object is created, modified, deleted, or provisioned; and when a workload is paired or unpaired.

  Each of these events have a severity level and they are exportable in JSON format. For a large number of events, you can narrow the search by event type, severity, or time filters.

Change Your Profile Settings

If you want to change the password you use to access the PCE web console, you can do so from your User menu located at the top right corner of the PCE web console.

To change your password:

1. From the User menu in the PCE web console, select **My Profile**.

2. Click **Change Password**.

3. On the change password screen, enter your current password, and then you new password twice.

4. Click **Change Password**.

Color Vision Deficiency Mode

Users with color vision deficiency (Deuteranopia, Protanopia, or Tritanopia) can select Color Vision Deficiency mode, which makes it easier for color vision deficiency users to distinguish between blocked and allowed traffic lines in the Illumination map. This mode can be enabled on a per-user basis.

The color vision deficiency mode is disabled by default. To enable it:

1. From the User menu in the PCE web console, select **My Profile**.

2. In the *Accessibility* section, select the Color vision deficiency radio button.

> ✅ NOTE:
> To restore the default setting, select the Normal vision radio button.

3. Click **Save**.

Role-based Access for Application Owners

The enhancements made to the Role-based Access Control (RBAC) framework in the Illumio Core 20.1.0 release enable organizations to address several use cases related to application owners.

Overview

These enhancements include:

- Delegation of policy writing to downstream application teams.
- Assigning read-only privileges to application owners. Those users get read access based on the assigned scopes.
- Flexibility to assign read/write or read-only privileges to the same user for different applications.
- For example, the same user can have read-write privileges in a staging environment but has read-only privileges in a production environment.

Although the RBAC controls in releases prior to Illumio Core 20.1.0 restricted "writes" based on user role and scope, users had visibility into all aspects of the PCE irrespective of the role. With these new RBAC controls, application owners get visibility into the applications within their assigned scopes, specifically the PCE information relevant to their applications. Depending on the user's role, application owners can:

- Read/write policies to manage application segmentation.
- View inbound and outbound traffic flows as well as use Explorer.
- View labeled objects used in policies.
- View details of global objects such as, IP Lists and Services used by their applications.

Benefits

The key benefits of the RBAC framework in the PCE are as follows:

- Provides a label based approach to define user permissions.
- Provides roles based on application owner personas to manage application segmentation.
- Provides a building block based approach to stack permissions for users.
- Offers flexibility to delegate read-write and read-only privileges to same user for different sets of applications.

- Enables enforcement of least privilege by hiding information outside of an application scope.
- Allows application owners to effectively manage segmentation for their applications.

Updates to Roles

As described in About Roles, Scopes, and Granted Access, Illumio Core provides two types of user roles - Global and Scoped. It also provides the ability to stack multiple roles for the same user. A PCE owner can assign a combination of multiple roles to the same user. The resulting set of permissions is the summation of all permissions included with each of the stacked roles. With these updates:

- Existing scoped roles enhanced to restrict reads by scope.
- New scope based *read-only* role limits read access by labels.
- Scoped users get limited visibility into objects 1-hop away (this applies to Explorer, App Group Maps, Rule Search, and Traffic).
- Global read-only disabled by default for new PCE installations.
- PCE performance and scale enhanced to support concurrently active users.

Global Roles

Global roles provide the user with permissions to view everything and to perform operations globally. The four Global roles are :

- Global Organization Owner: Allowed to manage all aspects of the PCE, including user management.
- Global Administrator: Allowed to managed most aspects of the PCE, with the exception of user management.
- Global Viewer: Allowed to view everything within the PCE in a read-only capacity. This role was previously called "Global Read-only".
- Global Policy Object Provisioner: Allowed to provision global objects that

require provisioning such as, Services and Label Groups.

Scoped Roles

The Scoped roles are defined using labels. The permissions included with the assigned role apply only to the assigned scope where the scope is defined using a combination of Application, Environment, and Location labels. To provide permissions to different applications for a user, each of the application scopes has to be added to the same user.

All the Scoped roles have been enhanced to restrict reads and writes by Scope. The four Scoped roles are :

- Ruleset Viewer: A new scope-based read-only role. A user with this role has read-only permissions within the assigned scope. The user can view policy, application groups, incoming and outgoing traffic, and labeled objects such as, workloads, within the assigned scope.
- Ruleset Manager: An existing scope-based read/write role. A user with this role can read/write policy within the assigned scope. The user can also view application groups, incoming and outgoing traffic, and labeled objects, within the assigned scope.
- Ruleset Provisioner: This role allows a user to provision changes to the scoped objects, provided the objects are inside the user's assigned scope. A user with this role can provision changes to policies within the assigned scope. The user can also view application groups, incoming and outgoing traffic, and labeled objects, within the assigned scope.
- Workload Manager: Allows a user to perform workload-specific operations such as, pairing, unpairing, assignment of labels, and changing of policy state. A user

with this role cannot view policies and traffic, and cannot provision changes.

Configuration

The Global Read-only user setting should be disabled to enforce scoped reads for users with scoped roles. To disable this setting, make sure that the *Read Only User* setting under Role based Access > Global Roles > Global Viewer is set to **Off**.

> ✅ NOTE:
> In PCE versions 20.1.0 and higher, the Global Read-only user setting is disabled by default.

On PCE versions that are upgraded from prior releases, this setting must be manually turned off for users to have reads restricted by scope. If this setting is set to **On**, users with scoped roles will get global visibility by default.
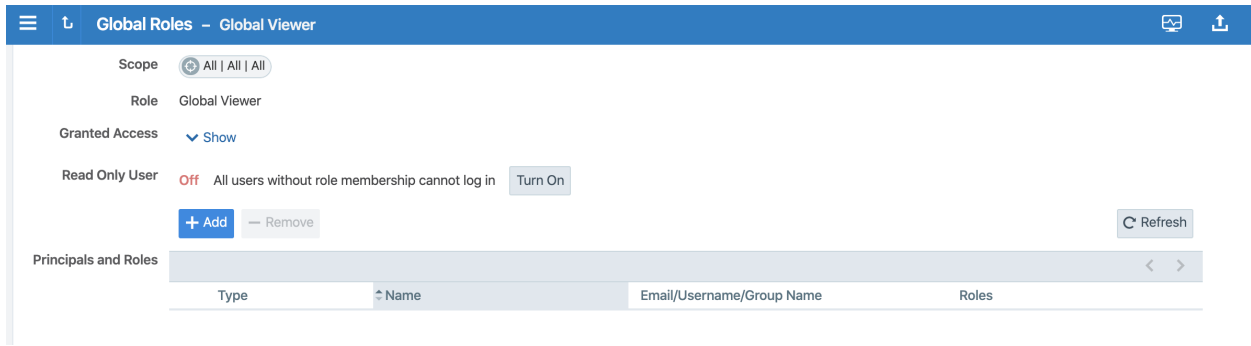
Facet Searches for Scoped Roles

The Scopes page now features a search bar with auto-complete and facets. This is restricted to users with a Global Organization Owner role. To use this feature, navigate to Role based Access > Scopes. The search bar allows Organization Owners to query a list of users by a user's role. They can search by label type such as Application, Environment, or Location to get a list of users with the selected label(s) in their assigned scope(s). They can also select Principals to search for a specific user.
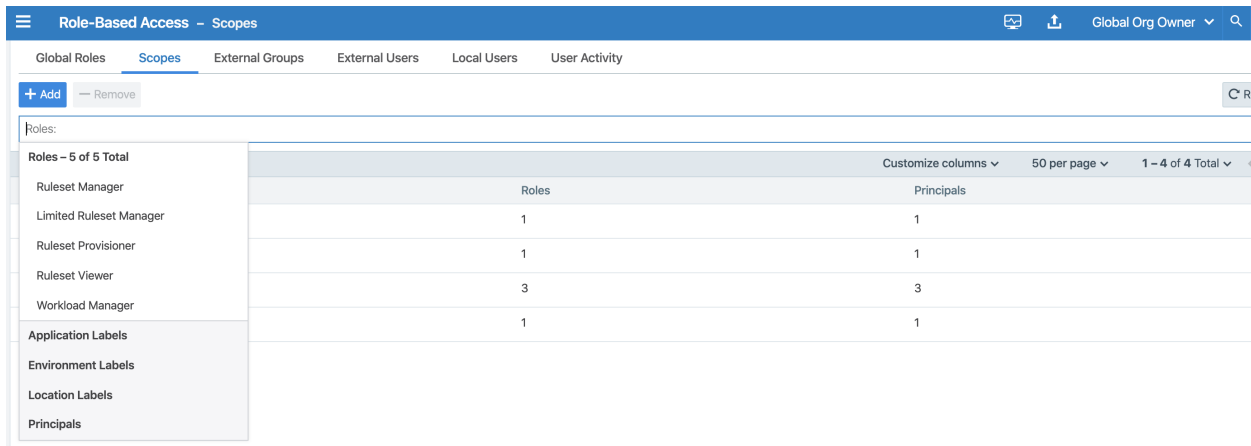
Ruleset Viewer

Ruleset Viewer is a new scope-based read-only role. When assigned, a user get read-only visibility into the assigned application scope. As a Ruleset Viewer, you can view all the Rulesets and Rules within the assigned scope. However, you cannot edit any of the rules or create new rules. You can use Policy Generator to preview the policies that will be generated. However, you are not allowed to save policy after previewing it using Policy Generator.

A Ruleset Viewer is allowed to view everything that a Ruleset Manager with the same scope is allowed to view. This includes traffic flows, labeled objects, application groups, global objects, and so on. The only difference between a Ruleset Manager and

a Ruleset Viewer is the absence of write privileges for a Ruleset Viewer. A Ruleset Manager is allowed to create and update policy within the application scope.

Scoped Roles and Permissions

The following table provides a summary of the different permissions provided with each of the scoped roles.

- (R) = Restricted based on scope
- (T) = Restricted based on resource type
- --- = Not applicable

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
Traffic - Illumination, App Group, Explorer					
Illumination Location Map	---	---	---	---	---
App Group Policy Map	Read (R)	Read (R)	Read (R)	---	Read (R)
App Group Vulnerability Map	Read (R)	Read (R)	Read (R)	---	Read (R)
App Group List	Read (R)	Read (R)	Read (R)		Read (R)
Explorer	Read (R)	Read (R)	Read (R)	---	Read (R)
Blocked Traffic	Read (R)	Read (R)	Read (R)	---	Read (R)
Policy					
Policy Generator	Read (R)	Read+Write (R)	Read (R)	---	Read+Write (R)
Rulesets and Rules	Read (R)	Read+Write (R)	Read (R)	---	Read+Write (R)
Rule Search	Read (R)	Read (R)	Read (R)	---	Read (R)
Policy Check	Read (R)	Read (R)	Read (R)	---	Read (R)
Provisioning Draft Changes	Read (R)	Read (R)	Read+Write (R)	---	Read+Write (R)
Policy Ver-	Read (R)	Read (R)	Read (R)	---	Read (R)

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
sions					
Provisioning Status	Read (R)	Read (R)	Read (R)	---	Read (R)
Labeled Objects					
Workloads	Read (R)	Read (R)	Read (R)	Read+Write (R)	Read+Write (R)
Container Workloads	Read (R)	Read (R)	Read (R)	Read (R)	Read (R)
Virtual Enforcement Nodes	Read (R)	Read (R)	Read (R)	Read+Write (R)	Read+Write (R)
Pairing Profiles	---	---	---	Read+Write (R)	Read+Write (R)
Virtual Services	Read (R)	Read (R)	Read (R)	Read (R)	Read (R)
Virtual Servers	Read	Read	Read	Read	Read
Global Policy Objects					
Services	Read	Read	Read	Read	Read
IP Lists	Read	Read	Read	Read	Read
User Groups	Read	Read	Read	Read	Read
Labels	Read	Read	Read	Read	Read
Label Groups	Read	Read	Read	Read	Read
Settings					
Segmentation Templates	---	---	---	---	---
Role-Based Access Global Roles	---	---	---	---	---
Role-Based Access Scoped Roles	---	---	---	---	---
Role-Based	---	---	---	---	---

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
Access Users and Groups					
Role-Based Access User Activity	---	---	---	---	---
Load Balancers	---	---	---	---	---
Container Clusters	---	---	---	---	---
Bi-directional Routing Networks	---	---	---	---	---
Event Settings	---	---	---	---	---
Setting Security	---	---	---	---	---
Setting Single Sign-On	---	---	---	---	---
Setting Password Policy	---	---	---	---	---
Setting Offline Timers	---	---	---	---	---
VEN Library	---	---	---	Read	Read
My Profile	Read+Write	Read+Write	Read+Write	Read+Write	Read+Write
My API Keys	Read+Write	Read+Write	Read+Write	Read+Write	Read+Write
Other					
Support Reports	---	---	---	Read+Write (R)	Read+Write (R)
Events	---	---	---	---	---
Reports	Read (R, T)	Read (R, T)	Read (R, T)	Read (R, T)	Read (R)
Support	Read	Read	Read	Read	Read
PCE Health	---	---	---	---	---
Product Version	Read	Read	Read	Read	Read

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
Help	Read	Read	Read	Read	Read
Terms	Read	Read	Read	Read	Read
Privacy	Read	Read	Read	Read	Read
Patents	Read	Read	Read	Read	Read
About Illumio	Read	Read	Read	Read	Read

Scoped Users and PCE

Each scoped role has different permissions that impact an application owner's visibility into various aspects of the PCE. Application owners can be assigned scoped roles that come with different permissions.

Navigation Menus

The PCE navigation menu options vary based on the user's role. The navigation menu options available for Application Owner are limited. For example, a user is logged in as a Global Organization Owner has more (complete) menu options displayed than when a user logs in as a scoped user (Application Owner).

Global Roles = Full Menu
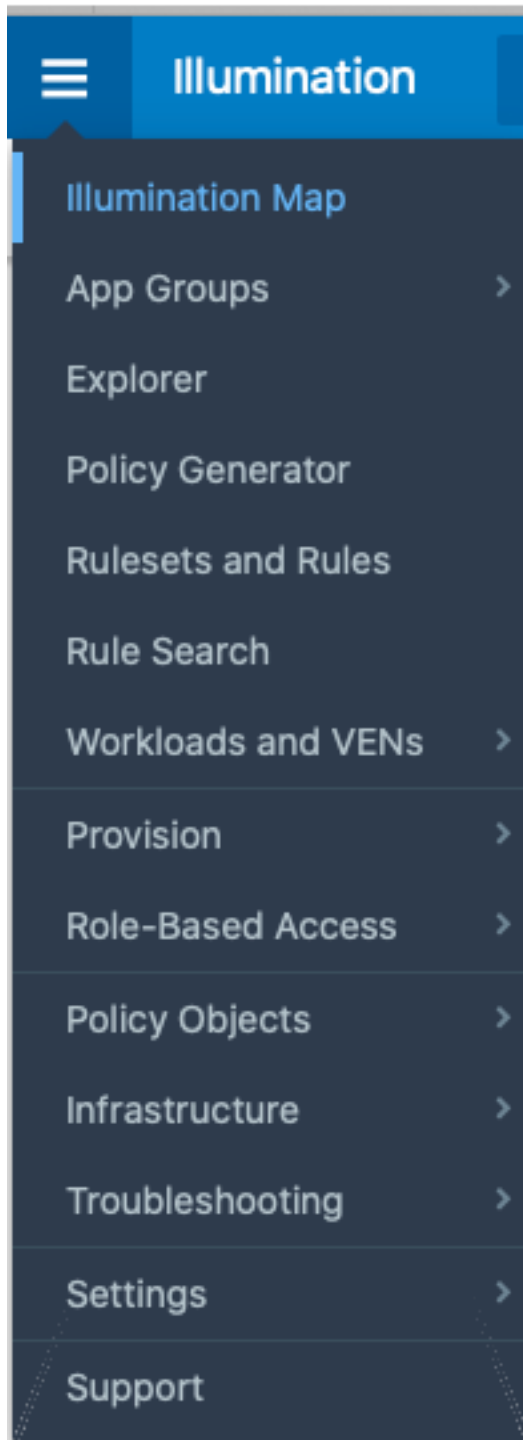
Scoped Roles = Limited Menu
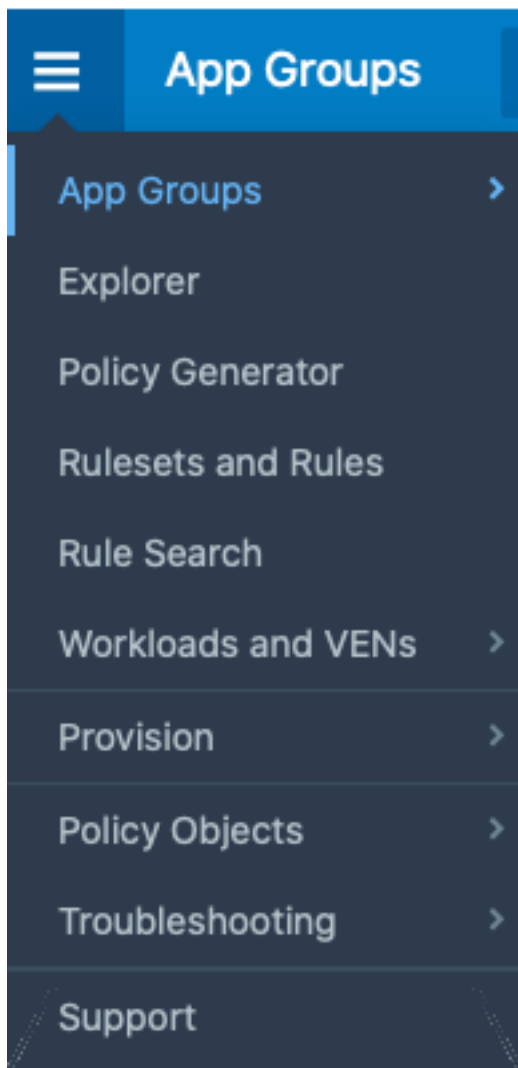
The following table provides the menu options available for different scoped users.

- Y = Yes (menu option is displayed for the user)
- N/A = Not applicable (menu option is hidden from the user)

Page	Ruleset Viewer	Ruleset Manager	Ruleset Provisioner	Workload Manager
Illumination Map	N/A	N/A	N/A	N/A
Role-based Access	N/A	N/A	N/A	N/A
Policy Objects > Segmentation Templates	N/A	N/A	N/A	N/A

Page	Ruleset Viewer	Ruleset Manager	Ruleset Provisioner	Workload Manager
Policy Objects > Pairing Profiles	N/A	N/A	N/A	Y
Infrastructure	N/A	N/A	N/A	N/A
Troubleshooting > Events	N/A	N/A	N/A	N/A
Troubleshooting > Support Reports	N/A	N/A	N/A	Y
Settings	N/A	N/A	N/A	See row below
Settings > VEN Library	N/A	N/A	N/A	Y
PCE Health	N/A	N/A	N/A	N/A
App Groups > Map	Y	Y	Y	N/A (App Group Members are visible)
App Groups > List	Y	Y	Y	Y
App Groups > Vulnerability Map	Y	Y	Y	N/A
Explorer	Y	Y	Y	N/A
Policy Generator	Y	Y	Y	N/A
Rulesets and Rules	Y	Y	Y	N/A
Rule Search	Y	Y	Y	N/A
Workload Management > Workloads	Y	Y	Y	Y
Workload Management > Container Workloads	Y	Y	Y	Y
Workload Management > Virtual Enforcement Nodes (Agents)	Y	Y	Y	Y
Provision > Draft Changes	Y	Y	Y	N/A
Provision > Policy Versions	Y	Y	Y	N/A
Policy Objects > IP Lists	Y	Y	Y	Y
Policy Objects > Services	Y	Y	Y	Y
Policy Objects > Labels	Y	Y	Y	Y
Policy Objects > User Groups	Y	Y	Y	Y
Policy Objects > Label Groups	Y	Y	Y	Y
Policy Objects > Virtual Ser-	Y	Y	Y	Y

Page	Ruleset Viewer	Ruleset Manager	Ruleset Provisioner	Workload Manager
vices				
Policy Objects > Virtual Servers	Y	Y	Y	Y
Troubleshooting > Blocked Traffic	Y	Y	Y	N/A
Troubleshooting > Export Reports	Y	Y	Y	Y
Troubleshooting > Policy Check	Y	Y	Y	N/A
Troubleshooting > Product Version	Y	Y	Y	Y
Support	Y	Y	Y	Y
My Profile	Y	Y	Y	Y
My Roles	Y	Y	Y	Y
My API Keys	Y	Y	Y	Y
Help	Y	Y	Y	Y
Terms	Y	Y	Y	Y
Patents	Y	Y	Y	Y
Privacy	Y	Y	Y	Y
About Illumio	Y	Y	Y	Y

Landing Page

The PCE landing page changes dynamically based on the user's role. When you log in to your account as an Organization Owner, the Illumination page opens. However, when you log in as a Scoped user, the landing page changes to the App Groups List page where you can see the list of App Groups assigned.

Labeled Objects

Labeled objects, such as workloads are filtered by the scope of the user. On the Workloads page, you will only see the list of the workloads within the application scope. You cannot see any workloads that are outside the application scope. This applies to any labeled object, such as workloads, containers, Virtual Services, and Virtual Enforcement Nodes (VENs).

The menu functions and buttons change dynamically to reflect a user's permissions. If you are logged in as a Ruleset Manager, you are not allowed to manage workloads. So, all the workload-specific operations buttons are disabled. However, you are allowed to view the list of workloads within the scope and get details for individual workloads, except for Virtual Servers.

> **NOTE:**
> While Virtual Servers are considered labeled objects, they are visible to all scoped users regardless of object scope.

Facet Searches and Auto-complete

The search bar with auto-complete and facets is scoped for labeled objects and Rulesets. For example, you search for Application Labels, then you can only select the Application Labels under the assigned scope. This applies to other label types such as Environment labels and Location labels. However, Role labels are excluded since Role labels are not part of the user scope. The restriction of visibility by scope applies to facets such as hostname, IP address, and others. The search bar automatically filters the facets to the list of facets in the user's assigned scope.

Global Objects

Scoped users get full read-only visibility into all global objects. This includes IP Lists, services, labels, label groups, and user groups. However, scoped users are not allowed to create, modify, or provision global objects.

> **NOTE:**
> Only Global Organization Owner and Global Administrator can create, modify, and provision global objects.
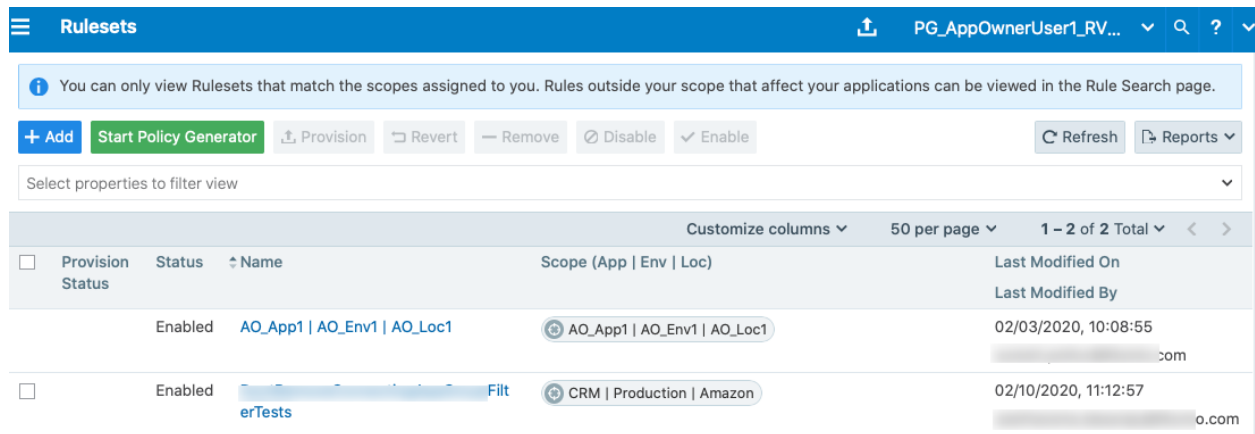
Rulesets and Rules

Scoped users, with the exception of Workload Managers, are allowed to see rulesets and rules which apply to their application. A Ruleset Manager is allowed to edit the

ruleset whereas the other scoped roles (Ruleset Viewer and Ruleset Provisioner) are allowed to view rulesets. A scoped user can see all the rules within the application ruleset.

When label groups are used within the scope of a ruleset, a Ruleset Manager may not be allowed to edit the ruleset and it's rules even if there is a scope match between the user's assigned scope and the underlying scope of the ruleset. The user will however be able to view the rules within such a ruleset.

In addition, scoped users can also see rules which apply to their application. For example, scoped users are allowed to view rules written by other applications that apply to their application. To see those rules, click **Rule Search** from the navigation menu.

On the Rule Search page, a scoped user can see all the rules that apply to their application. This includes rules for incoming and outgoing traffic flows. The rules highlighted in the screenshot below are the outbound rules which are for your application. Application Owner provides the visibility to see all the rules that are applied to your application.

App Group Map

The App Group Map provides complete visibility into applications and everything inside the application. Scoped users, with the exception of Workload Managers, can view App Group Maps. Scoped users get complete visibility into everything inside their application group. Scoped users can see workload objects, labels, traffic flows and every other detail within their application group.

For connected App Groups such as Providing App Groups and Consuming App Groups, scoped users get limited visibility. Scoped users get limited information on endpoints with traffic flows to their application. For an endpoint in a connected App Group from which there is traffic flow, scoped users can get limited information such as labels, role name, and hostname. The scoped user is not allowed to view any other endpoints in the connected App Group from which there are no traffic flows. To view the Illumination Map, the user should be assigned a Global role such as Global Organization Owner, Global Administrator, or Global Viewer.
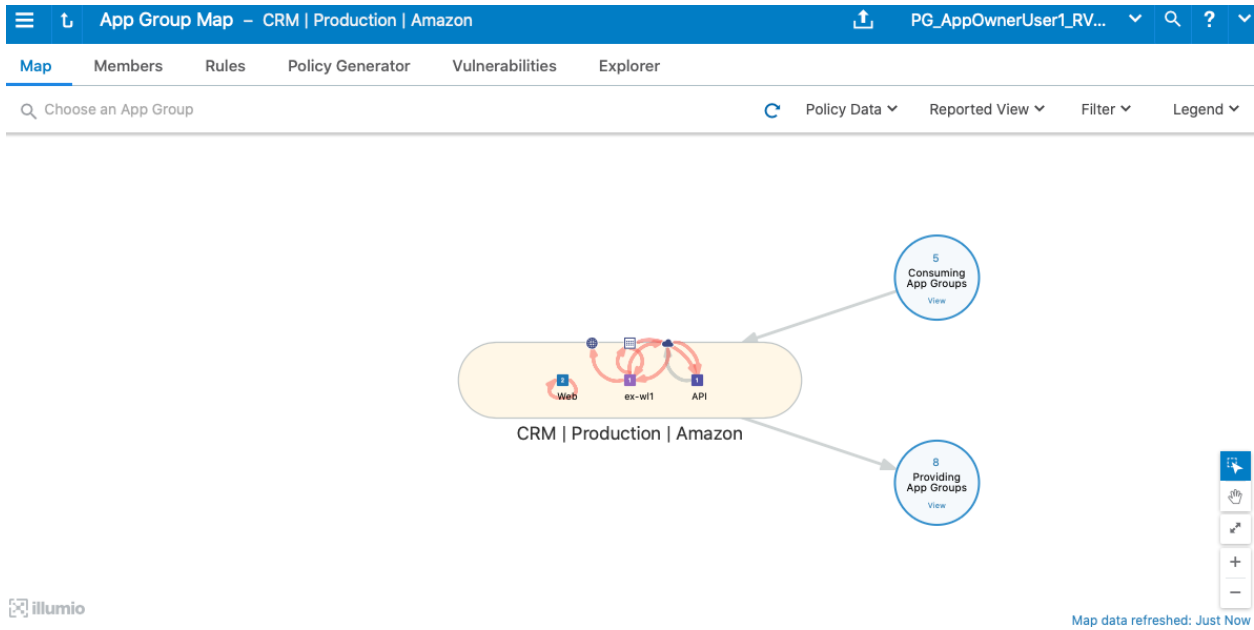
> **NOTE:**
> For Scoped Roles, only the App-Group Map is available and the Illumination
> Map is not available.

Policy Generator and Explorer

With Policy Generator, scoped users can generate policies only for their applications. Only Ruleset Managers are allowed to generate policy with Policy Generator. Ruleset Viewers are allowed to preview Policy Generator without the ability to save policy.

Explorer views are also filtered for scoped users. To use Explorer, one of the end-points has to be within the scoped user's application. The same applies to Blocked Traffic.

My Roles

"My Roles" is a new feature that allows you to view the list of assigned permissions (roles).

Configure Access Restrictions and Trusted Proxy IPs

To employ automation for managing the PCE environment, you can use API Keys cre-ated by an admin user and automate PCE management tasks. This section tells how you can restrict the use of API keys and the PCE web interface by IP address. In this way, you can block API requests and users coming in from non-allowed IP addresses.

Configure Access Restrictions

This section tells how to use the Illumio web console UI to configure access restric-tions. You can also configure access restrictions programmatically using the REST API calls described in Access Restrictions and Trusted Proxy IPs in the Illumio REST API Developer Guide.

- You must have the global Org Owner role to view or change access restrictions.
- A maximum of 50 access restrictions can be defined.

To configure access restrictions:

1. Log in to the PCE web console as a user with the Global Org Owner role.
2. Open the menu and choose **Access Management** - **Access Restrictions**.

   The Access Restriction page opens with a list that shows which IP addresses are allowed and where the restrictions have been applied.

3. To add a new restriction, click **Add**.

   The Add Access Restriction page opens.

   Provide the required attributes:

   - Provide a name.
   - In **Restriction Applies To**, choose User Session, API Key, or Both. Access restrictions can be applied to these different types of user authentication.
   - List a maximum of eight IPv4 adresses or CIDR blocks.

4. Click **Edit** to edit the restriction.
5. View the access restrictions applied to local users. The default is blank, no restric-tions.
6. You can assign access restrictions to local and external users or user groups. To add a local user:

   a. Click **Add**.
   b. In **Access Restriction**, choose the type of access restriction.
   c. Click **Add**.

7. View the local user's detail page. To modify the user settings, click **Edit User**.
8. Use the Edit User dialog to apply restrictions.

   If an Org Owner assigns an access restriction to any Org Owner, a warning is shown, because this can result in the Org Owner user losing access to the PCE.

9. View the list of API keys in the API Keys page and the Event page.

Configure Trusted Proxy IPs

This section tells how to use the Illumio web console UI to configure trusted proxy IPs. You can also configure trusted proxy IPs programmatically using the REST API calls as described in Access Restrictions and Trusted Proxy IPs in the Illumio REST API Developer Guide.

When a client is connected to the PCE's haproxy server, this connection can traverse one or more load balancers or proxies. Therefore, the source IP address of a client connection to haproxy might not be the actual public IP address of the client.

1. Log in to the PCE web console as a user with the Global Org Owner role.
2. Open the menu and choose **Settings - Trusted Proxy IPs**.
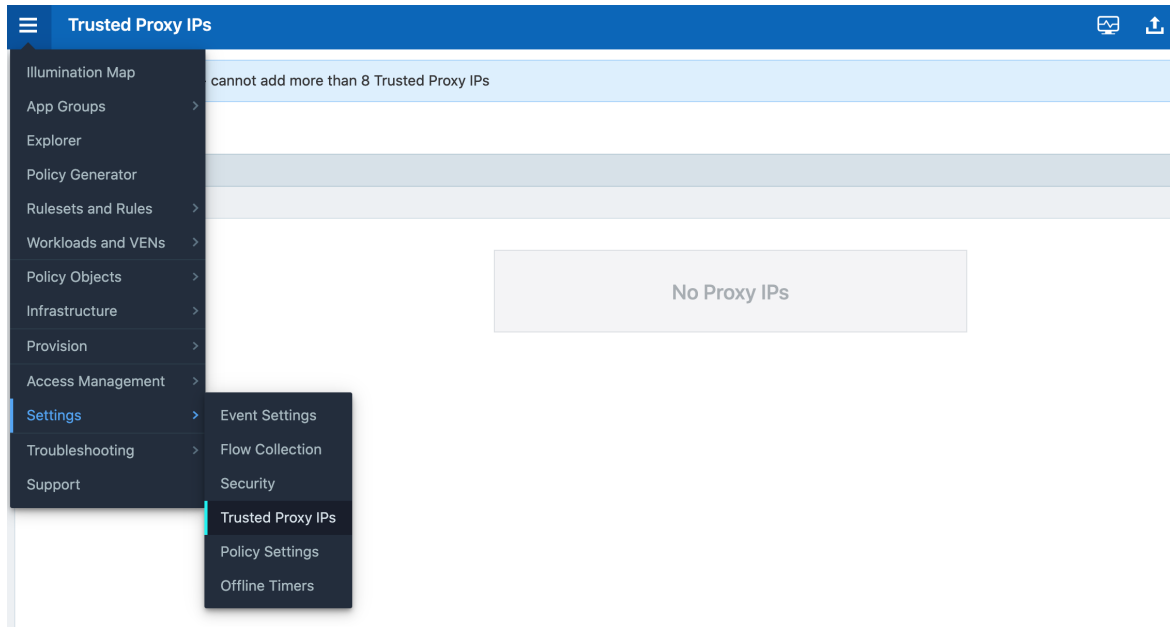
3. Click **Edit**.
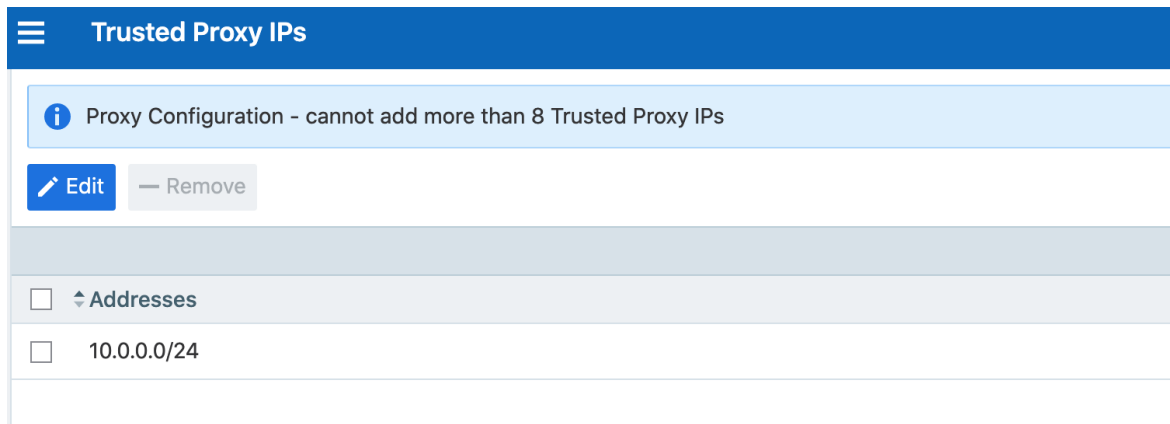
4. In **IP Addresses**, enter up to eight IPv4 addresses or CIDR blocks.
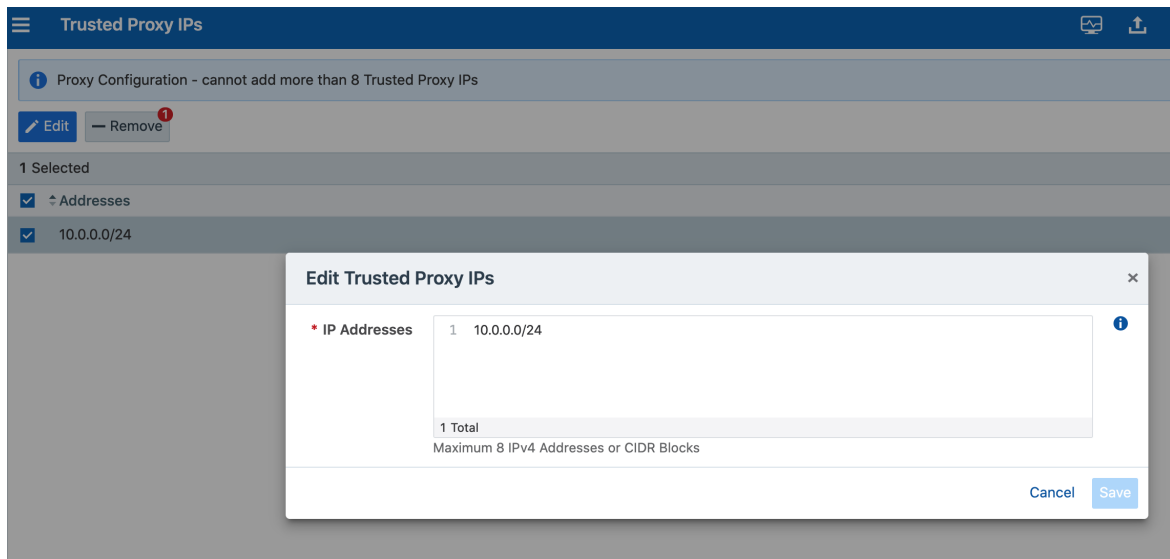
5. Click **Save**.

Password Policy Configuration

The PCE enforces password policies that only a Global Organization Owner can configure. In the PCE web console, you set password policies that the PCE enforces, such as password length, composition (required number and types of characters), and password expiration, re-use, and history.

About Password Policy for the PCE

You need to be a Global Organization Owner to view the Password Policy feature under the Settings > Authentication menu options.

Prior to Illumio Core 18.2.0, a Global Organization Owner set the password in the PCE by using the PCE runtime script. The settings in the PCE runtime script are the same as before Illumio Core 18.2.0, except that the password length can now be set to a maximum of 64 characters.

> NOTE:
> The Password Policy feature is not applicable for organizations using SAML authentication.

> NOTE:
> Permission to edit this setting is dependent on your role. See About Roles, Scopes, and Granted Access for information.

Password Requirements

The password requirements you set are displayed to users when they are required to change their passwords. You can set the minimum character length, ranging from a minimum of 8 characters to a maximum of 64 characters. The default length is 8 characters.

A Global Organization Owner should configure passwords based on the following categories:

- Uppercase English letters
- Lowercase English letters
- Numbers 0 through 9 inclusive
- Any of the following special characters: ! @ # $ % ^ & * < > ?

You have to select at least three of the above categories. The default password requirement is one number, one uppercase character, and one lowercase character. You can set the password to use either one or two characters from each category.

Password Expiration and Reuse

You can set the password expiration range from 1 day to 999 days. The default setting for password expiration is "Never."

You can set the password reuse history from 1 to 24 passwords before a user can reuse the old password. The default setting is five password changes before reuse of the password is allowed.

> ✅ NOTE:
> The number of password changes before password reuse is allowed is the value you enter + 1 (the current password). For example, when you specify 3, the number of passwords before reuse is allowed is 4.

You can also set the similarity of a password by not allowing a user to change their password unless it changes from a minimum of 1 to a maximum of 4 characters and positions from their current password.

Allowable password reuse and password history can be set to from 1 to 24 passwords before reuse is allowed. The default setting for password reuse is five password changes before reuse is permitted.

Caveats

- When a Global Organization Owner increases the required minimum password length policy or increases the password complexity requirements and enables the password expiration (1-999 days), all the existing users must reset their passwords based on the new policy.
- When a Global Organization Owner configures the password to never expire, all users who were migrated from an older release to 18.2.0 must reset their passwords when they next log in.
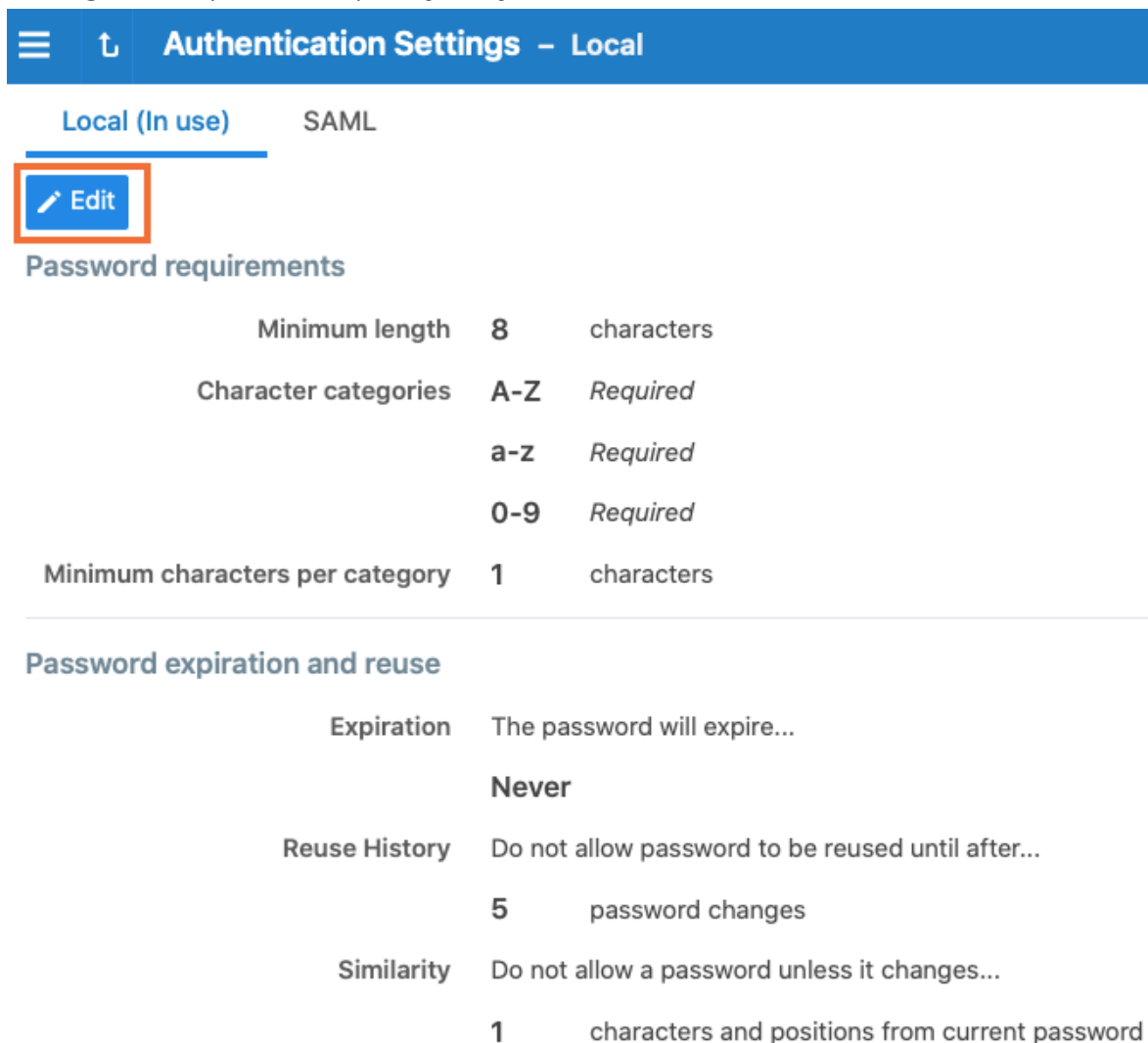
Change Password Policy Settings

1. From the PCE web console menu, choose **Settings** > **Authentication**.
2. Click **Configure** (Local).
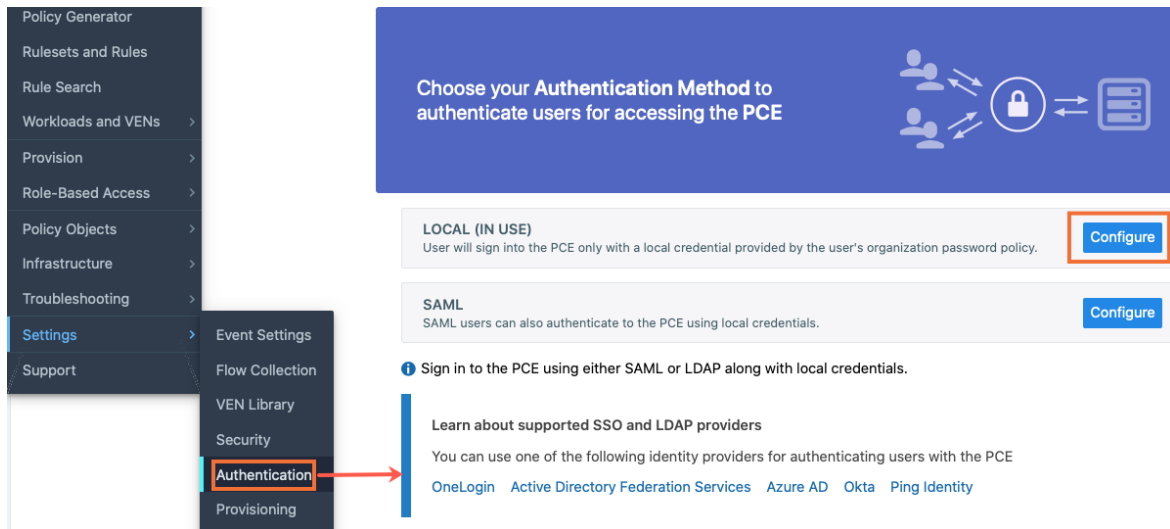
3. Click **Edit**.

4. Configure the password policy for your Illumio Core users:

5. Click **Confirm** and then **Save** to save the password policy for your local users.

Configure Session Timeout

You can configure the session timeout value using the PCE web console. The session expiration timeout values must be set accordingly to balance security and usability so that your users can comfortably complete operations within the PCE web console without their session frequently expiring. The timeout value is dependent on how crit-ical the application and its data are. For example, you might set the timeout to 3-5 minutes for high-value applications and 15-30 minutes for low-risk applications.

1. From the PCE web console menu, choose **Settings** > **Authentication**.
2. Click **Configure** (Local).

3. Click **Edit**.

4. In the *Session Timeout* section, set a value between 3 minutes and 30 minutes. By default, the value is 10 minutes.

5. Click **Confirm** and then **Save**.

> ✅ NOTE:
> The changed session timeout value applies to new browser sessions. Existing browser sessions are not affected when the session timeout value is changed.

Authentication

The Illumio PCE supports the use of either SAML SSO or LDAP as an external authentication method. Both SAML SSO and LDAP cannot be used at the same time. When LDAP is turned on, the use of SAML SSO, if already configured, is disabled. Similarly, enabling SAML SSO after LDAP is enabled will disable LDAP authentication.

SAML SSO Authentication

When you use a third-party SAML-based Identity provider (IdP) to manage user authentication in your organization, you can configure that IdP to work with the PCE. By configuring a single sign-on (SSO) IdP in the PCE, you can validate usernames and passwords against your own user management system, rather than having to create additional user passwords managed by the Illumio Core.

Illumio Core currently supports the following SAML-based IdPs:

- Azure AD
- Microsoft Active Directory Federation Services (AD FS)
- Okta
- OneLogin
- Ping Identity

> NOTE:
> You can use other SAML-based IdPs; however, configuring those IdPs is your responsibility as an Illumio customer.

Before you configure SSO in the PCE, you need to configure SSO on your chosen IdP and obtain the required SSO information. After obtaining the IdP SSO information, log into the PCE web console and complete the configuration.

PCE Information Needed to Configure SSO

Before you configure SSO in the PCE, obtain the following information from your IdP:

- x.509 certificate
- Remote Login URL
- Logout Landing URL

The PCE supports the following optional attributes in the SAML response from the IdP:

- User.FirstName - First Name
- User.LastName - Last Name
- User.MemberOf - Member of

Details

User email address is the primary attribute used by the PCE to uniquely identify users.

> **IMPORTANT:**
> The client browser must have access to both the PCE and the IdP service.
> The Illumio PCE uses HTTP-redirect binding to transmit SAML messages.

To obtain the SSO information from the PCE:

1. From the PCE web console menu, choose **Access Management** > **Authentication**.
2. On the Authentication Settings screen, locate the SAML configuration panel and click **Configure**.
3. Use the displayed information (as shown in the example below) while configuring your specific IdP.

Information for Identity Provider

Authentication Method	Unspecified
Force Re-authentication	No
SAML Version	2.0
Issuer	https://c 3/login
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer URL	https:// 3/login/acs/a63e 49598e
Logout URL	https:// 43/login/logout/a63 49598e

> **NOTE:**
> Even though the SAML NameID format specifies an emailAddress, the PCE can support any unique identifier such as, userPrincipalName (UPN), common name (CN), or samAccountName as long as the IdP is configured to map to the corresponding unique user identifier.

Signing for SAML Requests

There are four new APIs you can use to sign SAML requests:

- `GET /authentication_settings/saml_configs`

- `GET /authentication_settings/saml_configs/:uuid`

- `PUT /authentication_settings/saml_configs/:uuid`

- `POST /authentication_settings/saml_configs/:uuid/pce_signing_cert`

These APIs are covered in detail in the *REST API Developer Guide*.

Signing of SAML requests is, however, disabled by default.

To enable SAML request signing:

1. Using the Web Console, go to **Access Management > Authentication**.

2. In the *Authentication Setting* screen, select **Configure** button for SAML.

3. In the SAML screen, click **Turn On**.
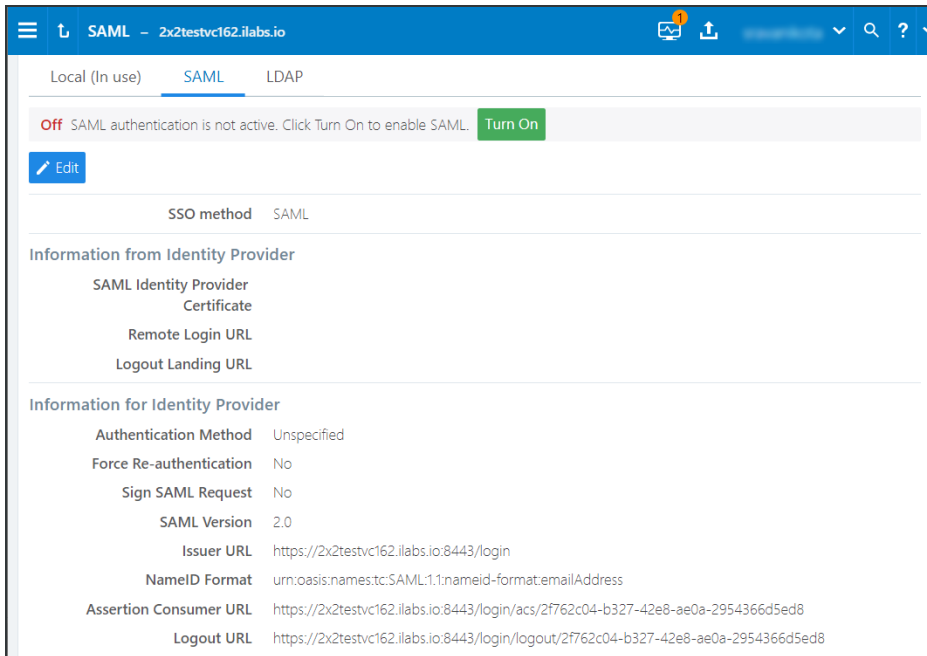
4. In the pop-up screen, click **Confirm**.
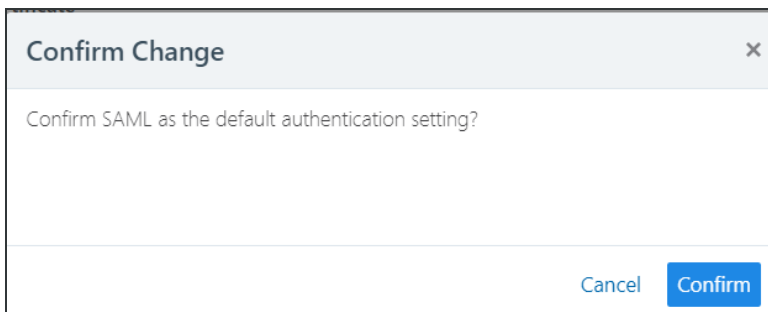
The updated SAML screen shows that SAML authentication is active.
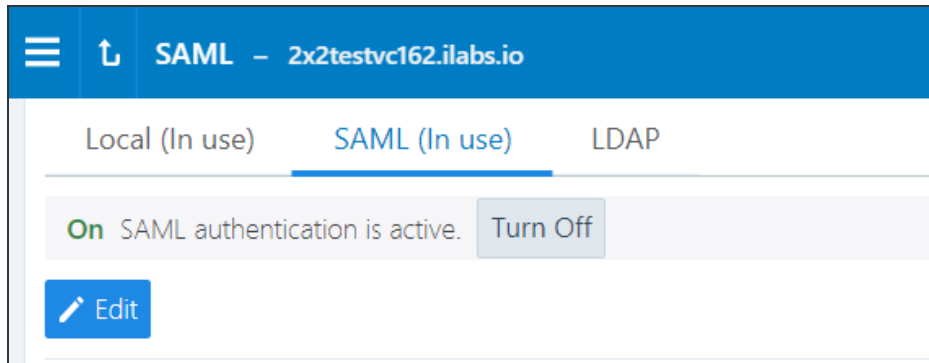
> If necessary, you can disable it at any time.

LDAP Authentication

The PCE supports LDAP authentication for users with OpenLDAP and Active Directory. The PCE supports user and role configuration for LDAP users and groups. You can configure up to three LDAP servers and map users and user groups from your LDAP servers to PCE roles.

To use LDAP authentication:

1. Review the Prerequisites and Limitations.
2. Enable the PCE to use LDAP authentication. See Enable LDAP Authentication.
3. Set up an LDAP configuration. See Configure LDAP Authentication.
4. Map your LDAP groups to one or more PCE roles. See Map LDAP Groups to User Roles.

Prerequisites and Limitations

Before configuring LDAP for authentication with the PCE, complete the following prerequisites, and review the limitations.

Determine Your User Base DN (Distinguished Name)

Before you map your LDAP settings to PCE settings, determine your user base distinguished name ("DN"). The DN is the location in the directory where authentication information is stored.

If you are unable to get this information, contact your LDAP administrator for assistance.

Additional Considerations

When configuring the PCE to work with LDAP, be aware of the following support:

- PCE uses LDAP protocol version 3 (″v3″).
- Supported LDAP distributions include OpenLDAP 2.4 and Active Directory.
- Supported LDAP protocols include LDAP, LDAPS, or LDAP with STARTTLS.

Limitations

- Any user that is created locally will have precedence over an LDAP user of the same name. For example, if the LDAP server has a user with a username attribute (such as, cn or uid) of johndoe and the default PCE user of the same name is present, the PCE user takes precedence. Only the local password will be accepted and on login, the roles mapped to the local user will be in effect. To work around this limitation, you must delete the specific local user.
- LDAP and SAML single sign-on cannot be used together. An organization can either use LDAP or SAML single sign-on for authenticating external users.

Enable LDAP Authentication

To enable LDAP authentication:

1. Log in to the PCE web console as a Global Organization Owner.
2. Choose **Access Management** > **Authentication**.
3. In the Authentication Settings screen, locate the LDAP configuration panel and select **Configure**.
4. In the LDAP Authentication screen, select **Turn On**.

Configure LDAP Authentication

Follow these steps to configure LDAP authentication on the PCE. Make sure you have first followed the steps in Enable LDAP Authentication.

1. Log in to the PCE as a Global Organization Owner.
2. Choose **Access Management** > **Authentication**.
3. On the Authentication Settings screen, locate the LDAP configuration panel and click **Configure**.
4. In the LDAP Authentication screen, make sure LDAP is enabled.
5. Click **+ Create Server**.
6. In the LDAP Server Create Screen, enter information to configure LDAP as follows:

   - Name: Enter a friendly name for the LDAP server.
   - IP Address or Hostname: The IP address or hostname of the LDAP server.

- ○ Protocol: Select one from LDAP, LDAPS (Secure LDAP) or LDAP with STARTTLS.
- ○ Port: Enter a port number if you are not using a default port. Default ports are 389 for standard LDAP, 636 for LDAPS, and 389 for LDAP with STARTTLS.
- ○ Anonymous Bind: When using an Open LDAP server, you can use anonymous bind. Choose **Allow** if you want to use anonymous bind. When using Active Directory, the use of Anonymous Bind is not recommended. Choose **Do not Allow** and specify values for Bind DN and Bind Password.
- ○ Bind DN: Distinguished name (DN) used to bind to the LDAP server. The bind DN is required only when Anonymous Bind is set to **Do not Allow**.
- ○ Bind Password: Required only when Bind DN is required. When using Anonymous Bind, no bind password is used.
- ○ Request Timeout Period: This is the number of seconds to wait for a response from the LDAP server. The default is 5 seconds. It can be configured to any value from 1-60 seconds.
- ○ Trusted CA Bundle: The bundle of certificates including the chain of trust to use when the LDAP server uses either LDAPS or LDAP with STARTTLS.
- ○ Verify TLS: Enabled by default. This flag specifies whether to verify the server certificate when establishing an SSL connection to the LDAP server. Disabling this is not recommended.
- ○ User Base DN: Base DN of the LDAP directory to search for users.
- ○ User Search Filter: Search filter used to query the LDAP tree for users.
- ○ User Name Attribute: Attribute on a user object that contains the username. For example, uid, sAMAccountName, userPrincipalName.
- ○ Full Name Attribute: Attribute of a user object that contains the full name. For example, cn, commonName, displayName.
- ○ Group Membership Attribute: Attribute of a user object containing group membership information. For example, memberOf, isMemberOf.
7. Click **Test Connection** to verify that the PCE is able to successfully connect to the LDAP server. If Test Connection fails, check your LDAP configuration and retry.

You can enter up to three LDAP server configurations for a PCE. For more information about using multiple LDAP servers, see How the PCE Works with Multiple LDAP Servers.

Map LDAP Groups to User Roles

After you configure the PCE to use LDAP authentication, map PCE user roles to the LDAP server's groups. When a user attempts to log in, the PCE queries the server(s) to find the user. It grants the user permissions based on any PCE user roles associated with the LDAP groups in which the user is a member.

To change user permissions, use one of the following options:

- To change the permissions for a group of users, you can remap the LDAP group to a different PCE role.
- To change the permissions for an individual user, you can move the user to an LDAP group mapped to a different PCE role. You do this action on the LDAP server.

You can also perform these user management activities:

- Add a user to a PCE role: On the PCE, map the PCE role to an LDAP group. Then, on your LDAP server, add the user to that LDAP group.
- Remove a user from a PCE role: Remove the user from the corresponding LDAP group on your LDAP server.

A user can have membership in several roles. In that case, the user has access to all the capabilities available for any of those roles. For example, if a user is a member of both the docs and eng LDAP server groups, and the docs group is mapped to the PCE user role "Ruleset Manager" and the eng group is mapped to "Ruleset Provisioner," the user obtains all permissions assigned to both the "Ruleset Manager" and "Ruleset Provisioner" roles.

> ✅ **NOTE:**
> The PCE checks LDAP membership information when a user attempts to log in. You do not need to reload the authentication configuration when adding or removing users.

For details about how to map external groups to PCE user roles, see Setup for Role-based Access Control.

Modify LDAP Configuration

Follow these steps to update or delete an LDAP configuration in the PCE. It is assumed you have already followed the steps in Enable LDAP Authentication and Configure LDAP Authentication.

1. Log in to the PCE as a Global Organization Owner.
2. Choose **Access Management** > **Authentication**.
3. On the Authentication Settings screen, locate the LDAP configuration panel and click **Configure**.
4. In the LDAP Authentication screen, make sure LDAP is enabled.
5. Choose the desired action:

    o To delete a configuration, click the **Remove** icon.
    o To modify a configuration, click the **Edit** icon.

Verify LDAP Connectivity

Follow these steps to test the PCE's connection to the LDAP server(s). It is assumed you have already followed the steps in Enable LDAP Authentication and Configure LDAP Authentication.

1. Log in to the PCE as a Global Organization Owner.
2. Choose **Access Management** > **Authentication**.
3. On the Authentication Settings screen, locate the LDAP configuration panel and click **Configure**.
4. In the LDAP Authentication screen, make sure LDAP is enabled.
5. The LDAP Authentication screen displays a list of configured LDAP server entries. Click **Test Connection** next to each entry to check whether the configuration is working.

Secure LDAP with SSL/TLS Certificates

The PCE supports LDAPS and LDAP with STARTTLS. To use the PCE with secure LDAP, add the certificate chain to the local certificate store on the PCE. Follow these steps to configure secure LDAP. It is assumed you have already followed the steps in Enable LDAP Authentication and Configure LDAP Authentication.

1. Log in to the PCE as a Global Organization Owner.
2. Choose **Access Management** > **Authentication**.
3. On the Authentication Settings screen, locate the LDAP configuration panel and click **Configure**.
4. In the LDAP Authentication screen, make sure LDAP is enabled.
5. Select your LDAP server from the list of configured server entries and click the **Edit** icon.
6. Make sure **Protocol selected** is set to either LDAPS or LDAP with StartTLS.

7. For the Trusted CA bundle, click **Choose File** and upload the chain of certificate authority (CA) certificates for the LDAP server.

8. If your LDAP server uses self-signed certificates, uncheck the **Verify TLS** option.

> ✅ NOTE:
> The use of self-signed certificates for an LDAP server is not recommended. Illumio recommends the use of certificates signed by a valid CA.

Authentication Precedence

PCE local authentication takes precedence over any external systems. When the PCE authenticates a user, it follows this order:

1. The PCE attempts local authentication first. If the account is expired or otherwise fails, the PCE does not attempt to log in by using LDAP authentication.

2. If the local user does not exist, the PCE attempts LDAP login (if enabled).

How the PCE Works with Multiple LDAP Servers

You can configure up to three LDAP servers for each PCE. In a PCE supercluster deployment, the Illumio Core platform can support up to three LDAP servers per region.

When attempting to connect to an LDAP server, the PCE follows the order in which the servers were configured. When the request timeout expires, the PCE attempts to connect to the next server in the configuration. The PCE request timeout is configurable. By default, the timeout is 5 seconds.

For example, assume that you configure three LDAP servers in this order: A, B, C. The PCE attempts to connect to the servers in that order: A, B, C. If the PCE fails to connect to A, it attempts to connect to the remaining servers: first B, then C, after the expiration of the connection timeout.

When the PCE successfully connects to an LDAP server, it searches for the user on that server. If the user is found, the PCE stops looking. If the user is found on server A, even if the user also exists on B and C, the PCE will only use A's credentials for that user.

If the PCE successfully connects to an LDAP server but the user is not found, the PCE attempts to connect to the next server in the configured order, and searches for the user again.

You can not dynamically change the order in which the LDAP servers are contacted. To change this priority order, delete the configured entries and add them back in the desired order.

Active Directory Single Sign-on

This section describes how to configure Microsoft Active Directory Federation Services (AD FS) 3.0 for Single Sign-on (SSO) 2.0 authentication with the PCE.

Overview of AD FS SSO Configuration

To enable AD FS for the PCE, the PCE needs three fields returned as claims from:

- NameID
- Surname
- Given Name

There are two ways for AD FS to produce the NameID claim for an SSO user. The first uses the email field in an Active Directory user account for the NameID.

The second way to return a NameID of an Active Directory user is to use the User Principal Name (UPN). Each user created in Active Directory has an extension to their username that's ADUserName@yourADDomanName. For example, a user named "test" in an Active Directory domain called "testing.com" would have a UPN of test@testing.com.

Configure AD Users to Use Different UPN Suffixes

To configure different UPN suffix as the source for NameID:

1. Add a UPN suffix. On your system under Server Manager Tools, click **Active Directory Domains and Trusts**.
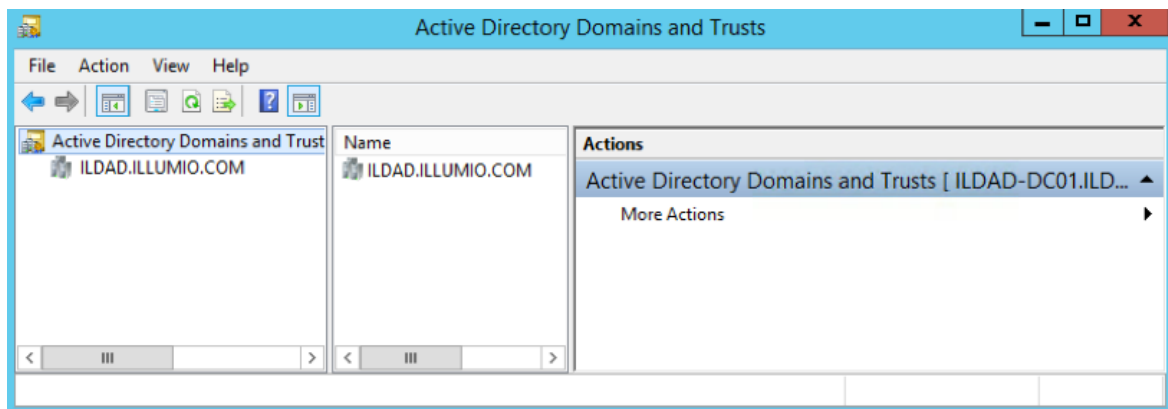
2. From the left side of the window, right-click *Active Directory Domains and Trusts*, and select **Properties**. In this dialog, you can create new suffixes for Active Directory usernames.
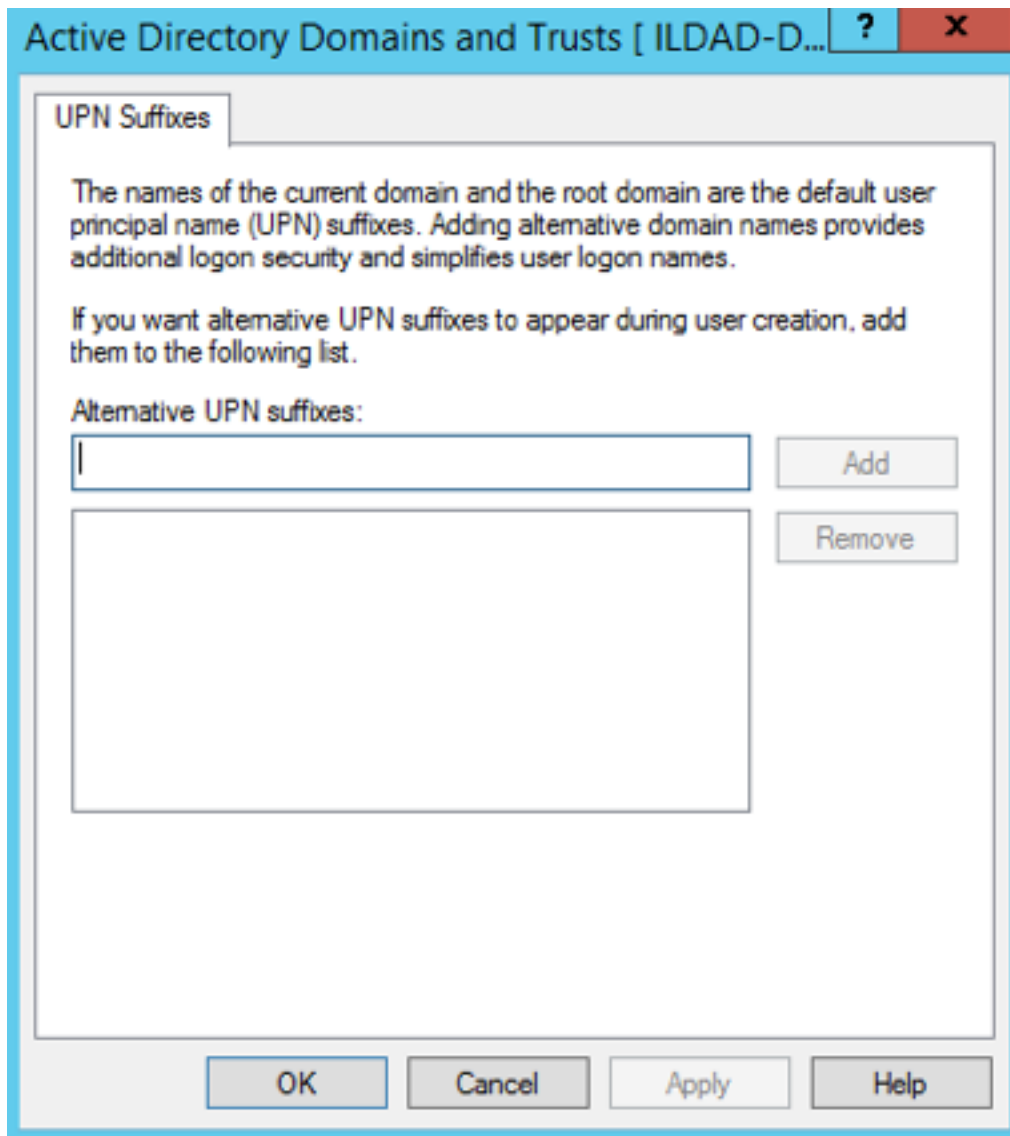
3. Create a suffix that matches the external namespace you'll be using and click **Add**.
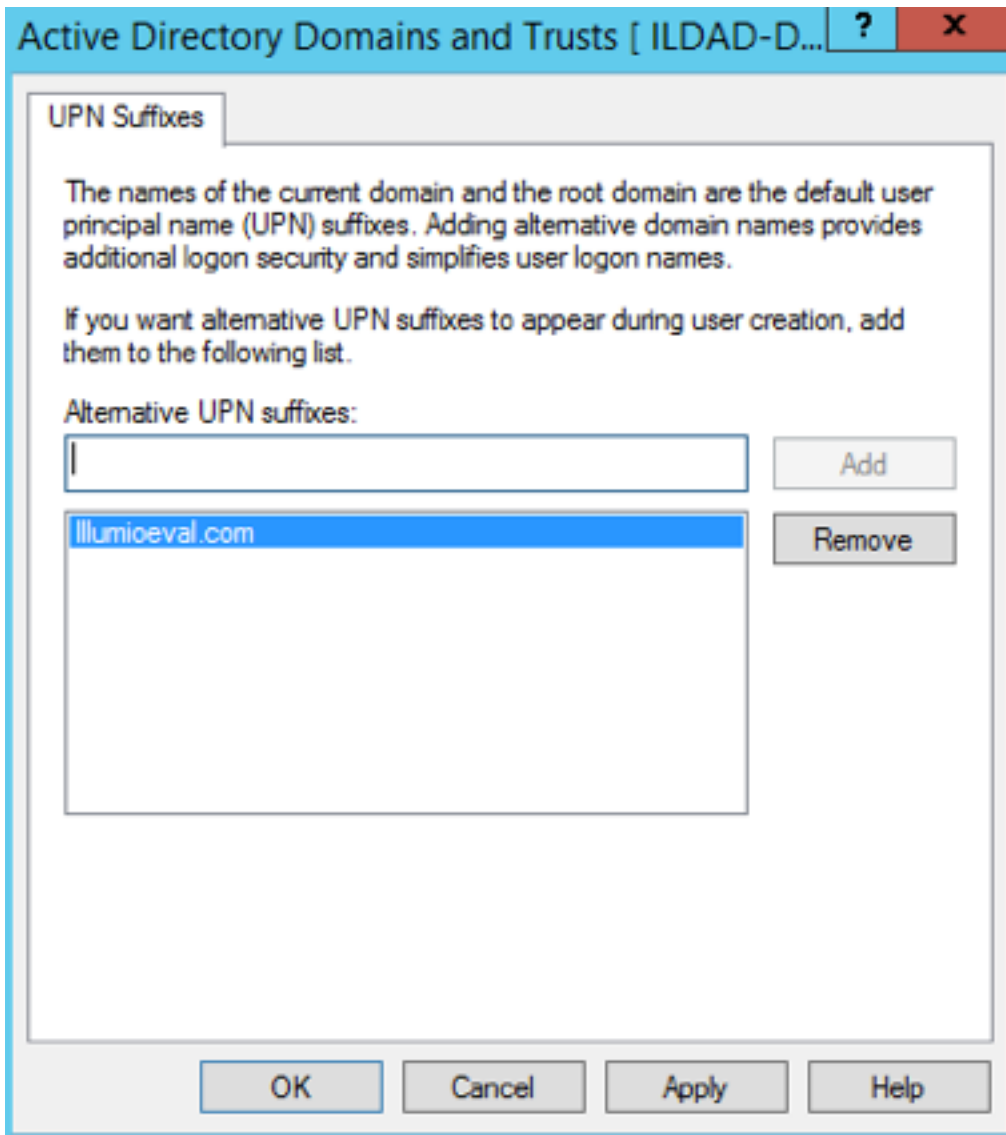
You can now assign an Active Directory user your custom UPN for the SAML response.

4. You can add multiple UPNs if needed. As shown below, you can select the UPN created in the previous steps.
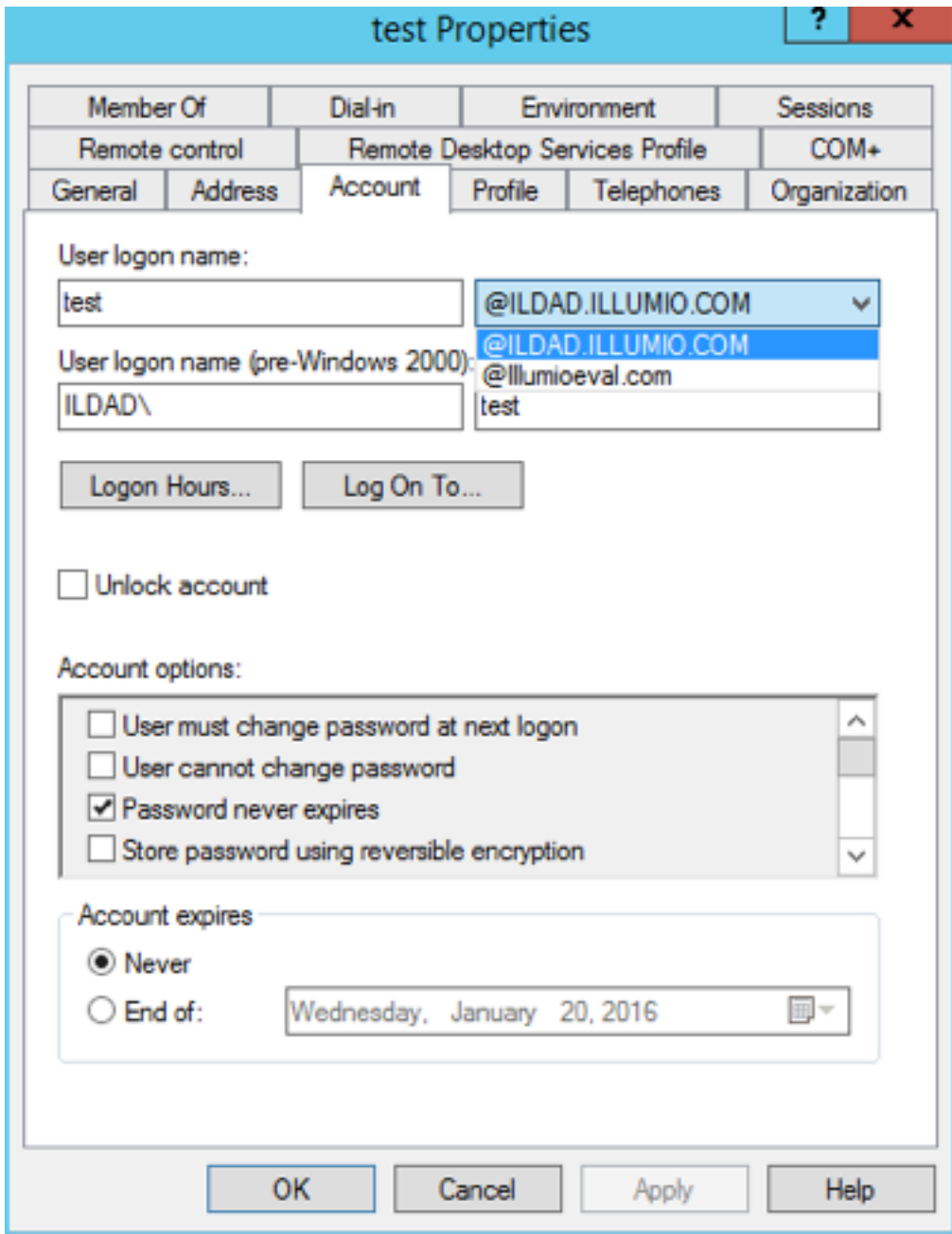
Your UPN configuration is set up and you can begin configuring AD FS for SSO with the PCE.

Initial AD FS SSO Configuration

This task explains how to perform the initial configuration of AD FS to be your SSO IdP for Illumio Core.

To configure AD FS:

1. Open Microsoft Server Manager and click the notification icon.

2. Click the "Configure the federation service on this server" link.

3. Select the "Create the first federation server in a federation server farm" option and click **Next**.
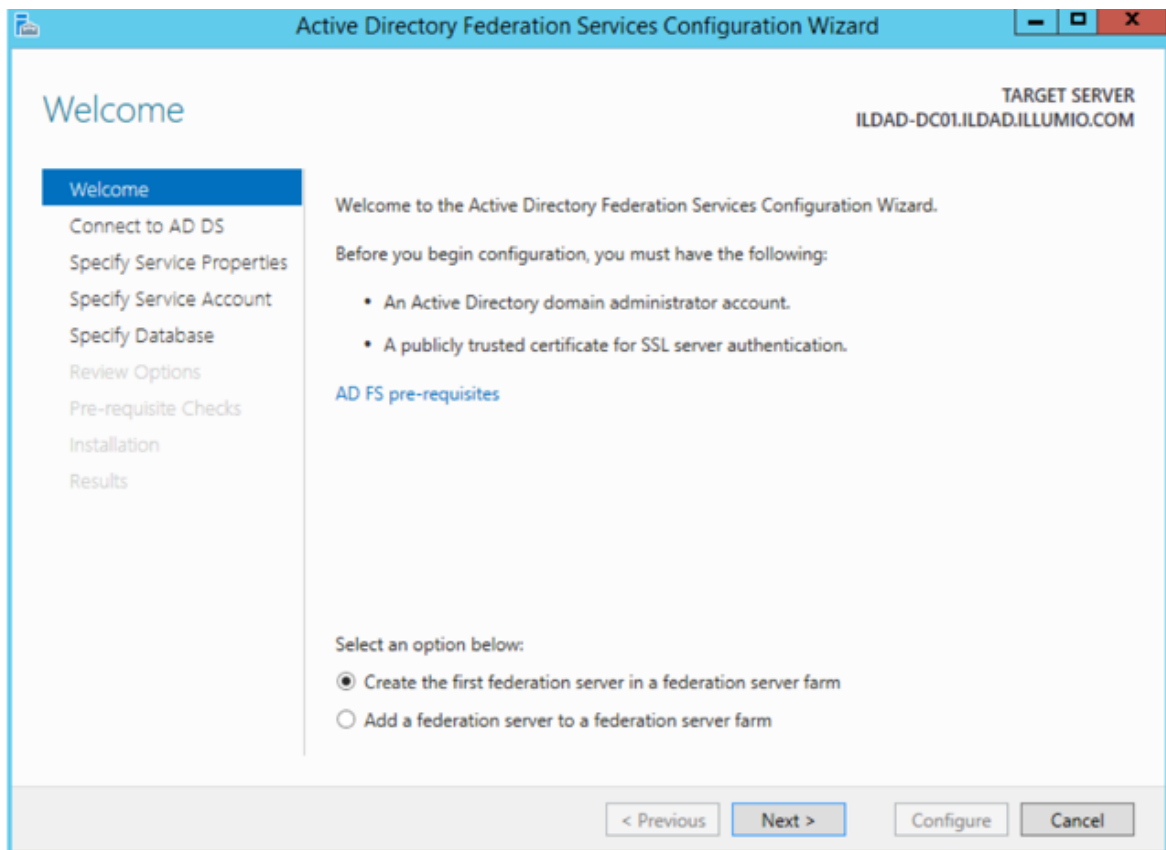
4. Specify a domain admin account for AD FS configuration.
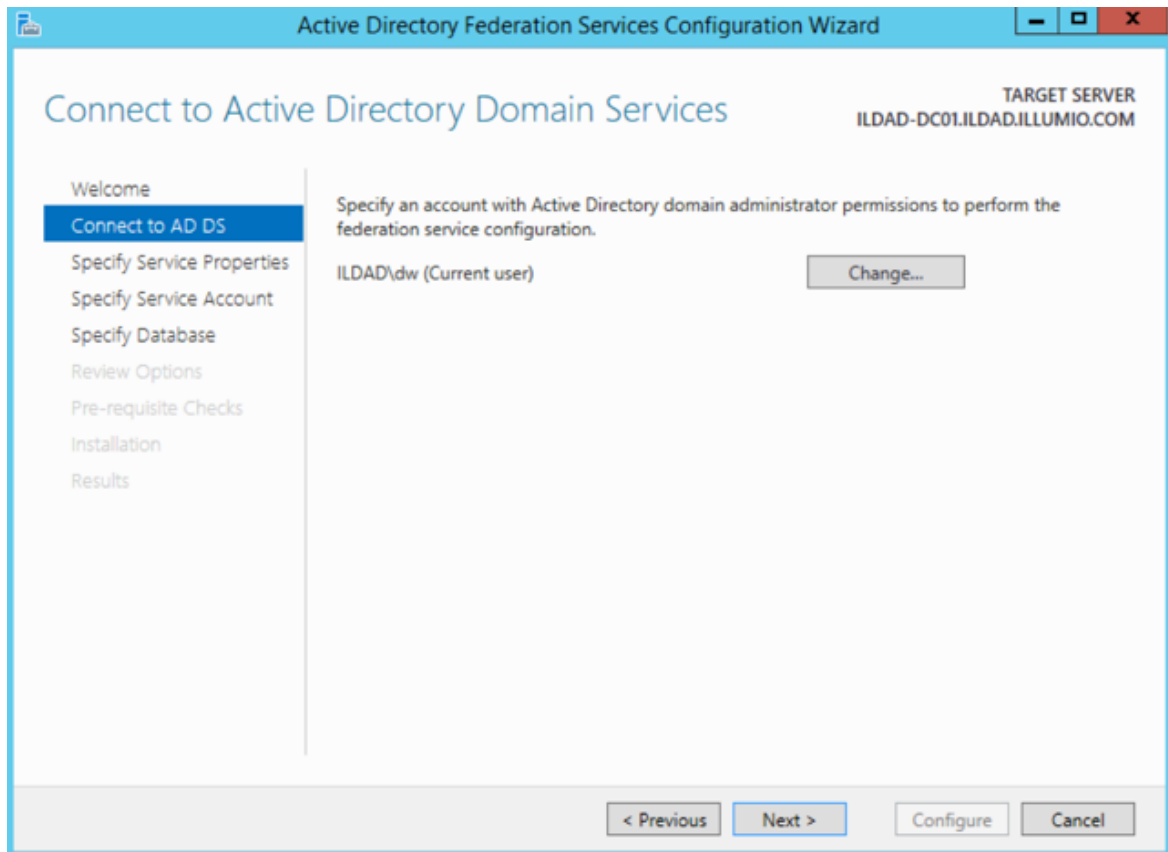
5. Select or import a certificate. This certificate can be a self-signed certificate.

6. Specify your Federated Service Name, enter a display name for this instance of AD FS, and click **Next**.
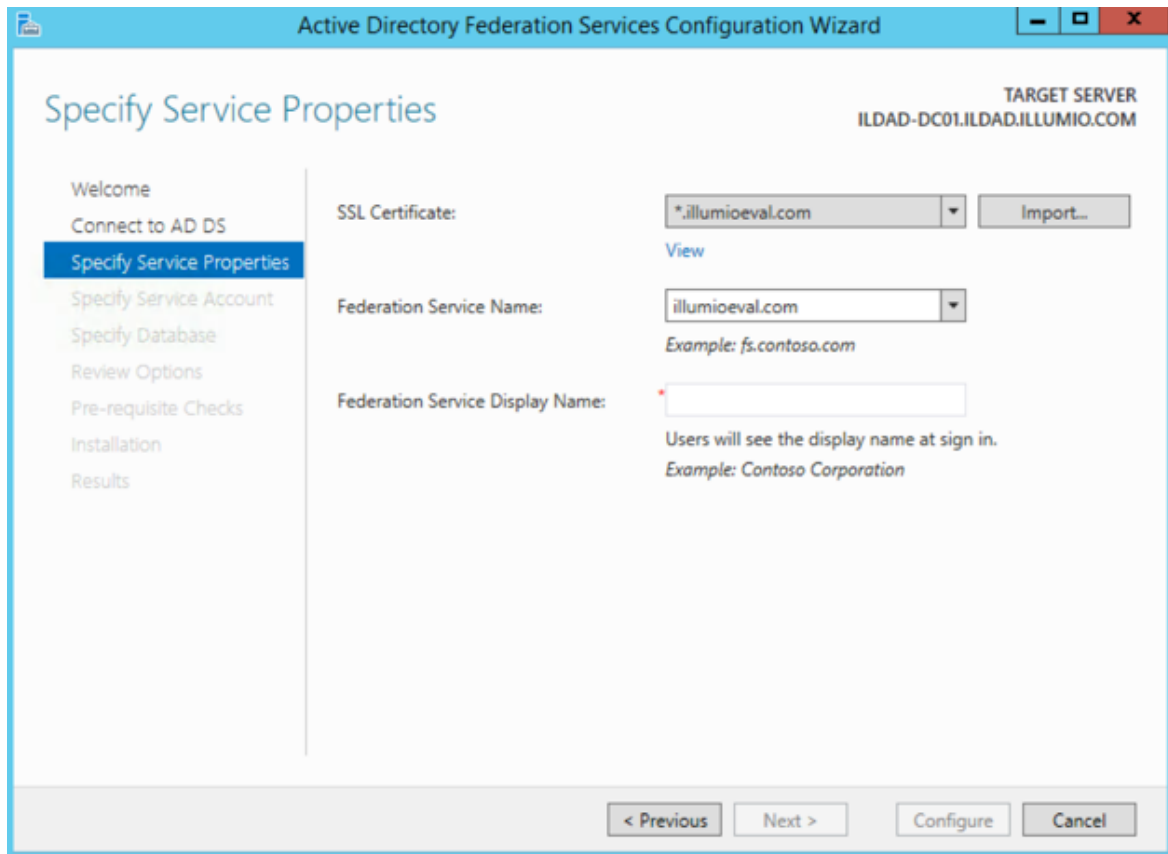
7. Specify your service account and click **Next**.
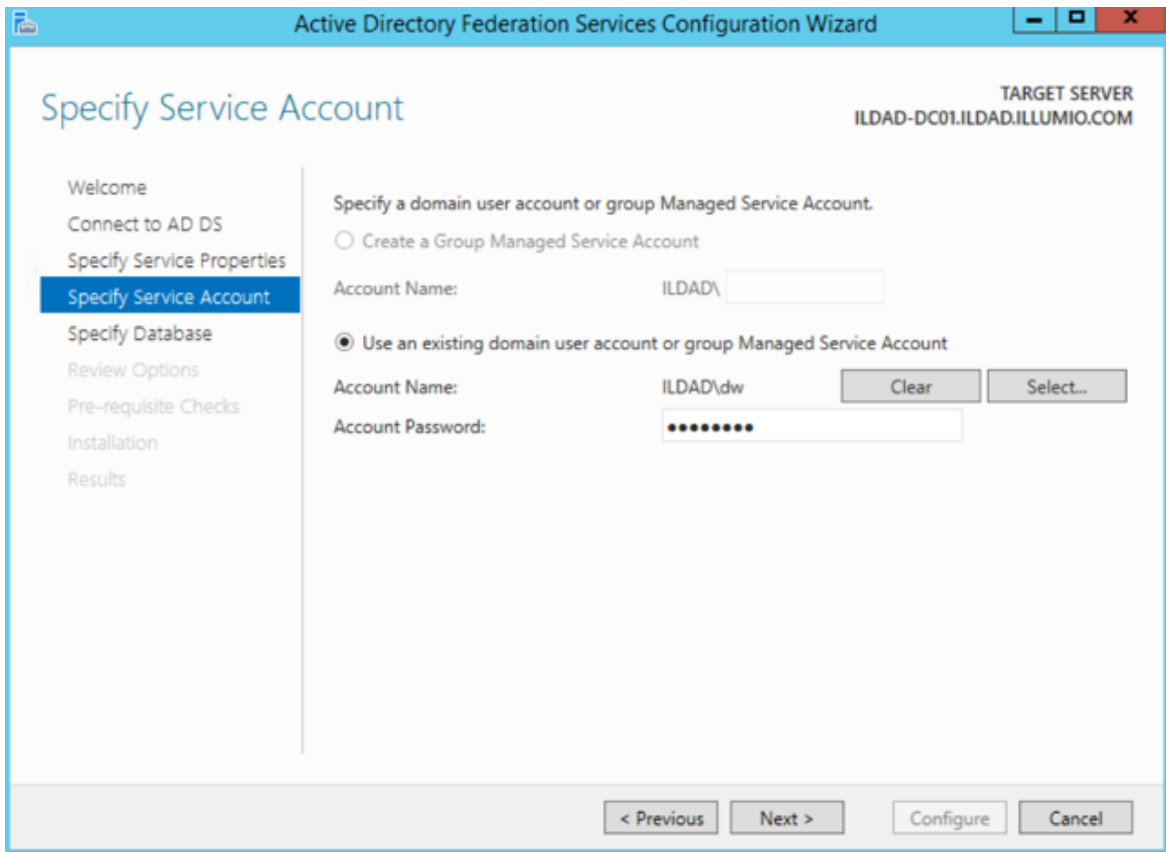
8. Select "Create a database on this server using Windows Internal Database" or choose the SQL server option, and click **Next**.
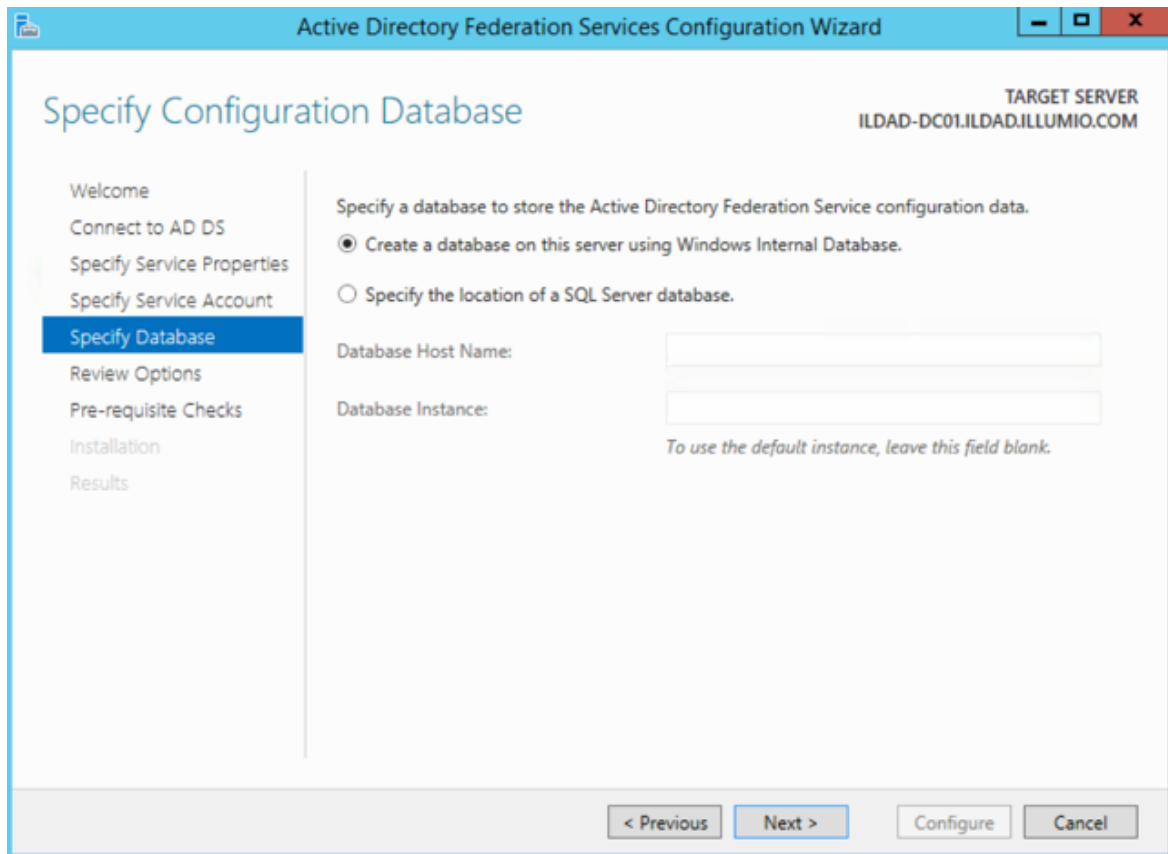
9. Review your selected options and click **Next**.
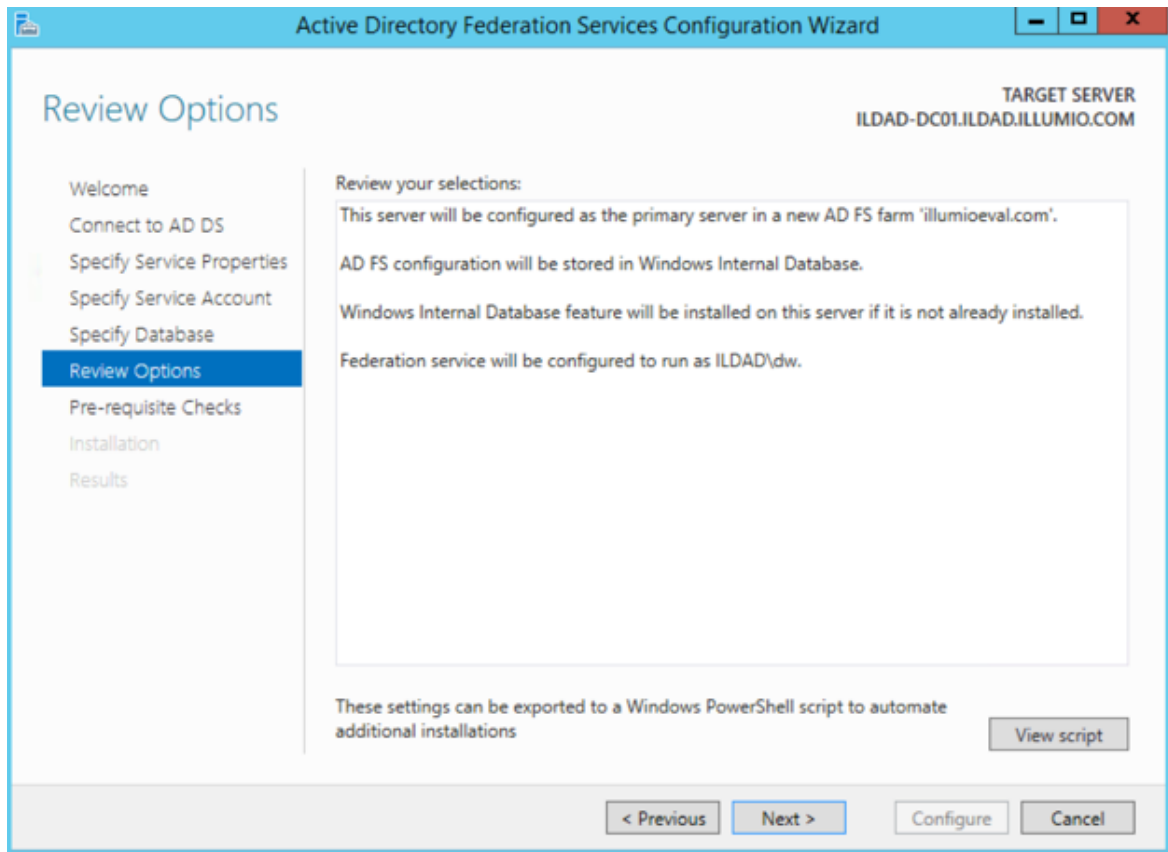
10. Click **Configure** to finish the basic configuration of AD FS.
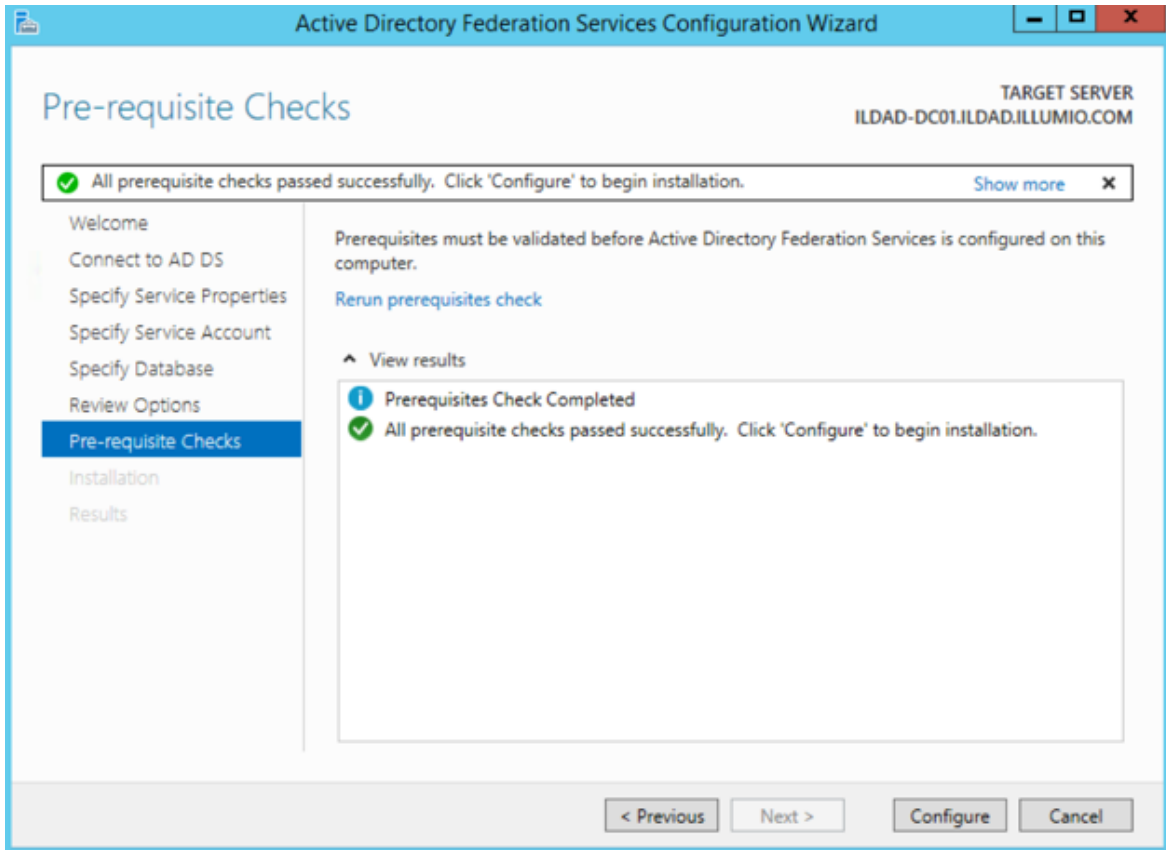
11. In the results screen, click **Close**.

    AD FS is now installed with the basic configuration on this host.

Create a Relying Party Trust

To start configuring AD FS for SSO with the PCE, you need to create a Relying Party Trust for your Illumio PCE.

1. From Server Manager/Tools, open the AD FS Manager.
2. From the left panel, choose **Relying Party Trusts** > **Add Relying Party Trust**.
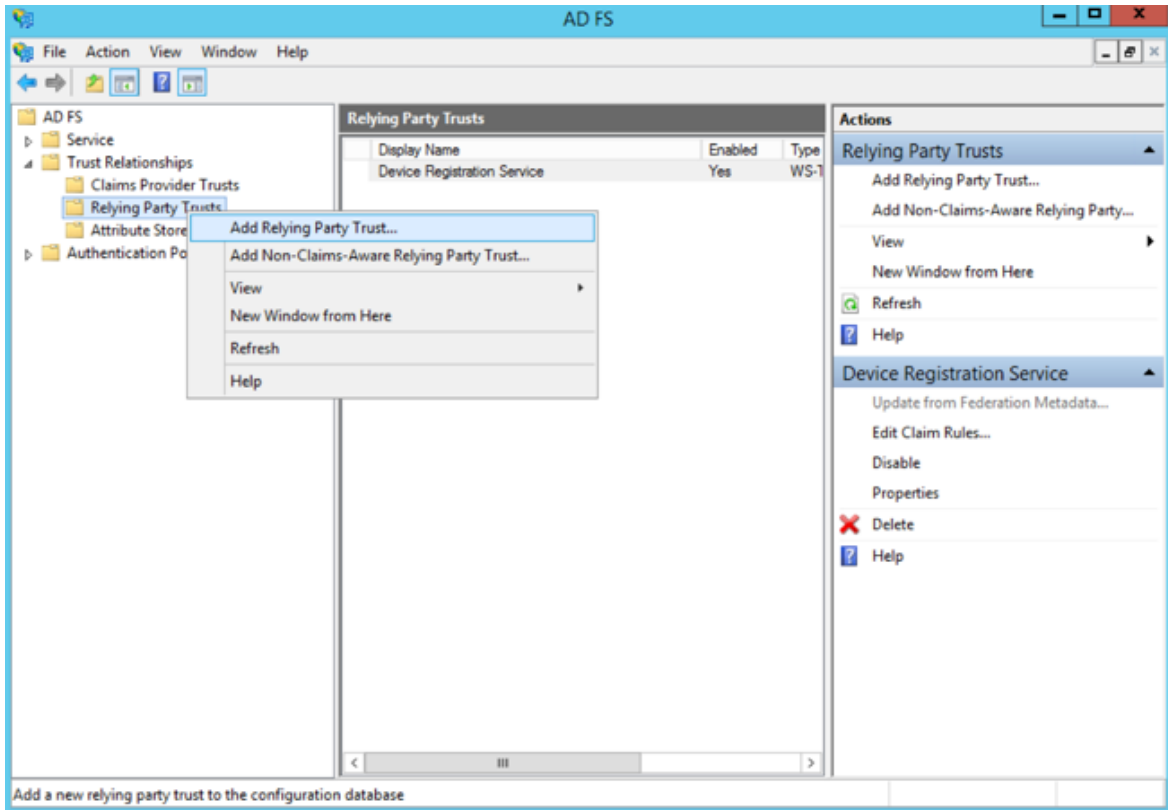
The Add Relying Party Trust Wizard appears.
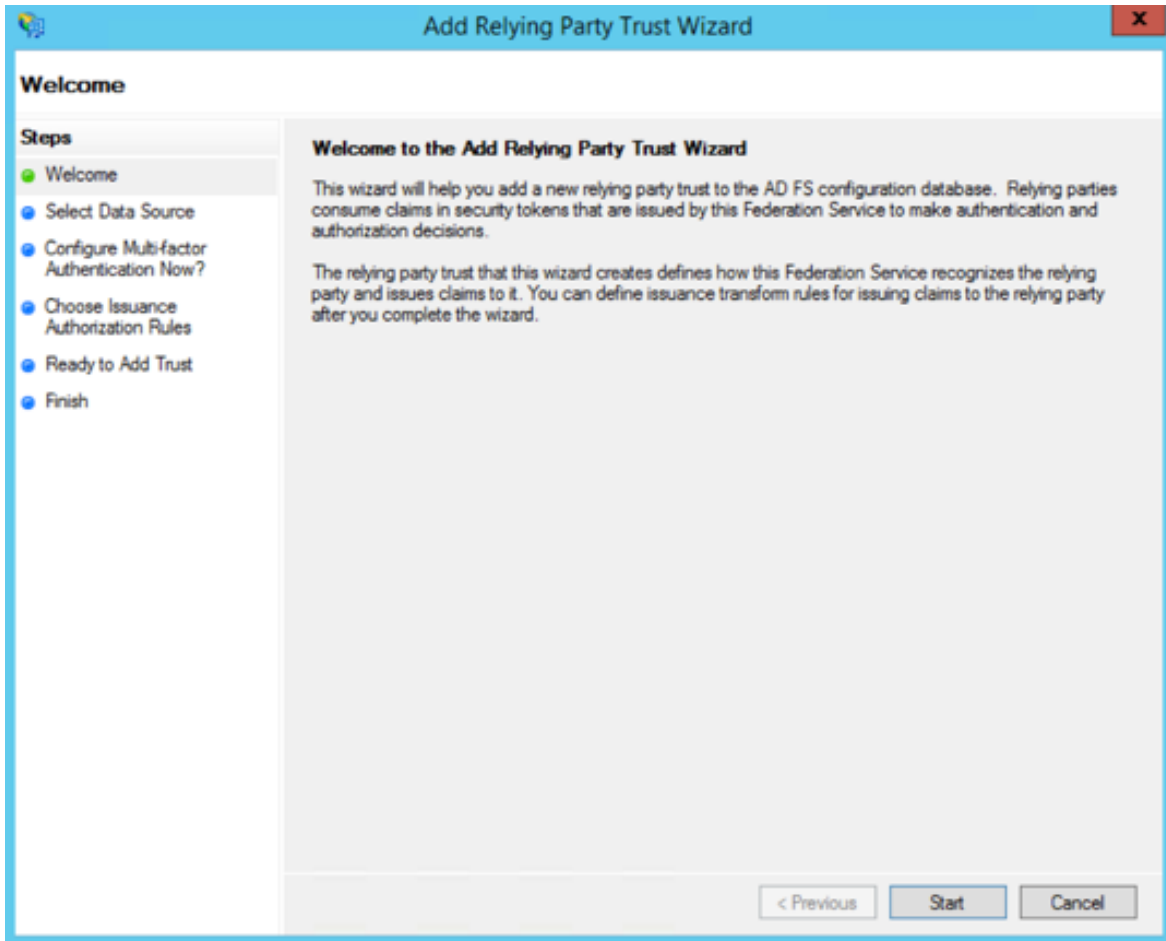
3. Click **Start**.

4. Select the "Enter data about the relying party manually" option and click **Next**.

5. Name your Relying Party Trust and click **Next**.

6. Select "ADFS profile" and click **Next**.
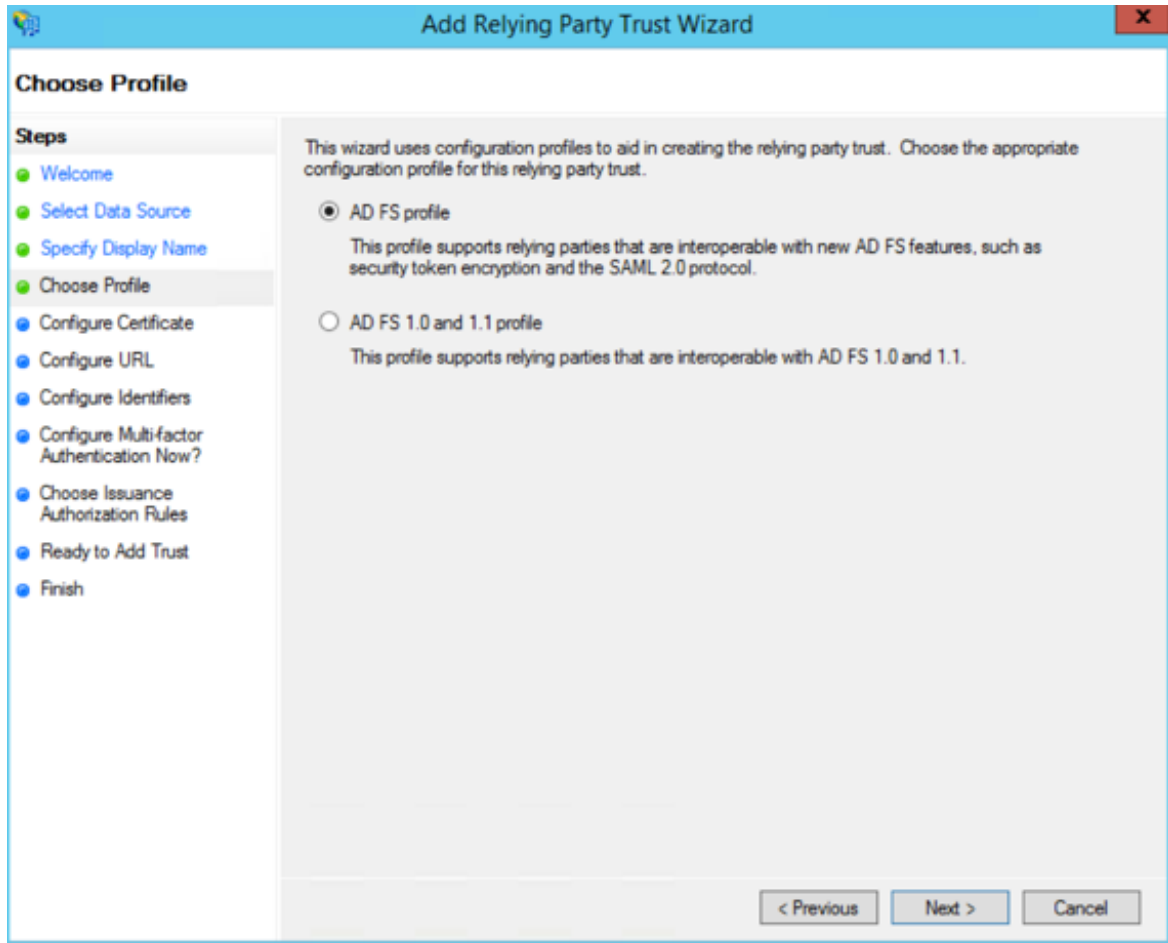
7. When you have a separate certificate for token encryption, browse to, select it, and click **Next**.

> ✔ NOTE:
> To use the standard AD FS certificate (created during AD FS install-ation) for token signing, don't select anything in this step and click **Next**.
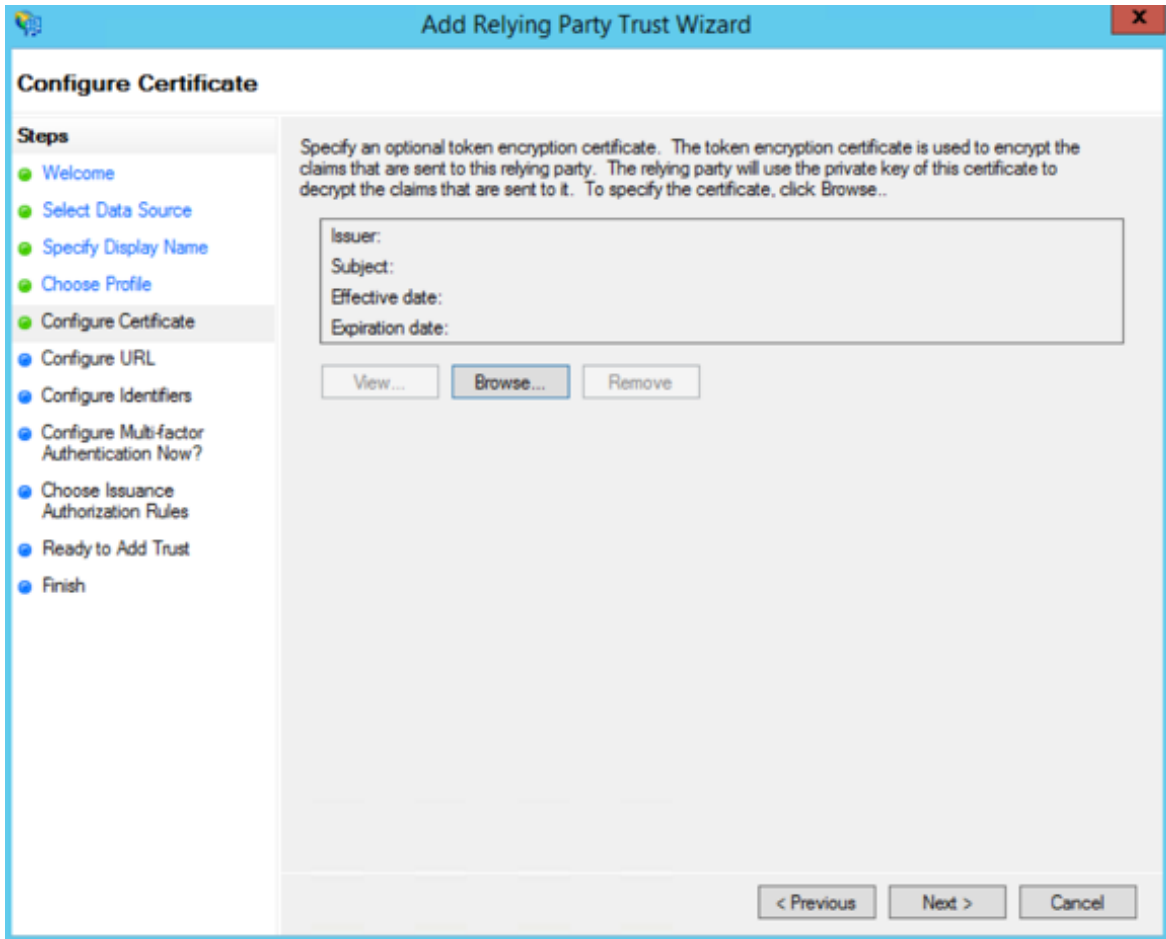
8. Select "Enable support for the SAML 2.0 WebSSO protocol." In the *Relying party SAML 2.0 SSO service URL* field, add your "Assertion Consumer URL" (obtained from the PCE web console).
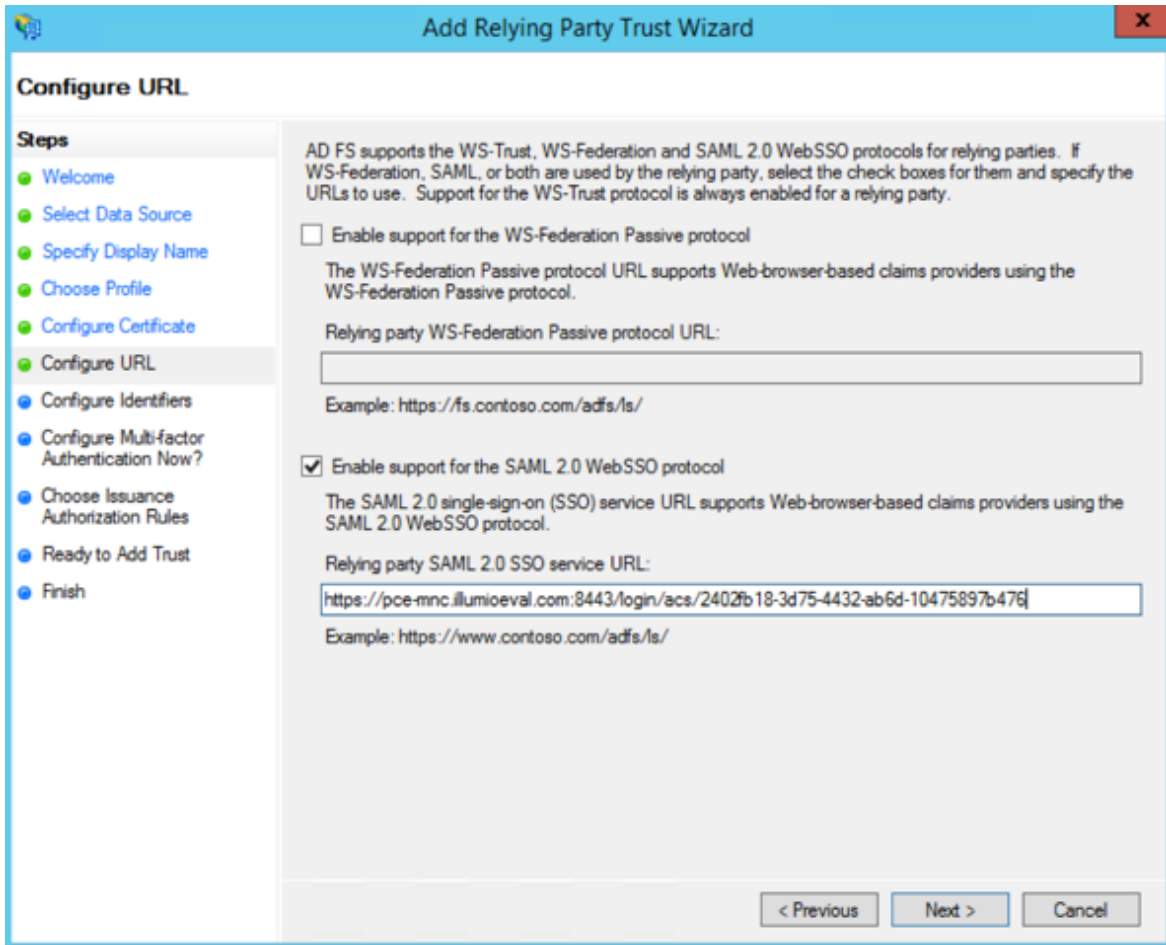
To locate the "Assertion Consumer URL," go to **Settings** > **Authentication** >
Information for Identity Provider in the PCE web console:

9. On the Configure Identifiers page, use the same URL for the Relying party trust
   identifier, without the `/acs/<randomNumbers>`. For example: `https://pce-mnc.il-`
   `lumioeval.com:8443/login`. Click **Next**.
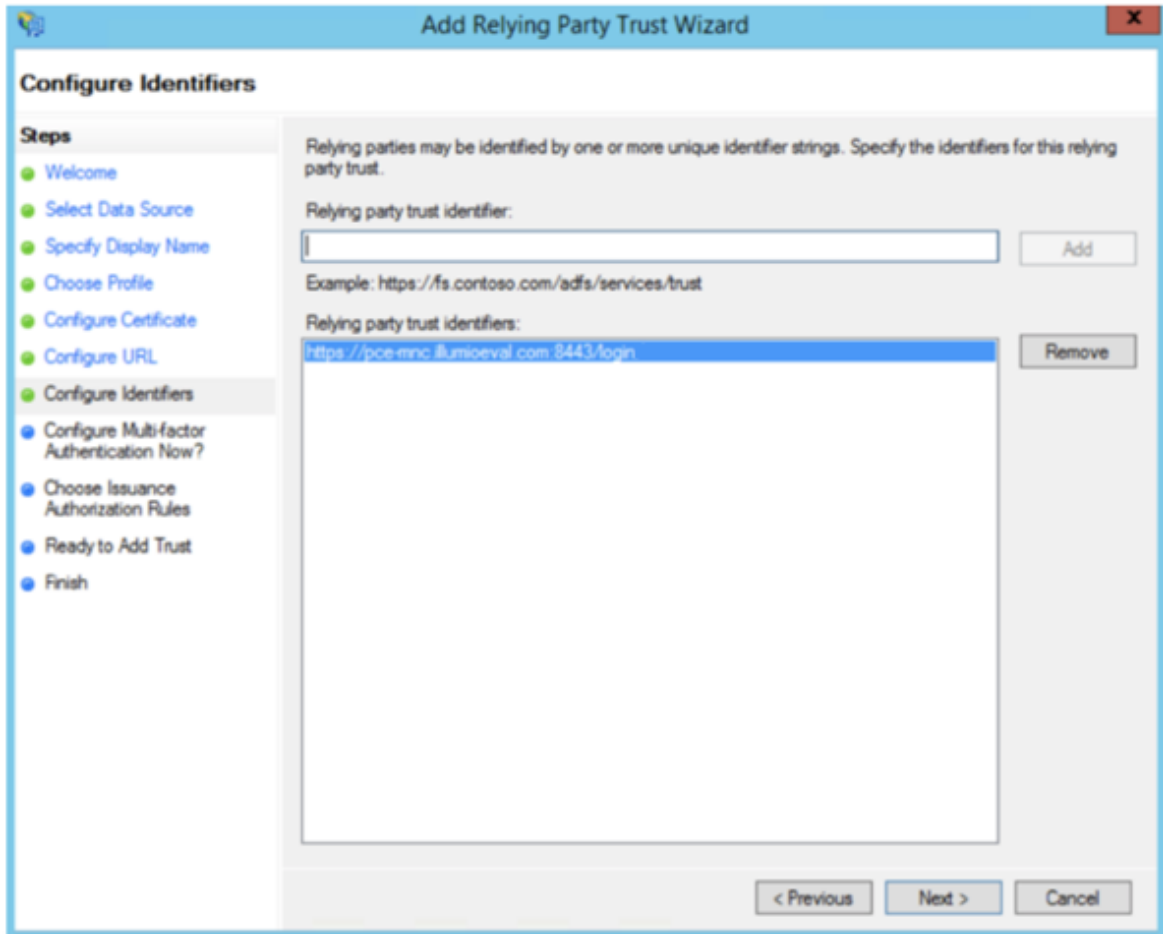
10. Select the "I do not want to configure multi-factor authentication..." and click
Next.
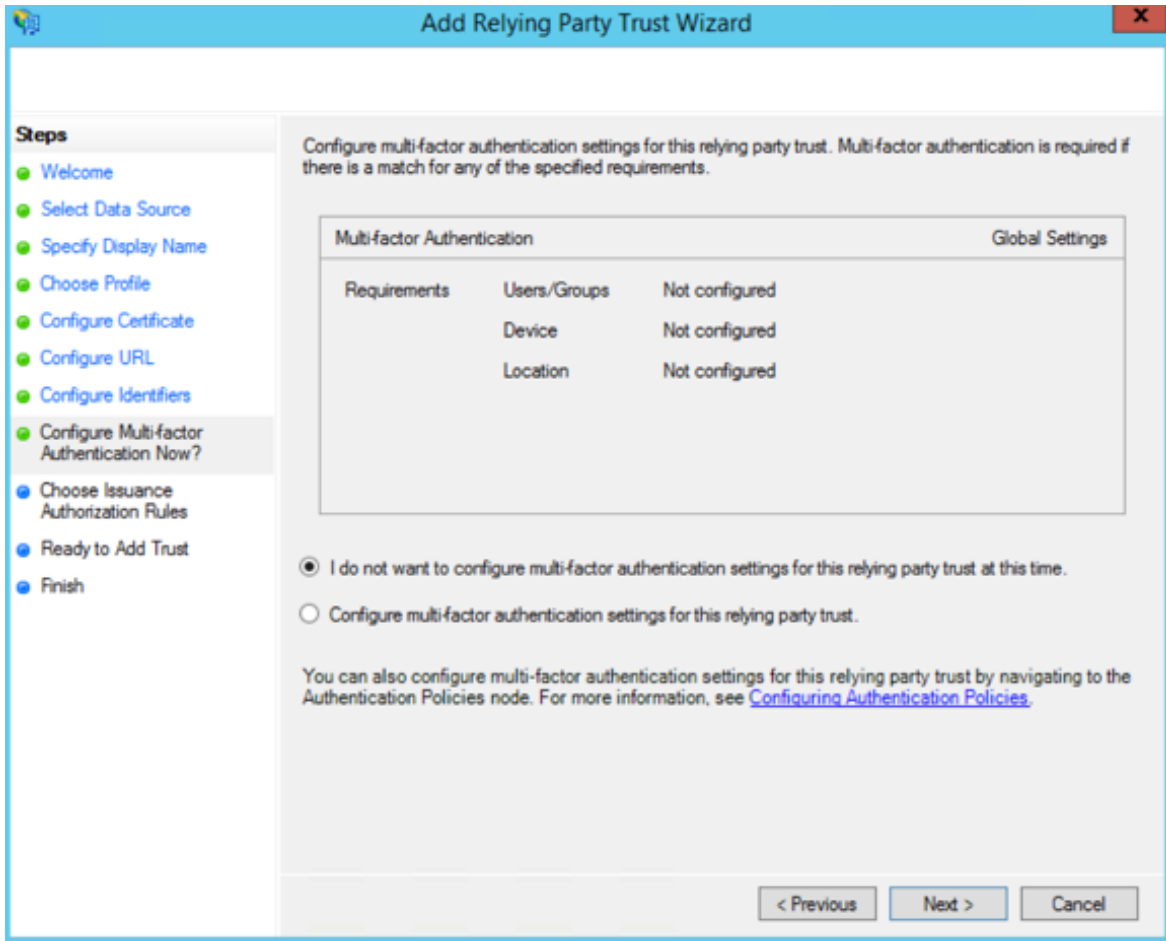
11. Select "Permit all users to access this relying party" and click **Next**.
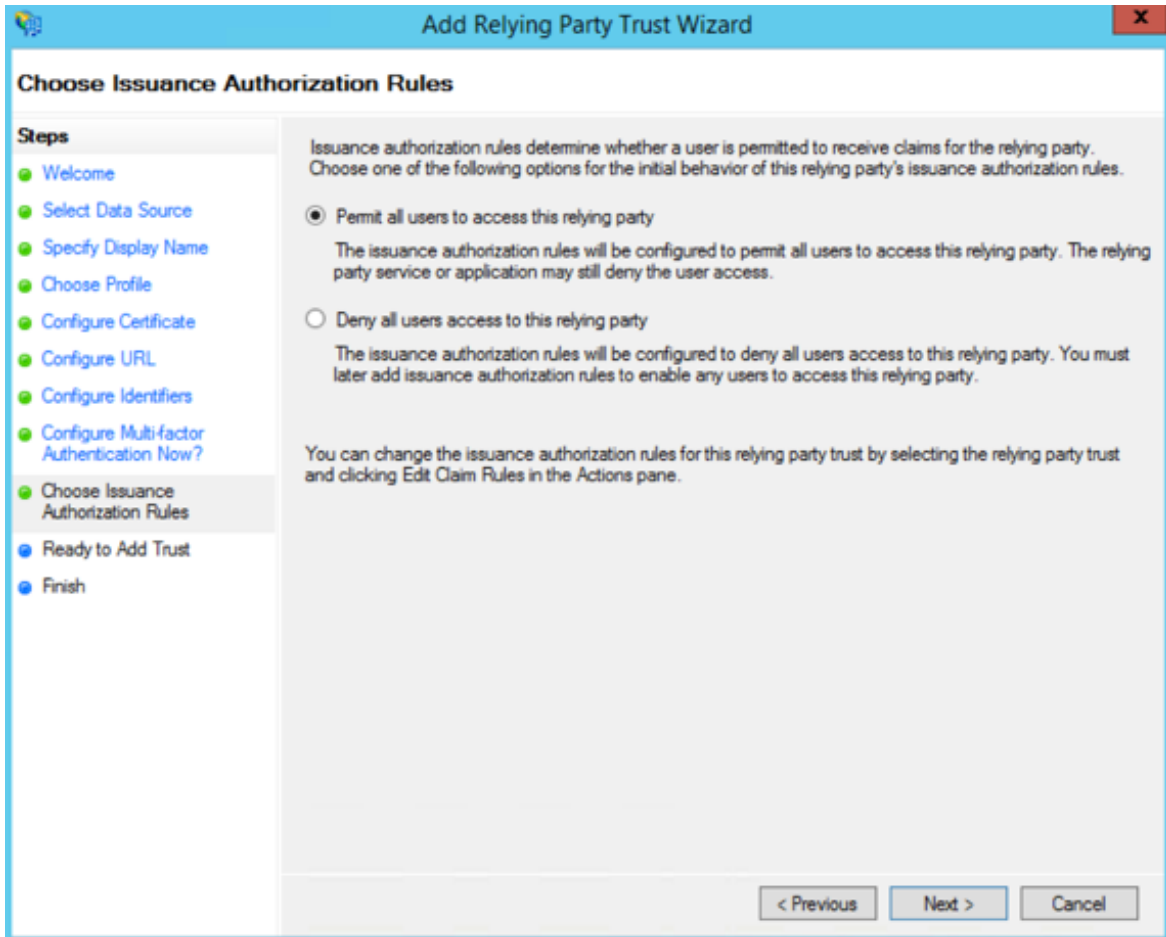
12. On the Ready to Add Trust page, click **Next**.
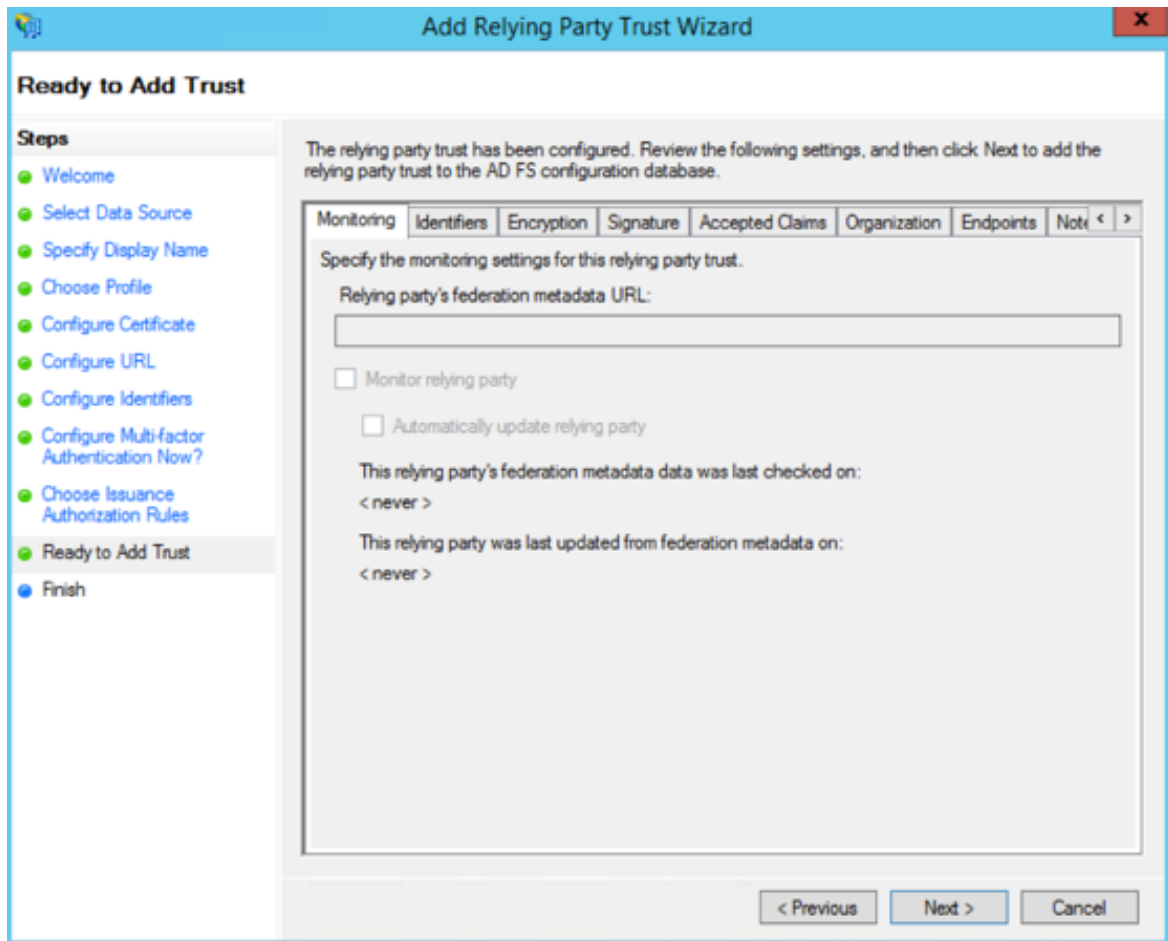
13. Leave the *Open the Edit Claim Rules* checkbox selected and click **Close**.
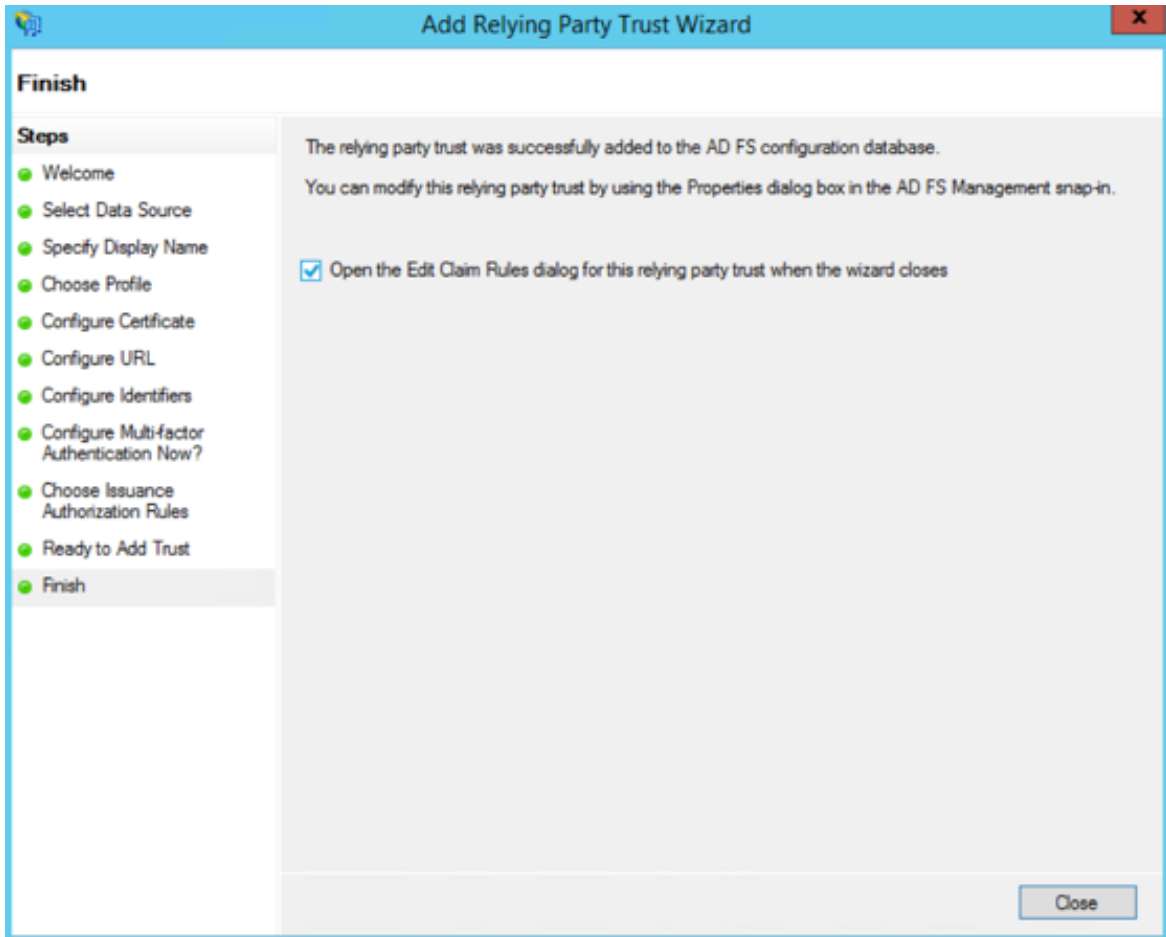
Create Claim Rules

You need to create claim rules to enable proper communication between AD FS and the PCE.

1. In the Edit Claim Rules dialog, click **Add Rule**.
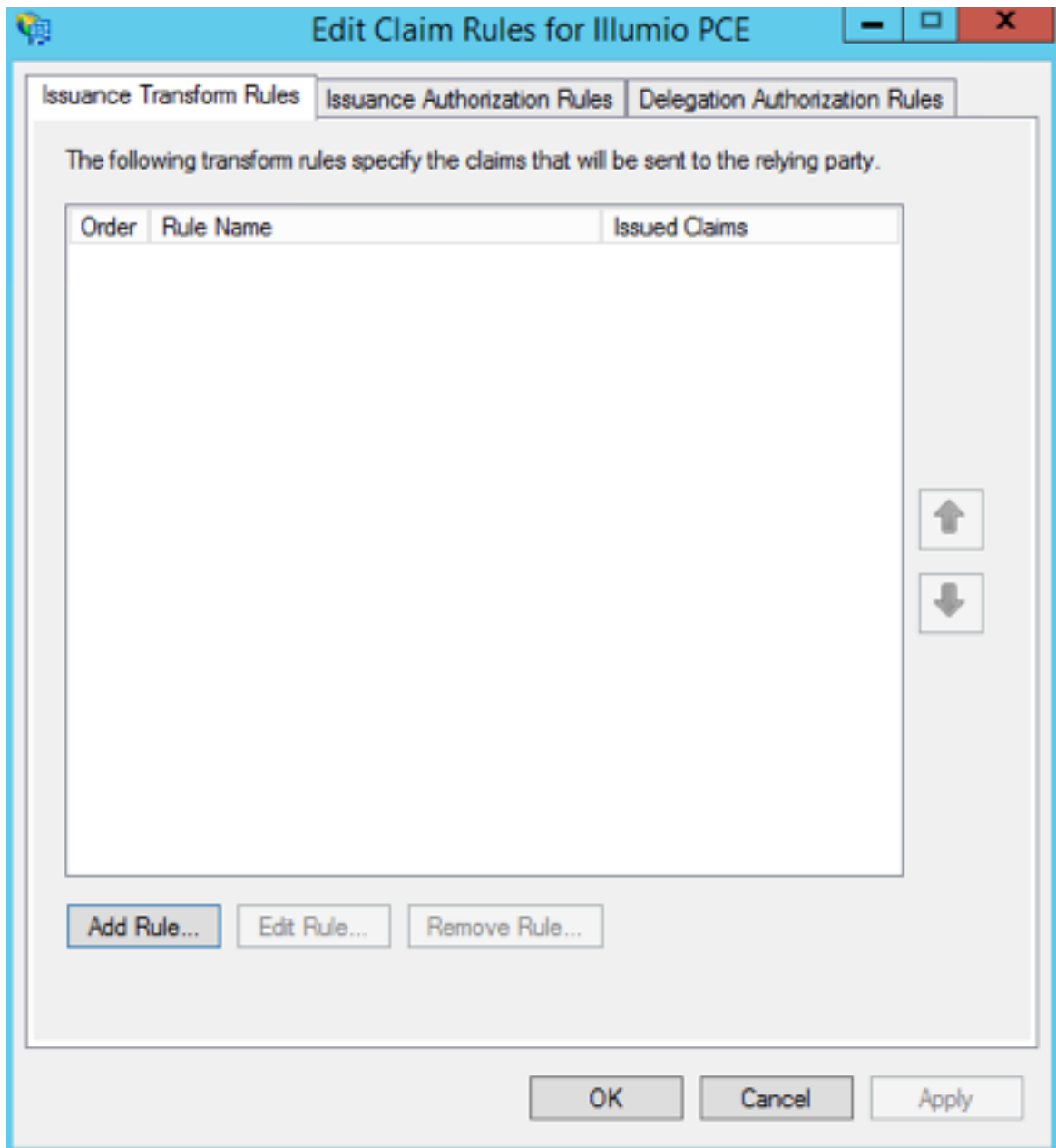
2. Under Select Rule Template, select "Send LDAP Attributes as Claims" and click **Next**.
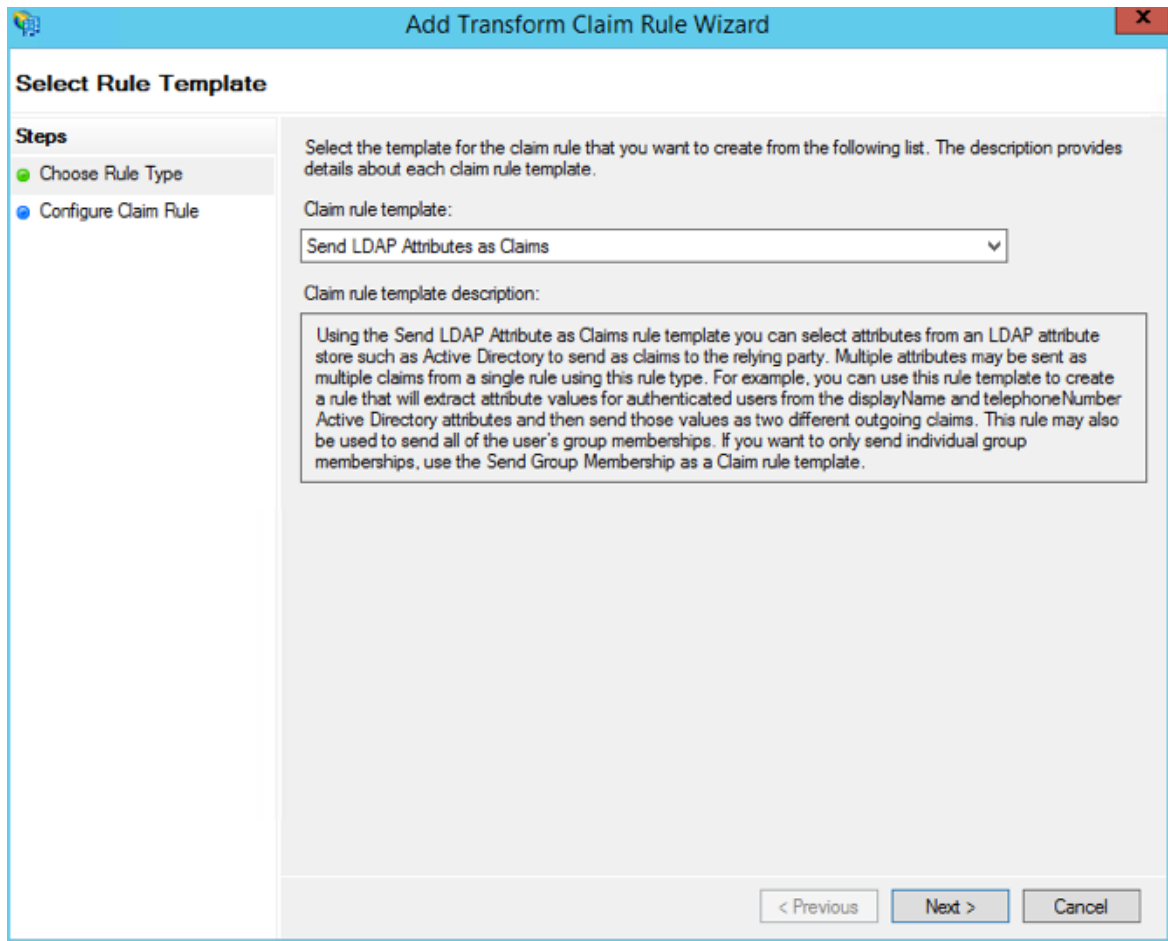
3. Name the Claim rule "Illumio Attributes" and select **Active Directory** as the Attribute store. Under the first attribute, select "User-Principal-Name" and "E-Mail Address" as the outgoing. Select "Surname" and type the custom field name of "User.LastName" in the outgoing field. Repeat the values for "Given-Name" and "User.FirstName" and click **Finish**.
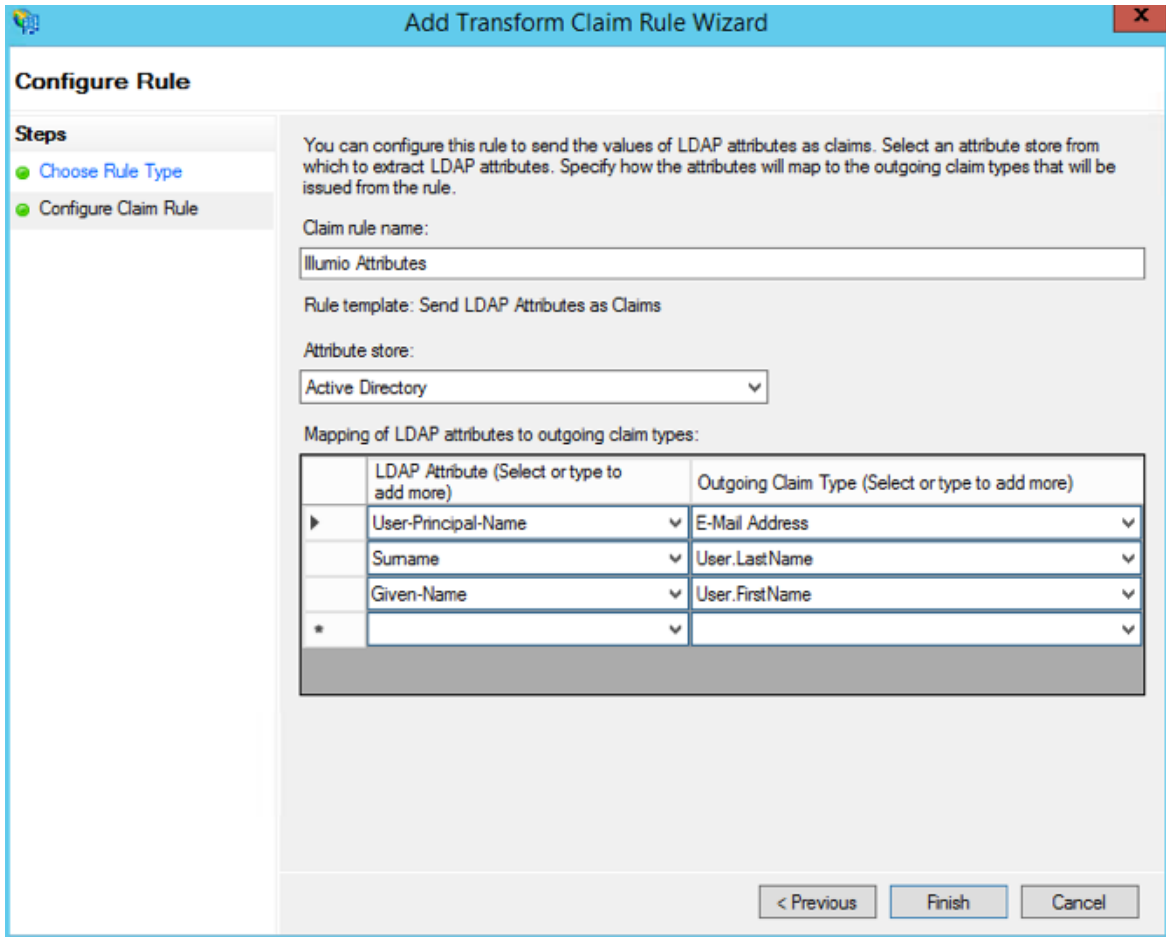
4. In the Edit Claim Rules dialog with your new rule added, click **Add Rule** to add the final rule.
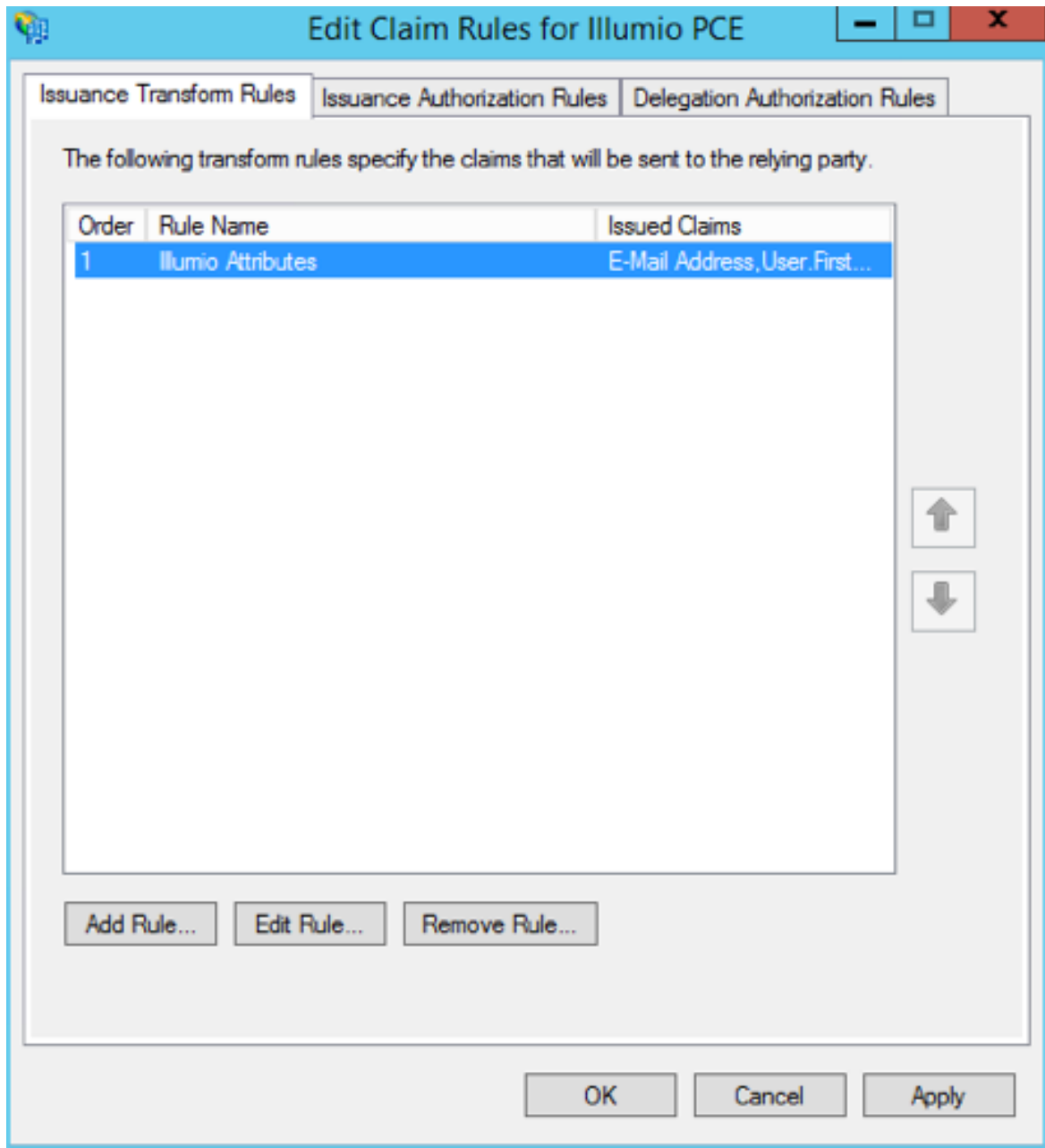
5. Under the Claim Rule Template, select "Transform and Incoming Claim" and click **Next**.
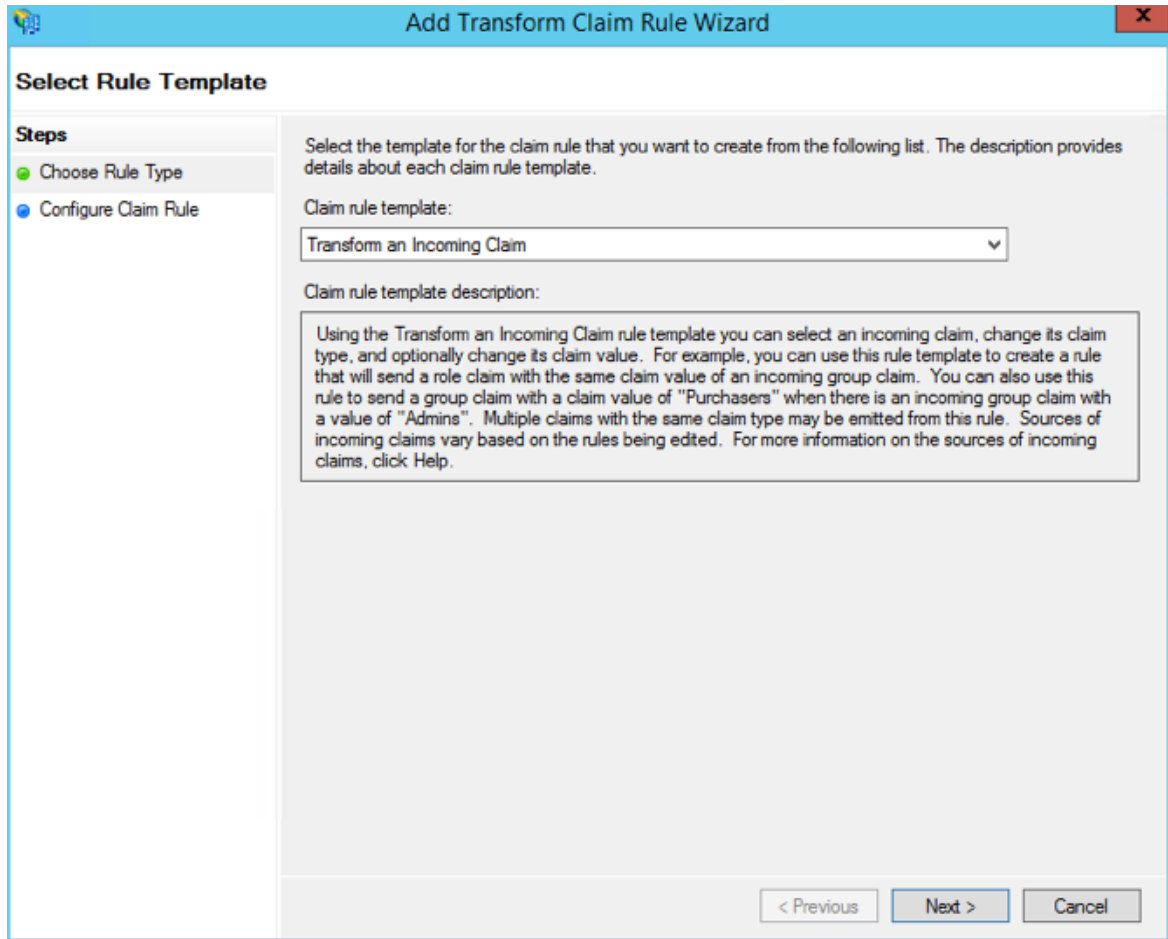
6. Name the rule "Email to NameID Transform" and change the incoming claim type to "E-Mail Address." Set the Outgoing claim type to "Name ID" and the Outgoing name ID format to "Email" and click **Finish**.

The Edit Claim Rules window opens.

7. (Windows 2016 and Windows 2019) Skip to step 12.

   The Edit Claim Rules window has three tabs. You have already filled out the first tab. The other two tabs are not available in Windows 2016 or Windows 2019. Therefore, skip steps 8 - 11.

8. Select the Issuance Authorization Rules tab.

9. To allow all your Active Directory Users to access the PCE, leave the "Permit Access to All Users" as is. Otherwise, you should restrict access to a single group

or groups of users.
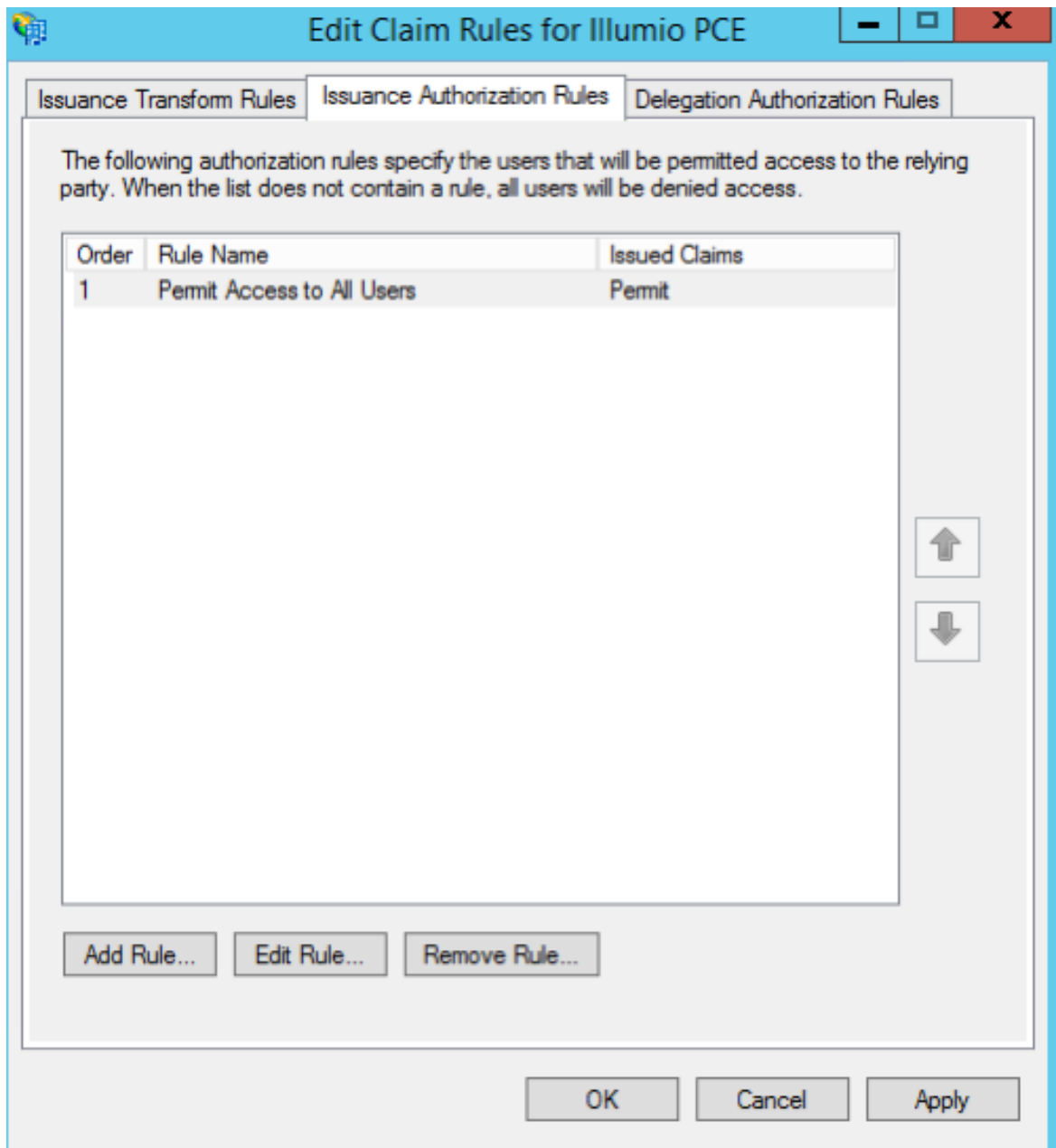
10. Select "Permit or Deny Users Based on an Incoming Claim" and click **Next**.
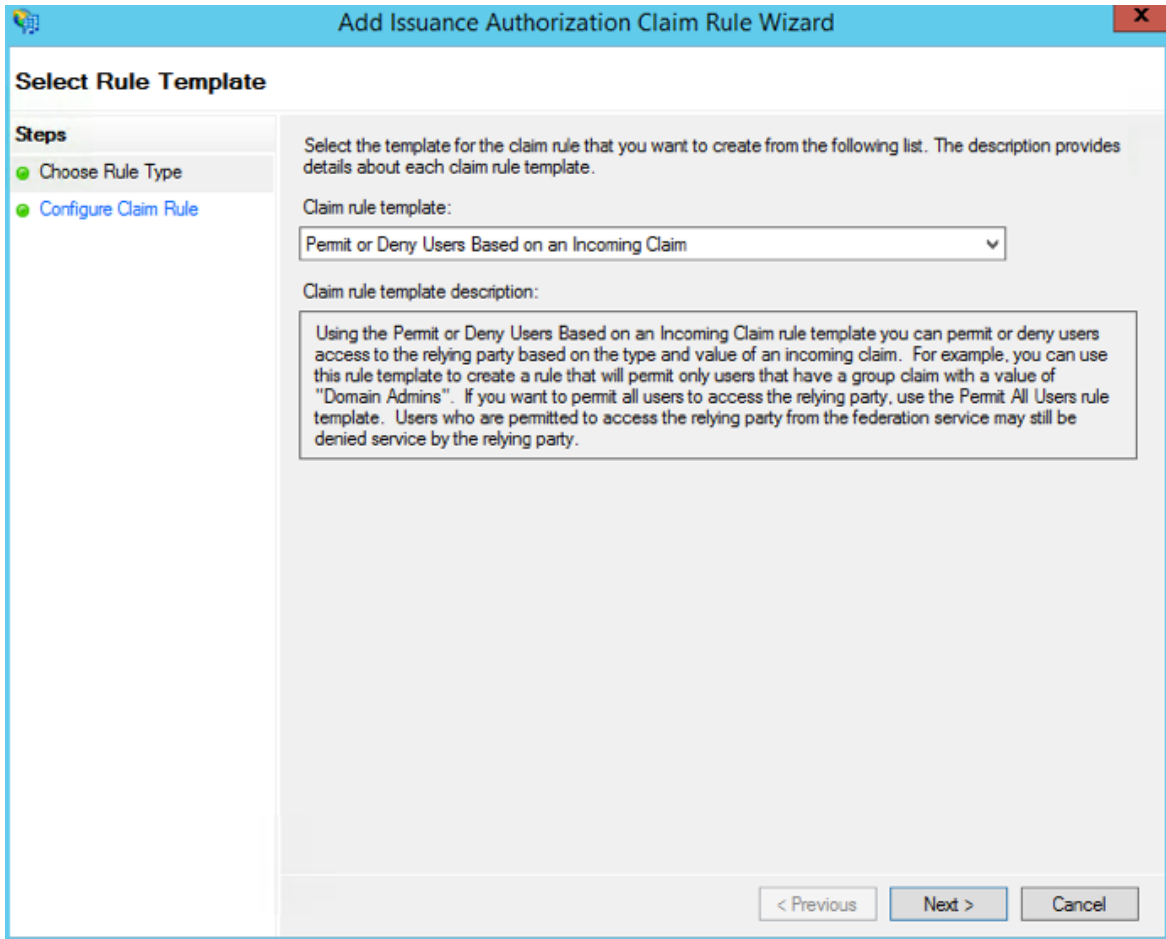
11. Name the rule "AD FS Users" and change the Incoming claim type to "Group SID" (you might have to scroll to find it). In Incoming claim value, browse to the group of users you want to give access. Make sure "Permit access" is selected and click **Finish**.

12. If you are using RBAC with groups, you need to create a Goup Claim Rule.

    To add groups to AD FS claim rule configuration, click **Edit Rule**. Add the require-
    ment for "LDAP Attribute: memberOf" by selecting the Outgoing Claim Type as
    "User.MemberOf." Click **OK**.

Obtain ADFS SSO Information for the PCE

Before you can configure the PCE to use AD FS for SSO, obtain the following inform-
ation from your AD FS configuration:

- x.509 certificate supplied by ADFS
- Remote Login URL
- Logout Landing URL

To obtain the AD FS SSO information for the PCE:

1. To find the certificate in your AD FS configuration, log into the AD FS server and open the management console.

2. Browse to the certificates and export the Token-Signing certificate.

3. Right-click the certificate and select **View Certificate**.

4. Select the **Details** tab.

5. Click **Copy to File**.
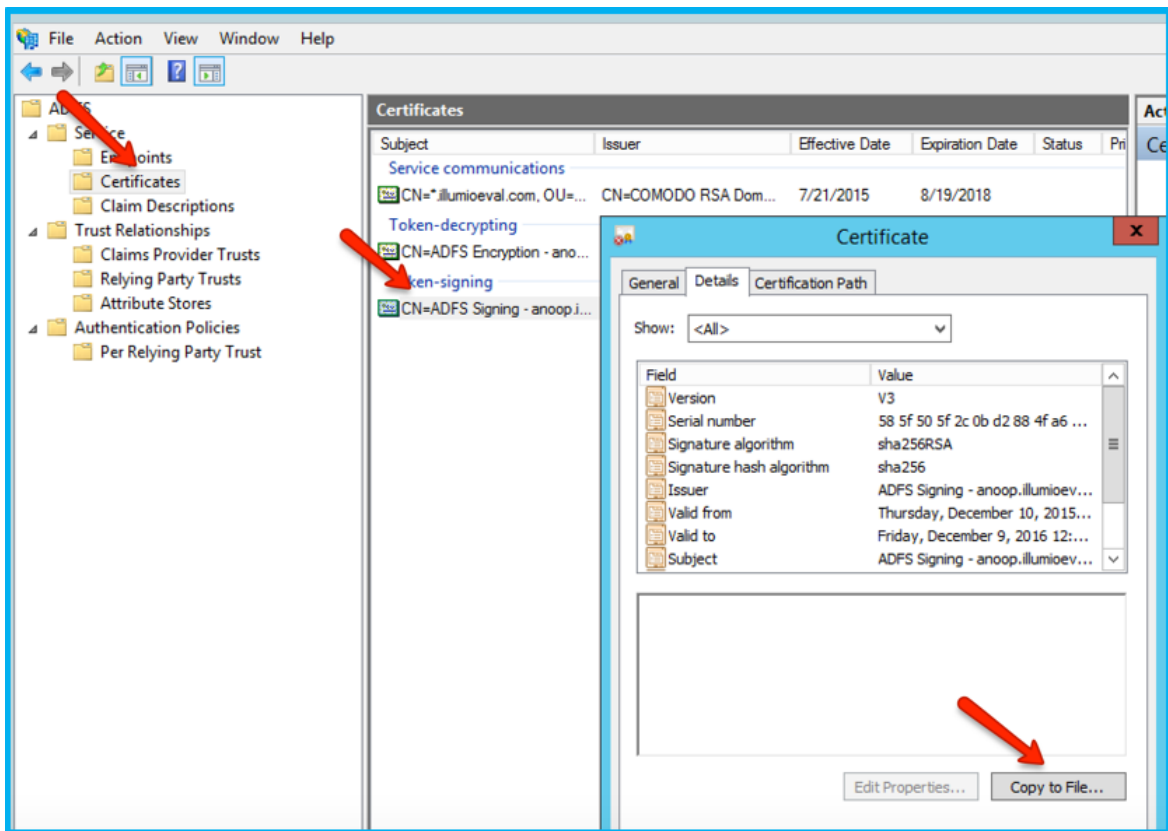
6. When the Certificate Export Wizard launches, click **Next**.

7. Verify that the "No - do not export the private key" option is selected and click **Next**.

8. Select Base 64 encoded binary X.509 (.cer) and click **Next**.

9. Select where you want to save the file, name the file, and click **Next**.

10. Click **Finish**.

11. After exporting the certificate to a file, open the file with a text editor. Copy and paste the contents of the exported x.509 certificate, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` delimiters in to the SAML Identity Provider Certificate field.

12. To find the **Remote Login URL** (which AD FS calls "Sign-On URL"), download and open the following metadata file from your AD FS server by navigating to `https://server.mydomain/FederationMetadata/2007-06/FederationMetadata.xml` and search for `SingleSignOnService`.

```
format:persistent</NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid
-format:transient</NameIDFormat><SingleSignOnService




                                                                       |
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location="https://_____.illumio_____.com/adfs/ls/"/><SingleSignOnService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://anoop.illumioeval.com/adfs/ls/"/><Attribute
    Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
```

13. To find the **Logout Landing URL** for the PCE, you can use the login URL of the PCE (preferred):

```
https://<myPCENameAndPort>/login
```

Or, a generic logout URL of AD FS:

```
https://<URLToMyADFSServer>/adfs/ls/?wa=wsignout1.0
```

You are now ready to configure the PCE to use AD FS for SSO.

Configure the PCE for AD FS SSO

Before you configure the PCE to use Microsoft AD FS for SSO, make sure you have the following information provided by your AD FS, which you configure in the PCE web console:

- x.509 certificate supplied by ADFS
- Remote Login URL
- Logout Landing URL

For more information, see Obtain ADFS SSO Information for the PCE.

> **NOTE:**
> When SSO is configured in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

To configure the PCE for AD FS:

1. From the PCE web console menu, choose **Settings** >**SSO Config**.
2. Click **Edit**.
3. Select the *Enabled* checkbox next to SAML Status.
4. In the *Information From Identity Provider* section, enter the following information:
    - SAML Identity Provider Certificate
    - Remote Login URL
    - Logout Landing URL
5. Select the authentication method from the drop-down list:
    - **Unspecified:** Uses the IdP default authentication mechanism.
    - **Password Protected Transport:** Requires the user to log in with a password using a protected session; select this option and check the Force Re-authorization checkbox to force user re-authorization.
6. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log into the PCE using a different login than their default computer login and is disabled by default.

> **NOTE:**
> You must select "Password Protected Transport" as the authen-tication method and check the Force Re-authentication checkbox to force users to re-authenticate.

7. Click **Save**.

    Your PCE is now configured to use AD FS for SSO authentication.

Azure Single Sign-on

This section describes how to configure Azure Active Directory (AD) for SSO authen-tication with the PCE.

Prerequisites

Before you begin configuration:

1. Log in to the PCE as a Global Organization Owner.
2. Navigate to the **Settings > Single Sign-On** page.
3. Copy the following URLs, which you will need to complete the Azure configuration:

- Issuer: https://pce.xxxx:8443/login
- NameID Format: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- Assertion Consumer URL: https://pce.xxxx:8443/login/acs/16884d35-036e-48c2-a685-c33f5458f407
- Logout URL: https://pce.xxxx:8443/login/logout/16884d35-036e-48c2-a685-c33f5458f407

Configure Azure

> ✅ NOTE:
> Only an Azure 'Application Administrator' can configure Azure AD.

To configure Azure AD:

1. Make sure you have already configured the necessary Azure AD User Groups. You can verify this by logging in to your Azure portal and browsing to **Azure Active Directory > Groups**. Make a note of the Group names you want to use because you will need them later on.

2. Navigate to **Azure Active Directory > Enterprise Applications > New application**.

3. Select **Non-gallery application** and enter a name, for example 'illumio-prod', and click **Add**.
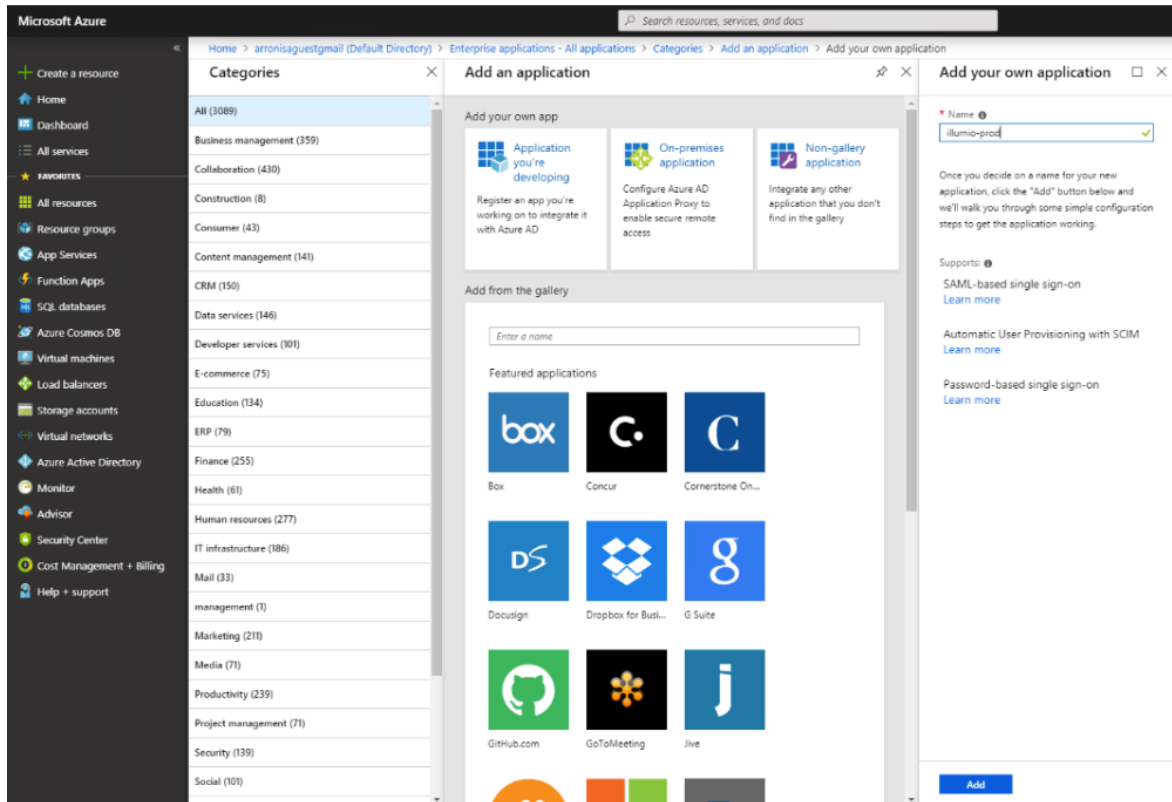
4. From the 'Getting Started' option, select **Configure single sign-on (required)** and select **SAML** from the list of single sign-on methods.

5. In **Basic SAML Configuration**, enter the URLs that you had noted down in step 3
    of Prerequisites.
    o Identifier (Entity ID) = Issuer
    o Reply URL (Assertion Consumer URL) = Assertion Consumer URL

6. Click the Edit button and enter the **User Attributes & Claims** configuration val-
    ues.

7. Download **Certificate (Base64)** and save it locally.

8. Download **Login URL** and **Logout URL**.
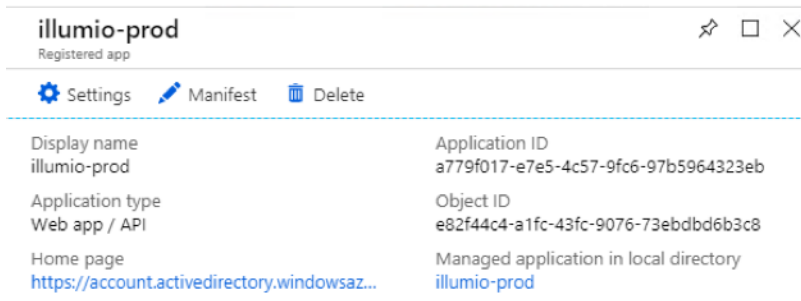
9. Create the 'Roles' that will have access to the `illumio-prod` application.

   ○ Navigate to **Azure Active Directory > App registrations** and select the `illu-mio-prod` application.

   ○ Click 'Manifest' to open the `.json` manifest:

   ○ Locate the `appRoles` section of the manifest and enter:

      ■ `displayName`: A display name.

      ■ `id`: The Azure object ID for the group you are going to use.

      ■ `description`: A description.

      ■ `value`: A value for the Illumio role.

```json
1  {
2      "appId": "4eec4819-b6d4-49bf-89e3-3efe456fb3ab",
3      "appRoles": [
4          {
5              "allowedMemberTypes": [
6                  "User"
7              ],
8              "displayName": "illumio readonly role",
9              "id": "ca321a03-0b22-46a9-bc4e-fc0495a65857",
10             "isEnabled": true,
11             "description": "Read Only Users",
12             "value": "R-illumio-readonly"
13         },
14         {
15             "allowedMemberTypes": [
16                 "User"
17             ],
18             "displayName": "illumio admins role",
19             "id": "6d6c5fee-0dfb-46a9-9c2f-95b716386d61",
20             "isEnabled": true,
21             "description": "Administrators",
22             "value": "R-illumio-admins"
23         }
24     ],
```

10. Add the required users or groups to the `illumio-prod` application and assign the necessary roles.
    - Navigate to Azure Active Directory > Enterprise Applications > illumio-prod > Users and groups.
    - Click Add and select the Azure user or group you want to add and assign a role.
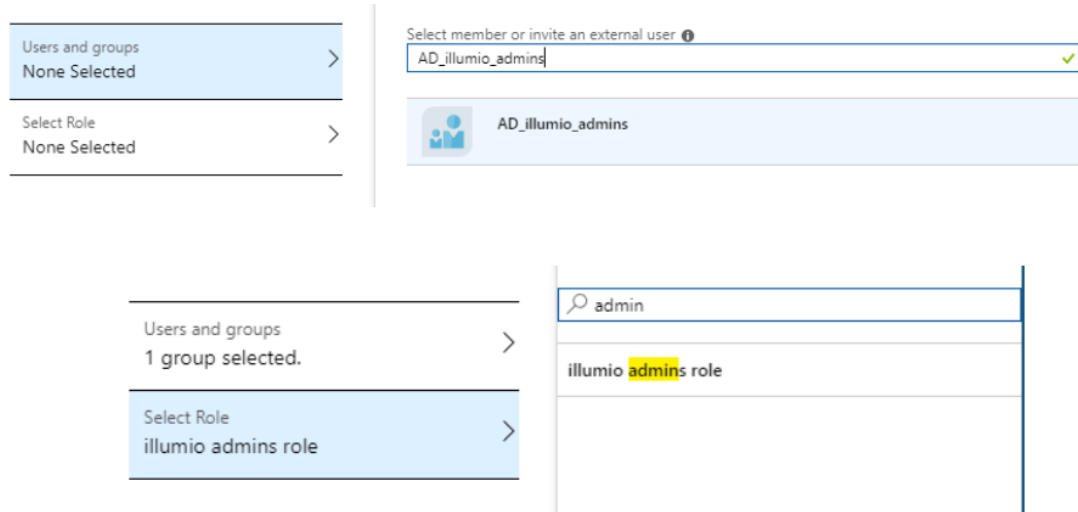
Configure PCE for Azure

> ✔ NOTE:
> Only an Illumio PCE 'Global Organizational Owner' can configure the PCE.

Before you begin, make sure you have the following information from your Azure AD:

- Certificate (Base64). See step 7 of Configure Azure
- Azure Login URL and Logout URL. See step 8 of Configure Azure

To configure the PCE for Azure AD:

1. Configure the Illumio PCE Single Sign-on SAML settings (information from the Identify Provider):
   a. Log in to the Illumio PCE web console.
   b. From the left navigation menu, select **Settings > Authentication**.
   c. Click **Configure** that is located next to 'SAML'.
   d. On the Single Sign-on Configuration page, click **Edit**.
   e. Enter the following information:

- SAML Identity Provider Certificate: Paste your Azure Base64 certificate.
- Remote Login URL: Enter the Azure Login URL.
- Logout Landing URL: Enter the Azure Logout URL.
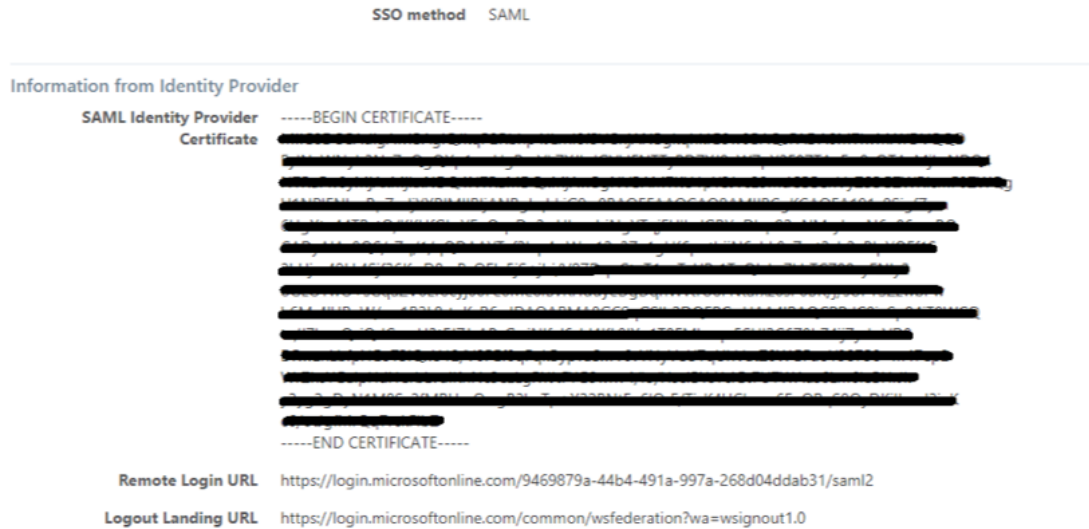
2. Configure the Illumio PCE Single Sign-on SAML settings (information for the Identify Provider):

   a. Select the authentication method from the drop-down list:

      - Unspecified: Uses the IdP default authentication mechanism.
      - Password Protected Transport: Requires the user to log in with a password in a protected session.

   b. To require users to re-enter their login information to access Illumio (even if the session is still valid), select the **Force Re-authentication** checkbox (disabled, by default). This allows users to log in to the PCE using login credentials different than their default computer login.

   c. Click **Save**.

   > ✅ NOTE:
   > If SSO is configured both in Illumio Core and for the IdP, the preferences in Illumio Core are used. If SSO is not configured in Illumio Core, the default IdP settings are used.

3. Add external groups and assign the necessary global or scoped roles in Illumio RBAC:

   a. From the menu, select **Role-Based Access > External Groups**.

   b. Click **Add**.

   c. Enter a **Name**.

   d. Enter an **External Group** name. This groups name must match the value you entered in step 8 (`value`: A value for the Illumio role) in Configure Azure

   e. Click **Save**.

   f. Repeat for additional groups.

   g. Select a group you created in the above step.

   ▪ Select **Add Role > Add Global Role** or **Add Scoped Role**.

   ▪ Select a **Role** and click **Grant Access**.

- Repeat for additional groups.

The PCE is now configured to use Azure AD for SSO authentication.

Okta Single Sign-on

This section explains how to configure SSO for user authentication with the PCE using Okta as your IdP.

Prerequisite for Okta SSO

Before you begin, make sure you have the following information from your Okta account:

- x.509 certificate
- Remote Login URL
- Logout Landing URL

> ✓ NOTE:
> Your PCE user account must have Owner or Admin privileges to perform
> this task.
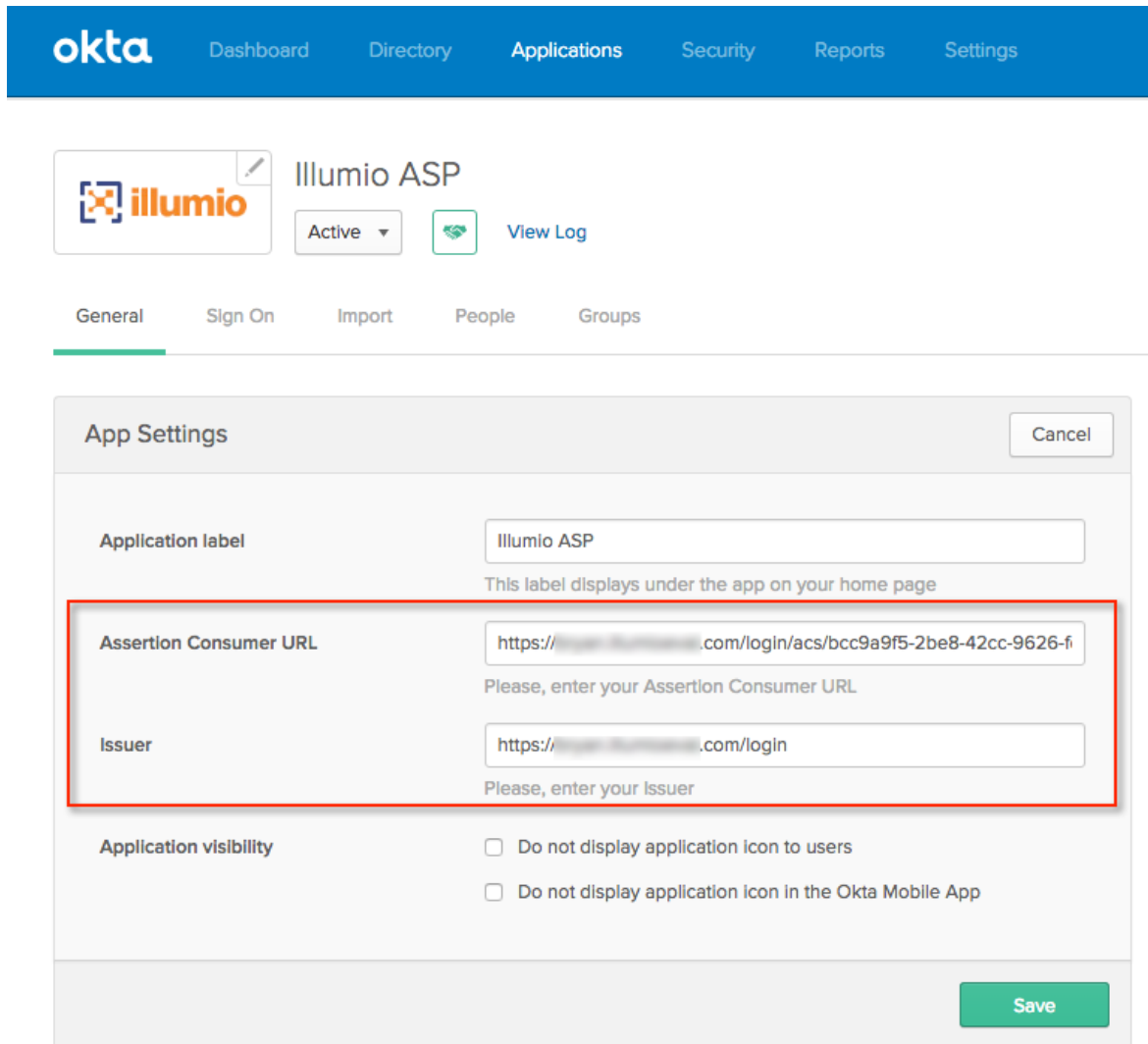
Configure the PCE for Okta SSO

1. From the PCE web console menu, choose **Access Management** > **Authentication**.
2. On the Authentication Settings screen, locate the SAML configuration panel and click **Configure**.
3. Enter the following information:
   - **SAML Identity Provider Certificate:** Paste your Okta x.509 certificate (in PEM text format):
   - **Remote Login URL:** Enter the Okta Remote Login URL.
   - **Logout Landing URL:** Enter the Okta Logout Landing URL.
4. In the Information for Identity Provider section, choose the Access Level for the users who will use Okta to authenticate with the PCE. When you select No Access, SSO users from your Okta account will have to be added manually before they can log into the PCE. (For more information on PCE user per-missions, see Role-based Access Control.)
5. In the Information for Identity Provider section, make note of the following fields:
   - Issuer
   - Assertion Consumer URL
6. Select the authentication method from the drop-down list:
   - **Unspecified:** Uses the IdP default authentication mechanism.
   - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
7. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log into the PCE using a different login than their default computer login and is disabled by default.

> ✓ NOTE:
> When SSO is configured both in Illumio Core and for the IdP, the pref-erences in Illumio Core are used. When SSO is not configured in Illu-mio Core, the default IdP settings are used.

8. Click **Save**.

9. Log into your Okta account.

10. Select the Illumio Core app, select the General tab, and click **Edit**.

11. Enter the values you copied from the Information for Identity Provider section of the PCE SSO Configuration page.

12. Click **Save**.

Your PCE is now configured to use Okta SSO for authenticating users with the PCE.

OneLogin Single Sign-on

This section describes how to configure SSO for OneLogin.

Configure SSO for OneLogin

This task shows you how to configure SSO for authenticating users with the PCE using OneLogin as your Identity Provider (IdP).

Before you begin, make sure you have the following information from your OneLogin account:

- x.509 certificate
- SAML 2.0 Endpoint (HTTP)
- SLO Endpoint (HTTP)

> NOTE:
> Your PCE user account must have Owner or Admin privileges to perform this task

To configure the PCE for OneLogin SSO:
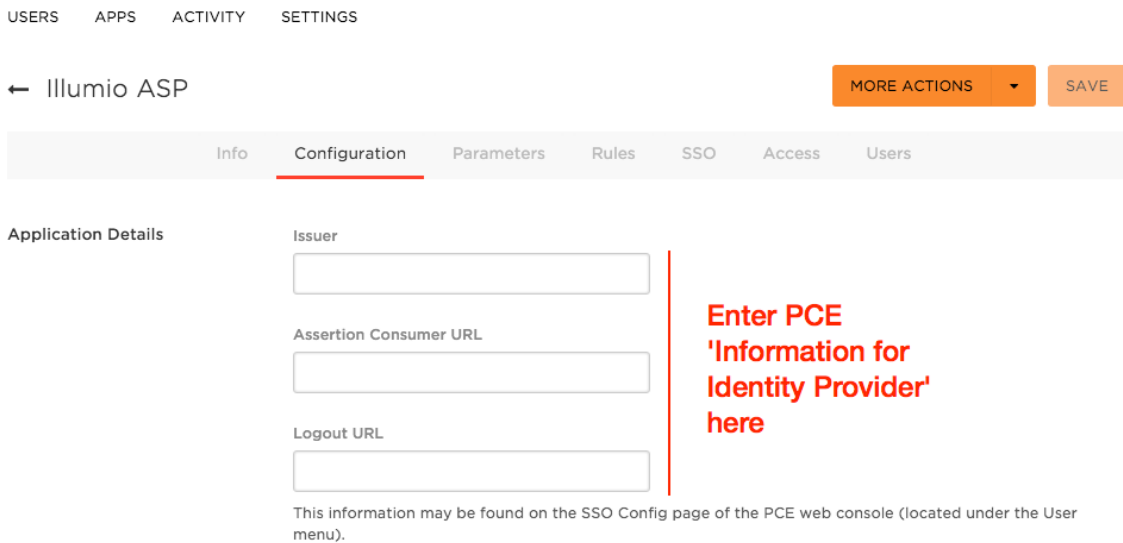
1. From the PCE web console menu, choose **Settings** > **SSO Config**.

2. Click **Edit**.

3. Select the Enabled checkbox for SAML Status.

4. Enter the following information:

   - **SAML Identity Provider Certificate:** Paste your OneLogin x.509 certificate (in PEM text format).
   - **Remote Login URL:** Enter the OneLogin SAML 2.0 Endpoint (HTTP) URL.
   - **Logout Landing URL:** Enter the OneLogin SLO Endpoint (HTTP) URL.

5. In the Information for Identity Provider section, choose the Access Level for the users who use OneLogin to authenticate with the PCE. When you select No Access, SSO users from your OneLogin account will have to be added manually before they can log in to the PCE. (For more information on PCE user permissions, see Role-based Access Control.)

6. In the Information for Identity Provider section, make note of the following fields:

   - Issuer
   - Assertion Consumer URL
   - Logout URL
     You will enter this information into your OneLogin SSO configuration.

7. Select the authentication method from the drop-down list:

- **Unspecified**: Uses the IdP default authentication mechanism.

- **Password Protected Transport**: Requires the user to log in with a password using a protected session.

8. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log in to the PCE using a different login than their default computer login and is disabled by default.

> ✅ **NOTE:**
> When SSO is configured both in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

9. Click **Save**.

10. Log in to your OneLogin account.

11. Select the Illumio Core app, and then click the Configuration tab.

12. Enter the values copied from the Information for Identity Provider section of the PCE SSO configuration page.

13. Click **Save**.

Your PCE is now configured to use OneLogin SSO for authenticating users with the PCE.

Ping Identity Single Sign-on

This section explains how to configure SSO for authentication users with the PCE using Ping Identity as your Identity Provider (IdP).

Configure SSO for Ping Identity

Before you begin, make sure you have this information from your Ping Identity SSO account:

- x.509 certificate
- Remote Login URL
- Logout Landing URL

> ✅ NOTE:
> Your PCE user account must have Owner or Admin privileges to perform this task.

To configure the PCE for Ping Identity SSO:

1. From the PCE web console menu, choose **Settings** > **SSO Config**.
2. Click **Edit**.
3. Select SAML from the Select SSO method drop-down list and click **Configure**.
4. Enter the following information:

   - **SAML Identity Provider Certificate**: Paste your Ping Identity x.509 certificate (in PEM text format).
   - **Remote Login URL**: Enter the Ping Identity Remote Login URL.
   - **Logout Landing URL**: Enter the Ping Identity Logout Landing URL.

5. In the Information for Identity Provider section, make note of the following fields:

   - Issuer
   - NameID Format
   - Assertion Consumer URL
   - Logout URL

6. Select the authentication method from the drop-down list:

   - **Unspecified**: Uses the IdP default authentication mechanism.
   - **Password Protected Transport**: Requires the user to log in with a password using a protected session.

7. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log in to the PCE using a different login than their default computer login and is disabled by default.

> NOTE:
> When SSO is configured both in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

8. Click **Save**.
9. Log in to your Ping Identity account.
10. Select the Applications tab and add the Illumio app.
11. Click **Edit** and enter the following values you just noted from Illumio:

   - **ACS URL:** Enter the value from the Assertion Consumer URL field in the PCE web console.
   - **Entity ID:** Enter the value from the Issuer field in the PCE web console.
   - **Single Logout Endpoint:** Enter the value from the Logout URL field in the PCE web console.
   - **Single Logout Response Endpoint:** Enter the value from the Logout URL field in the PCE web console.

12. Click **Continue to Next Step**.

13. You will now configure the SAML_SUBJECT attribute mapping. Under Advanced Attribute Mapping, next to the Name ID Format to send to SP, select `urn:oas-is:names:tc:SAML:1.1:nameid-format:emailAddress`.

14. Click **Save**.

Your PCE is now configured to use Ping Identity SSO for authenticating users with the PCE.