

PCE Administration

24.4

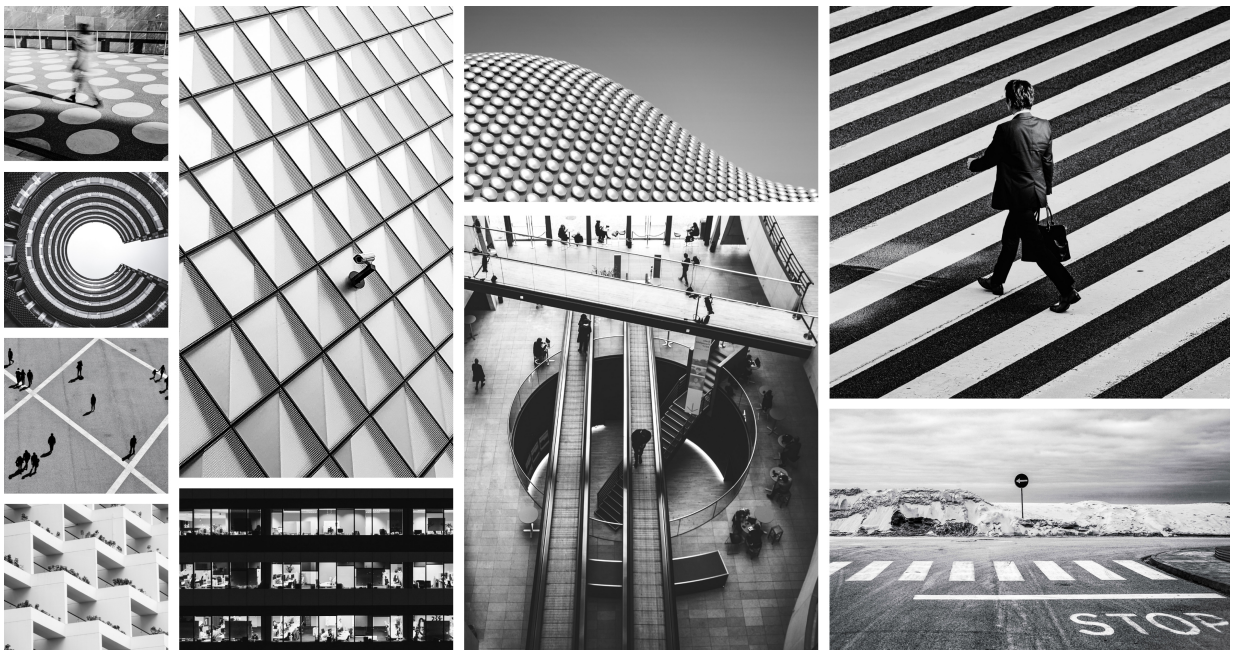


Table of Contents

| | |
|---|----|
| Overview of PCE Administration | 4 |
| Before You Begin | 4 |
| Notational Conventions | 4 |
| Review these Notational Conventions | 4 |
| PCE Architecture and Components | 4 |
| About the PCE Architecture | 5 |
| Description of PCE Components | 6 |
| Management Interfaces for PCE and VEN | 7 |
| PCE Control Interface and Commands | 8 |
| Control Command Access with <code>/usr/bin</code> | 9 |
| Syntax of <code>illumio-pce-ctl</code> | 9 |
| PCE Organization and Users | 10 |
| Invite Users to Your Organization | 10 |
| Connectivity Configuration for PCE | 11 |
| Connectivity Settings | 11 |
| Private Data Centers | 11 |
| Offline Timers | 11 |
| Set the IP Version for Workloads | 14 |
| Manage Security Settings | 15 |
| Enable IP Forwarding | 16 |
| SecureConnect Setup | 16 |
| SecureConnect Features | 17 |
| Prerequisites, Limitations, and Caveats | 18 |
| Use Pre-Shared Keys with SecureConnect | 19 |
| Use PKI Certificates with SecureConnect | 20 |
| AdminConnect Setup | 22 |
| Certificates for AdminConnect | 22 |
| Secure Laptops with AdminConnect | 23 |
| Access Configuration for PCE | 25 |
| Role-based Access Control | 25 |
| Overview of Role-based Access Control | 25 |
| Use Cases | 25 |
| Features of Role-based Access Control | 26 |
| About Roles, Scopes, and Granted Access | 27 |
| Prerequisites and Limitations | 32 |
| Setup for Role-based Access Control | 33 |
| Add a Scoped Role | 33 |
| Manage a Local User | 33 |
| Add or Remove an External User | 35 |
| Add or Remove an External Group | 36 |
| Change Users and Groups Added to Roles | 37 |
| View User Activity | 38 |
| Change Your Profile Settings | 38 |
| Role-based Access for Application Owners | 39 |
| Overview | 39 |
| Updates to Roles | 39 |
| Configuration | 41 |
| Facet Searches for Scoped Roles | 41 |
| Ruleset Viewer | 41 |
| Scoped Roles and Permissions | 42 |
| Scoped Users and PCE | 45 |
| Labeled Objects | 47 |
| Rulesets and Rules | 48 |

| | |
|---|----|
| Policy Generator and Explorer | 48 |
| My Roles | 48 |
| Configure Access Restrictions and Trusted Proxy IPs | 49 |
| Configure Access Restrictions | 49 |
| Configure Trusted Proxy IPs | 49 |
| Manage API Keys | 50 |
| Password Policy Configuration | 51 |
| About Password Policy for the PCE | 51 |
| Password Requirements | 52 |
| Password Expiration and Reuse | 52 |
| Change Password Policy Settings | 53 |
| Authentication | 55 |
| SAML SSO Authentication | 55 |
| Signing for SAML Requests | 57 |
| Active Directory Single Sign-on | 59 |
| Overview of AD FS SSO Configuration | 59 |
| Configure AD Users to Use Different UPN Suffixes | 59 |
| Initial AD FS SSO Configuration | 61 |
| Create a Relying Party Trust | 65 |
| Create Claim Rules | 73 |
| Obtain ADFS SSO Information for the PCE | 83 |
| Configure the PCE for AD FS SSO | 85 |
| Azure AD Single Sign-on | 86 |
| Prerequisites | 86 |
| STEP 1: Obtain URLs from the Illumio PCE Web Console | 86 |
| STEP 2: Configure SSO settings in Azure AD | 87 |
| STEP 3: Obtain SAML certificate and URLs from Azure AD | 89 |
| STEP 3: Create and assign a test user in Azure AD | 90 |
| STEP 4: Configure SAML SSO settings in the Illumio PCE | 91 |
| STEP 5: Create App Roles in Azure AD | 92 |
| STEP 6: Assign users and groups to app roles in Azure AD | 93 |
| STEP 7: Add External Groups and assign roles in the PCE Web Console | 93 |
| STEP 8: Turn on SAML authentication in the PCE Web Console | 95 |
| STEP 9: Test SSO | 95 |
| Okta Single Sign-on | 96 |
| Prerequisite for Okta SSO | 96 |
| Configure the PCE for Okta SSO | 96 |
| OneLogin Single Sign-on | 98 |
| Configure SSO for OneLogin | 98 |
| Ping Identity Single Sign-on | 99 |
| Configure SSO for Ping Identity | 99 |

Overview of PCE Administration

This section describes how to maintain and operate the Policy Compute Engine (PCE). It also includes other tasks required to manage your PCE deployment and help you with ongoing PCE operations and administration.

Before You Begin

Before you begin, become familiar with the following technology:

- Your organization's security goals
- 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

This section gives information about the notational conventions used here.

Review these Notational Conventions

- 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:

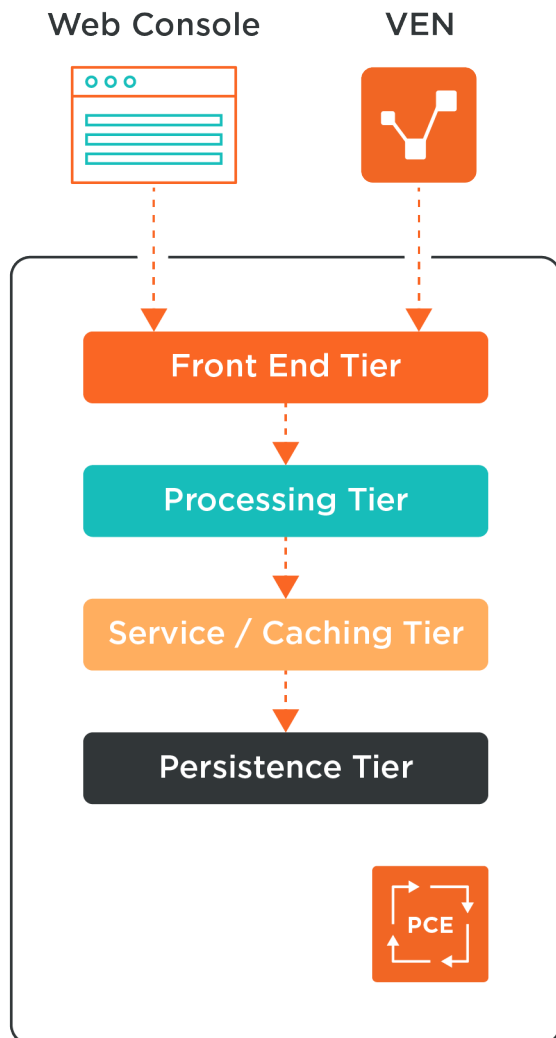
```
...  
some command or command output  
...
```

PCE Architecture and Components

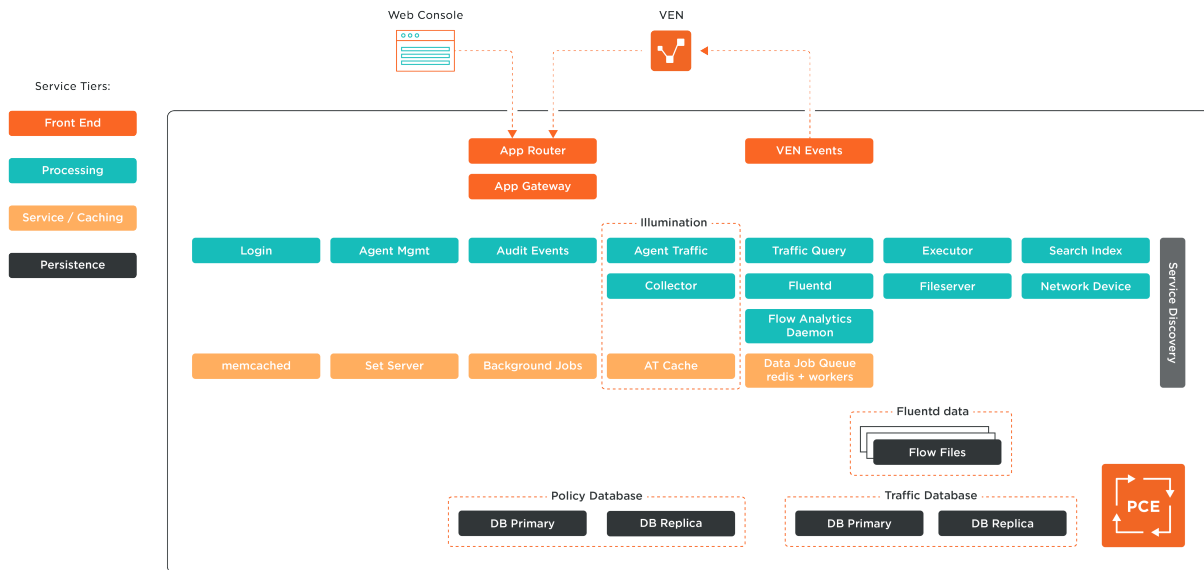
This section describes how the PCE functions, and provides an overview of its components and how they function together.

About the PCE Architecture

The PCE has four main service tiers that are used by both the PCE Web Console UI and the VEN:



Each of these service tiers are responsible for various functions, as shown below and described further in the following table.



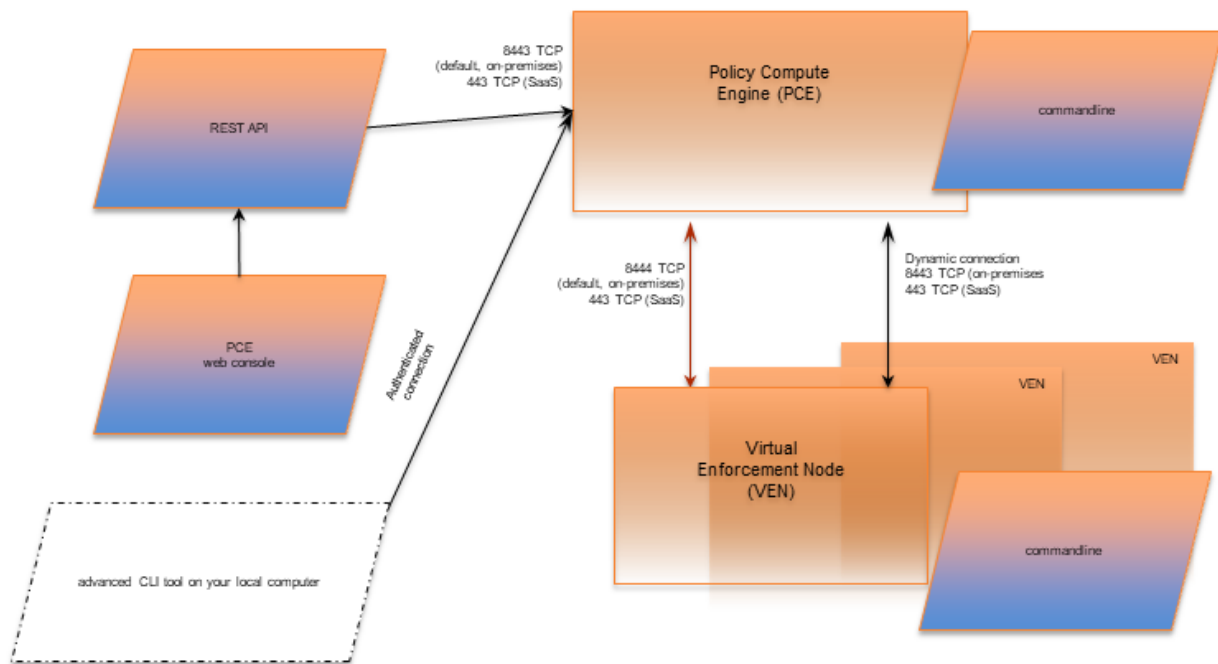
Description of PCE Components

| Tier | PCE component | Description |
|------------|-------------------------------------|---|
| Front-end | Management | Management interfaces include: |
| | interfaces: PCE web console and VEN | <ul style="list-style-type: none">• PCE web console• REST API• PCE command line• VEN command line |
| | VEN events | For information, see VEN Administration Guide. |
| | App Router | Directs requests to the proper service. |
| | App Gateway | Ensures that all communication between cluster nodes is encrypted and that only cluster nodes can connect to internal services. Most services connect via the application gateway. |
| Processing | Login | Central server for authentication. |
| | Agent Manager | Manages data in the policy domain, such as workload context and policy definitions. Also, manages data for all user and organization authentication and authorization, 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 Illumination. |
| | 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. |

| Tier | PCE component | Description |
|-------------|--------------------------------------|--|
| Service | Fileserver | Central storage and retrieval for large data files. |
| | Search Index | Supports auto-completion in the PCE web console. |
| | Traffic Query | API for traffic explorer |
| | Flow Analytics Daemon | Flow analytics daemon |
| | Network Device | Manages network devices such as switches and server load balancers that are managed by the PCE. |
| | memcached | Open source component: in-memory cache. |
| | Background Jobs | The 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." |
| | Data Job Queue (Redis + workers) | Data job queue |
| Persistence | Fluentd data | Flow files |
| | Policy primary database and replica | Postgres database that contains all the policy and agent related data. The primary and replica databases run on separate data nodes. |
| | Traffic database primary and replica | Postgres database that contains all the historical traffic flow data. Traffic Explorer is backed by this data store. 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 |
|------------------|---|
| PCE web console | With the PCE web console, you can perform many common tasks for managing the Illumio Core. |
| PCE command line | Use of the command line directly on the PCE. The <code>illumio-pce-ctl</code> 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. |
| REST API | With the Illumio Core REST API, you can perform many common management tasks, such as automating 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. |
| VEN command line | The <code>illumio-ven-ctl</code> command-line tool is the primary management tool for the VEN. |

PCE Control Interface and Commands

The Illumio PCE control interface `illumio-pce-ctl` is a command-line tool for performing 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 are 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 environment.
- `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 (policies, 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.

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 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 depends on your role.

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 **Settings > Offline Timers** and choose appropriate settings 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.



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 offline. The VEN sends a heartbeat message to the PCE every 5 minutes and a goodbye message when it is gracefully shutdown. The PCE marks a workload offline when these conditions occur:

- The PCE hasn't received a heartbeat message from:
 - Server VENs: for 3600 seconds (1 hour).
 - Endpoint VENs: for 24 hours
- The PCE receives a goodbye message from the VEN.

Under the following conditions, you can change the default Offline Timer settings before putting your workloads in enforcement:

- 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 how much time must elapse before a managed workload is marked "offline" after it sends a goodbye message. By default, the High Security setting is:

- Server VENs: Wait 15 minutes .
- Endpoint VENs: Wait 1 day.

Wait 1 hour/1 day - High Security (Default)

The PCE performs the following actions:

1. Listens for Goodbye messages from the VEN.
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.

- *Never remove IP addresses - 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*

Enter a time period (minimum: 0 seconds).

The PCE performs the following actions:

- Listens for Goodbye messages from the VEN.
- Waits for the specified time period before cleanup of those workloads IP addresses from its active policy.
- Pushes an updated policy to the peer workloads that were previously allowed to communicate with the removed workloads.

Disconnect and Quarantine Timer

Sets how much time must elapse before a managed workload is marked "offline" after the PCE has received no heartbeat from the VEN. By default, the High Security setting is:

- Server VENs: Wait 1 hour.
- Endpoint VENs: Wait 1 day.

Wait 1 hour/1 day - High Security (Default)

The PCE performs the following actions:

1. Waits for the configured time to receive a heartbeat from the disconnected workloads and then quarantines workloads that do not respond within that time period.
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.

Never remove IP addresses - 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

Enter a time period (minimum: 300 seconds).

The PCE performs the following actions:

1. Waits for the specified time period for the VEN to heartbeat.
2. Quarantines those workloads that do not respond within that time period.
3. Removes the quarantined workloads IP addresses from its active policy.
4. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the quarantined workloads.

Disconnect and Quarantine Warning

Sets how much time must elapse before the PCE emits a warning event to indicate that the VEN missed heartbeats. The server VEN will appear in a warning state on the VEN pages.

The default settings are:

- Server VENs: Wait one-quarter of the Disconnect and Quarantine Timer.
- Endpoint VENs: Disabled.

Wait one-quarter of the Disconnect and Quarantine Timer - (Default) (applies to Server VENs only)

The PCE performs the following actions:

1. Wait one-quarter of the *Disconnect and Quarantine Timer* setting for the server VEN to heartbeat before emitting a warning event indicating that the server VEN has missed heartbeats. The server VEN appears in a warning state on the VEN pages.
2. If the *Disconnect and Quarantine Timer* is set to *Never remove IP addresses - Highest Availability*, the PCE emits a warning event 15 minutes after receiving the previous VEN heartbeat.
3. If you set a custom time of 20 minutes or less for the *Disconnect and Quarantine Timer* and the PCE receives no heartbeat from the VEN at least 5 minutes after receiving the previous heartbeat, the PCE emits a warning event to indicate the missed heartbeat. The endpoint VEN will appear in a warning state on the VEN pages.

Custom Timeout (applies to Server and Endpoint VENs)

Enter a time period greater than 5 minutes (300 seconds) and less than the value specified for the Disconnect and Quarantine Timer.

1. Waits for the specified time period for the VEN to heartbeat.
2. VENs appear in a warning state on the VEN pages.

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 workload'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
```

Manage Security Settings

You can manage security settings by accessing the page **Settings -> Security**:

| Security for | Options | Description |
|-----------------------------------|---------------------|--|
| VENS (Versions 20.2.0 and higher) | IPv6 traffic | Allow IPv6 traffic |
| | | Blocked only in Enforcement state. Always allowed on AIX and Solaris workloads |
| VENS (Versions lower than 20.2.0) | IPv6 traffic | Allow IPv6 traffic |
| | | Blocked only in Enforcement state. Always allowed on AIX and Solaris workloads |
| IKE Authentication | Authentication type | PSK |
| | | Certificate |
| Public cloud configuration | NAT Detection | Private Data Center or |
| | | Public Cloud with 1:1 NAT (default) |

| Security for | Options | Description |
|--------------|---|--|
| | Public Cloud with SNAT/NAT Gateway (recommended setting if using a NAT gateway in AWS or Azure or the default outbound access in Azure) | The PCE will ignore the public IP address of the workload in policy computation. This setting is used in environments where workloads in a known public cloud (e.g, AWS or Azure) that connect to other workloads or the PCE outside the VPC or cloud via the SNAT IP address or SNAT pool (e.g, NAT Gateway in AWS) as the public IP seen by the PCE is not specific to any workloads. Only the IP address of the network interfaces on the workload (usually the private IP addresses) is distributed in the policy. |

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 Container 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.



NOTE

Use the API call to the PCE to enable this feature so it appears in the Security menu as an option.

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, datacenter, 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 pub-

lic cloud environments. Additionally, configuring and managing IPsec connections becomes more difficult as the number of hosts increases.

SecureConnect Features

SecureConnect has the following key features.

Supported Platforms

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.

Prerequisites, Limitations, and Caveats

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

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 SecureConnect 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 traversal 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 mis-configured, 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.



| No. | Provision Status | Status | Providers | Providing Service | SecureConnect Off | Consumers | Note |
|-----|------------------|---------|-----------|-------------------|--------------------------|-----------|------|
| 1 | ADDICOM PENDING | Enabled | Database | MYSQL 80 TCP | <input type="checkbox"/> | Database | |

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.

Use Pre-Shared Keys with SecureConnect

SecureConnect supports the use of 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 Core PCE does not support multiple Organizations when you have installed the PCE in your datacenter.

asfasdfasdf

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**.

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 authentication 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.

Requirements and Caveats

- 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.
- Only use certificates obtained from trusted sources.
- 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.

Leaf certificate X.509 field requirement


- Version 3
- Subject Name DN must contain Common Name (example: OU=VEN, CN=centos6.ilabs.io)
- SubjectAltName (required for better compatibility) must contain an email address field that is identical to the Common Name of DN (example: DNS:centos6, email:centos6@ilabs.io)
- Must contain key usage with
 - Digital Signature
 - Key Encipherment
 - Data Encipherment

- Key Agreement
- Must contain Extended key Usage with
 - IPSec End System
 - IPSec User
 - TLS Web Server Authentication (optional for macOS X compatibility)
- Must Contain Authority Key Identifier

Set up Certificates on Workloads

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

File Requirements

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

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`

Configure PKI Certificates

You can 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 set up certificates on your Windows and Linux workloads independently. For information, see [Requirements for Certificate Setup on Workloads \[21\]](#).

1. Go to **Settings > Security Settings**.
2. Choose **Edit > Configure SecureConnect**.
3. In the Default IPsec Authority field, select **Certificate Authority**.
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 workloads in your organization enabled with SecureConnect.)
5. Click **Save**.

AdminConnect Setup

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.

For more information, see [SecureConnect Setup \[16\]](#) and [AdminConnect Setup \[22\]](#).

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 a certificate for SecureConnect, see [Configure SecureConnect to Use Certificates \[21\]](#).

The same prerequisites and limitations for certificate setup apply to 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](#). [22]
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. For information, see "Enable AdminConnect for a Rule" in the Security Policy Guide.
4. Configure IPsec on a laptop.

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

To manage a laptop with AdminConnect, add the laptop to the PCE as an unmanaged workload.

1. Choose **Workloads > Add > Add Unmanaged Workload**.
2. Complete the fields in the General, Labels, Attributes, and Processes sections.
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.

```


Access Configuration for PCE

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 \[27\]](#) 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 Rule-set Manager | <ul style="list-style-type: none"> Add, edit, and delete all rulesets within the specified scope. Add, edit, and delete rules when the provider matches the specified scope. The rule consumer can match any scope. <div>  <p>NOTE You can choose the All Applications, All Environments, and All Locations scope with the Full Ruleset Manager role.</p> </div> |

| Role | Granted Access |
|-------------------------|---|
| Limited Ruleset Manager | <ul style="list-style-type: none"> 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. <div>  NOTE You cannot choose the All Applications, All Environments, and All Locations scope with the Limited Ruleset Manager role. </div> |
| Ruleset Provisioner | Provision rulesets within specified scope. <div>  NOTE You can choose the All Applications, All Environments, and All Locations scope and custom scopes with the Ruleset Provisioner role. </div> |
| Workload Manager | Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources. <div>  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. </div> |

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.

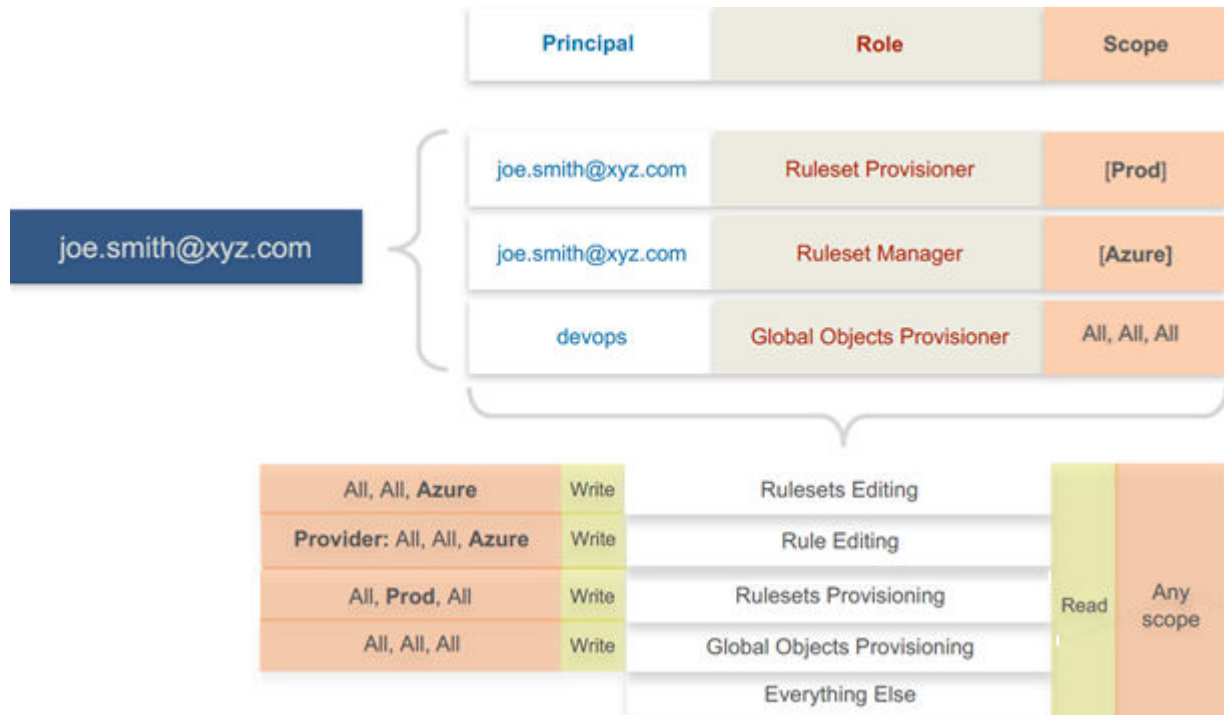
Global Organization Owner or Administrator Roles

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.



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.

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.



NOTE

Permission to configure these settings is dependent on your role.

Add a Scoped Role

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

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

When adding a scoped role:

- use the Access Wizard
- Define the scope of the role by selecting labels or label groups for applications, environment, and location.
- Add a local user, external user, or user group to the role.
- Select roles and confirm your choice.

Manage a Local User

Local users are created in the PCE (an IdP does not manage them). 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 inaccessible.

To add a local user:

- In the Local Users tab, click **Add**.
- Enter a name and an email address. The email address must use the format xxxx@yyyy.zzzz and be 255 characters or less.
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 to the address you specified an invitation to with a link to create their Illumio user account. The link in the invitation email is valid only for 7 days, after which it expires.
- Select a role for the user: None, Global Organization Owner, Global Administrator, or Global Read Only.

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. The "My Roles" feature allows you to view the list of assigned permissions (roles).

To remove a local user

Select it in the Users and Groups and remove it.

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

In Users and Groups, find the user you want to edit. change the user's name and 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 and Users and Groups pages. The name is not changed in the user's profile or on the RBAC User Activity pages.



NOTE

Local and external users can change their names when they create their accounts or from their profiles.

To convert a local user

In Users and Groups, select the name of the user and click **Convert**.

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

In Users and Groups, select the name of the user and click **Re-Invite**.

You can send a new email to users 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

In Users and Groups, select the name of the user and click **Lock**.

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

Add or Remove an External User

Using RBAC, you can control access to Illumio Core for users who a corporate IdP externally authenticates. 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.

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:

Use the External Users tab to click Add and enter a name, 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 duplicate 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 Illumio PCE web console URL.

Select the role: None, Global Organization Owner, Global Administrator, or Global Read Only.

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:

Use the External Users tab to select the user you want to remove and click **Remove**.

Removing an external user removes the user from the External Users tab and all the user's RBAC role memberships. Your corporate IdP still manages the user's authentication.

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 logs the user out for their next action 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 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:

- Use the External Users tab to add an external group
- 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 the PCE, check the **memberOf** attribute in the SAML assertion from your IdP. The **memberOf** attribute is a multiple-value attribute that contains a list of distinguished names for groups that contain the group.

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: Click **Edit Group** from the group's details page to change an external group's name.

Use the External Users tab to remove an external group, select it, and 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. Your corporate IdP still manages user authentication for the group members.

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.

Change Users and Groups Added to Roles

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

When you revoke a user's access to scopes or global objects while the user is online, the PCE logs them out of the next action they can take after revoking their access.

- In Global Roles, click the name of the role you want to assign users or groups to
- To remove a user or group from the role, select it and click **Remove**.
- To add a user or group to a role, click **Add**.
- 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.
- Select the user or group to add to the role.
- 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, and 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 appear 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 events 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 has a severity level and are exportable in JSON format. You can narrow the search for many events 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

- In My Profile, click on **Change Password**.
- Enter your current password and then your new password twice.
- Click **Change Password**.

Color Vision Deficiency Mode

Users with color vision deficiency (Deuteranopia, Protanopia, or Tritanopia) can select Color Vision Deficiency mode, making it easier for them 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 color vision deficiency mode

- In My Profile, Accessibility section, select the **Color Vision Deficiency** button.

**NOTE**

To restore the default setting, select the **Normal Vision** button.

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

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 multiple roles to the same

user. The resulting set of permissions is the summation of all permissions included with each stacked. With these updates:

- Existing scoped roles were enhanced to restrict reads by scope.
- The 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 is disabled by default for new PCE installations.
- PCE performance and scale enhanced to support concurrently active users.

Global Roles

Global roles allow the user to view everything and 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 manage most aspects of the PCE, except 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 as many label types as you have defined (and with only one label value per type). 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 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 (Limited or Full): 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 scoped objects, provided the objects are inside the user's assigned scope. A user with this role can also 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: This role allows a user to perform workload-specific operations such as pairing, unpairing, label assignment, and changing 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 **Access Management > 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 upgraded from prior releases, this setting must be manually turned **off** for users to have reads restricted by scope. If this setting is set **On**, users with scoped roles will get global visibility by default.

Figure 1. Global Viewer Setup

Global Viewer

Scope: All

Role: Global Viewer

Granted Access: Show

Read Only User: Off All users without role membership cannot log in [Turn On](#)

[Add](#) [Remove](#) [Refresh](#)

| | Type | Name | Email/Username/Group Name | Roles |
|--------------------------|--------|-------------|-----------------------------|---------------|
| <input type="checkbox"/> | Person | Aditeya | aditeya.pandey@illumio.com | Global Viewer |
| <input type="checkbox"/> | Person | asdfasdf | greg.konush+303@illumio.com | Global Viewer |
| <input type="checkbox"/> | Person | asdfasdf | greg.konush+44@illumio.com | Global Viewer |
| <input type="checkbox"/> | Person | asdfasdf | sadfsdaf@illumio.com | Global Viewer |
| <input type="checkbox"/> | Person | asdfasdfsaf | asdfasf@illumio.com | Global Viewer |

Manage Global Owners

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 **Access Management > Scopes**. The search bar allows Organization Owners to query a list of users by a user's role. They can search by labels and label groups to get a list of users with the selected label(s) in their assigned scope(s), or for users with no labels assigned. 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) |

| Page | Ruleset Viewer (Scoped Read-Only) | Ruleset Manager | Ruleset Provisioner | Workload Manager | Application Owner (Combined Permissions) |
|------------------------------------|--------------------------------------|-----------------|---------------------|------------------|---|
| Policy Versions | Read (R) | Read (R) | Read (R) | --- | Read (R) |
| 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 Access Users and Groups | --- | --- | --- | --- | --- |

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

| Page | Ruleset Viewer (Scoped Read-Only) | Ruleset Manager | Ruleset Provisioner | Workload Manager | Application Owner (Combined Permissions) |
|---------------|--------------------------------------|-----------------|---------------------|------------------|---|
| 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).

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 |
| 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 |

| Page | Ruleset Viewer | Ruleset Manager | Ruleset Provisioner | Workload Manager |
|--|----------------|-----------------|---------------------|-------------------------------------|
| 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 Services | Y | Y | Y | Y |
| 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 |

| Page | Ruleset Viewer | Ruleset Manager | Ruleset Provisioner | Workload Manager |
|---------------|----------------|-----------------|---------------------|------------------|
| 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. The Illumination page opens when you log in to your account as an Organization Owner. 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

The scope of the user filters labeled objects, such as workloads. 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 logged in as a Ruleset Manager, you cannot manage workloads. So, all the workload-specific operations buttons are disabled. However, you can 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, if you search for Application Labels, 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, etc. The search bar automatically filters the facets to the list of facets in the user's assigned scope.

Global Objects

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



NOTE

Only the Global Organization Owner and Global Administrator can create, modify, and provision global objects.

Rulesets and Rules

Scoped users, except Workload Managers, can see rulesets and rules that apply to their applications. A Ruleset Manager can edit the ruleset, whereas the other scoped roles (Ruleset Viewer and Ruleset Provisioner) can 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 its 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 that apply to their applications. For example, scoped users can 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. The application owner provides visibility to all the rules that are applied to your application.

Policy Generator and Explorer

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

Explorer views are also filtered for scoped users. To use Explorer, one of the endpoints 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 created 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 restrictions. You can also configure access restrictions programmatically using the REST API calls described in "Access Restrictions and Trusted Proxy IPs" in the 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:

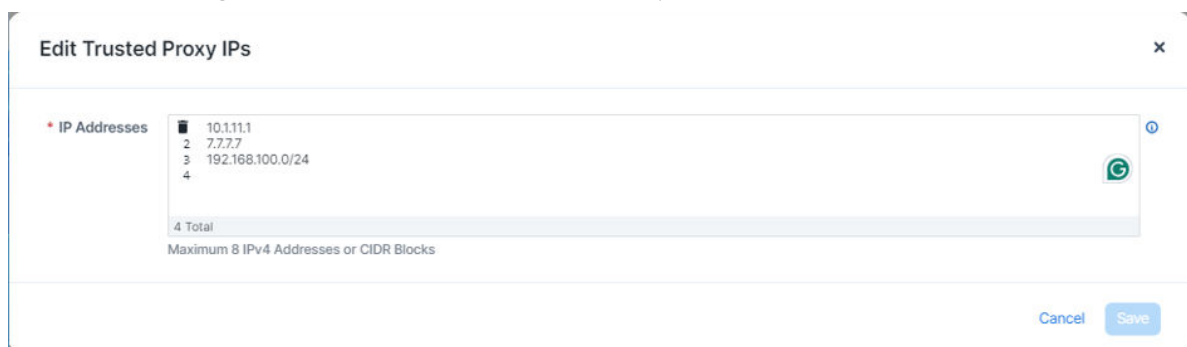
1. Log in to the PCE web console as a user with the Global Org Owner role.
2. Open the menu and choose **Access Management - Access Restrictions**.
The Access Restriction page opens with a list that shows which IP addresses are allowed and where the restrictions have been applied.
3. To add a new restriction, 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 addresses or CIDR blocks.
4. Click **Edit** to edit the restriction.
5. View the access restrictions applied to local users. The default is blank, no restrictions.
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 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. Select **Settings > Trusted Proxy**.
3. In the Trusted Proxy IPs page, click **Edit**.
4. A list of trusted proxy IPs is displayed. Proxy configuration can have upto 8 Trusted Proxy IPs.
5. To remove any of the proxies from the list, select the checkbox in front of the proxy address and click **Remove**.
6. To edit Trusted Proxy IPs, click **Edit**.
7. In the Edit Trusted Proxy IPs dialog box, you can add a proxy IP address to the list, or delete any of the existing addresses by hovering over the number in front of the address and then clicking the Trash Can icon that shows up.



8. Once you have added or deleted the proxy addresses for your needs, click **Save**.

Manage API Keys

You can add and edit API keys using the PCE console;

Creating API Keys

1. In the Web console, type "API keys" in the Search field.
2. In the API Keys page, click **Add**.
3. In the "Create API Key" pop-up dialog, add the
 - a. Key Name
 - b. Description of the key
 - c. Org ID
4. Click Create.
5. The confirmation dialog appears to show the data for the created API key.

API Key Created

This is the only time these credentials will be available to download. You can manage and recreate these credentials at any time.

| | |
|--------------------------------|--|
| Name | Pubs-key |
| Description | Pubs group key |
| Key ID | 13b0b856607c48a49 |
| Authentication Username | api_13b0b856607c48a49 |
| Secret | 1b04e723f8e0ada762daa00980bbbb987916e215a5b5baf4139652d0b903274e |

Close

Download Credentials

- To download the credentials, click on **Download Credentials**.
You can download the credentials only after the key is created. You can, however, manage the credentials at any time.
- The credentials will be downloaded in the default download directory on your hard drive, with the name API-Key-<your-key-name>. The format of the credential is a TXT file.

```
{ "key_id": "13b0b856607c48a49", "auth_username": "api_13b0b856607c48a49",  
  "secret": "1b04e723f8e0ada762daa00980bbbb987916e215a5b5baf4139652d0b903274e" }
```

Editing Expiration of API Keys

To edit expiration of the Service account API keys using the PCE console:

- Select **Settings > API Keys**.
- On the API Key Settings page, click **Edit**.
- By default, API Key for Service Account expires in:
Select from the dropdown list: **Never expires**, **1 day**, **30 days**, **60 days**, or **90 days**.
If you change this setting, expiration of the existing API keys will not be impacted.
- Keep expired API keys for:
Select from the dropdown list: **1 day**, **30 days**, **60 days**, **90 days**, or **custom**.

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.

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: ! @ # \$ % ^ & * < > ? .

**WARNING**

Any other special characters are neither tested nor supported.

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 **Access > Authentication**.
2. In the Authentication Settings screen, choose the Authentication Method to authenticate users for accessing the PCE:
 LOCAL (IN USE) : User will sign in to the PCE only with a local credential provided by the user's organization password policy.
 SAML (IN USE) : SAML users can also authenticate to the PCE using local credentials.
 LDAP: LDAP user can also authenticate to the PCE using local credentials>
3. Once you decide which option to take, click on the **Configure** button.
4. Depending on the authentication method, these are the available options:
 Choose option LOCAL, SAML, or LDAP:

LOCAL (in use)

Password requirements

| | |
|-------------|--------------|
| Min lengths | 8 characters |
|-------------|--------------|

LOCAL (in use)

Character categories A-Z (required),

a-z (required),

0-9 (required)

Min characters per category 1

Password expiration and reuse

Expiration Never

Reuse history 1 password changes

Similarity 1 character and position from the current password

Session timeout

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 critical 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.

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

The PCE Org owner can go to **Access > Authentication > Local** to configure Session Timeout. This PCE session timeout is applicable to any user belonging to the same organization, regardless whether they are local or external users.

Timeout 30 minutes

SAML (in use)**Information from Identity provider**

SAML Identity provider certificate

```
-----BEGIN CERTIFICATE----- MIICpDC-
CAYwCCQD05WZgX RugDANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQD-
DAlsb2NhbGhvc 3QwHhcNMTgxMTE0MjAyNmM2WhcNMjgxMTE0Mj-
jAyNmM2WjAUMRIw EAYDVQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBA-
QUAA4I BDwAwggEKAoIBAQDXs/OhH90IPQ8qBrUMqzQZb5MI72fu+Ay0s
P8gI1v8RiUqS1+WJNo8s9L8GNI9hnQT+OXg99PNmoE41xiAlnx
qx8T78Qxb9zX3uc4hec+9bMSF7iieUiFXWQrIUVM3g8TWI6B5g
Uapt0vZcxNok2eNhiFvVTlgPzB06vb2/yU68ilwQ8wz/MGO00Un/ 1Rw3LORy-
nEAluMeT6terWtX8JQGbvclqYddnXD86Y5MOP1AXU+ 1w1w1JFxD0uKiuOHJv-
NYfJjkisEbDis9b0/E00SyayVA7ABELaw QTfeWM6xLrNhZCTGeQiKb4XHMBgeliA-
loEvNDDofKbLDQrWUyIf7 TAgMBAAEwDQYJKoZIhvcNAQELBQADggEBANLhqsZs-
FUng7kc+B5a vMmOXbCNJmSaASBULsX+akexhyJdMZUxmN6wfLjZ3F0wvFuhe-
Ta Zpkp1UtC+2E9YlxY//FxOX/YyvNT/xf0BzqZ9SCsNxpCBsSRK5X4
DS+2jGQuz3fwbJDxTXP4sKNUZ/E9Z+dC9Npdq7xtcXr7pWhI2qe
MO8E9LdvfWLcsqq8Z0VtxyHYZYh8KN0Q6ObfK1sPC4QZ/292B
xm2ckxsWDTyONV8ytLQKwp93exxqmzpzpzb6qi23y0B4u4af+/SW9 ukjzD/
atP34bY1YjeLBCsKEgylnDTVgypAZSEy46kJ9mAu6t3r4/gEg XTkMYQDtrPA= -----END
CERTIFICATE-----
```

Remote login URL https://hohoho.illumio.com

| SAML (in use) | |
|--|--|
| Logout landing URL | https://hohoho.illumios.com/!logout |
| Information for Identity provider | |
| Authentication method | unspecified |
| Force re-authentication | no |
| Sign SAML request | no |
| SAML version | 2.0 |
| Issuer URL | https://2x2testlab360.ilabs.io:8443/login |
| NameID format | urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress |
| Assertion consumer URL | https://2x2testlab360.mylabs.io:8443/login/acs/6b5243ef-2305-4ffd-bf81-4fa97fb91a5b |
| Logout URL | https://2x2testlab360.mylabs.io:8443/login/logout/6b5243ef-2305-4ffd-bf81-4fa97fb91a5b |
| Timeout | 30 minutes |

5. LDAP authentication is not active. Click **Turn On** to apply on all the LDAP servers.

6. To create an LDAP server, click on **Create Server**.

To continue with LDAP server configuration, see the "LDAP Authentication" topic.

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[REDACTED]l3/login |
| NameID Format | urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress |
| Assertion Consumer URL | https://[REDACTED]l3/login/acs/a63e[REDACTED]49598e |
| Logout URL | https://[REDACTED]43/login/logout/a63e[REDACTED]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:

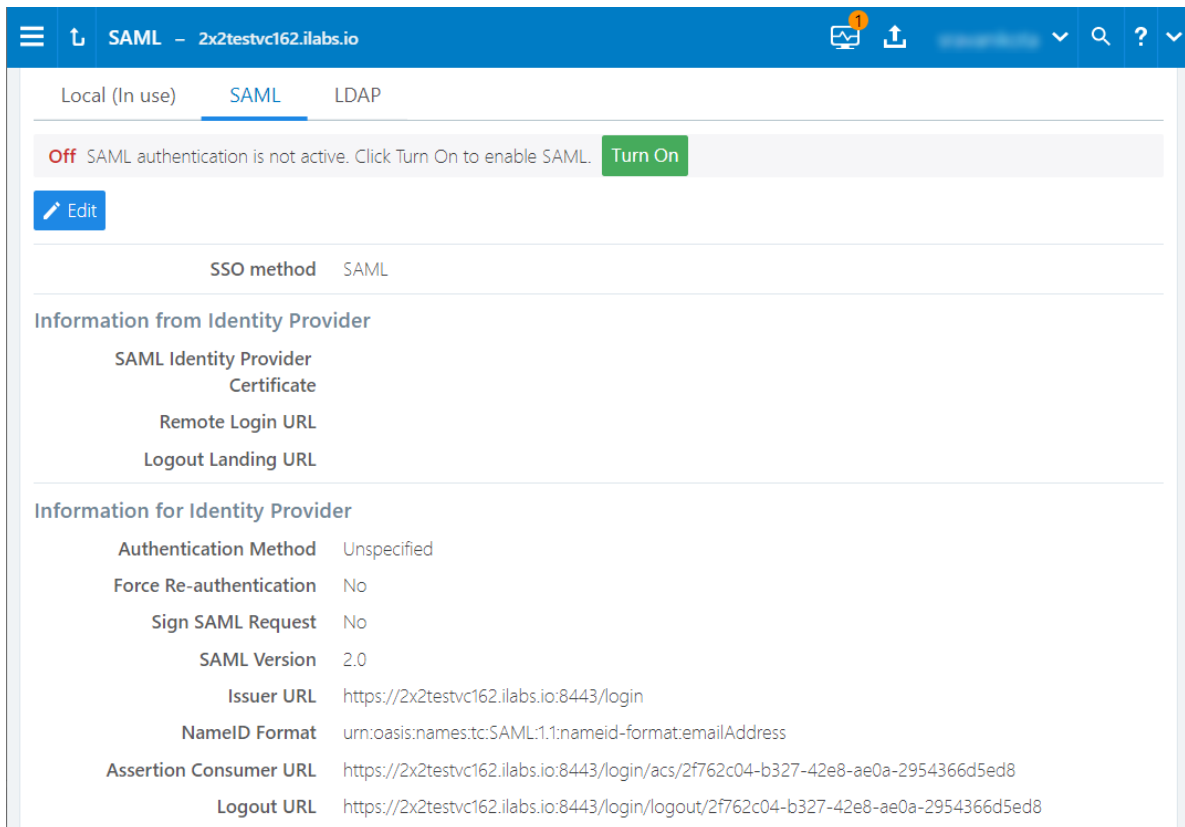
- GET /authentication_settings/saml_configs
- GET /authentication_settings/saml_configs/:uuid
- PUT /authentication_settings/saml_configs/:uuid
- POST /authentication_settings/saml_configs/:uuid/pce_signing_cert

These APIs are covered in detail in 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**.



Local (In use) SAML LDAP

Off SAML authentication is not active. Click Turn On to enable SAML. [Turn On](#)

[Edit](#)

SSO method SAML

Information from Identity Provider

SAML Identity Provider Certificate

Remote Login URL

Logout Landing URL

Information for Identity Provider

Authentication Method Unspecified

Force Re-authentication No

Sign SAML Request No

SAML Version 2.0

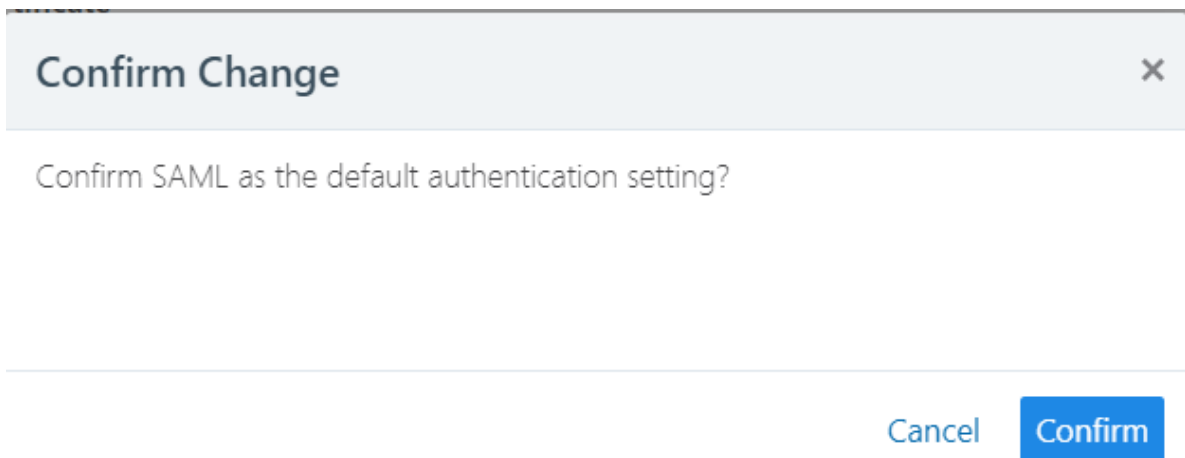
Issuer URL https://2x2testvc162.ilabs.io:8443/login

NameID Format urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Assertion Consumer URL https://2x2testvc162.ilabs.io:8443/login/acs/2f762c04-b327-42e8-ae0a-2954366d5ed8

Logout URL https://2x2testvc162.ilabs.io:8443/login/logout/2f762c04-b327-42e8-ae0a-2954366d5ed8

4. In the pop-up screen, click **Confirm**.

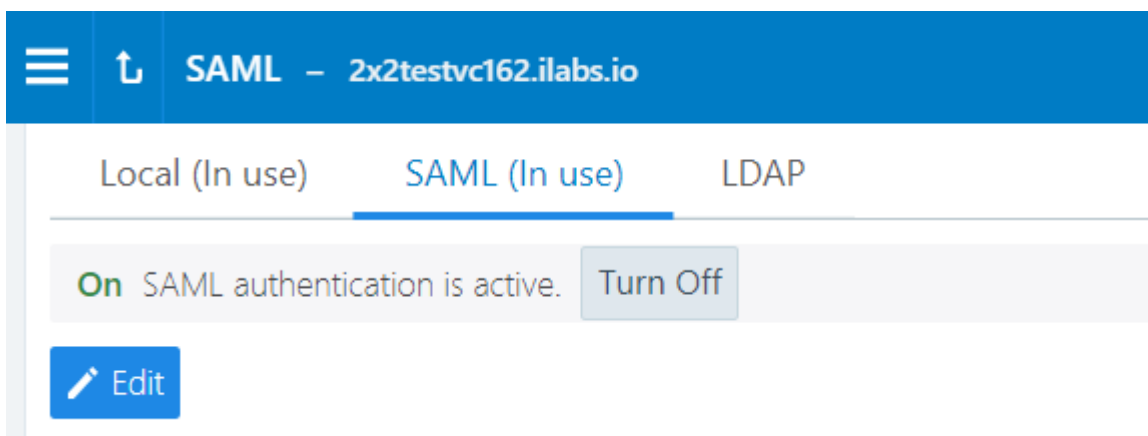


Confirm Change ×

Confirm SAML as the default authentication setting?

[Cancel](#) [Confirm](#)

The updated SAML screen shows that SAML authentication is active.



Local (In use) SAML (In use) LDAP

On SAML authentication is active. [Turn Off](#)

[Edit](#)

If necessary, you can disable it at any time.

Once configured using these steps, the lifetime of the SAML certificate is ten years.

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

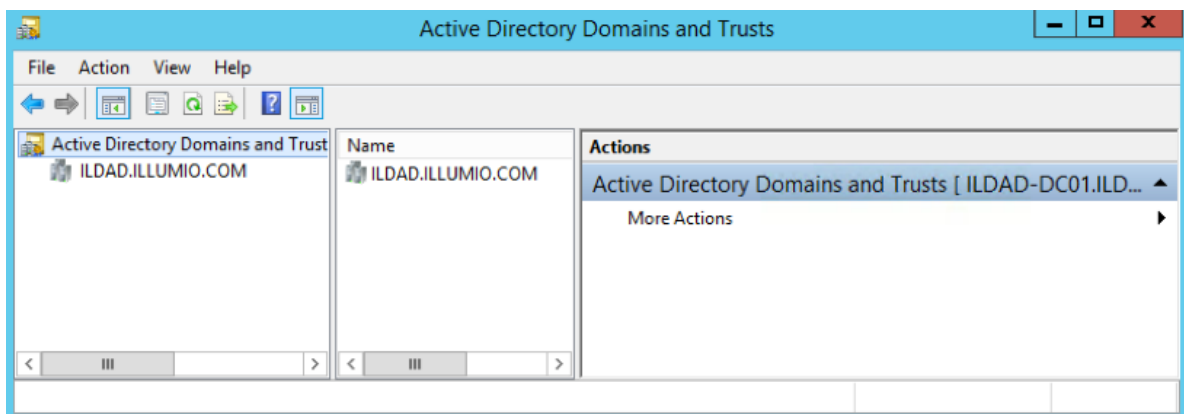
There are two ways for AD FS to produce the NameID claim for an SSO user. The first uses the email field in an Active Directory user account for the NameID.

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.

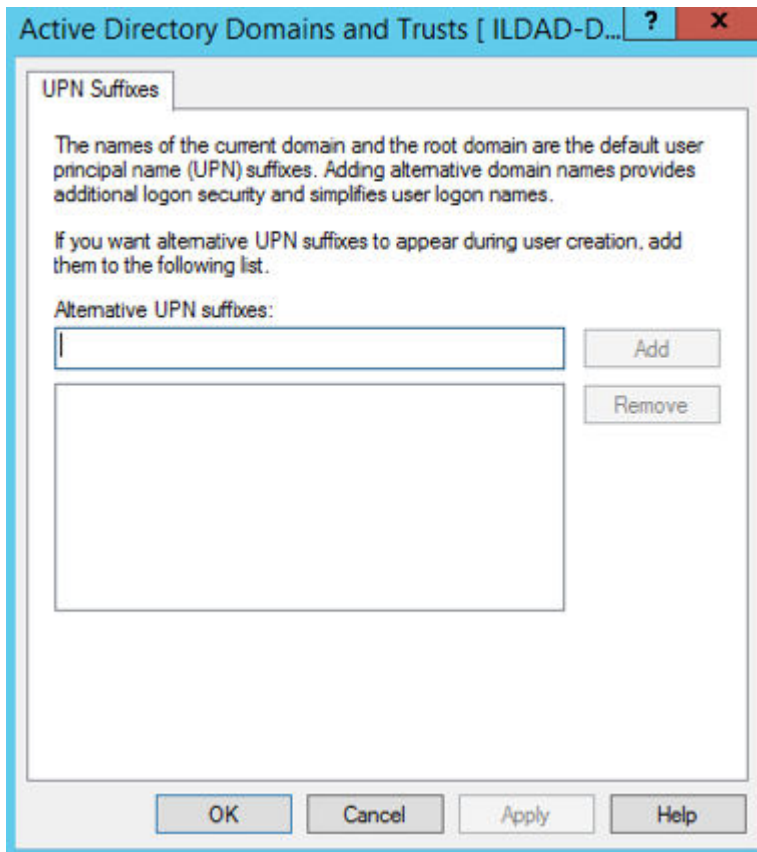
Configure AD Users to Use Different UPN Suffixes

To configure different UPN suffix as the source for NameID:

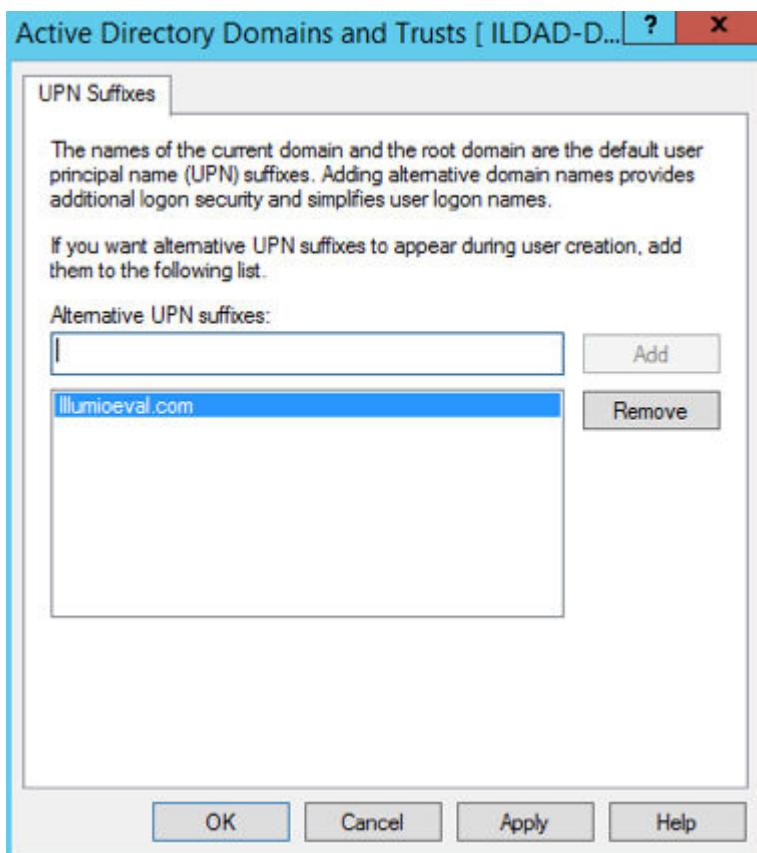
1. Add a UPN suffix. On your system under Server Manager Tools, click **Active Directory Domains and Trusts**.



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.

The screenshot shows the 'test Properties' dialog box with the 'Account' tab selected. The 'User logon name' field contains 'test' and the dropdown menu shows '@ILDAD.ILLUMIO.COM' selected. The 'User logon name (pre-Windows 2000)' field contains 'ILDAD\' and the dropdown menu shows '@illumioeval.com' selected. The 'Logon Hours...' and 'Log On To...' buttons are visible. The 'Account options' section has 'Password never expires' checked. The 'Account expires' section has 'Never' selected.

Your UPN configuration is set up and you can begin configuring AD FS for SSO with the PCE.

Initial AD FS SSO Configuration

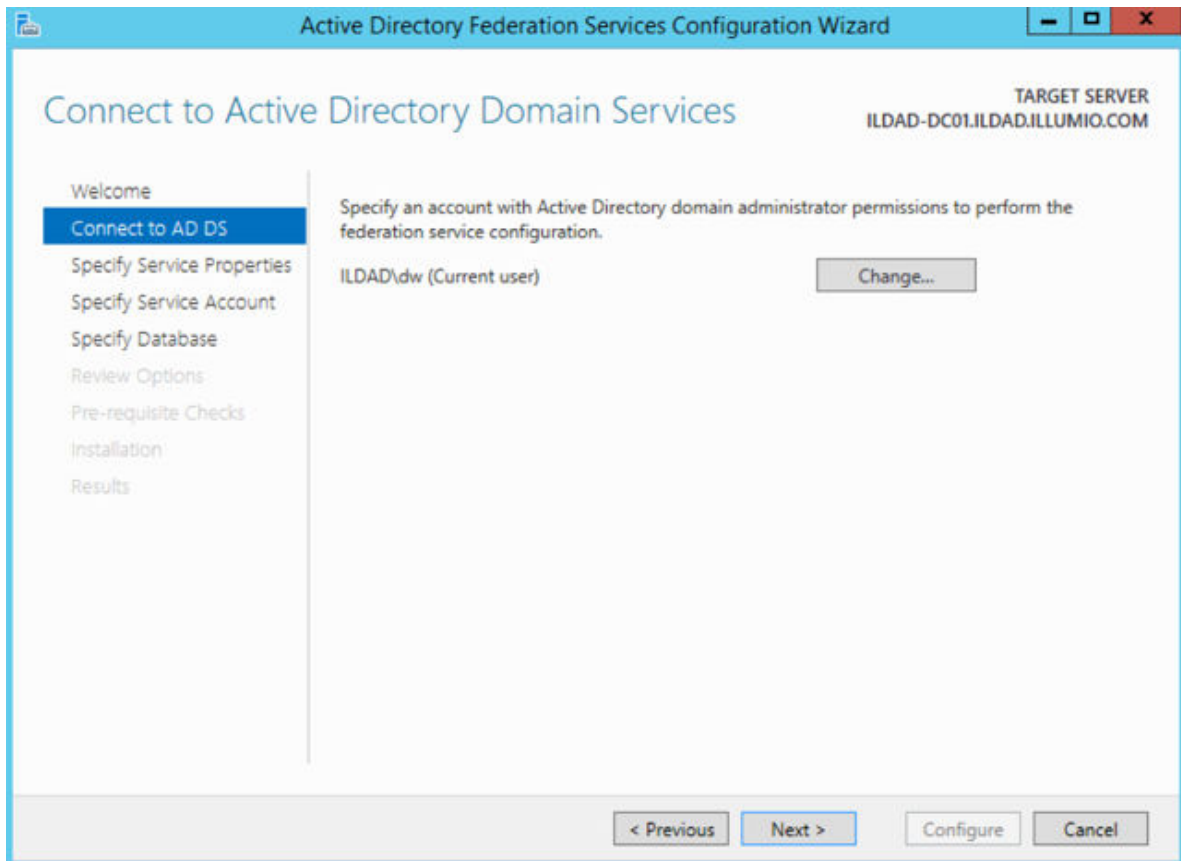
This task explains how to perform the initial configuration of AD FS to be your SSO IdP for Illumio Core.

To configure AD FS:

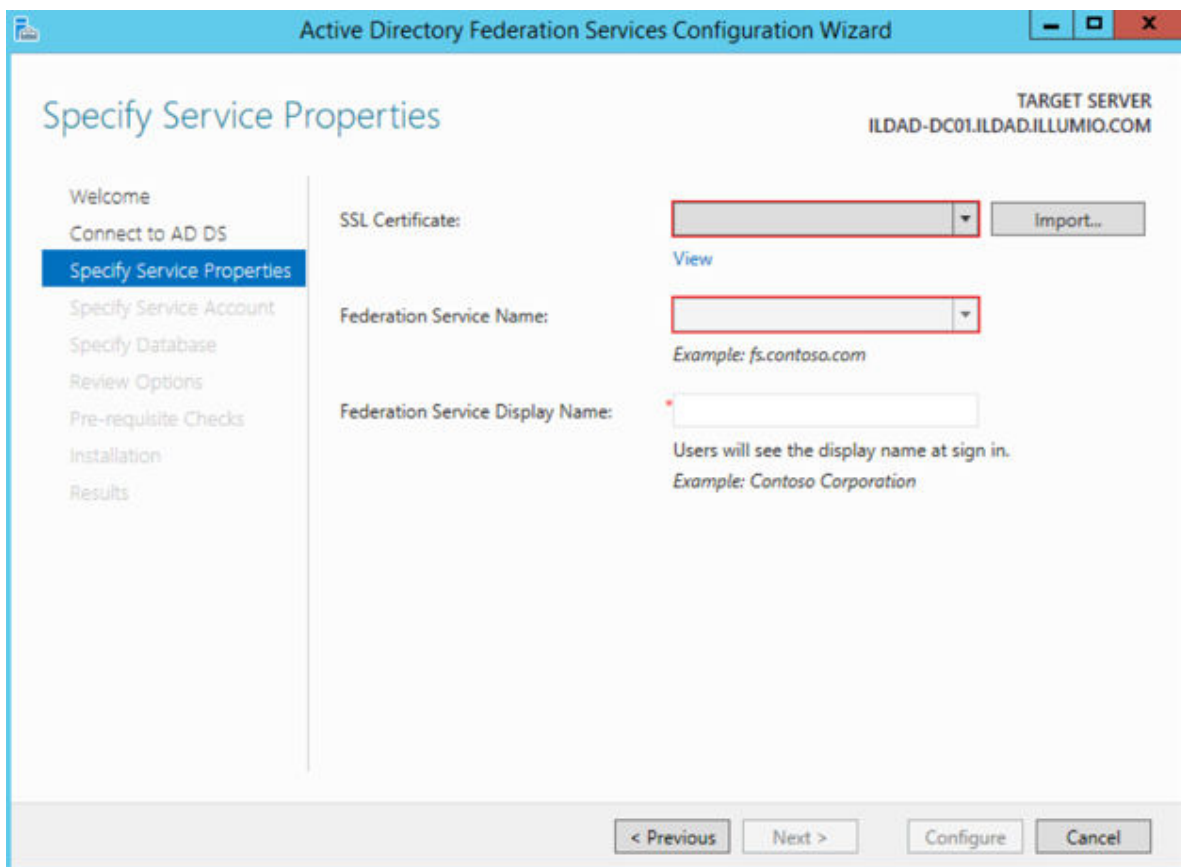
1. Open Microsoft Server Manager and click the notification icon.



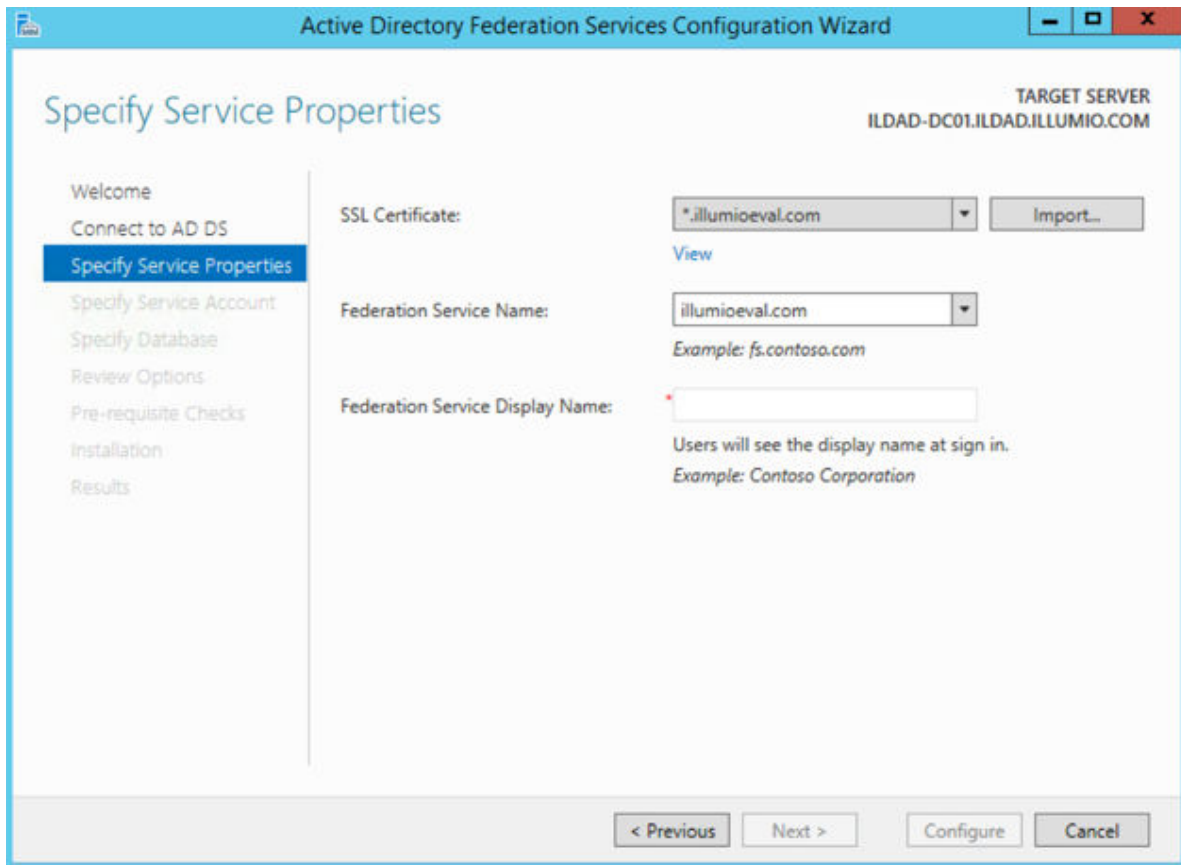
2. Click the "Configure the federation service on this server" link.
3. Select "Create the first federation server in a federation server farm" option and click **Next**.
4. Specify a domain admin account for AD FS configuration.



5. Select or import a certificate. This certificate can be a self-signed certificate.



6. Specify your Federation Service Name, enter a display name for this instance of AD FS, and click **Next**



Active Directory Federation Services Configuration Wizard

TARGET SERVER
ILDAD-DC01.ILDAD.ILLUMIO.COM

Specify Service Properties

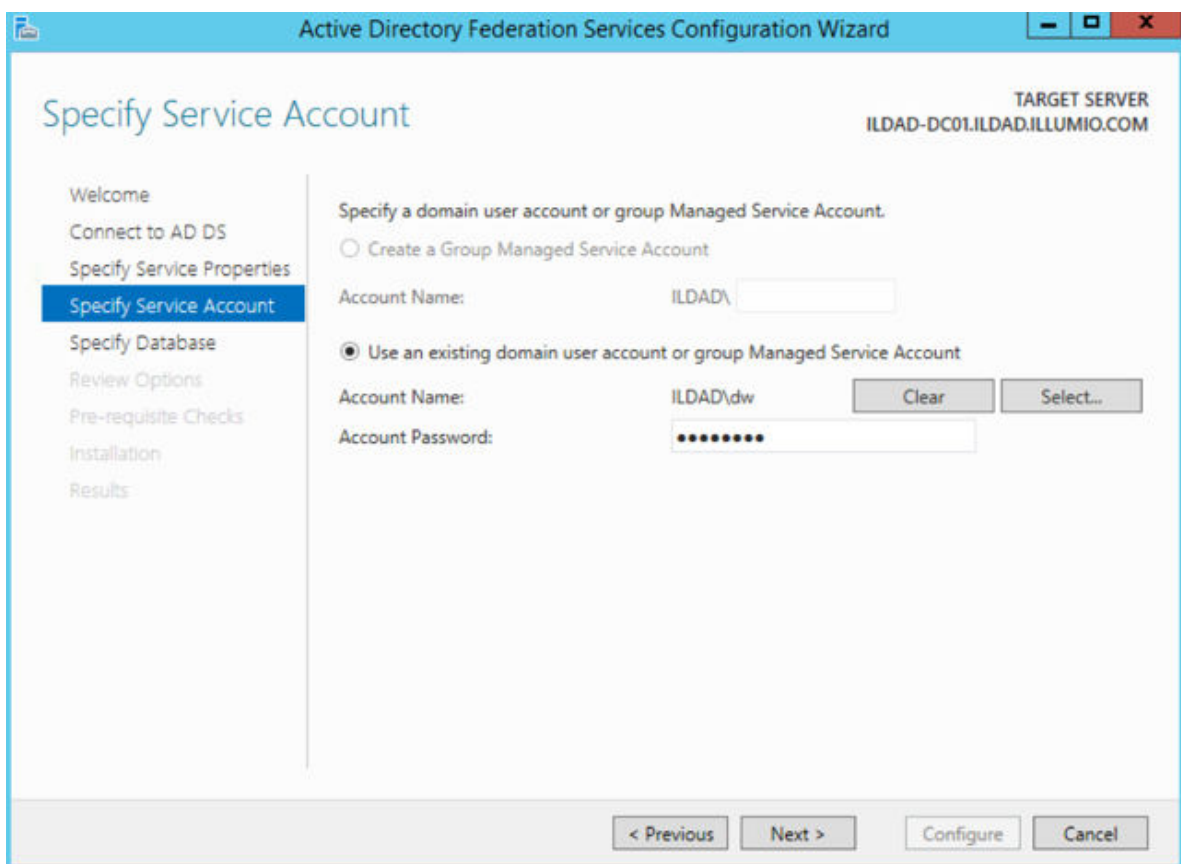
Welcome
 Connect to AD DS
Specify Service Properties
 Specify Service Account
 Specify Database
 Review Options
 Pre-requisite Checks
 Installation
 Results

SSL Certificate:
 View

Federation Service Name:
 Example: fs.contoso.com

Federation Service Display Name:
 Users will see the display name at sign in.
 Example: Contoso Corporation

7. Specify your service account and click **Next**.



Active Directory Federation Services Configuration Wizard

TARGET SERVER
ILDAD-DC01.ILDAD.ILLUMIO.COM

Specify Service Account

Welcome
 Connect to AD DS
 Specify Service Properties
Specify Service Account
 Specify Database
 Review Options
 Pre-requisite Checks
 Installation
 Results

Specify a domain user account or group Managed Service Account.

☐ Create a Group Managed Service Account

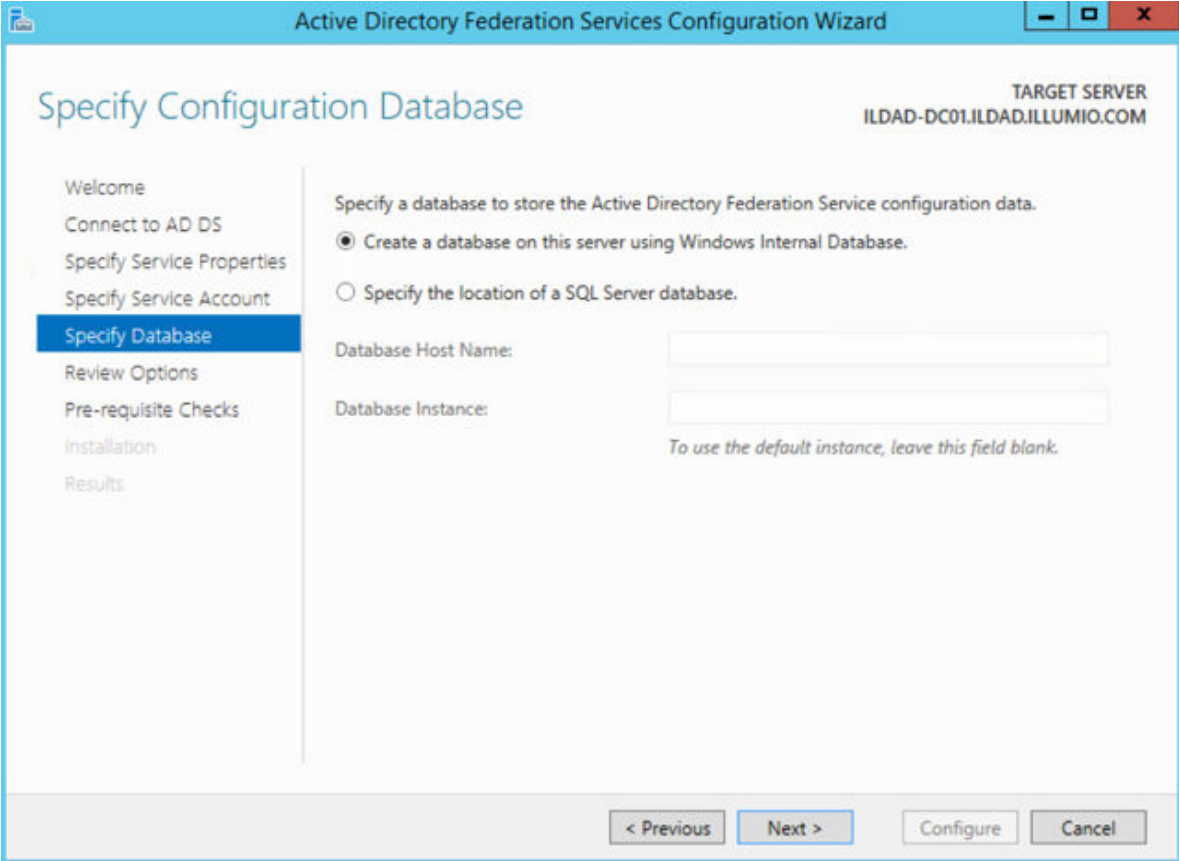
Account Name:

☒ Use an existing domain user account or group Managed Service Account

Account Name:

Account Password:

8. Select "Create a database on this server using Windows Internal Database" or choose the SQL server option, and click **Next**.



The screenshot shows the 'Specify Configuration Database' step of the Active Directory Federation Services Configuration Wizard. The title bar reads 'Active Directory Federation Services Configuration Wizard'. The left sidebar contains a list of steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account, Specify Database (highlighted), Review Options, Pre-requisite Checks, Installation, and Results. The main area is titled 'Specify Configuration Database' and shows the 'TARGET SERVER' as 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. It instructs the user to 'Specify a database to store the Active Directory Federation Service configuration data.' and offers two options: 'Create a database on this server using Windows Internal Database.' (selected with a radio button) and 'Specify the location of a SQL Server database.' (unselected). Below these options are input fields for 'Database Host Name:' and 'Database Instance:'. A note states 'To use the default instance, leave this field blank.' At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

Active Directory Federation Services Configuration Wizard

TARGET SERVER
ILDAD-DC01.ILDAD.ILLUMIO.COM

Specify Configuration Database

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a database to store the Active Directory Federation Service configuration data.

☒ Create a database on this server using Windows Internal Database.

☐ Specify the location of a SQL Server database.

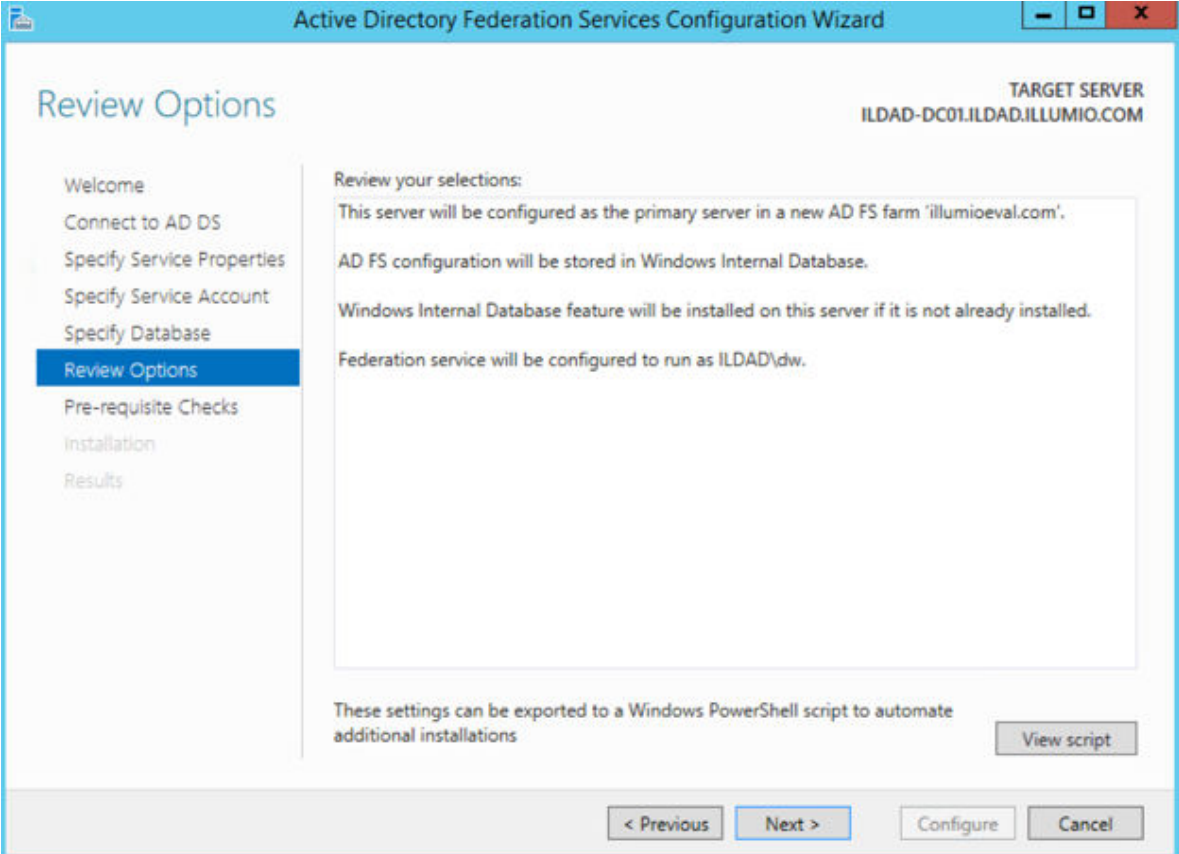
Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

< Previous Next > Configure Cancel

9. Review your selected options and click **Next**.



The screenshot shows the 'Review Options' step of the Active Directory Federation Services Configuration Wizard. The title bar reads 'Active Directory Federation Services Configuration Wizard'. The left sidebar contains a list of steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account, Specify Database, Review Options (highlighted), Pre-requisite Checks, Installation, and Results. The main area is titled 'Review Options' and shows the 'TARGET SERVER' as 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. It instructs the user to 'Review your selections:' and lists the following configuration details: 'This server will be configured as the primary server in a new AD FS farm 'illumioeval.com'.', 'AD FS configuration will be stored in Windows Internal Database.', 'Windows Internal Database feature will be installed on this server if it is not already installed.', and 'Federation service will be configured to run as ILDAD\dw.' At the bottom, there is a note 'These settings can be exported to a Windows PowerShell script to automate additional installations' and a 'View script' button. At the bottom of the wizard, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

Active Directory Federation Services Configuration Wizard

TARGET SERVER
ILDAD-DC01.ILDAD.ILLUMIO.COM

Review Options

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'illumioeval.com'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

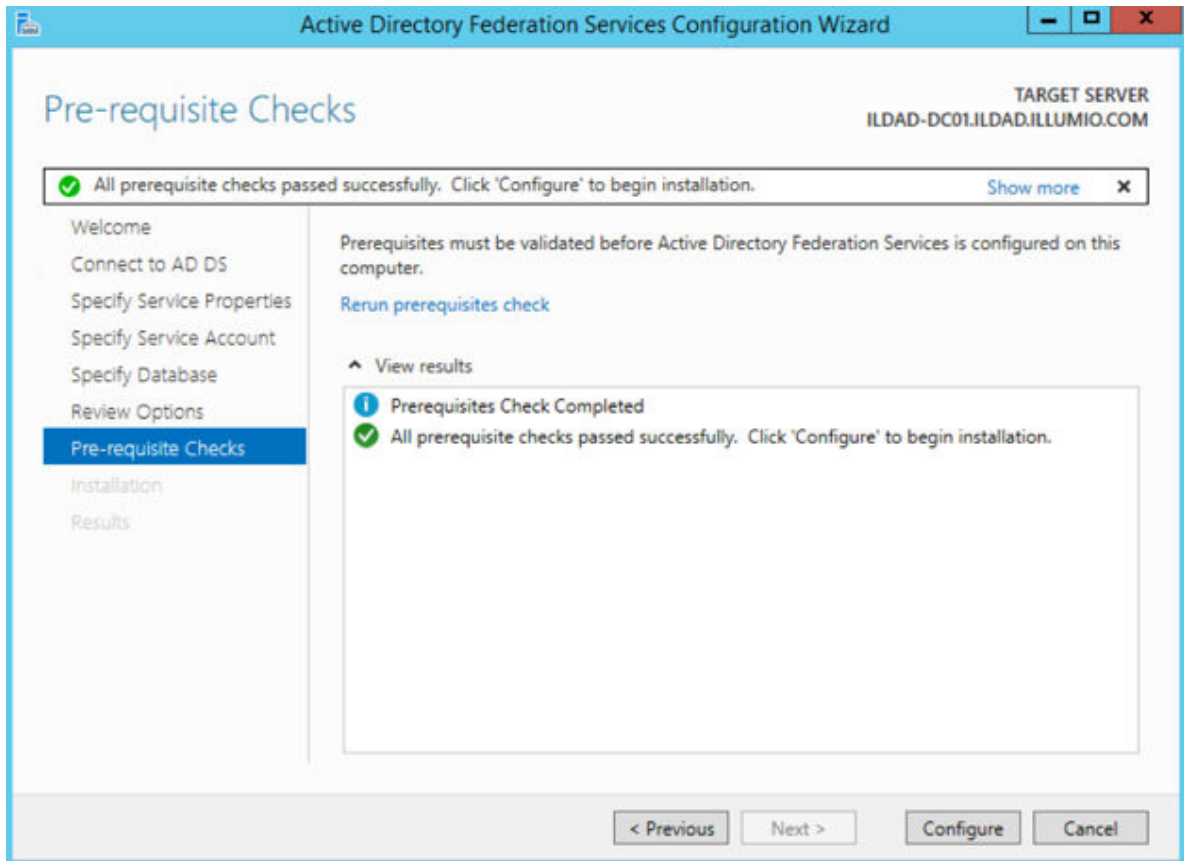
Federation service will be configured to run as ILDAD\dw.

These settings can be exported to a Windows PowerShell script to automate additional installations

View script

< Previous Next > Configure Cancel

- 10 Click **Configure** to finish the basic configuration of AD FS.



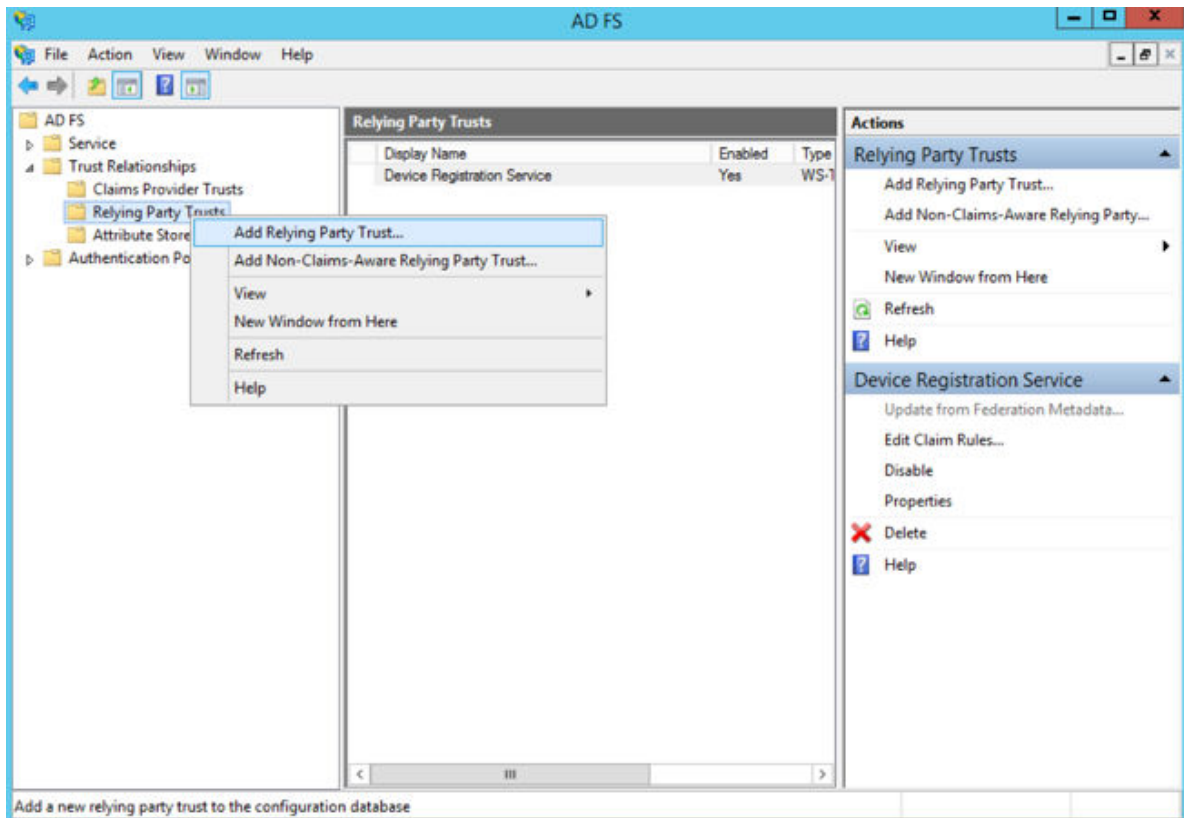
11. In the results screen, click **Close**.

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

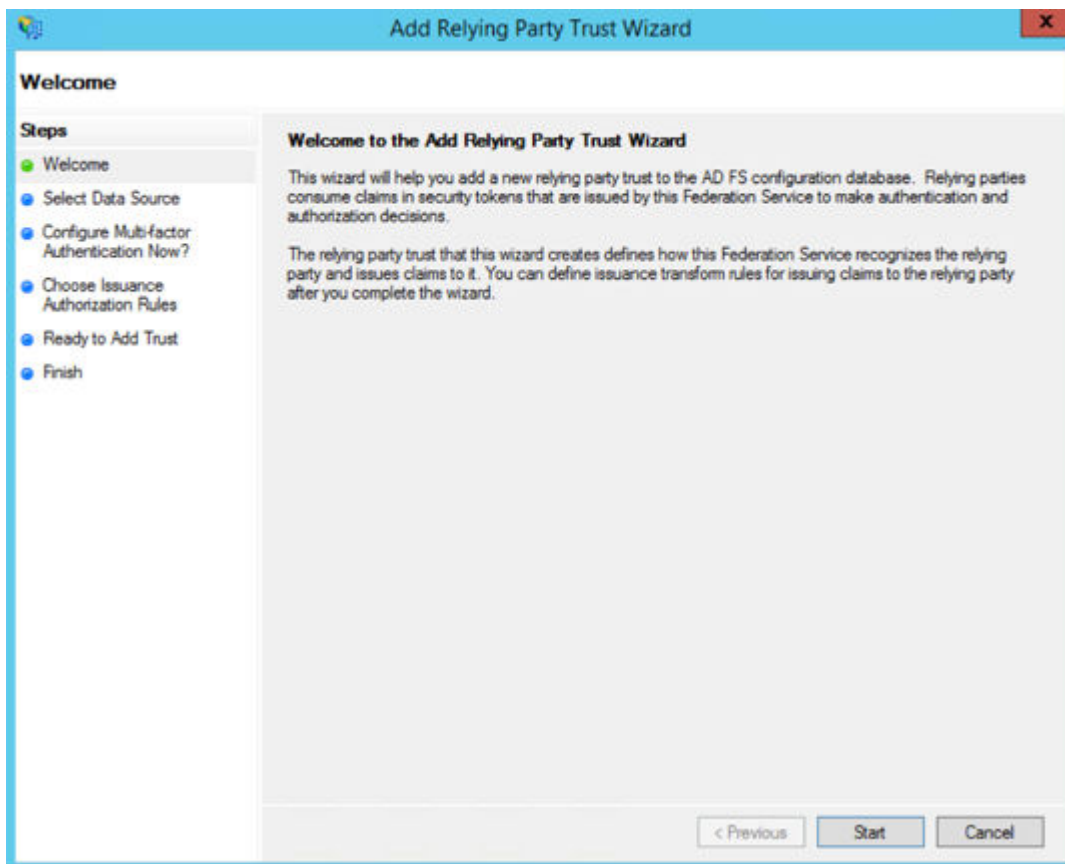
Create a Relying Party Trust

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**.



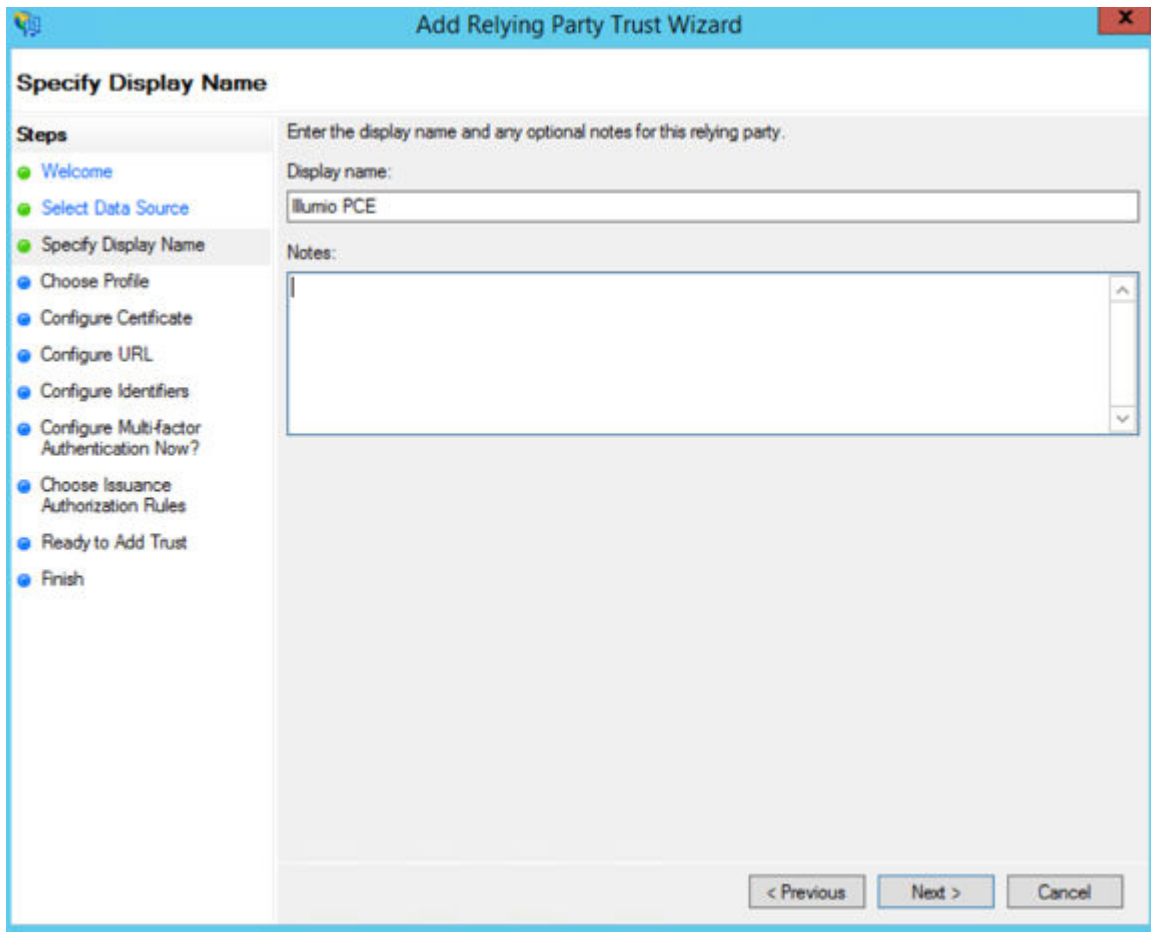
The Add Relying Party Trust Wizard appears.



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

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main window has a light gray background. On the left, there is a 'Steps' pane with a list of steps: 'Welcome', 'Select Data Source' (highlighted with a green dot), 'Specify Display Name', 'Choose Profile', 'Configure Certificate', 'Configure URL', 'Configure Identifiers', 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area of the wizard is titled 'Select Data Source' and contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network'. Below this is the text: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' followed by a text box labeled 'Federation metadata address (host name or URL):' with an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Below this is the text: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' followed by a text box labeled 'Federation metadata file location:' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected with a radio button). Below this is the text: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right of the wizard are three buttons: '< Previous', 'Next >', and 'Cancel'.

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



The image shows a Windows wizard window titled "Add Relying Party Trust Wizard". The current step is "Specify Display Name". On the left, a "Steps" list shows the progression: Welcome, Select Data Source, Specify Display Name (current), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction "Enter the display name and any optional notes for this relying party." Below this, the "Display name:" field is populated with "Illumio PCE". The "Notes:" field is empty. At the bottom right, there are three buttons: "< Previous", "Next >", and "Cancel".

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

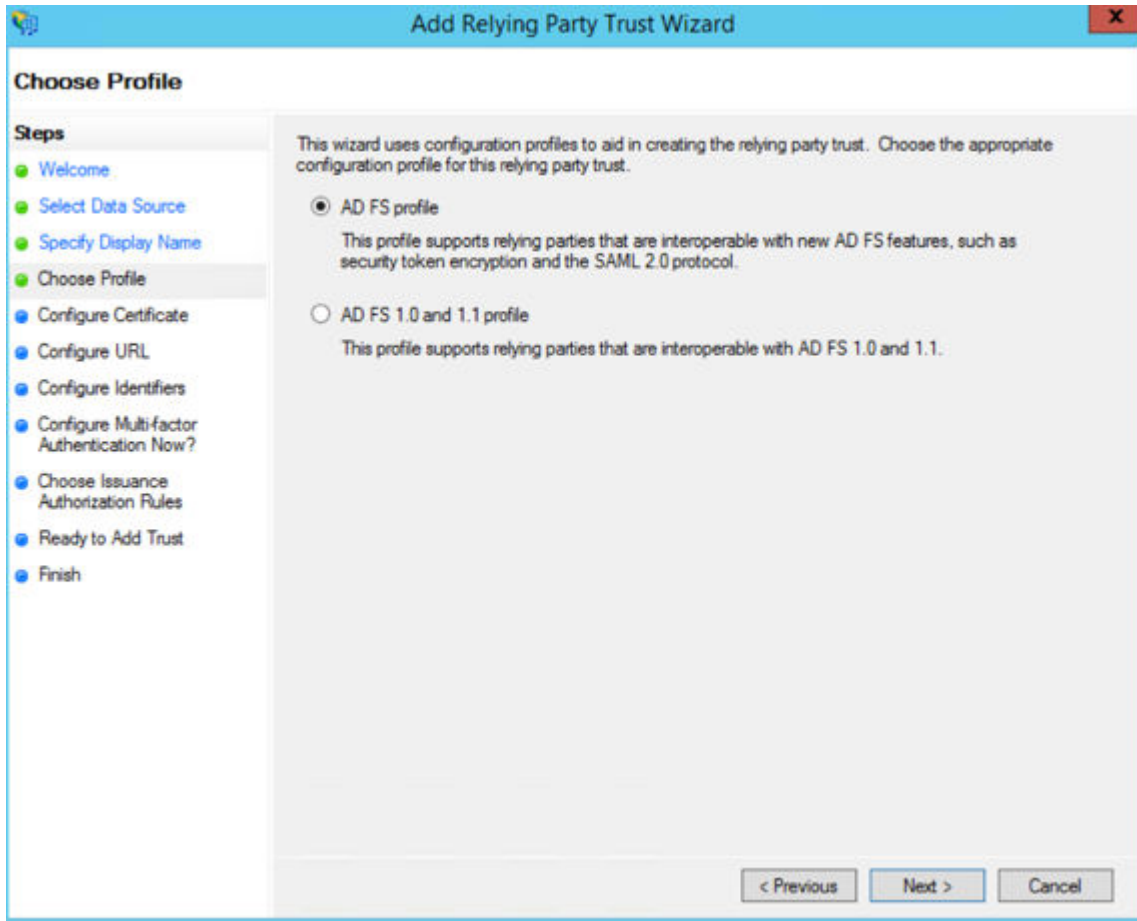
Display name:

Illumio PCE

Notes:

< Previous Next > Cancel

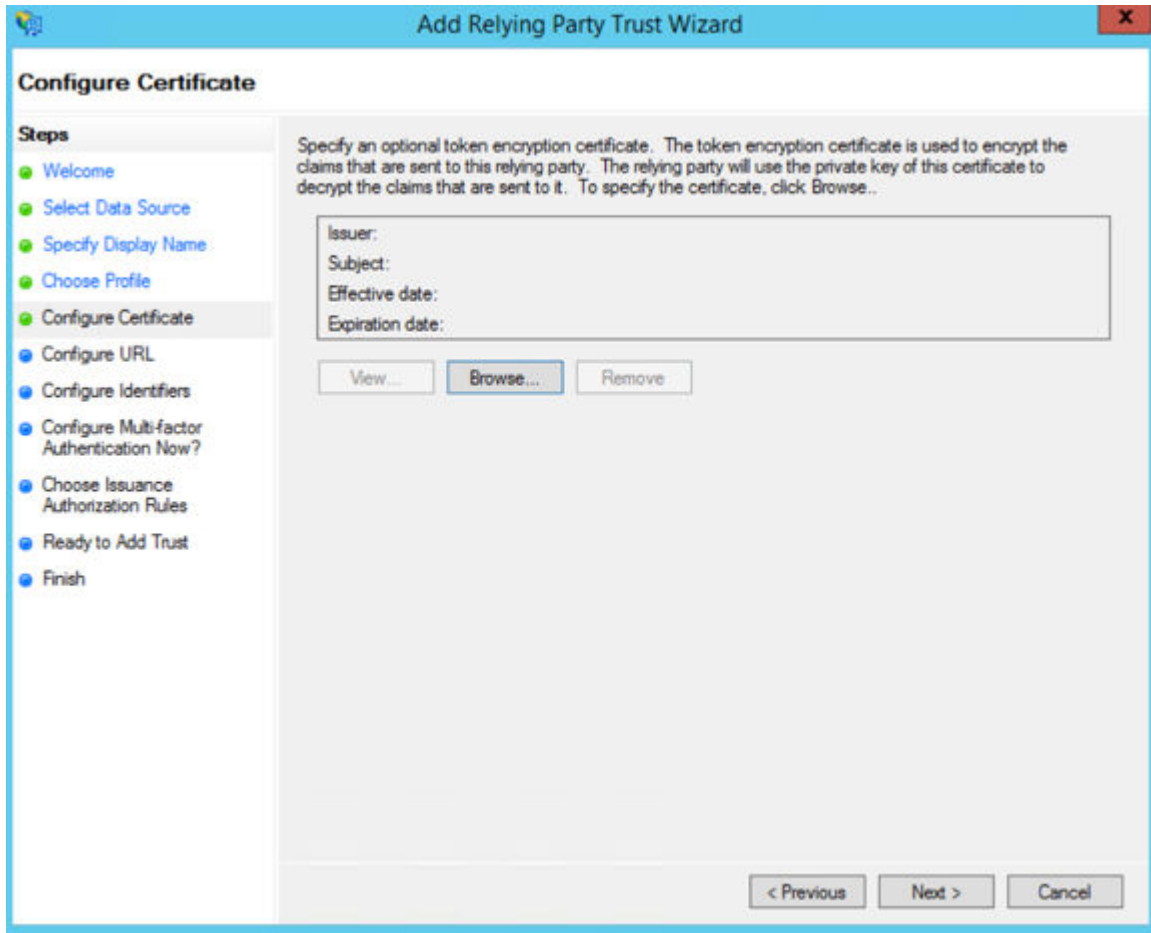
6. Select "ADFS profile" and click **Next**.



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 installation) 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:

| | |
|-----------------------------------|--|
| Information for Identity Provider | |
| Default User Role | Read Only |
| SAML Version | 2.0 |
| Issuer | https://pce-mnc.illumioeval.com:8443/login |
| NameID Format | urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress |
| Assertion Consumer URL | https://pce-mnc.illumioeval.com:8443/login/acs/2402fb18-3d75-4432-ab6d-10475897b476 |
| Logout URL | https://pce-mnc.illumioeval.com:8443/login/logout/2402fb18-3d75-4432-ab6d-10475897b476 |

9. On the Configure Identifiers page, use the same URL for the Relying party trust identifier, without the /acs/<randomNumbers>.

For example: https://pce.domain.com:8443/login.

Click **Next**.

10. Select the radio button “I do not want to configure multi-factor authentication settings for this relying party at this time” 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**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Ready to Add Trust' step. The left pane lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust (selected), and Finish. The main pane displays a summary of the configuration and monitoring settings. At the top, it states: 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this is a tabbed interface with tabs for Monitoring, Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Notes. The 'Monitoring' tab is active, showing a text box for 'Relying party's federation metadata URL:' and two checkboxes: 'Monitor relying party' and 'Automatically update relying party'. Below these are two labels: 'This relying party's federation metadata data was last checked on: < never >' and 'This relying party was last updated from federation metadata on: < never >'. At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Notes < >

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☐ Monitor relying party

☐ Automatically update relying party

This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

< Previous Next > Cancel

13. Leave the Open the Edit Claim Rules checkbox selected and click **Close**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Finish' step. The left pane lists the steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish (selected). The main pane displays a confirmation message: 'The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.' Below this is a checkbox labeled 'Open the Edit Claim Rules dialog for this relying party trust when the wizard closes', which is checked. At the bottom right is a 'Close' button.

Add Relying Party Trust Wizard

Finish

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

The relying party trust was successfully added to the AD FS configuration database.
You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

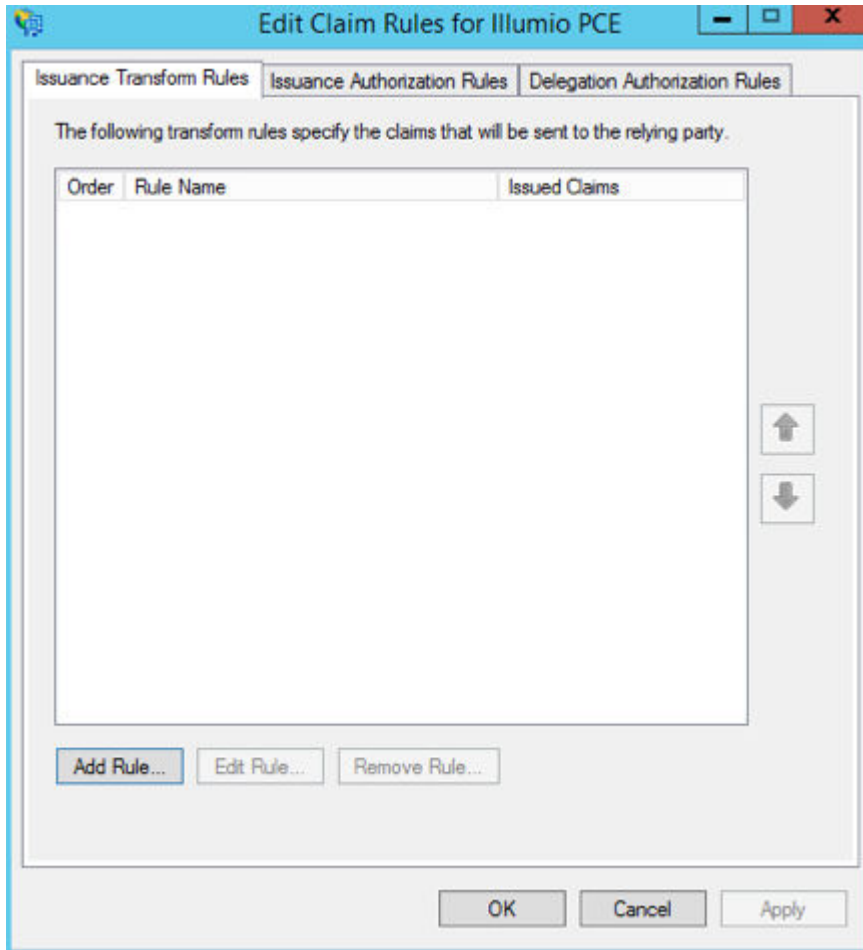
☒ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

Close

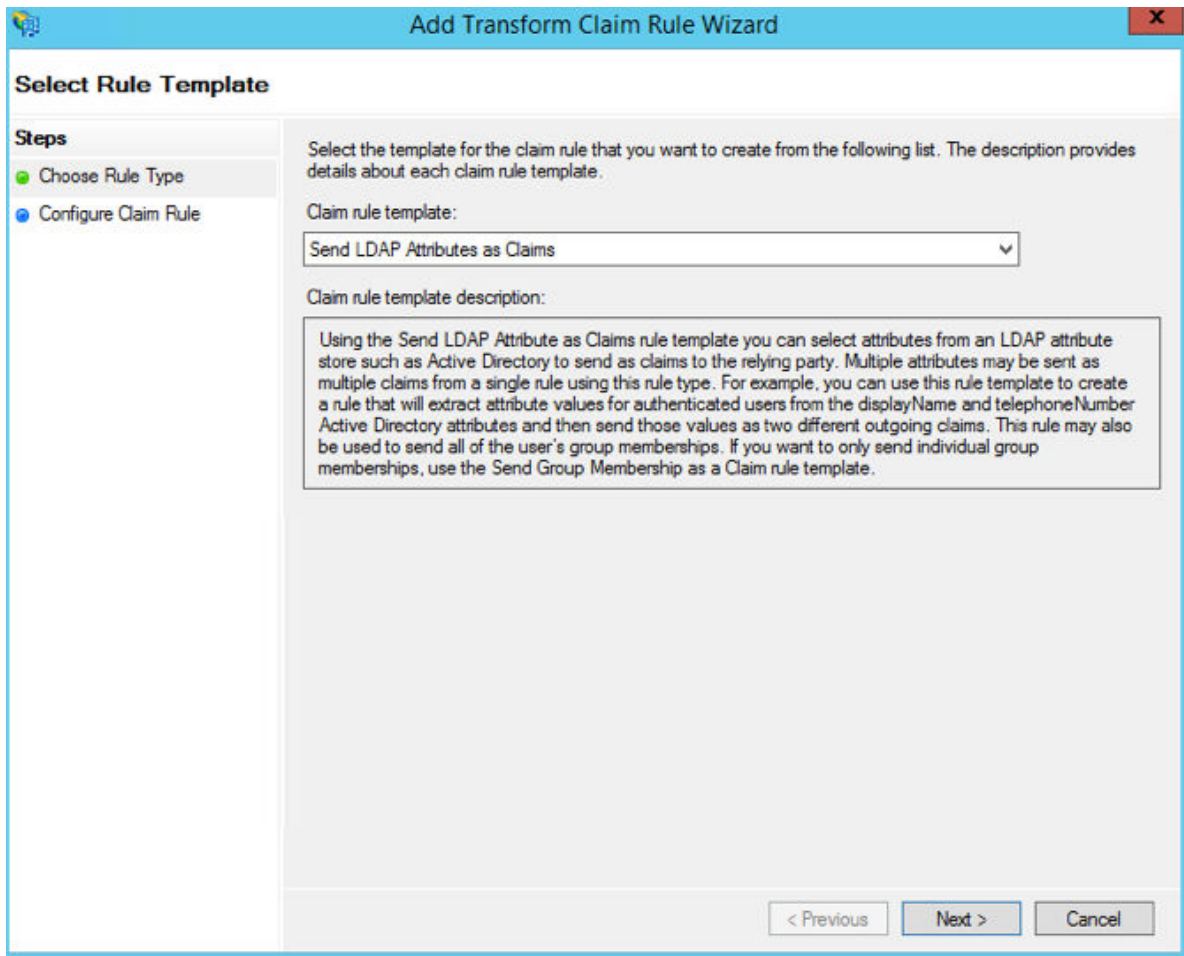
Create Claim Rules

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

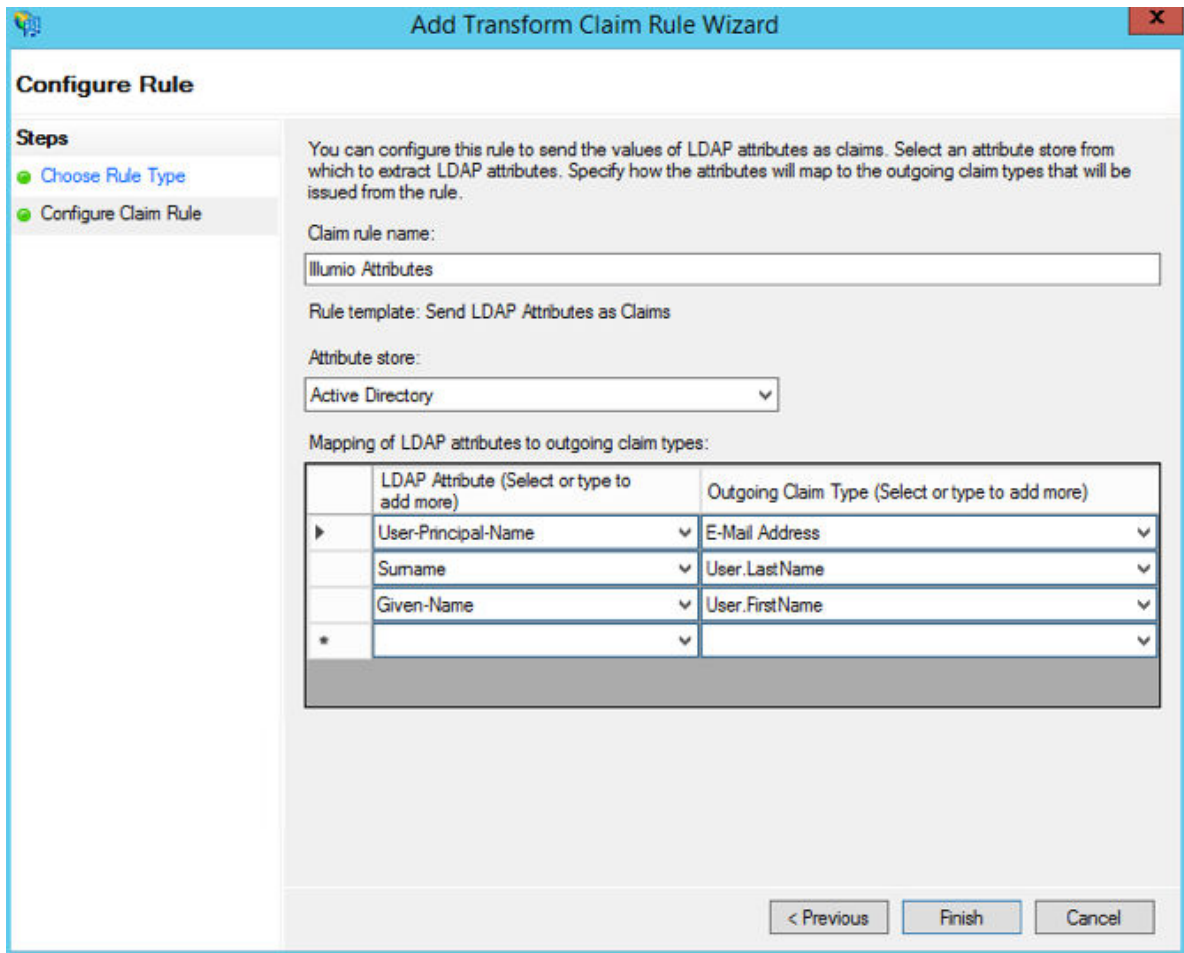
1. In the Edit Claim Rules dialog, click **Add Rule**.



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**.



Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Illumio.Attributes

Rule template: Send LDAP Attributes as Claims

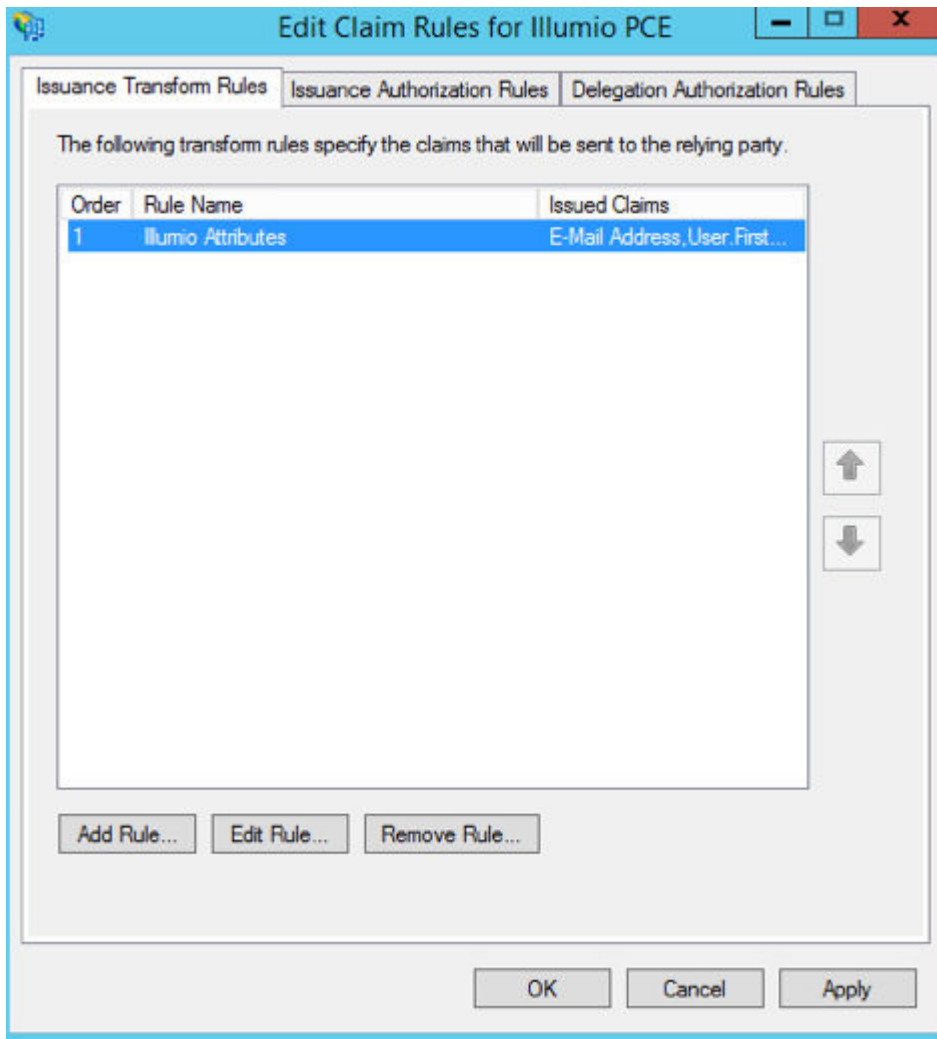
Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | User-Principal-Name | E-Mail Address |
| | Surname | User.LastName |
| | Given-Name | User.FirstName |
| * | | |

< Previous Finish Cancel

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**.

The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard". On the left, a "Steps" pane lists two steps: "Choose Rule Type" (marked with a green dot) and "Configure Claim Rule" (marked with a blue dot). The main area is titled "Select Rule Template" and contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a "Claim rule template:" label followed by a dropdown menu showing "Transform an Incoming Claim". Underneath is a "Claim rule template description:" label followed by a text box containing the following text: "Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of 'Purchasers' when there is an incoming group claim with a value of 'Admins'. Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help." At the bottom right of the dialog are three buttons: "< Previous", "Next >" (highlighted with a blue border), and "Cancel".

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 screenshot shows the 'Add Transform Claim Rule Wizard' window, specifically the 'Configure Rule' step. The window has a blue title bar with the text 'Add Transform Claim Rule Wizard' and a close button. On the left, there is a 'Steps' pane with two items: 'Choose Rule Type' (highlighted with a green dot) and 'Configure Claim Rule' (with a green dot). The main area contains a text box for 'Claim rule name' with the value 'Email to NameID Transform'. Below it, the 'Rule template' is set to 'Transform an Incoming Claim'. There are four dropdown menus: 'Incoming claim type' (E-Mail Address), 'Incoming name ID format' (Unspecified), 'Outgoing claim type' (Name ID), and 'Outgoing name ID format' (Email). Three radio buttons are present: 'Pass through all claim values' (selected), 'Replace an incoming claim value with a different outgoing claim value', and 'Replace incoming e-mail suffix claims with a new e-mail suffix'. The 'Replace an incoming claim value...' option has input fields for 'Incoming claim value' and 'Outgoing claim value' (with a 'Browse...' button). The 'Replace incoming e-mail suffix...' option has a 'New e-mail suffix' input field with an example 'fabrikam.com' below it. At the bottom right are three buttons: '< Previous', 'Finish', and 'Cancel'.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Email to NameID Transform

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

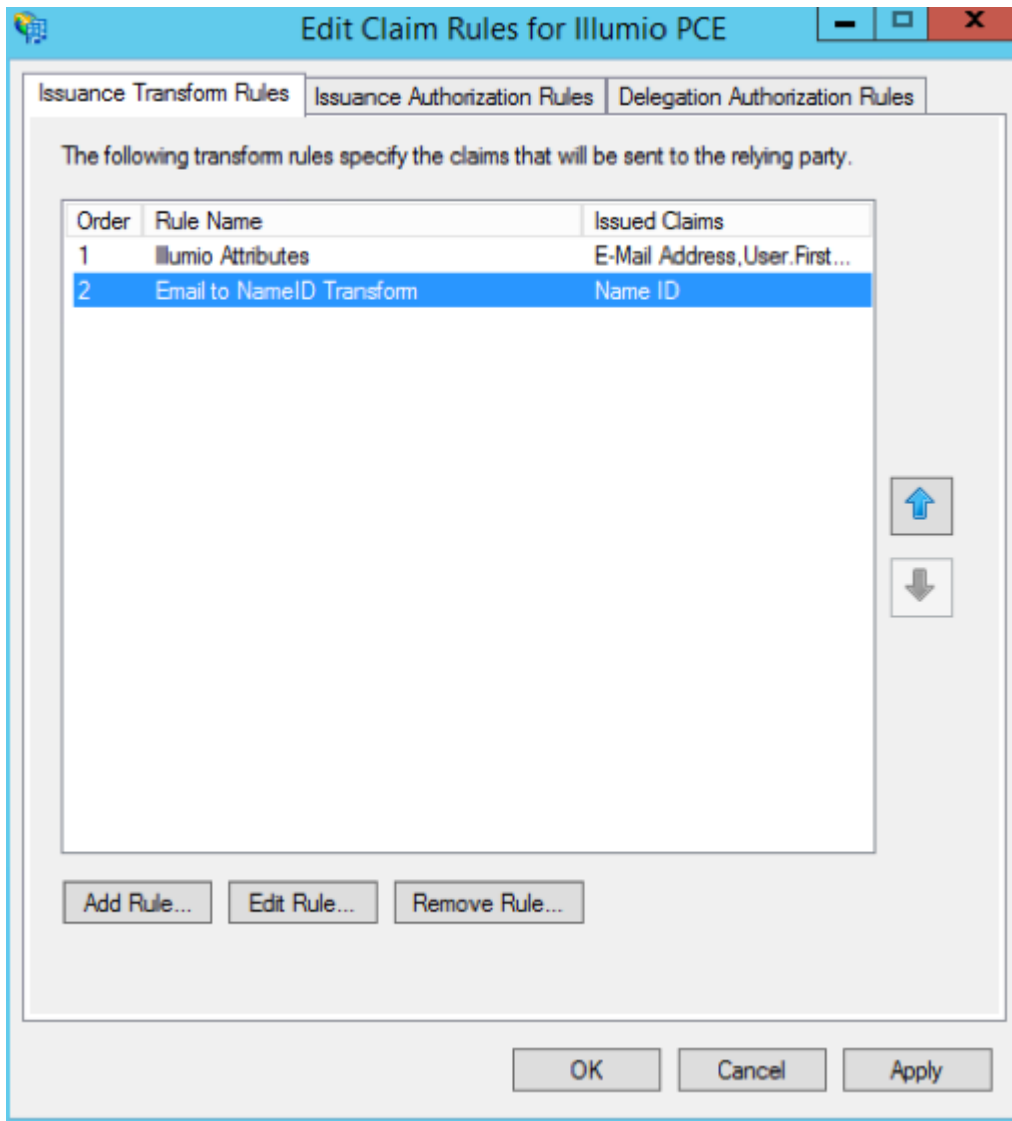
☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

< Previous Finish Cancel

The Edit Claim Rules window opens.

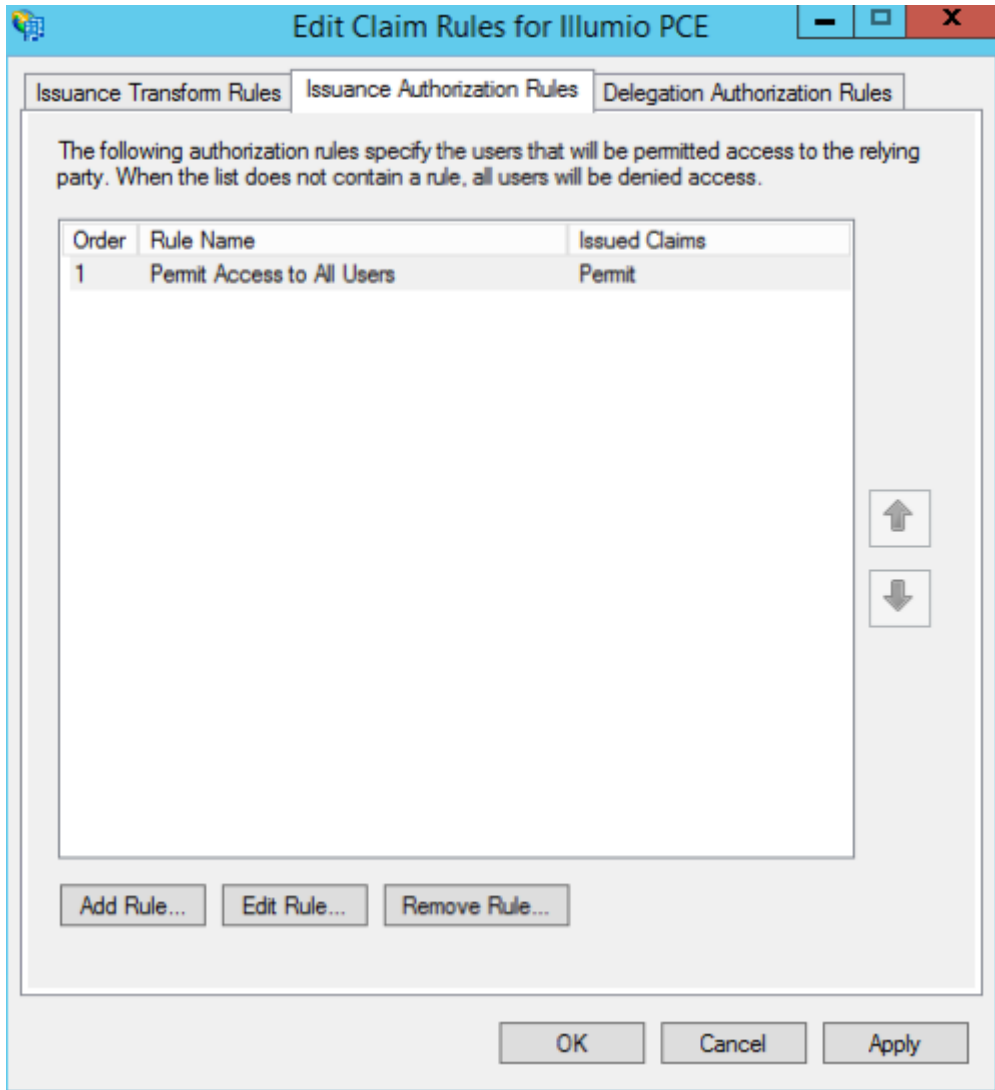


7. (Windows 2016 and Windows 2019) Skip to step 12.

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**.

The screenshot shows a Windows-style wizard window titled "Add Issuance Authorization Claim Rule Wizard". On the left, a "Steps" pane shows two steps: "Choose Rule Type" (active) and "Configure Claim Rule". The main area is titled "Select Rule Template" and contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a "Claim rule template:" label and a dropdown menu showing "Permit or Deny Users Based on an Incoming Claim". Underneath is a "Claim rule template description:" label and a text box containing the following text: "Using the Permit or Deny Users Based on an Incoming Claim rule template you can permit or deny users access to the relying party based on the type and value of an incoming claim. For example, you can use this rule template to create a rule that will permit only users that have a group claim with a value of 'Domain Admins'. If you want to permit all users to access the relying party, use the Permit All Users rule template. Users who are permitted to access the relying party from the federation service may still be denied service by the relying party." At the bottom right are three buttons: "< Previous", "Next >", and "Cancel".

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**.

The screenshot shows the 'Add Issuance Authorization Claim Rule Wizard' window, specifically the 'Configure Rule' step. The window has a blue title bar and a standard Windows interface. On the left, a 'Steps' pane shows two steps: 'Choose Rule Type' (highlighted with a green dot) and 'Configure Claim Rule' (also with a green dot). The main area contains the following fields and options:

- Claim rule name:** A text box containing 'AD FS Users'.
- Rule template:** A label indicating 'Authorize Users Based on an Incoming Claim'.
- Incoming claim type:** A dropdown menu currently set to 'Group SID'.
- Incoming claim value:** A text box containing 'ILDAD\ADFS Users' and a 'Browse...' button to its right.
- Access options:** Two radio buttons. The first, 'Permit access to users with this incoming claim', is selected. The second is 'Deny access to users with this incoming claim'.
- Navigation buttons:** At the bottom right, there are three buttons: '< Previous' (disabled), 'Finish' (active/highlighted), and 'Cancel'.

12. If you are using RBAC with groups, you need to create a Group Claim Rule. To add groups to AD FS claim rule configuration, click **Edit Rule**. Add the requirement for "LDAP Attribute: memberOf" by selecting the Outgoing Claim Type as "User.MemberOf." Click **OK**.

Edit Rule - Groups
X

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | Token-Groups - Unqualified Names ▼ | User.MemberOf ▼ |
| * | ▼ | ▼ |

View Rule Language...

OK
Cancel

Obtain ADFS SSO Information for the PCE

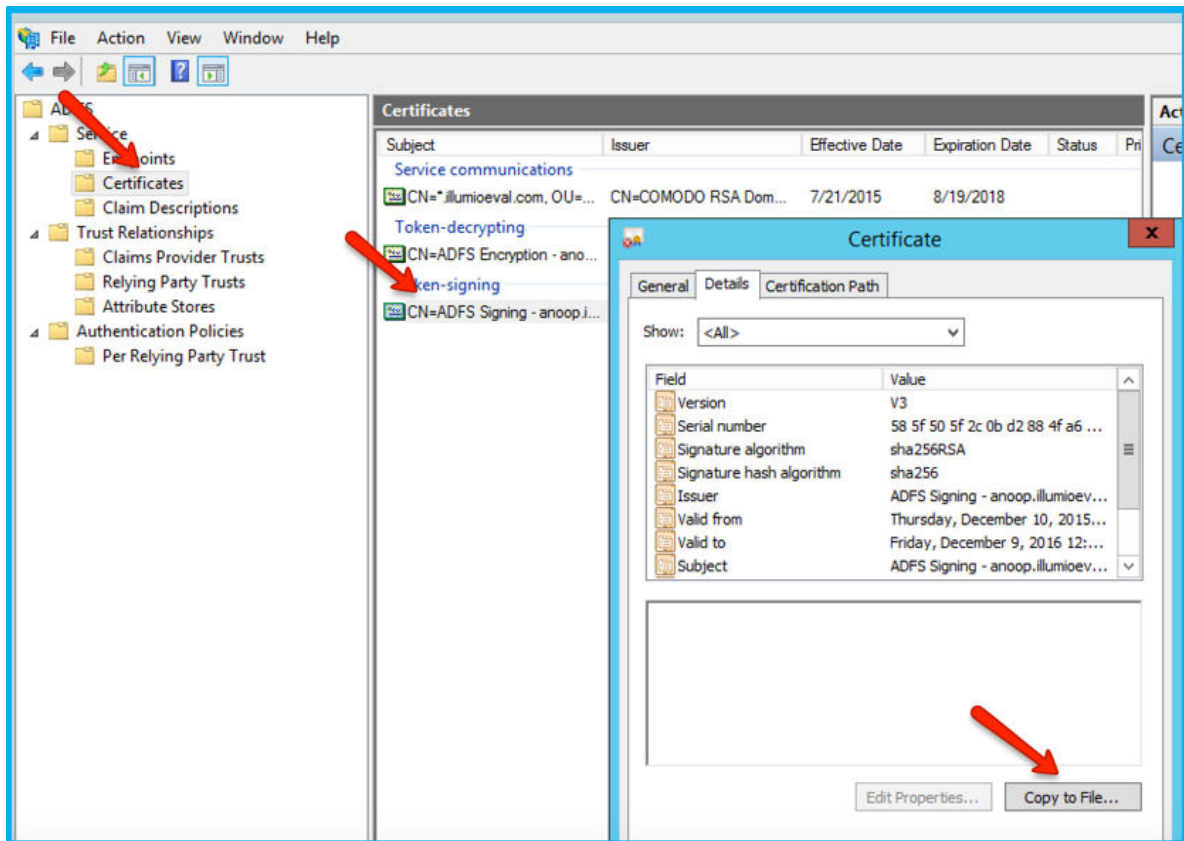
Before you can configure the PCE to use AD FS for SSO, obtain the following information from your AD FS configuration:

- 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://<myPCNameAndPort>/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 \[83\]](#).



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-authorization 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 authentication method and check the Force Re-authorization checkbox to force users to re-authenticate.

7. Click **Save**.
Your PCE is now configured to use AD FS for SSO authentication.

Azure AD Single Sign-on

This topic describes how to configure Azure Active Directory (AD) to provide SSO authentication to the Illumio PCE.

**TIP**

Because you'll configure settings in both the Illumio PCE Web Console and in Azure AD, have both applications open in adjacent browser tabs.

Prerequisites

To perform this configuration, you need the following:

- An Azure AD subscription. If you don't have a subscription, you can get a [free account](#).
- An Illumio single sign-on (SSO) enabled subscription.

STEP 1: Obtain URLs from the Illumio PCE Web Console

In this step you'll copy and preserve URLs from the Illumio PCE for use in Step2.

1. Log in to the PCE as a Global Organization Owner.

2. Go to **Access Management > Authentication**.
3. On the **SAML** tile, click **Configure**.
4. Copy and preserve the following URLs needed to complete the Azure configuration in a later step:

**TIP**

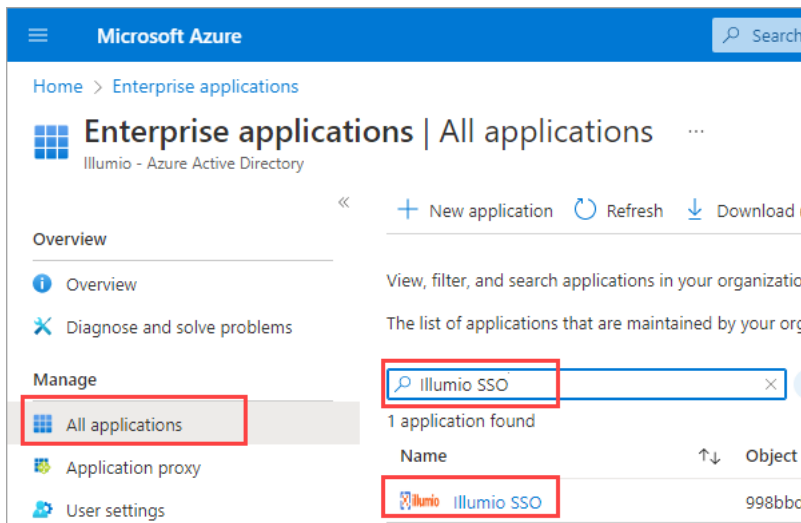
Make sure to replace the x's in the URLs below with the actual values from your implementation.

STEP 2: Configure SSO settings in Azure AD

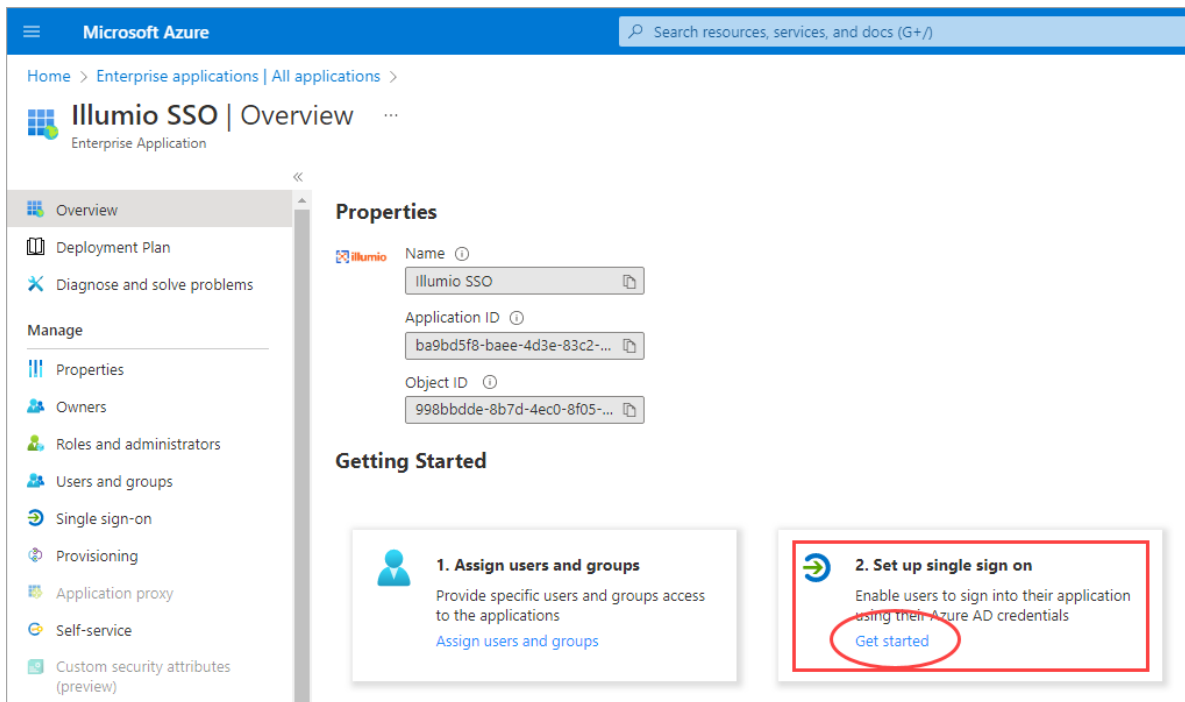
**NOTE**

Only an Azure Application Administrator can configure Azure AD.

1. In a different browser tab, log in to Azure AD as an Application Administrator.
2. Go to **Enterprise applications > All applications**.
3. Search for the **Illumio SSO** app and then click the app.



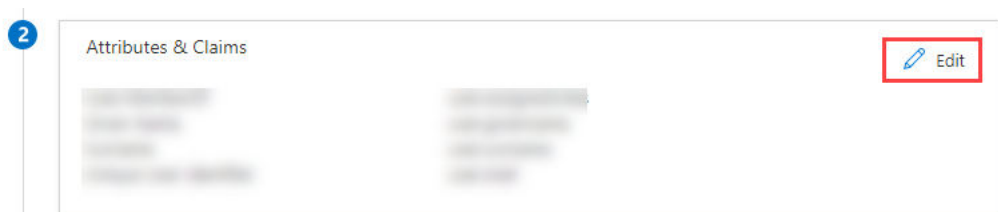
4. In the center of the page under **Getting Started**, click **Get started** on the **Set up single sign on** tile.



5. If prompted to select a single sign-on method, click **SAML**.
6. Configure Basic SAML:
 - a. On the **Set up Single-Sign On with SAML** page **Basic SAML Configuration** tile, click **Edit**.



- b. On the **Basic SAML Configuration** panel that opens, populate the fields with the values you copied and preserved.
 - In the **Identifier (Entity ID)** field, paste the **Issuer URL** you copied from the Illumio PCE.
 - In the **Reply URL (Assertion Consumer Service URL)** field, click **Add reply URL** and then paste the **Assertion Source URL** you copied from the Illumio PCE. **Note:** Your Reply URL must have a subdomain such as www, wd2, wd3, wd3-impl, wd5, wd5-impl. For example, *http://www.myIllumio.com* will work but *http://myIllumio.com* won't.
 - c. Click **Save** and close the **Basic SAML Configuration** panel.
7. Click **Edit** on the **Attributes & Claims** tile.



8. Under **Required claim**, update the **Claim name**:

Attributes & Claims ...

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

| Claim name | Type | Value |
|----------------------------------|------|-----------------------------|
| Unique User Identifier (Name ID) | SAML | user.mail [nameid-forma...] |

Additional claims

| Claim name | Type | Value |
|------------|------|-------|
| | | |
| | | |
| | | |

Advanced settings

- Click the three dots.
 - On the **Manage claim** page, click in the **Source attribute** field and select **user.mail** from the dropdown.
 - Click **Save**.
9. Back on the **Attributes & Claims** page, delete **all** of the existing claims in the **Additional claims** section by clicking the three dots for each one and then clicking **Delete**.

Additional claims

| Claim name | Type | Value |
|---|------|------------------------|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd... | SAML | user.mail |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | SAML | user.givenname |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | SAML | user.userprincipalname |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | SAML | user.surname |

- 10 Click **Add new claim** and add three new claims:

Attributes & Claims ...

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

| Claim name | Type | Value |
|----------------------------------|------|-----------------------------|
| Unique User Identifier (Name ID) | SAML | user.mail [nameid-forma...] |

Additional claims

| Claim name | Type | Value |
|---------------|------|--------------------|
| Given Name | SAML | user.givenname |
| Surname | SAML | user.surname |
| User.MemberOf | SAML | user.assignedroles |

Given Name

Surname

User.MemberOf

STEP 3: Obtain SAML certificate and URLs from Azure AD

In this step, you'll download a certificate and copy two URLs that you'll later paste into the Illumio PCE SAML setup.

- On the **SAML Certificates** tile, click **Download** for the **Certificate (Base64)** certificate and save the certificate to your computer.

SAML Certificates

Token signing certificate Edit

| | |
|-----------------------------|---|
| Status | Active |
| Thumbprint | A1... |
| Expiration | 10/5/2025, 2:20:54 PM |
| Notification Email | haider.jarral@illumio.com |
| App Federation Metadata Url | https://login.microsoftonline.com/68b76eeb-dd53... |
| Certificate (Base64) | Download |
| Certificate (Raw) | Download |
| Federation Metadata XML | Download |

Verification certificates (optional) (Preview) Edit

| | |
|----------|----|
| Required | No |
| Active | 0 |
| Expired | 0 |

- On the **Set up Illumio SSO** tile, copy and preserve the following URLs that you'll later paste into the Illumio PCE SAML setup.

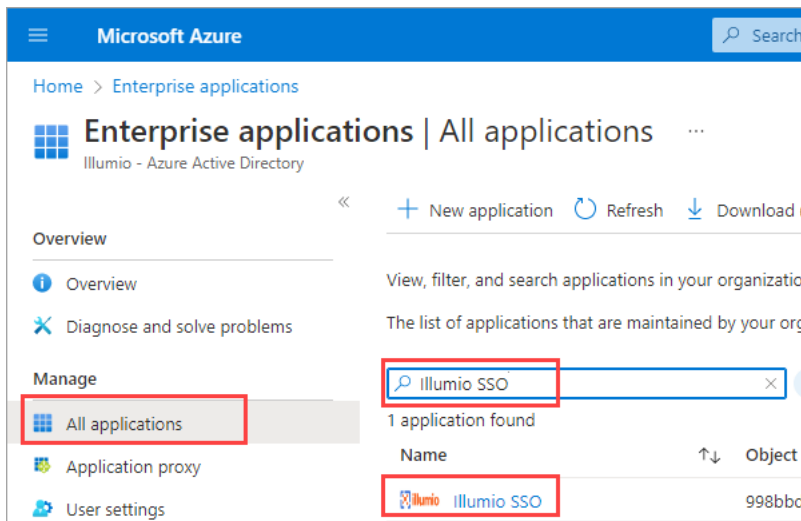
Set up Illumio SSO

You'll need to configure the application to link with Azure AD.

| | |
|---------------------|---|
| Login URL | https://login.microsoftonline.com/68b76eeb-dd53.. |
| Azure AD Identifier | https://sts.windows.net/68b76eeb-dd53-4531-955.. |
| Logout URL | https://login.microsoftonline.com/68b76eeb-dd53.. |

STEP 3: Create and assign a test user in Azure AD

- In Azure, go to **Azure Active Directory**.
- In the left pane, click **Users** and then **All users**.
- Click **+ New user**.
- In the **User** properties:
 - In the **Name** field, enter a name (Example.Name).
 - In the **User name** field, enter the user name in the form of an email address (Example.Name@example.com).
 - Select **Show password**, and then make a note of the value that appears in the **Password** box.
- Click **Create**.
- Go to **Home > Azure Active Directory**.
- Under **Overview > Manage**, click **Enterprise applications > All applications**.
- Search for and click the **Illumio SSO** app.



9. In the left pane under **Manage**, click **Users and Groups**.
10. Click **+ Add user/group**.
- .
11. On the **Add Assignment** page, click **Users and groups**.
12. In the **Users and groups** panel that opens, click the user you created in a previous step (Example.Name).
13. Click **Select**.
14. On the **Add Assignment** page under **Select a role**, click one of the roles you created in a previous step.
15. Click **Assign**.

STEP 4: Configure SAML SSO settings in the Illumio PCE

In this procedure you'll paste the following information that you copied and preserved from Azure:

- Certificate (Base64)
- Azure Login URL
- Logout URL

1. In the Illumio PCE Web Console, go to **Access Management > Authentication**.
2. On the **SAML** tile, click **Configure**.
3. Click **Edit**.
4. In the **Information from Identity Destination** section, enter the following information that you obtained from Azure AD:
 - **SAML Identity Destination Certificate**: Open the certificate that you downloaded and then copy and paste the contents.
 - **Remote Login URL**: Paste the Login URL you copied from Azure AD.
 - **Logout Landing URL**: Paste the Logout URL you copied from Azure AD.
5. In the **Information for Identity Destination** section:
 - a. Choose an authentication method:
 - **Unspecified** uses the IdP default authentication mechanism.
 - **Password Protected Transport** requires the user to log in with a password in a protected session.
 - b. If you want to require users to re-enter login credentials to access Illumio (even if the session is still valid), select **Force Re-authentication**. This allows users to log in to the PCE using login credentials different from their default computer login credentials.

6. Click **Save**.

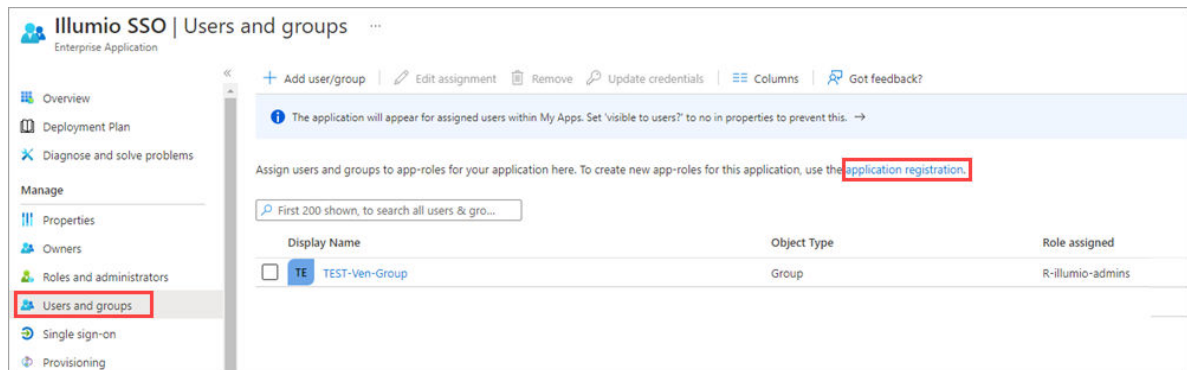
STEP 5: Create App Roles in Azure AD

In this step you'll create app roles in Azure AD that you'll map to roles in the Illumio PCE Web Console.

For reference in this step, here's a list of the Global Roles available in the PCE Web Console:

- Global Organization Owner
- Global Administrator
- Global Viewer
- Globally Policy Object Provisioner

1. In Azure AD, go to **Users and Groups** and then click **application registration**.



2. Create the roles you want by clicking **+ Create app role** and entering the required information for each role:

- **Display name:** For example, enter one of the Global Roles that appear in the PCE Web Console.
- **Value:** This must match the name you'll enter in the **Add External Groups** dialog box.
- **Description:** The description will appear as help text in the app assignment and consent experiences.

3. Click **Apply** for each role that you create.

4. Delete the default app role **mslam_access**.

Note: You first need to disable the default app role before you can delete it.

- Click **mslam_access** to open the **Edit app role** panel.
- Deselect **Do you want to enable the app role?**
- Click **Apply**. The side panel closes.
- Click **mslam_access** again to open the **Edit app role** panel again.
- Click **Delete**.

When you're done creating roles in Azure AD, the **App roles** section should look similar to this:

| App roles | | | | |
|--|----------------------------------|----------------------|-------|-----------|
| App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets as permissions during authorization. | | | | |
| How do I assign App roles | | | | |
| Display name | Description | Allowed member types | Value | ID |
| Global Organization O... | Global Organization Owner | Users/Groups | GOO | 309c156d |
| Global Administrator | Global Administrator | Users/Groups | GA | f6473e65- |
| Global Viewer | Global Viewer | Users/Groups | GV | cb677852 |
| Global Policy Object P... | Global Policy Object Provisioner | Users/Groups | GPOP | d07b17b1 |

STEP 6: Assign users and groups to app roles in Azure AD

In this step, you'll assign users and groups to the app roles you created.

1. In Azure AD, go to **Users and groups**.
2. Select the Illumio SSO app.
3. Click **Remove** to remove the current app assignments.
4. Click **Yes** to confirm removal.
5. Click **Add user/group**.
6. On the **Add Assignment** page, assign desired role(s) to users or groups:
 - a. Under **User and groups**, click **None Selected**.
 - b. In the **Users and groups** panel that opens, search for your desired user/group, click to select it, and then click **Select** at the bottom of the panel.
 - c. Back on the **Add Assignment** page, under **Select a role***, click **None Selected**.
 - d. In the **Select a role** panel that opens, find and click the role you want to assign, and then click **Select** at the bottom of the panel.
 - e. Back on the **Add Assignment** page, click **Assign** at the bottom of the page.
 - f. Repeat these sub-steps for each user and/or to which you want to assign app roles.

STEP 7: Add External Groups and assign roles in the PCE Web Console

In this step, you'll add external groups in the PCE Web Console and assign them the relevant global or scoped roles in Illumio RBAC.



TIP

Alternatively, you can add individual users by going to the **External Users** tab and following the onscreen prompts.

1. On the PCE Web Console, go to **Access Management > External Groups**.
2. Click **Add**.
3. In the **Add External Group** dialog box:
 - Enter a **Name**.
 - Enter an **External Group**.

**IMPORTANT**

This must match the **Value** that you specified for the app role.

- Click **Add**.

4. Repeat for additional groups.

Add External Group

*

Name

Global Organization Owner

*

External Group

GOO

Cancel

Add

Access Management – External Groups

Global Roles

Scopes

External Groups

External Users

+ Add

– Remove

Select a principal

Customize columns ▾

☐

↕ Name

Global Administrator

Global Organization Owner

Global Policy Object Provisioner

Global Viewer

GA

GOO

GPOP

GV

5. Click to open a group you created in the above step.
6. Click **Add Role > Add Global Role** or **Add Scoped Role**.
7. In the **Access Wizard**, select the appropriate **Role** and then click **Grant Access**.
8. Repeat for additional groups.

Access Management – Access Wizard

Scope ⊕ All

Name ml-test

Email or Username ml-test-group

1 Select Roles

- ☒ **Global Viewer**
Global read-only access to all resources
- ☐ **Global Policy Object Provisioner**
Provision Services, IP Lists, Label Groups, and Security Settings. Read-only access to all other resources.
- ☐ **Global Administrator**
Manage all resources and Security Settings. Cannot manage users and roles.
- ☐ **Global Organization Owner**
Manage all resources, users and Security Settings.

Summary Scope ⊕ All

Principals ml-test

Role Please select a role

– Cancel + Grant Access

STEP 8: Turn on SAML authentication in the PCE Web Console

1. In the PCE Web Console, go to **Access Management > Authentication**.
2. On the SAML tile, click **Configure**.
3. On the SAML page, click **Turn On** and then click **Confirm**.

SAML

Local (In use) **SAML** LDAP

Off SAML authentication is not active. Click Turn On to enable SAML.

Turn On

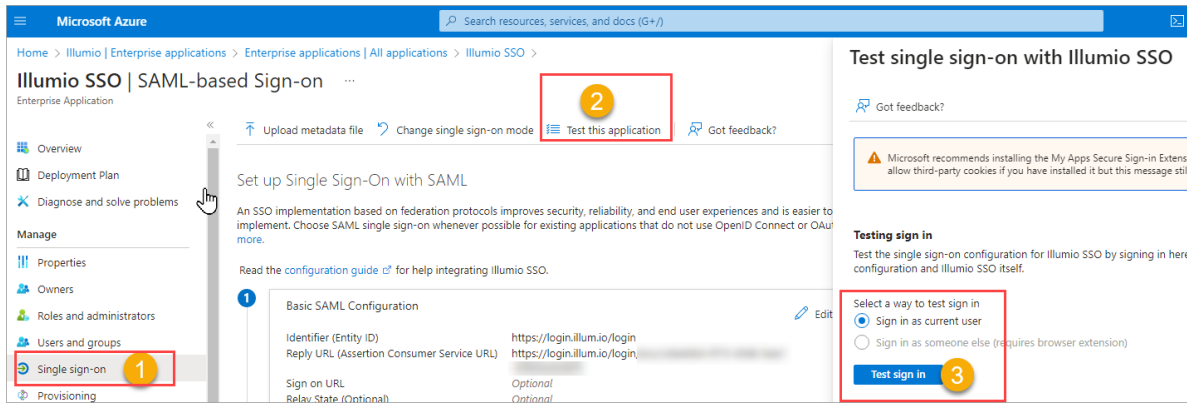
Edit

SSO method SAML

STEP 9: Test SSO

Perform this procedure to test the SSO authentication you configured in the previous steps.

1. In Azure AD, go to **Single sign-on**.
2. Click **Test this application**.
3. In the panel that opens, select a way to sign in and then click **Test sign in**.



4. If the test is successful, the PCE will log you in to the **Welcome to Illumio** screen.

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.
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 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 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.

okta Dashboard Directory Applications Security Reports Settings

 **Illumio ASP** Active  View Log

General Sign On Import People Groups

App Settings Cancel

Application label
This label displays under the app on your home page

Assertion Consumer URL
Please, enter your Assertion Consumer URL

Issuer
Please, enter your Issuer

Application visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile App

Save

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.
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.

USERS APPS ACTIVITY SETTINGS

← Illumio ASP

MORE ACTIONS ▾ SAVE

Info **Configuration** Parameters Rules SSO Access Users

Application Details

Issuer

Assertion Consumer URL

Logout URL

Enter PCE
'Information for
Identity Provider'
here

This information may be found on the SSO Config page of the PCE web console (located under the User menu).

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 **Access Management > Authentication**.
2. On the **SAML** tile, click **Configure**.
3. On the SAML page, click **Edit**.
4. In the Information From Identity Provider section, 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. Click **Turn On** to enable SAML, and then click **Confirm**.
10. Log in to your Ping Identity account.
- .
11. Select the Applications tab and add the Illumio app.
12. 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.

The screenshot shows the Ping Identity Admin console interface. At the top, there's a navigation bar with 'Dashboard', 'Applications', 'Users', 'Setup', and 'Account'. The 'Applications' tab is selected. Below the navigation bar, there's a sub-header 'My Applications' with a breadcrumb trail 'Applications / My Applications'. The main content area is titled 'My Applications' and contains a table listing applications. The table has columns: Application Name, Type, Status, and Enabled. The first application listed is 'Illumio ASP' with Type 'SAML' and Status 'Incomplete'. Below the table, there's a section '1. Configure your connection' with the instruction 'Assign the attribute values for single sign-on (SSO) to the application.' The configuration form includes fields for 'ACS URL' (https://\$(Enter Assertion Consumer U...), 'Entity ID' (\$(Enter Issuer from the SSO Config p...), 'Single Logout Endpoint' (https://\$(Enter Logout URL from the S...), and 'Single Logout Response Endpoint' (https://\$(Enter Logout URL from the S...). There are also buttons for 'Upload Metadata', 'Select File', 'Or use URL', 'Choose File', and 'No file chosen'. At the bottom, there's a 'PingOne dock URL' section with a default URL and a 'Use Custom URL' option. The 'NEXT: Attribute Mapping' button is visible at the bottom right.

| Application Name | Type | Status | Enabled |
|------------------|------|------------|------------------------------|
| Illumio ASP | SAML | Incomplete | Yes <input type="checkbox"/> |

1. Configure your connection

Assign the attribute values for single sign-on (SSO) to the application.

Upload Metadata [Or use URL](#)

ACS URL *

Replace the parameter(s) '\$(Enter Assertion Consumer URL from the SSO Config page of the PCE web console)' above with your configuration information.

Entity ID *

Replace the parameter(s) '\$(Enter Issuer from the SSO Config page of the PCE web console)' above with your configuration information.

Target Resource

Single Logout Endpoint *

Single Logout Response Endpoint *

Verification Certificate No file chosen

Force Re-authentication ☐

PingOne dock URL

Default PingOne dock URL <https://sso.connect.pingidentity.com/sso/sp/intsso?saasid=27af9ebf-f019-44f8-9b31-c6dc51dae78c&idpid=58d7f05a-ad70-4da6-812f-5706dc3a27a7>

☐ Use Custom URL

NEXT: Attribute Mapping

13. Click **Continue to Next Step**.

14. 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:oa-sis:names:tc:SAML:1.1:nameid-format:emailAddress`.

Advanced Attribute Options

Advanced Attribute Options for SAML_SUBJECT

Advanced Attribute Options

NameIDFormat ⓘ

Name ID Format to send to SP:

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName

urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos

urn:oasis:names:tc:SAML:2.0:nameid-format:entity

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

Attribute Mapping

You can build an attribute mapping using the following syntax:

An example of a possible SAML_SUBJECT attribute mapping:

firstName + "." + lastName + "

SAML_SUBJECT = SAML_SUBJECT

| IDP Attribute Name or Literal Value | As Literal | Function |
|-------------------------------------|-------------------------------------|----------|
| 1 SAML_SUBJECT | <input type="checkbox"/> As Literal | |

Close

Save

15. Click **Save.**

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