Illumio Core®

v22.2.30

Common Criteria Guide

February 2023

11500-000-22.2.30

Legal Notices

Product Version

PCE Version: 22.2.30

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

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

Resources

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

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

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

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

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

Contact Information

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

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

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

Contents

Chapter 1

Common Criteria Introduction

This section introduces you to the Common Criteria information for Illumio Core 22.2.30.

Illumio Core Common Criteria Overview

This guide provides the information an administrator would need to install and configure the Illumio Core 22.2.30 in compliance with the Common Criteria evaluated configuration. Follow this guide in its entirety to ensure that the settings of each parameter match the specific configuration that was evaluated and certified by the Common Criteria certification.

Product and Version

The Illumio Policy Compute Engine (PCE) and Illumio Virtual Enforcement Node (VEN) are components of theIllumio Core version 22.2.30.

Intended Audience

This document is intended for use by administrators who are responsible for installing, configuring, and operating enterprise infrastructure for their organization. To use this guide you must have knowledge of your organization's network infrastructure, applicable policies, and have administrative access to configure operational environment.

About Common Criteria

The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for certification of the security of computer systems, networks, and application software. The certification provides independent confirmation that the claims about the security attributes of the evaluated product were independently verified in the evaluated configuration operated in the specific environment. The certification assumes specific evaluated configuration

and does not validate any security claims when the product is used outside of this specific evaluated configuration.

Related Documents

Identifer	Edition	Title
Security Target	Version 0.6	Illumio Core v22.2.30 Security Target
PCE User Guides	22.2.1	PCE Installation and Upgrade Guide v.22.2.1 contains information that is also applicable to the evaluation version, Illumio Core 22.2.30. PCE Administration Guide v.22.2.1 contains information that is also applicable to the evaluation version, Illumio Core 22.2.30.
VEN User Guide	22.2.0	VEN Administration Guide v.22.2.0 contains information that is also applicable to the evaluation version, Illumio Core 22.2.30.
Security Policy	Version 1.1	Red Hat Enterprise Linux OpenSSL Cryptographic Module v5.0 FIPS 140-2 Non-proprietary Security Policy

Evaluated Configuration

The Target of Evaluation (TOE), Illumio Core 22.2.30, is an enterprise policy management product.

Target of Evaluation (TOE)

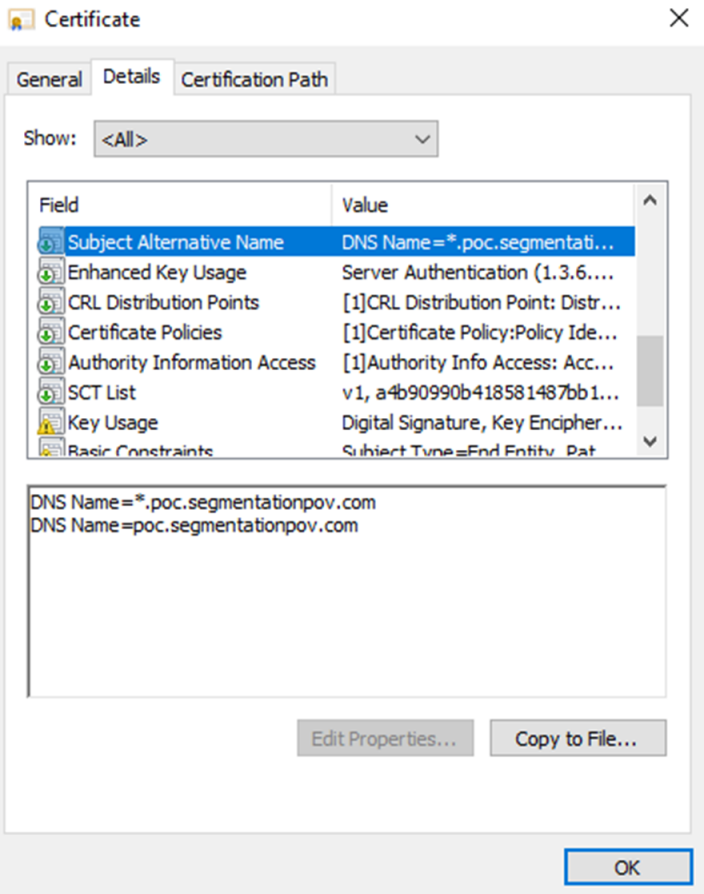
The TOE's primary purpose is to manage communications within, and across, tiers of applications by defining access control policy. The TOE is a distributed software application that consists of the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN). The VEN is an Access Control product which consumes policies created by the PCE. Together, these components form a distributed software platform designed to continuously protect communications within and, across, tiers of applications and hosts. The PCE enables administrators to create access control policies to secure and to implement granular segmentation of hosts and applications within enterprise network, effectively reducing the attack surface and securing the network. The PCE can be configured to operate in number of different modes depending upon the deployment scenario including Single-Node Cluster (SNC), Multi-Node Cluster (MNC) and Super-Cluster mode.

In the evaluated configuration, the PCE is a software application running on Red Hat Enterprise Linux 8.2 (and later versions) with FIPS mode enabled and deployed as a single node cluster

(SNC) with both the Core and Data components residing on the same node. Virtualization, clustering, and high-availability configurations were not evaluated.

In the evaluated configuration PCE is authenticated with an X.509v3 certificate signed by a trusted CA, where the certificate contains a unique fully qualified domain name (FQDN) identifier in the Subject Alternative Name (SAN) extension. Additionally, that FQDN must resolve to the PCE's host system using DNS. See the following example configuration:

Figure: FQDN Identifier in SAN



The evaluated configuration of Illumio Core 22.2.30 is integrated with an Authentication Server (via SAML), a remote Audit Server (syslog), and an NTP server.

Assumptions and Operational Environment

There are specific conditions that are assumed to exist in the TOE's Operational Environment. The following table lists assumptions about the Operational Environment as specified by the Protection Profile:

Table 2: Operational Environment Assumptions

Assumption Name	Assumption Definition
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.

Table 3: Personnel Assumptions

Assumption Name	Assumption Definition
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

The following table identifies the organizational security policies applicable to the TOE as specified by the Protection Profile:

Table 4: Organizational Security Policies

Policy Name	Policy Definition
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Chapter 2

PCE Installation

This section describes how to install the PCE for Common Criteria.

FIPS Compliance for PCE

This section describes the operational requirements for compliance with Federal Information Processing Standard (FIPS) 140-2 for the PCE and VEN.

FIPS Prerequisites

RHEL 8.2 running in FIPS mode and satisfying the Security Policy as stated in Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module version rhel8.20200305.1.

Enable PCE FIPS Compliance

1. After installing RHEL8.x, follow the required steps in Section 9.1, Crypto Officer Guidance, Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module NIST Security Policy.
2. Reboot the system.
3. After the system starts, check that FIPS mode is enabled:
   ```
   $ fips-mode-setup --check
   FIPS mode is enabled.
   ```
4. Install the Illumio PCE RPM.
5. During PCE installation, provide the PCE with SSL certificates that have a minimum RSA key size of 2048.
6. After PCE installation, disable PCE metrics collection. Add the following to `runtime_env.yml` on all nodes in the cluster and restart the PCEs: `metrics_collection_enabled: false`

> NOTE:
> This step is required because metrics collection currently uses non FIPS compliant components.

After completing the PCE setup, the PCE is FIPS compliant.

PCE Installation Prerequisites

This topic describes the prerequisites for PCE Installation for Common Criteria. If PCE installation is performed without Internet access, then all required RPM packages must be present on server prior to installation.

Recommended Hardware

Use these guidelines and requirements to estimate host system capacity based on typical usage patterns.

The exact requirements vary based on a large number of factors, including, but not limited to:

- Number of managed workloads
- Number of unmanaged workloads and other labeled objects, such as virtual services
- Policy complexity, which includes the following factors:
  - Number of rules in your rulesets
  - Number of labels, IP lists, and other objects in your rules
  - Number of IP ranges in your IP lists
  - Number of workloads affected by your rules
- Frequency at which your policies change
- Frequency at which workloads are added or deleted, or workload context changes, such as, change of IP address
- Volume of traffic flows per second reported to the PCE from all VENs

  See the “Maximum Flow Capacity” table for information about maximum flow capacity of the PCE.
- Total number of unique flows reported to the PCE from all VENs

Physical Hardware

The PCE can be installed on physical hardware, using these recommendations:

MNC Type + Workloads/VENs	Cores/Clock Speed	RAM per Node	Storage Device Size and IOPS	
			Core Nodes	Data Nodes
SNC • 250 VENs[1] • 2500 workloads	• 3 cores[2] • Intel® Xeon(R) CPU E5-2695 v4 at 2.10GHz or equivalent	16GB	A single node including both core and data: • 1 x 50GB[3] • 100 IOPS per device[4]	N/A

Footnotes:

[1] Number of VENs/workloads is the sum of both the number of managed VENs and the number of unmanaged workloads.

[2] CPUs:

- The recommended number of cores is based only on physical cores from allocated CPUs, irrespective of hyper-threading.

[3] Additional disk notes:

- Storage requirements for network traffic data can increase rapidly as the amount of network traffic increases.
- Network File Systems (NFS) is not supported for Illumio directories specified in runtime; for example, data_dir, persistent_data_dir, ephemeral_data_dir.

[4] Input/output operations per second (IOPS) are based on 8K random write operations. IOPS specified for an average of 300 flow summaries (80% unique `src_ip, dest_ip, dest_port, proto`) per workload every 10 minutes. Different traffic profiles might require higher IOPS.

Required Software Packages and Shared Libraries

Supported browsers:

- Chrome (latest version)
- Firefox (latest version)
- Microsoft Edge (latest version)

Supported operating systems:

- Red Hat Enterprise Linux (RHEL) 8.2

For FIPS compliance, the following additional libraries are required:

- libcrypto
- libssl

Operational Environment Servers

Audit Server recommended versions:

- syslog-ng-3.1.8 or later version
- rsyslog-8.24.0 or later version

Preparing the Operating System

Before installing the PCE, be sure your underlying systems are sufficient to successfully install and run the PCE. Check all the following system requirements.

PCE IP Address

Illumio recommends a statically-assigned IP address. By default, the PCE automatically uses the first available private IP address on the node. The PCE does not automatically bind to a public IP address.

When you use a public IP address or the node has multiple interfaces, you need to configure the PCE with the interface you want to use. To do so, set `internal_service_ip` in the configuration file `runtime_env.yml`. For example:

```
internal_service_ip: 10.2.8.89
```

To configure networking, edit:

`/etc/sysconfig/network-scripts/ifcfg-eth<X>`

Where `<X>` is the interface number. For example `eth0`:

```
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=#.#.#.#
PREFIX=#
GATEWAY=#.#.#.#
DNS1=#.#.#.#
DNS2=#.#.#.#
```

```
DOMAIN="mydomain.com [localdomain 1] [localdomain 2 etc...]"
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="eth0"
```

Restart Network Service:

```
$ systemctl stop network
$ systemctl start network
```

DNS Requirements

Your Domain Name System (DNS) must resolve the PCE's fully qualified domain name (FQDN). The FQDN must be resolvable on all managed workloads, on all nodes in the PCE cluster, and for all users of the PCE web console and REST API.

If you are using DNS-level load balancing, the PCE FQDN should resolve to the IP addresses of the core nodes. If you are using a server load balancer, the PCE FQDN should resolve to the VIPs of the server load balancer.

SMTP Requirements

An SMTP relay is required to send user invitations and “forgot password” email replies from the PCE.

The SMTP configuration parameter during PCE installation is `smtp_relay_address`. Allowable values are either an IP address with its SMTP port (default 587) or a resolvable FQDN with the SMTP port.

Configure Timezones

```
$ timedatectl list-timezones
$ timedatectl set-timezone [select location]  date
```

X.509 Certificate

An X.509 server certificate must be installed on each PCE node during installation. When any client (the VEN) opens a TLS session to the PCE (for example, pairing a workload, accessing the PCE web console, retrieving updated policy), the PCE presents the server certificate to secure the communication. The server certificate is uploaded as part of a certificate bundle that contains

the server certificate and the chain of CA certificates (Intermediate or Root) to establish the chain of trust back to a Root CA.

> CAUTION:
> The client must be able to validate the chain of trust back to the Root CA for this certificate; otherwise, the TLS handshake fails. You might need to add all the certificates in the chain of trust to the keychain of the client.

The certificate package for the Illumio PCE must meet the following basic criteria:

- The file must contain PEM-encoded certificates.
- The subject value and issuer of the certificate must start with a leading slash character (/).
- As a best practice, duplicate the subject in the Subject Alternative Name (`subjectAltName`).
- The certificate's signature algorithm must be SHA256WithRSA Encryption.
- The certificate's signature algorithm must *not* be RSASSA-PSS.
- The file must contain the server certificate and the entire certificate chain necessary to establish the chain of trust back to a Root CA.
    a. The package must include all of the CA certificates (Intermediate and/or Root) needed to establish the chain of trust back to a Root CA.
        - If the certificate is generated by a Private CA, all certificates in the chain of trust back to the Root CA must be included. This includes the Root CA certificate and any applicable Intermediate CA certificates.
        - If the certificate is generated by a major Public CA (such as, VeriSign, GeoTrust, Entrust, or Thawte), any Intermediate CA certificates needed to establish the chain of trust back to the Public Root CA must be included.
    b. Pay careful attention to the order of the certificates in the bundle. The server certificate must be first. If you have an Apache-style bundle generated by a standard certificate request process, you need to open the file in a text editor and reverse the order of the certificates. Apache always expects the root certificate to come first, then any intermediates in order (from the root down), and the server certificate is last. The PCE uses nginx, which expects the opposite order. For additional details, see the Nginx documentation.

        The certificate bundle should look something like this:

```
-----BEGIN CERTIFICATE-----
<server cert goes here>
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
<intermediate CA cert goes here>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<root CA cert goes here>
-----END CERTIFICATE-----
```

- All certificates in the bundle must be valid for the current date, which depends on the system time being set correctly.
- A trusted root store must be available for OpenSSL to validate certificates.
- The certificate must match the PCE FQDN, which can be an exact match (for example, pce.mycompany.com) or a wildcard match (for example, *. mycompany.com)

The certificate must support both Server and Client authentication. Client authentication is used between nodes in an MNC. Run the following command and verify `TLS Web Server Authentication, TLS Web Client Authentication` appears within the `X509v3 Extended Key Usage` section.

```
$ openssl x509 -text -noout -in pce.mycompany.com.bundle.crt
...
X509v3 Extended Key Usage:
         TLS Web Server Authentication, TLS Web Client Authentication
...
```

RSASSA-PSS Signature Algorithm Not Supported

The certificate signature algorithm RSASSA-PSS, which is based on PKCS 1 version 2.1, is not supported, because it cannot be validated. This limitation is a widely known problem with this signature algorithm.

The PCE certificate requires the SHA256WithRSA encryption signature.

> CAUTION:
> If you use Microsoft Certificate Authority (CA) to sign PCE certificates, make sure to use the SHA256WithRSA encryption. PKCS#1 version 2.1 is enabled by default on Microsoft CAs and produces the unsupported RSASSA-PSS signature algorithm.

Private Keys

The private key that matches the X.509 certificate must be installed on each PCE node during installation, and the following guidelines must be met:

- The private key must be PEM-encoded.
- The file must not be encoded.
- The file must not be password protected.

Trusted Public CA Store

A trusted root public Certificate Authority (CA) store must be available for OpenSSL to validate certificates.

If you rely on a certificate signed by a public CA, be sure to install the latest public root CA certificates `ca-certificates` package.

```
# yum install ca-certificates
```

When your certificate is signed by a private CA or the signing CAs are already included in each node's trusted root CA store, the `ca-certificates` package is not required.

Private Certificates

Add Private Certificates

To add a certificate signed by a private CA, the recommended procedure is to place your private `.pem` file(s) into:

`/etc/pki/ca-trust/source/anchors/`

This can consist of individual `.pem` files, or a single `.pem` file with concatenated certificates (root and intermediate). Then, run following command which will re-write the new bundle file:

`/bin/update-ca-trust extract`

Verify Private CA Certificates in the Bundle File

To verify whether your private files were included in `/etc/ssl/certs/ca-bundle.crt`, first determine the certificate subject:

`openssl x509 -in cert.pem -subject -noout`

The `ca-bundle.crt` file typically contains a comment with the CN or OU of the subject name. Run the following command to search for the file:

`grep <subjectCN|subjectOU> /etc/ssl/certs/ca-bundle.crt`

Compare the corresponding PEM contents found in `/etc/ssl/certs/ca-bundle.crt` with the file found in `/etc/pki/ca-trust/source/anchors`.

Installation Example

```
root% cp cert.pem /etc/pki/ca-trust/source/anchors/
root% update-ca-trust extract
```

Additional Information on Verification

To verify the certificates contained in `/etc/ssl/certs/ca-bundle.crt` use a command-line tool and enumerate all the certificates as follows:

```
openssl crl2pkcs7 -nocrl -certfile ca-bundle.crt | openssl pkcs7 -print_certs -outform pem
```

This will output all the certificates as follows:

```
subject=/C=US…
-----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----
```

To isolate a particular certificate set, use the following commands:

```
openssl crl2pkcs7 -nocrl -certfile ca-bundle.crt | openssl pkcs7 -print_certs -outform pem | sed -n "/subject=.*orgname/,/END CERTIFICATE/p"
```

Then, compare the PEM contents against the expected PEM source file.

Configure Certificates

Copy certificates to directories with the following commands:

```
cp tls.toe.good.key /etc/pki/tls/private/
cp tls.toe.good.crt /etc/pki/tls/certs/
cp bundle.good.crt /etc/pki/tls/certs/
cp bundle.good.crt /etc/pki/ca-trust/source/anchors/
```

Configure permissions on the certificates with the following commands:

```
chmod 755 /etc/pki/tls/certs
chmod 755 /etc/pki/tls/private
chmod 444 /etc/pki/ca-trust/source/anchors/
chmod 755 /etc/pki/tls/certs/tls.toe.good.crt
chmod 755 /etc/pki/tls/certs/bundle.good.crt
```

```
chmod 400 /etc/pki/tls/private/tls.toe.good.key
chmod 755 /etc/pki/ca-trust/source/anchors/bundle.good.crt
```

Enable dynamic CA trust with the following commands:

```
update-ca-trust force-enable
update-ca-trust extract
update-ca-trust check
```

Verify that the certificate is valid with the following commands:

```
openssl verify /etc/pki/tls/certs/bundle.good.crt
bundle.good.crt: OK will be returned
```

NTP

Set up a Network Time Protocol (NTP) client for time synchronization. It is recommended that you use chrony, although ntpd can also be used. On RHEL8, chrony is the default.

To install and configure the NTP client, use the procedure in the documentation for the client on your operating system.

After you finish installing the PCE, you can use the following command to verify that the NTP client is installed, running, and synchronized to a time source:

```
# sudo -u ilo-pce illumio-pce-env check
```

> NOTE:
> For more information about the ilo-pce system account, see PCE System Account.

NFTables

For the initial installation, you should disable nftables.

If nftables is enabled, you must configure it to allow inbound HTTPS connections to the PCE core nodes and service ports.

```
# sudo systemctl stop nftables
# sudo systemctl stop firewalld
# sudo systemctl status nftables
```

Process and File Limits and Kernel Parameters

This section describes how to set the process and file limits and OS kernel parameters that are required for PCE operation. The approach is different depending on whether you are configuring an SNC or MNC, and which operating system you are using, so look for the appropriate sections in the discussion that follows.

Three categories of settings must be configured:

- Process and file limits
- OS kernel parameters
- Kernel module tuning

> WARNING:The parameter modifications described in this section are strict requirements and must be followed to ensure proper functionality of the Illumio Core. If an Illumio support case is opened, and analysis finds that these parameters are not met, you will be directed to meet these requirements before any additional troubleshooting can be performed.

Keep the following in mind when managing these parameters:

- Root access is needed for many of these procedures. Befor you start, be sure you have login credentials for a user account with root permissions.
- When your settings are already greater than these, you do not need to reduce them to these values.
- Make sure you do not have any automated processes that change these values.

SNC Process and File Limits and OS Kernel Parameters

The following table shows the required process and file limits for single-node clusters.

Parameter	Value
`core (hard)`	`0`
`core (soft)`	`0`
`nofile (hard)`[1]	`65535`
`nofile (soft)`[1]	`65535`
`nproc (hard)`	`65535`
`nproc (soft)`	`65535`

[1] When you run additional processes on the PCE, such as monitoring or other operations processes, you might need to increase the value of `nofile`.

The following table shows the required OS kernel parameter values for single-node clusters.

Parameter	Value
fs.file-max	2000000
net.core.somaxconn	16384
kernel.shmmax	60000000
vm.overcommit_memory	1
nf_conntrack_max	1048576

The following table shows the required SNC kernel module tuning.

Parameter	Value
nf_conntrack hashsize	262144

Configure PCE as a SNC (Single Node Cluster)

The following section describes how to install and configure the PCE in the evaluated configuration as a Single Node Cluster (SNC).

Download the Software

1. Download the software from the Illumio Support portal (login required).
2. Copy the Illumio PCE UI RPM file to the `/tmp` folder. The following steps refer to this file as `illumio_ui_rpm`.
3. Copy the Illumio PCE software RPM file to the `/tmp` folder. The following steps refer to this file as `illumio_pce_rpm`.

Install the PCE as an SNC

As root, run the following command to install the PCE software:

```
$ rpm -ivh illumio-pce-22.2.30x.x86_64.rpm
```

Set operating shell for console:

```
$ usermod -s /sbin/nologin ilo-pce
```

Reboot the OS:

```
$ reboot
```

Values for Your PCE SNC

Runtime Parameter	Value to Use
$ service_discovery_fqdn: x.x.x.x	# IP address of PCE (this node)
$ cluster_public_ips/cluster_fqdn:	# Auto-generated
$ node_type: snc0	# Use snc0

Runtime Parameter	Value to Use
`$ datacenter [dc1]:`	# Leave as default (dc1)
`$ front_end_https_port: 8443`	# 8443 is default port
`$ web_service_private_key:`	# SNC domain key; for example, `/etc/pki/tls/private/your_snc_domain.key`
`$ web_service_certificate:`	# Certificate bundle; for example, `/etc/pki/tls/certs/good_cert_bundle.crt`
`$ trusted_ca_bundle:`	# Certificate bundle; for example, `/etc/pki/tls/certs/good_cert_bundle.crt`
`$ email_address:`	# `noreply@your-snc-domain`
`$ email_display_name: noreply`	# noreply should be the default
`$ service_discovery_encryption_key:`	# Leave blank or just press enter
`$ smtp_relay_address: 127.0.0.1:587`	# Use the default 127.0.0.1:587
`$ reporting_datastore: data_dir:`	# Leave default and press enter
`$ reporting_datastore: data_dir:`	# Leave default and press enter
`$ syslog_event_export_format: json`	# Use json default
`$ insecure_tls_weak_ciphers_enabled [true]:`	# Enter false
`$ standby_management_database: data_dir:`	# Leave default and press enter
`$ Save to configuration /etc/illumio-pce/runtime_env.yml [Y/n]?`	# Enter Y

After completing the prompts listed above in the PCE setup wizard, additional runtime environment parameters must be configured by editing the PCE runtime_env.yml file. Set each of the following parameters with specified value below:

Runtime Parameter	Value to Use
`common_criteria_events_enabled`	`true` Enables TLS events messages.
`min_tls_version`	`tls1_2` Sets the minimum TLS version.
`max_failed_login_attempts`	`5` The number of failed authentication attempts to allow before locking out the user.
`account_lockout_duration_minutes`	`15` (Minutes) How long to deny further authentication attempts after the maximum number of attempts has been used.

By setting the minimum TLS version configuration to “tls1_2” all communications to and from the PCE are protected by TLS v1.2. This includes communications between the PCE and the VEN, PCE and web console and PCE and remote syslog servers. When new security policies are created or updated on the PCE, the policies are transmitted to the VEN’s over a trusted channel using TLS v1.2.

Runtime Parameter	Value to Use
`server_load_balancer`	Enable HTST
`strict_transport_security_max_age_in_seconds`	`31536000` Sets the time in seconds.

If the IP address of the PCE is a public IP address, then configure an internal_service_ip and add it to the same file. (Not required if private IP is assigned to the NIC of the PCE node.)

Runtime Parameter	Value to Use
`internal_service_ip`	Enter the node public IP address.

To add a customized login warning banner, configure the runtime parameter `login_banner`.

Runtime Parameter	Value to Use
`login_banner`	Sets up a warning banner that appears when logging in to the PCE. Enter any desired string. For example: `login_banner: You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.`

Save the changes and exit `/etc/illumio-pce/runtime_env.yml`.

Description of Runtime Parameters

The following table lists the required `runtime_env.yml` file parameters for each PCE software node you deploy. All required parameters have no default values. All paths configured in this file must be absolute.

Required Parameter	Description	Exposure
`enabled_preview_features`	Includes sub-parameters to enable identified preview features	
`install_`	The full path to the location of the PCE binaries and scripts	Public

Required Parameter	Description	Exposure
`root`	The software does not write to any files in this directory, so it can be read-only. For example: `install_root: /opt/illumio-pce`	Stable
`runtime_data_root`	The full path to the location where the PCE writes runtime data This data can be deleted on reboot if necessary. This directory should have 700 permissions, but all of its files will have 600 permissions. This directory must be owned by the user that runs the PCE software. For example: `runtime_data_root: /var/lib/illumio-pce/runtime`	Public Stable
`persistent_data_root`	The full path to the location where the PCE writes persistent data This data must persist across reboots for the software to work properly. This directory should have 700 permissions, but all of its files will have 600 permissions. This directory must be owned by the user that runs the PCE software. For example: `persistent_data_root: /var/lib/illumio-pce/data`	Public Stable
`ephemeral_data_root`	The full path to the location where the PCE writes temporary files These files must not be deleted while the software is running, but they should be deleted on reboot. This directory should have 700 permissions, but all of its files will have 600 permissions. For example: `ephemeral_data_root: /var/lib/illumio-pce/tmp`	Public Stable
`log_dir`	The directory where the PCE software writes some text file logs (although most PCE services log to syslog) `logrotate` (or similar) should be used to manage these files.	Public Stable

Required Para-meter	Description	Exposure
	For example: `log_dir: /var/log/illumio-pce`	
`pce_fqdn`	The fully qualified domain name (FQDN) of the PCE cluster For example: `pce_fqdn: pce.mycompany.com`	Public Stable
`cluster_public_ips: cluster_fqdn`	The FQDN of your entire cluster NOTE: If you change the value of `cluster_public_ips`, wait for the paired VENs to receive the new IP addresses and begin heartbeating to them.	Public Stable
`web_service_certificate`	Full path to the X.509 public certificate used by this node for TLS See Preparing the Operating System for more information on the contents of the certificate files. For example: `web_service_certificate: /etc/pki/tls/certs/my_cert.crt`	Public Stable
`web_service_private_key`	The RSA private key for TLS that matches the public certificate The private key must be PEM encoded in PKCS#12 format without a password. For example: `web_service_private_key: /var/lib/illumio-pce/cert/rsa_private_key.key` Alternatively, you can specify a script (using `$` notation) that outputs the private key. This approach is useful when you need to store the key in a hardware security module (HSM) or other key store. For example:	Public Stable

Required Para-meter	Description	Exposure

	`web_service_private_key: $ /var/lib/illumio-pce/cert/get_rsa_private_key.sh`
	
	This script can be located anywhere on the file system as long as it is executable by the `ilo-pce user`.
	
	Example script output:
	
	`$ /local/scripts/get_rsa_private_key.sh`
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIE...`
	`many lines trimmed here`
	`-----END RSA PRIVATE KEY-----`	

`email_address`	Email sender address used by the PCE when sending emails from the system; for example, to send invitations and notifications For example: `email_address: noreply@exampleblocked_traffic.com`	Public Stable
`service_discovery_fqdn`	The FQDN or IP address of the first core node	Public Experimental
`service_discovery_encryption_key`	The key used to encrypt Service Discovery node traffic. This value must be the same for all PCE nodes. This key must be 16 bytes that are base64 encoded. For example: `service_discovery_encryption_key: 05TlqH1W0cKcK797DV73yg==`	Public Stable
`node_type`	The type of the PCE software node Allowable values: • `core`: core node • `data0`: data node	Public Stable

Required Parameter	Description	Exposure
	• `data1`: data node • `snc0`: single-node cluster • `citus_coordinator`: coordinator node for multi-node traffic database • `citus_worker`: worker node for multi-node traffic database For example: `node_type: core`	
`login_banner`	A custom message on the PCE login screen typically used to display legal notice or company policy when a user logs in	Public Stable
`cluster_type`	PCE cluster type. Required on every node in a multi-node cluster (MNC). Not required on a single-node cluster (SNC). One of the following: • `4node_v0`: 2x2 PCE cluster • `4node_v0_small`: 2x2 PCE cluster with fewer compute and memory resources • `6node_v0`: 4x2 PCE cluster • `4node_dx`: 2x2 PCE cluster with multi-node traffic database • `6node_dx`: 4x2 PCE cluster with multi-node traffic database **Default:** `4node_v0`	Public Stable

Optional Runtime Parameters

The following table lists common optional `runtime_env.yml` file parameters for each PCE software node you deploy. Your Illumio Professional Services representative might provide additional parameters to configure certain advanced functions.

Optional Parameter	Description	Exposure
`ven_repo_url`	The base URL used to fetch the VENs and to enable workload pairing with the PCE Required format: `https://host[:port]/repo_dir` You can use alternate ports by specifying the port at the end of host-	Public Stable

Optional Parameter	Description	Exposure
	name. `repo_dir` cannot be empty. For example: `https://repo.example.com:8443/onpremgCBURz8Y4zkGk1u7N9ialjPGlZ` **Default:** None	

`ven_repo_ips`	IP addresses of the VEN repository
	These IP addresses are injected into iptables to allow outbound access to the `yum/apt get` repositories without having to write an explicit PCE policy.
	Setting this parameter allows outbound access on ports 80 and 443 to these IP addresses. You can specify both single IP addresses or IP addresses with CIDR notation.
	When you do not specify this parameter, the VEN won't be allowed to access the repository containing VEN software packages.
	For example:
	`ven_repo_ips:`
	`- 1.2.3.4`
	`- 5.6.7.8/8`
	Default: None
		Public
		Stable

`internal_service_ip`	The IP address of the PCE Set this value manually only when you want to use a public IP address or the PCE node has multiple interfaces. For example: `internal_service_ip: 10.2.8.89` **Default:** The first available private IP address on the node	Public Stable
`front_end_https_port`	The front end HTTPS port When the cluster is front-ended by a server load balancer, such as	Public Stable

Optional Parameter	Description	Exposure
	F5, it must be configured to forward this port. For example: `front_end_https_port: 8443` **Default:** TCP 8443 if not set by `front_end_management_https_port` or `front_end_https_port`	
`front_end_event_service_port`	The front end Event Service port When the cluster is front-ended by a server load balancer, such as F5, it must be configured to forward this port. The idle connection timeout on the server load balancer might need to be configured to maintain the connections on this port. Please contact your Illumio Professional Services representative for information on configuring your server load balancer. For example: `front_end_event_service_port: 8444` **Default:** `8444`	Public Stable
`front_end_management_https_port`	The port for PCE web console and REST API This key separates different kinds of communication. See also `front_end_https_port`. **Default:** TCP 8443 if not set by `front_end_management_https_port` or `front_end_https_port`	Public Stable
`syslog_event_export_format`	The export format (CEF, LEEF, or JSON) for VEN flow summaries and Organization events. When you specify CEF or LEEF format, you will continue getting traffic flows and Organization events in JSON format. For example: `syslog_event_export_format: cef` **Default:** `json`	Public Stable

Optional Parameter	Description	Exposure
`min_tls_version`	The minimum Transport Layer Security (TLS) version used to secure VEN-to-PCE communications, the PCE's web server for the PCE web console, and the REST API. Use the default setting, 1.2. Set it as follows: `min_tls_version: tls1_2` **Default:** `tls1_2`	Public Stable
`insecure_tls_weak_ciphers_enabled`	Specifies whether to allow the use of weaker TLS ciphers, such as cipher block chaining (CBC) ciphers. Stronger ciphers are recommended. For most deployments, Illumio recommends that you change the value to `false` so that you use strong ciphers. Illumio recommends you keep the default value (`true`) for this setting only when using clients or operating systems that can only negotiate TLS using CBC ciphers. This parameter exists to support backward compatibility for such older versions of TLS. For example: `insecure_tls_weak_ciphers_enabled: false` **Default:** `true`	Public Stable

`trusted_ca_bundle`	The path to the trusted root certificate bundle.
	The PCE uses this parameter to validate that the certificates are trusted and indicates the path to the trusted root certificate bundle file.
	For example:
	`trusted_ca_bundle:`
	`/etc/ssl/certs/ca-bundle.crt`
	Default: `/etc/ssl/certs/ca-bundle.crt`
		Public
		Stable

`email_dis-`	Email display name to be used when sending email from the sys-	Public

Optional Parameter	Description	Exposure
`play_name`	tem. For example, to send invitations and notifications from the PCE. For example: `email_display_name:'noreply'` **Default:** `noreply`	Stable
`smtp_relay_address`	SMTP relay information used by the PCE to send email; for example, to send invitations and notifications. The PCE assumes that an SMTP Relay runs on localhost and listens on `127.0.0.1/587`. When this isn't the case, you must specify the configuration on the *core nodes*. Use *one* of the following formats: • `ip_address (e.g. 127.0.0.1)` • `ip_address:port (e.g. 127.0.0.1:587)` For example: `smtp_relay_address: 127.0.0.1:587` **Default:** `127.0.0.1:587`	Public Stable

`export_flow_summaries_to_fluentd`	The types of traffic flow summaries to export to Fluentd.
	Values: `accepted` (allowed), `potentially_blocked`, `blocked`
	For example:
	`export_flow_summaries_to_fluentd:`
	`- accepted`
	`- potentially_blocked`
	`- blocked`
		Public Experimental

`export_flow_summaries_to_syslog`	Enables traffic flow summaries to syslog. Values: `accepted` (allowed), `potentially_blocked`, `blocked` For example:	Public Experimental

Optional Parameter	Description	Exposure

	`export_flow_summaries_to_syslog:`
	`  - accepted`
	`  - potentially_blocked`
	`  - blocked`
	
	To export blocked traffic summaries, include only the flow summary type when specifying the parameter; for example:
	
	`export_flow_summaries_to_syslog:`
	`  - blocked`	

`internal_syslog_fqdn_enabled`	Specifies whether to use the PCE's fully-qualified domain name (FQDN) or the hostname in syslog messages. The FQDN can be more helpful if the short hostnames are difficult to distinguish. Values: `true` (the `host=` field uses the FQDN), `false` (default) For example: `internal_syslog_fqdn_enabled: true`	Public Experimental

Start and Initialize the PCE

Starting and initializing the PCE are the final steps in installing it. .

Start the PCE

As the PCE runtime user, perform the following steps:

1. On *all nodes*, start the PCE at runlevel 1:

   ```
   # sudo -u ilo-pce illumio-pce-ctl start --runlevel 1
   ```

   Troubleshooting: If this command fails, verify that you have set `service_discovery_encryption_key` to the same value in `runtime_env.yml` on all PCE nodes.

   Wait while all the nodes process the start command, which can take up to 10 minutes. When a node has finished, its status is `RUNNING`.

2. On *all nodes*, verify that they started:

```
# sudo -u ilo-pce illumio-pce-ctl status
```

Expected output:

```
Checking Illumio Runtime            RUNNING 0.38s
```

If any nodes do not start after 10 minutes, check the following issues:

- Network connectivity between nodes and iptables is configured correctly.
- The certificates must be configured correctly.
- The system locale must be UTF-8.
- The runtime environment is configured correctly.

Initialize the PCE

As the *PCE runtime user*, perform the following steps:

1. On *any node*, initialize the PCE database:

   ```
   # sudo -u ilo-pce illumio-pce-db-management setup
   ```

2. On the *data0 node*, bring the system up to runlevel 5:

   ```
   # sudo -u ilo-pce illumio-pce-ctl set-runlevel 5
   ```

3. On *any core node*, check the status of the cluster:

   ```
   # sudo -u ilo-pce illumio-pce-ctl cluster-status
   ```

   Make sure the cluster status is `RUNNING` before proceeding to the next step.

4. On *any core node*, create the initial PCE user and organization name:

   ```
   # sudo -u ilo-pce illumio-pce-db-management create-domain --user-name user-email-address --full-name user-full-name --org-name organization-name
   ```

   You are prompted for a password. The password must conform to these restrictions: at least 8 characters, no more than 64 characters, at least 1 upper case character, 1 lower

case character and 1 number. The recommended minimum length for Common Criteria deployments is 16 characters.

For example:

```
# sudo -u ilo-pce illumio-pce-db-management create-domain --user-name
myuser@mycompany.com --full-name
'Joe User' --org-name 'ACME Inc.'

Reading /var/illumio-pce-data/runtime_env.yml.
INSTALL_ROOT=/var/illumio-pce
RENV=production (defaulted because not set in runtime_env.yml)
Please enter a password with at least 8 characters with one uppercase, one
lowercase and
one number.

Enter Password:
Re-enter Password:
------------------------------------------------------------
Running cd /var/illumio-pce/illumio/webservices/people && RAILS_
ENV=production bundle exec rails
runner script/create_org_owner
--output-file /tmp/illumio/org.yml --user-name myuser@mycompany.com --create-
org
--org-name 'ACME Inc.'
Completed in 5.471846432 sec. Exit Code = 0
------------------------------------------------------------
Running cd /var/illumio-pce/illumio/webservices/agent && RAILS_ENV=production
bundle
exec rails runner script/create_org_defaults
--input-file /tmp/Illumio/org.yml
Completed in 5.609754678 sec. Exit Code = 0
------------------------------------------------------------
Running cd /var/illumio-pce/illumio/webservices/login && RAILS_ENV=production
ILO_********************bundle exec rails runner
script/setup_initial_config --org-data /tmp/Illumio/org.yml
--user-name myuser@mycompany.com
--full-name 'Joe User'
domain_name=mycompany.com
```

```
Completed in 5.303522871 sec. Exit Code = 0
Done.
```

5. Check to be sure the expected session limits for `nofile` and `nproc` meet the minimum requirements for the PCE.

   Use the following command:

   ```
   cat /proc/$(pgrep -f config_listener.rb)/limits | grep -e open -e processes
   ```

   If the limits are too low, correct the issue.

6. Point a web browser to the PCE FQDN and log in using the account you just created. You should see the PCE web console.

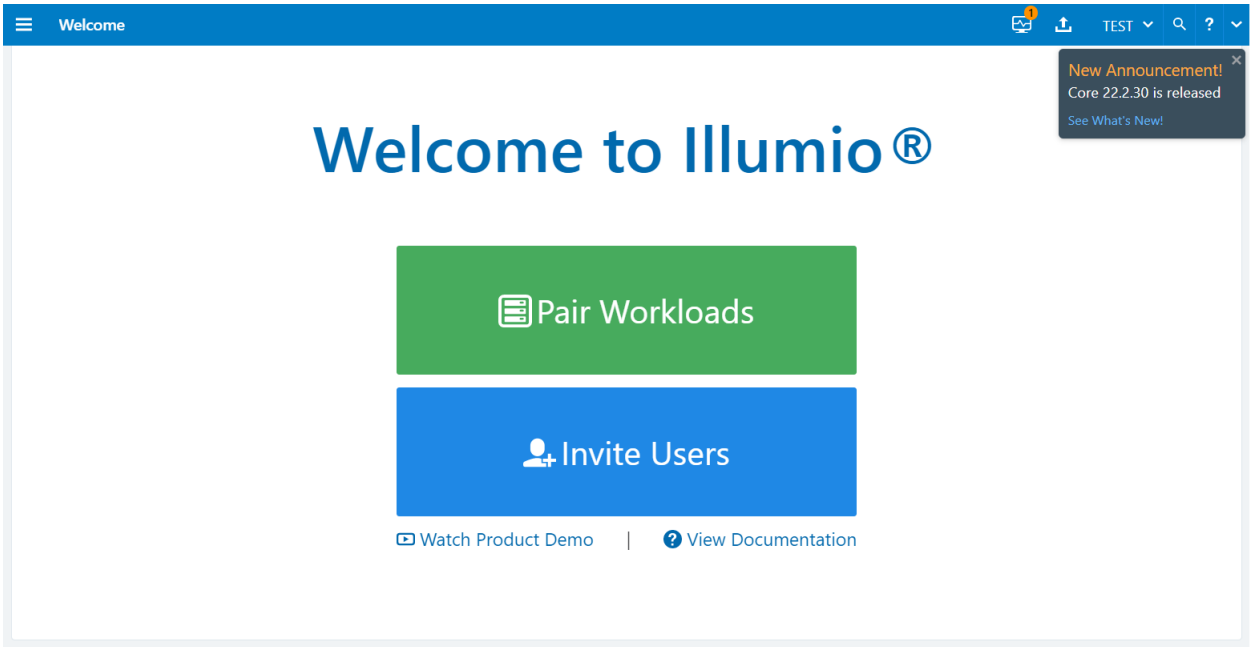
How to Access Your System

When logging into the PCE web console for the first time, do so using the credentials created during the setup process. This first user account is granted the "organization owner" role, so this user can invite other users to the organization and grant user permissions.

Log In to PCE Web Console

After an organization has been created during the PCE initialization, you can log in to the PCE web console by using a supported web browser.

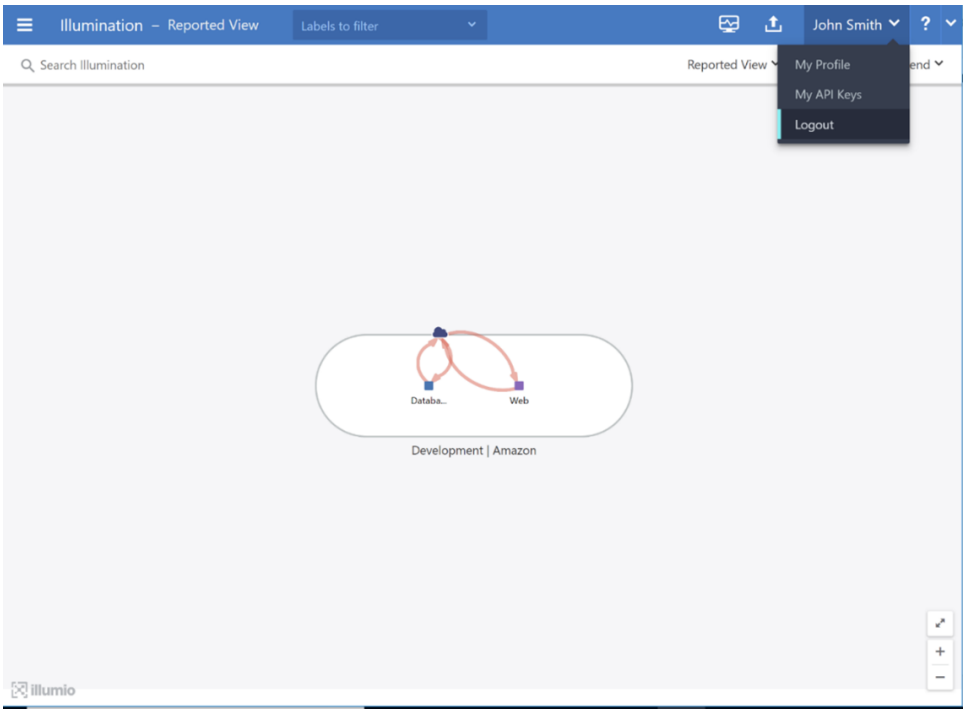
Figure: Web Console Login Screen



Log Out

To log out, click on the user name visible at the top right of the web console window. A drop down menu will appear below the account name. Click “Logout.”

Figure: Web Console Logout



Once the user is logged out, they are brought back to the web console login screen.

Chapter 3

Common Criteria Configuration

This chapter describes how to configure the PCE for Common Criteria.

Syslog Forwarding

The PCE ships with a pre-installed internal (namely, Local) syslog service which is configured and operational by default regardless of network connectivity. For the evaluated configuration, a remote audit server must also be configured so that all PCE audit logs are forwarded to a remote audit server.

RFC 5424 Message Format Required

Ensure that your remote syslog destination is configured to use the message format defined by RFC 5424, The Syslog Protocol , with the exception.

For a complete listing of the supported PCE audit record types see Appendix A.

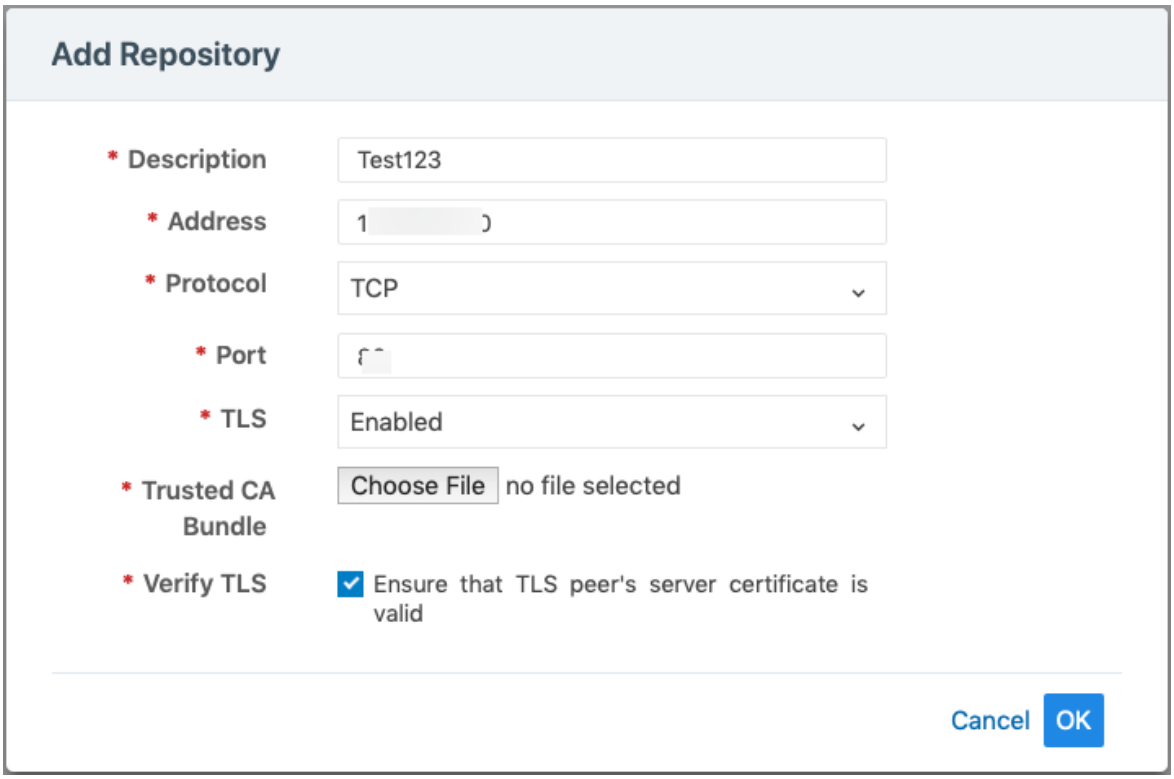
Forward Events to External Syslog Server

The PCE has an internal syslog repository, “Local” where all the events get stored. You can control and configure the relaying of syslog messages from the PCE to multiple external syslog servers.

To configure forwarding to an external syslog server:

1. From the PCE web console menu, choose **Settings** > **Event Settings**.
2. Click **Add**.

   The Event Settings - Add Event Forwarding page opens.
3. Click **Add Repository**.



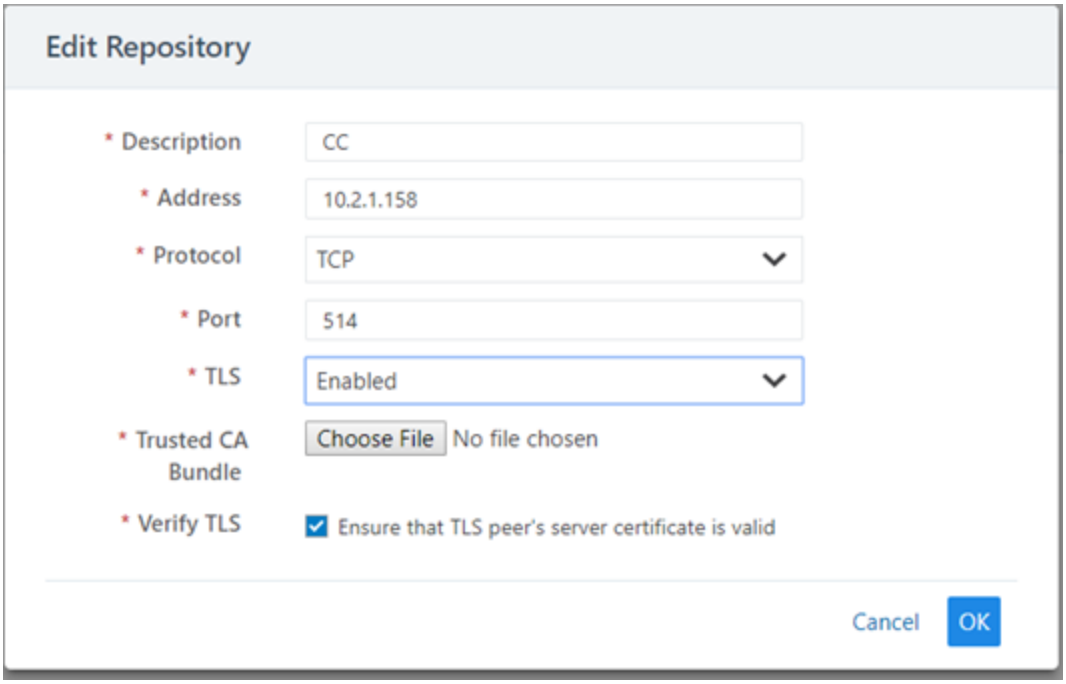
4. In the Add Repository dialog:
   - *Description*: Enter name of the syslog server.
   - *Address*: Enter the IP address for the syslog server.
   - *Protocol*: Select TCP or UDP. If you select UDP, you only need to enter the port number and click **OK** to save the configuration.
   - *Port*: Enter port number for the syslog server.
   - *TLS*: Select Disabled or Enabled. If you select Enabled, click “Choose File” and upload your organization's “Trusted CA Bundle” file from the location it is stored on.

     The Trusted CA Bundle contains all the certificates that the PCE (internal syslog service) needs to trust the external syslog server. If you are using a self-signed certificate, that certificate is uploaded. If you are using an internal CA, the certificate of the internal CA must be uploaded as the “Trusted CA Bundle”.
   - *Verify TLS*: Select the check-box to ensure that the TLS peer’s server certificate is valid.
5. Click **OK** to save the event forwarding configuration.

> NOTE:
> You cannot delete the “Local” server.

A repository that has been created with TLS “disabled” can be edited to support TLS by clicking on the TLS drop down menu and selecting “Enabled”. Once “Enabled” has been selected, the two related options “Trusted CA Bundle” and “Verify TLS” will appear (See screen shot below):

Figure: Trusted Bundle and Verify TLS



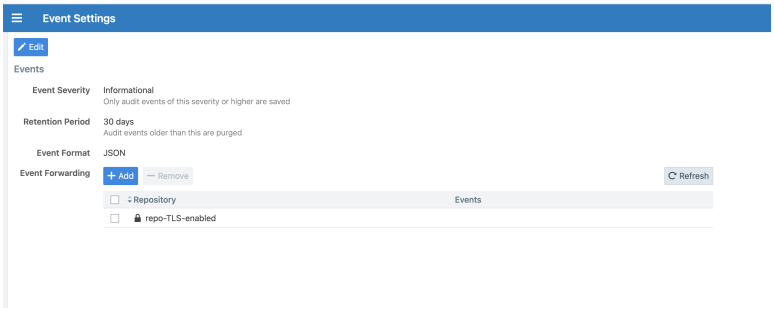
Configuring Remote Audit Server with TLS

For Common Criteria, the communications channel between the PCE and remote syslog destination must be secured by enabling TLS v1.2 as shown above. When adding a new remote syslog repository, a Trusted CA Bundle must be uploaded to the PCE by selecting the certificate bundle configured on the remote syslog server. The PCE TLS client only supports FIPS approved algorithms when communicating with a remote syslog server based on the following cipher suite:

- DHE_RSA_WITH_AES_128_GCM_SHA256

If a repository does not have TLS encryption enabled, or the establishment of a TLS connection fails, the Event Configuration page shows a warning icon. Events will not be sent in an unencrypted form.

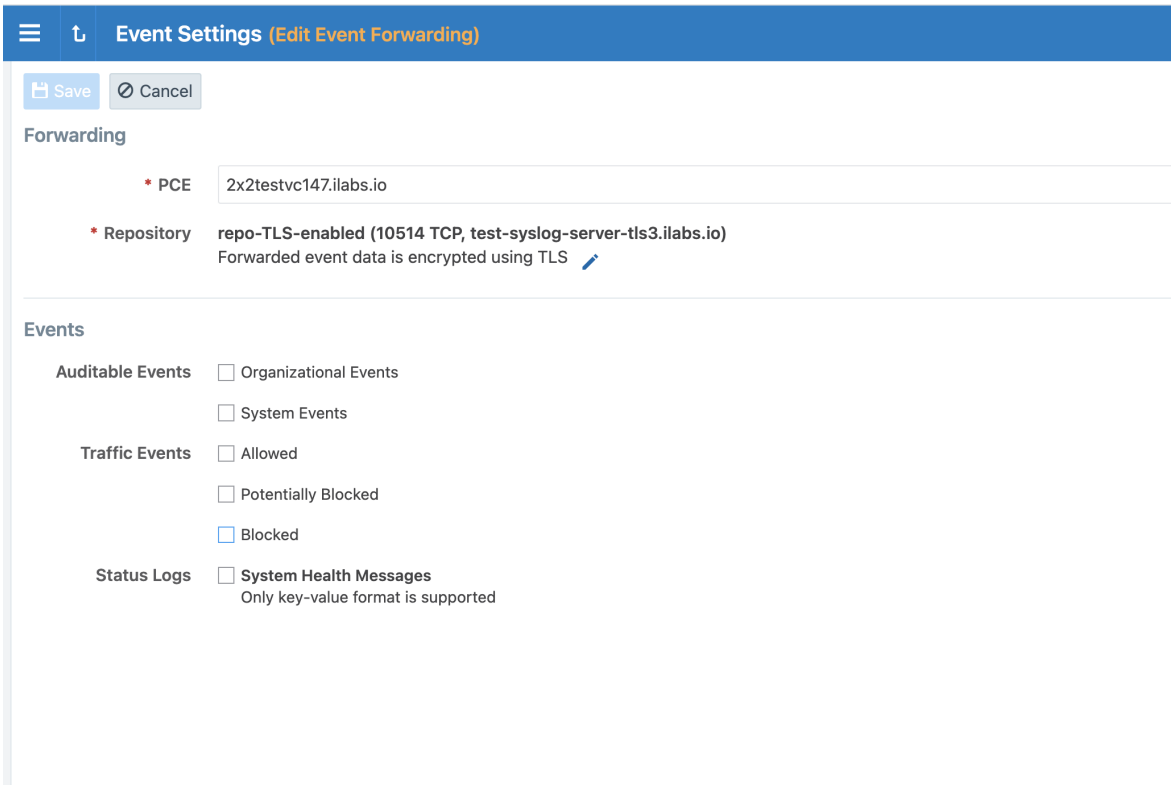
Figure: Event Settings



Selecting Message Types to Forward

Edit the Local syslog server settings and be sure to select all message types.

1. From the PCE web console menu, choose **Settings** > **Event Settings**.
2. Click **Edit**. The Event Settings dialog appears.



3. Click all the checkboxes for all the event types.

   The event types are:

- Organizational Events: actions such as users logging in and logging out, and failed login attempts; when a system object is created, modified, deleted, or provisioned; when a workload is paired or unpaired; and so on.
- System Events: events that relate to significant activity occurring on the platform that runs the PCE application.
- Allowed Traffic Events: events related to traffic that was allowed by the active policy.
- Potentially Blocked Traffic Events: events related to traffic that could be blocked; that is, a workload is in a Visibility Only state and the PCE doesn't have rules in the active policy to allow that traffic.
- Blocked Traffic Events: Events related to traffic that attempted to communicate with a workload but was blocked due to policy; that is, a workload is in the enforced state and the PCE doesn't have rules in the active policy to allow that traffic.
- System Health Messages: Each PCE node reports its status to the local syslog daemon once every minute.

4. Click **Save**.

Monitoring for Loss of Forwarded Syslog Messages

The PCE can detect the loss of log messages that should be forwarded to syslog remote destinations. The PCE maintains a queue of log messages to be forwarded. If log messages can not be forwarded to their destination for some reason, the PCE keeps them in the queue and monitors the length of the queue. The status of syslog message forwarding is displayed in the Health page of the Web Console. In the Core Node Health and Data Node Health sections of the PCE Health page, check the line for Syslog Forwarding Status. The possible status messages are Normal (fewer than 5,000 messages in queue), Long message queues (5,000 or more messages in queue), or Dropping messages. When PCE health becomes critical due to loss of the syslog forwarding connection, a message is logged in system_health.log.

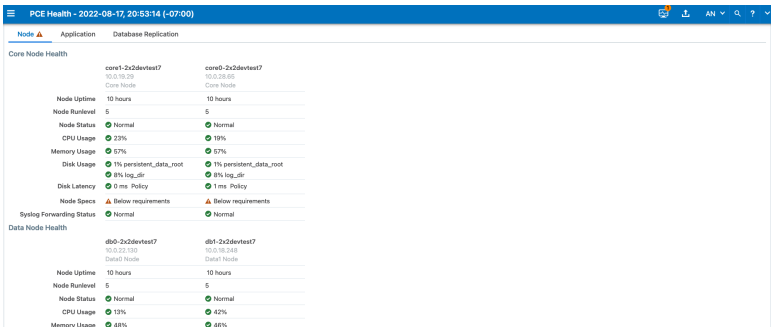
Below 5,000 queued messages, the syslog connection state is considered Normal. If the queue size exceeds a threshold of 5000 messages, the connection state changes to Warning. And when messages are dropped for a destination, the connection state changes to Critical.

To set up syslog forwarding monitoring when running in Common Criteria mode, run the following commands on each node:

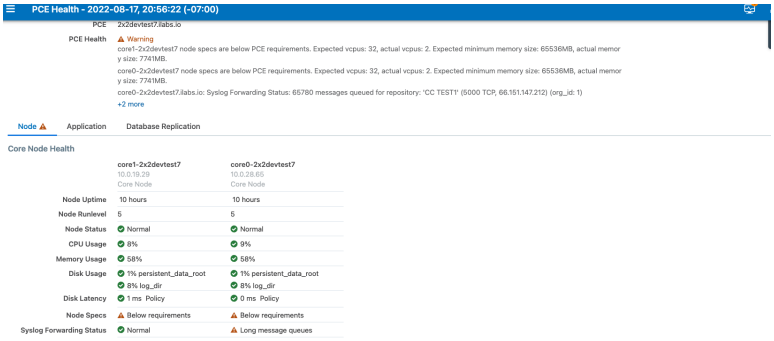
```
$ sudo -u ilo-pce illumio-pce-env metrics syslog_fwd_status:syslog_fwd_status_
critical=1 -w
$ sudo -u ilo-pce illumio-pce-ctl restart
```

The PCE does not do audit log reconciliation when the connection to the syslog server is lost. If the connection between the audit server and the PCE is broken, there may be a gap in the audit server audit record. If a syslog connection is broken, an attempt is made to reconnect to the external syslog destination every 60 seconds.

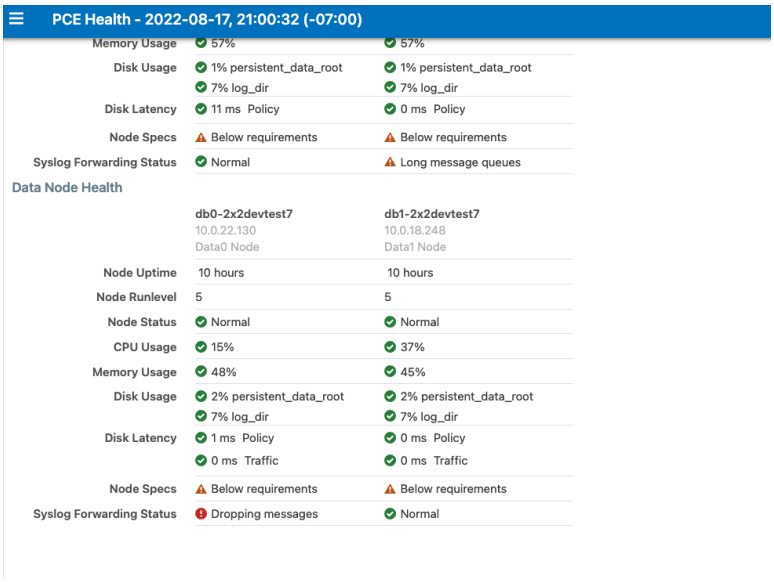
The following illustration shows the Syslog Forwarding Status when it is Normal:



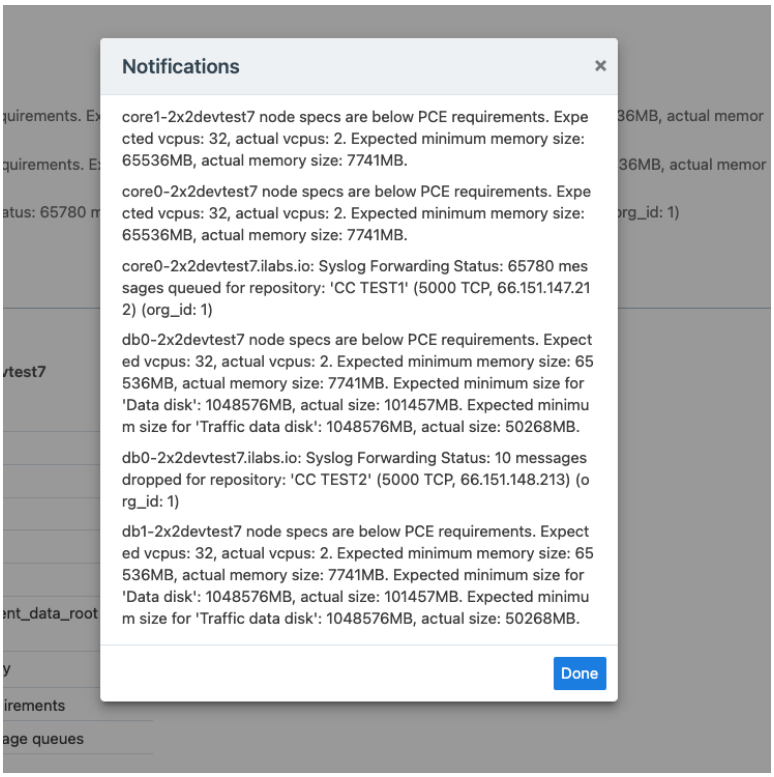
The following illustration shows the Syslog Forwarding Status when the message queues are getting long:



The following illustration shows the Syslog Forwarding Status when audit messages are being dropped on the data node:



The following illustration shows Syslog Forwarding Status notifications. One of the messages shows how many messages were lost when the syslog connection was lost: "10 messages dropped for repository."



The PCE Administrator can reset the syslog connection statistics by using the following command:

```
# sudo -u ilo-pce illumio-pce-ctl reset-syslog-stats
```

The underlying cause must also be fixed; otherwise, the status will go back to WARNING or CRITICAL.

Configuring Event Audit Levels

The following section describes how to configure the Events Settings in the PCE web console.

Events Are Always Enabled

Events are enabled by default in the PCE and cannot be disabled, in accordance with Common Criteria compliance.

Use the PCE web console to change event-related settings and the PCE `runtime_env.yml` for traffic flow summaries.

Event Settings in PCE Web Console

From the PCE web console, you can change the following event-related settings:

- **Event Severity:** Sets the severity level of events to record. Only messages at the set severity level and higher are recorded. The default severity is “Informational.”
- **Retention Period:** The system retains event records for a specified number of days; from 1 day to 200 days with the default period being 30 days.
- **Event Pruning:** The system automatically prunes events based on disk usage and the age of events; events older than the retention period are pruned. When pruning is complete, the `system_task.prune_old_log_events` event is recorded.
- **Event Format:** Sets the message output to one of the three formats. The selected message output format only applies to messages that are sent over syslog to a SIEM. The REST API always returns events in JSON.
    - JavaScript Object Notation (JSON): The default; accepted by Splunk and QRadar SIEMs
    - Common Event Format (CEF): Accepted by ArcSight
    - Log Event Extended Format (LEEF): Accepted by QRadar

Event Severity Levels

Severity	Description
Emergency	System is unusable
Alert	Should be corrected immediately

Severity	Description
Critical	Critical conditions
Error	Error conditions
Warning	Might indicate that an error will occur if action is not taken
Notice	Events that are unusual, but not error conditions
Informational	Normal operational messages that require no action Default audit level for the PCE
Debug	Information useful to developers for debugging the application

Output Format Change

The output format can be changed in the PCE web console:

- JSON (default)
- CEF
- LEEF

Records are in JSON format until you change to one of the other formats. Then, the new events are recorded in the new format; however, the earlier events are not changed to the selected format and they remain recorded in JSON.

Set Event Retention Values

You can set the event retention values depending on the specific conditions described below.

If you are using a SIEM, such as Splunk as the primary long-term storage for events and traffic in a dynamic environment, consider setting the event retention period to 7 days. On setting it to 7 days, you can use the PCE Troubleshooting or Events Viewer to quickly troubleshoot and diagnose events. The benefit of setting 7 days is that if an issue occurs on a Friday, it can still be diagnosed on the following Monday. A large number of events are generated in a dynamic environment, which increases the data stored (disk space used), backup size, and so on. The period of 7 days provides a good balance between disk usage and the ability to troubleshoot.

> NOTE:
> A dynamic environment is when applications and infrastructure are subject to frequent changes; for example, usage of APIs, ETL, Containers, and so on.

If you are using a SIEM in a non-dynamic environment, consider setting the event retention period to 30 days. A smaller number of events are generated, and less disk space is used in a non-dynamic environment.

If you not using a SIEM such as Splunk and the PCE is the primary storage for the events data used for reporting, diagnosis, and troubleshooting, set the event retention period as per the organization's record retention policy, for example 30 days. If you generate quarterly reporting using events, set the event retention period to 90 days.

SIEM	Consideration	Value
Yes: Primary storage for events	If primary storage of events is not on the PCE	7 days (PCE troubleshooting) 1 day (minimum)
No: Not primary storage for events	If primary storage of events is on the PCE, consider the organization's record retention policy as well as the available disk and event growth pattern	30 days (default)
No	• If the organization's record retention is more than 30 days • If disk monitoring is not set up, it is required to set up disk monitoring	As per your record retention policy 200 days (maximum)
Not applicable	If events data is not needed for reporting or troubleshooting	1 day (minimum)

If disk space availability and event growth projections indicate that the desired retention period cannot be safely supported, consider using a SIEM because the PCE might not store events for the desired period.

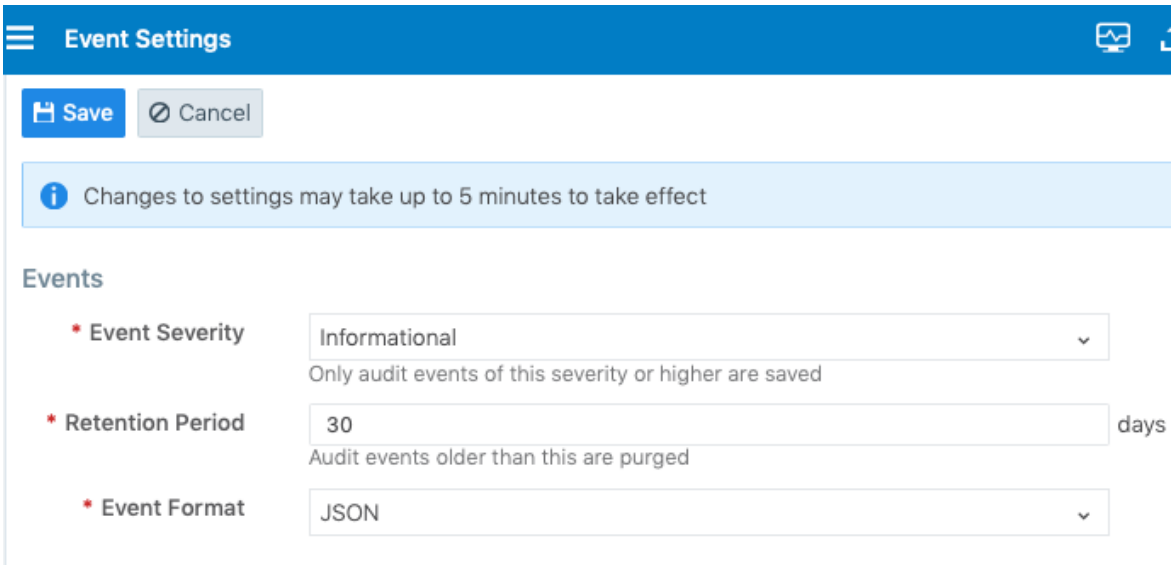
> NOTE:
> Running the `illumio-pce-db-management events-db` command provides an output of the average number of events and the storage used.

Configure Events Settings in PCE Web Console

1. From the PCE web console menu, choose **Settings** > **Event Settings** to view your current settings.
2. Click **Edit** to change the settings.
    - For Event Severity, select from the following options:
        - Error
        - Warning
        - Informational
    - For Retention Period, enter the number of days you want to retain data.

- For Event Format, select from the following options:
  - JSON
  - CEF
  - LEEF

3. Click **Save** once you're done.



Configuring VEN Audit

To configure the PCE to filter VEN audit events based on event type (severity) go the PCE web console main navigation menu and select **Settings** > **Event Configuration**. Next, click on **Edit** and select the event severity from the following list:

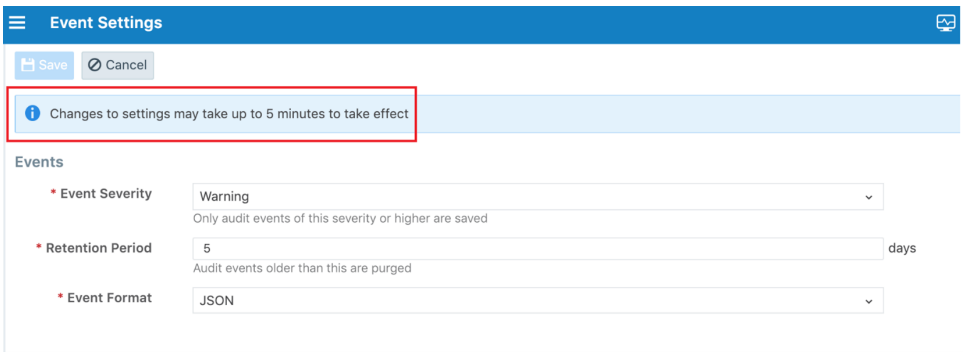
- Error
- Informational
- Warning

See “Configure Events Settings in PCE Web Console” for more information.

Sync Audit Logs between Local and Remote Syslog Servers

After configuring a new connection for a remote audit server, the PCE automatically resets the local syslog server so that events messages are synced between the local and remote servers. When making a change to the event log settings, it may take a few minutes for the cluster to reflect the updated configuration.

Figure 15: Changes to Event Settings



In the event of a network outage between the remote syslog server and the PCE, there is no log reconciliation between the PCE and remote syslog server.

View and Export Events

By default, you can view events in the PCE web console or by using the PCE command line. You can then export Organization events using the PCE web console.

View Events in PCE Web Console

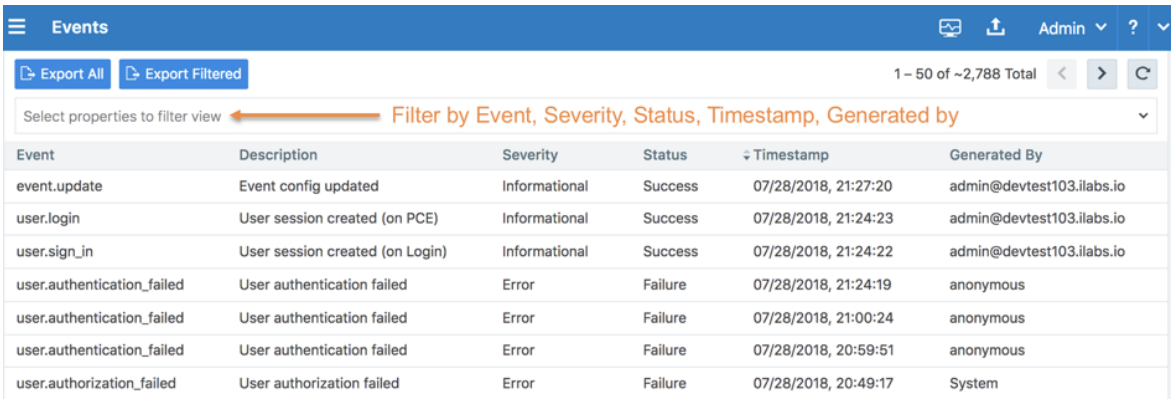
By default, the PCE web console shows events that occur in your organization, such as when a workload is paired, if a pairing failed, when a user logs in or logs out, when a user fails to authenticate, and so on.

If you want to see only certain events, you can filter by event ID to see events that interest you most. You can also search for Organization events by their universally unique identifier (UUID), and filter events by their severity.

You can also export the list of organization events as a CSV file.

To view Organization events:

1. From the PCE web console menu, choose **Troubleshooting** > **Events**.
2. At the top of the page, you can use the Event Filter to filter the list by event ID.



NOTE:
In the Events Viewer, the suggested values for the filters are generated from all possible values. For example, the “Generated By” filter shows all users on the system. However, the actual results displayed by that filter might not contain any data.

VEN Event Not Displayed in PCE Web Console

The following events related to VENs are not currently viewable in the PCE web console.

This is a two-column list of event names.

VEN Events not shown in PCE Web Console	
fw_tampering_revert_failure	lost_agent
fw_tampering_reverted	missing_os_updates
fw_tampering_subsystem_failure	pce_incompat_api_version
invoke_powershell_failure	pce_incompat_version
ipsec_conn_state_change	pce_reachable
ipsec_conn_state_failure	pce_unreachable
ipsec_monitoring_failure	proc_config_failure
ipsec_monitoring_started	proc_envsetup_failure
ipsec_monitoring_stopped	proc_init_failure
ipsec_subsystem_failure	proc_malloc_failure
ipsec_subsystem_started	proc_restart_failure
ipsec_subsystem_stopped	proc_started
refresh_token_failure	proc_stopped
refresh_token_success	

View Events Using PCE Command Line

Run this command at any runlevel to display:

- The total number of events
- The average number of events per day

```
$ sudo -u ilo-pce illumio-pce-db-management events-db events-db-show
```

Run this command at any runlevel to display:

- The amount of disk space used by events
- The total number of events

```
$ sudo -u ilo-pce illumio-pce-db-management events-db disk-usage-show
```

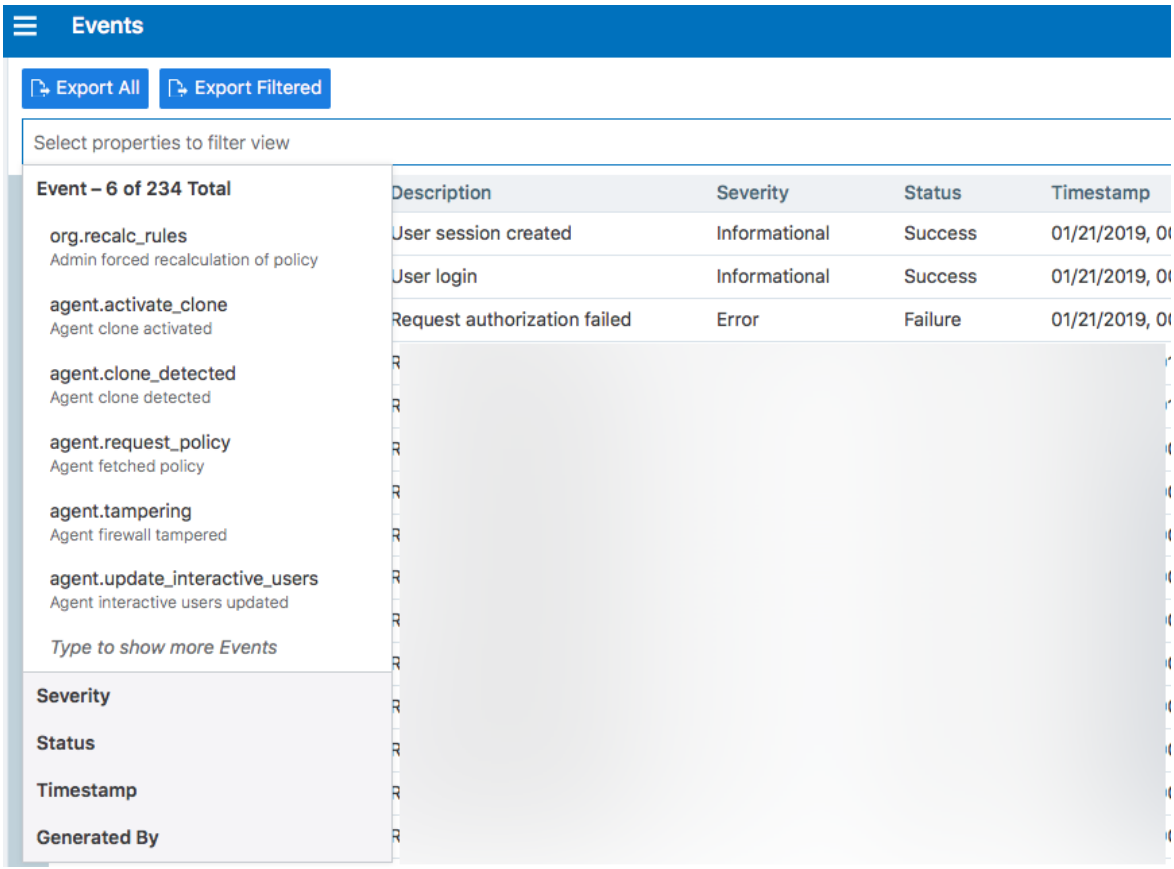
Export Events Using PCE Web Console

You can export all Organization events, or export a filtered list organization events to a CSV file.

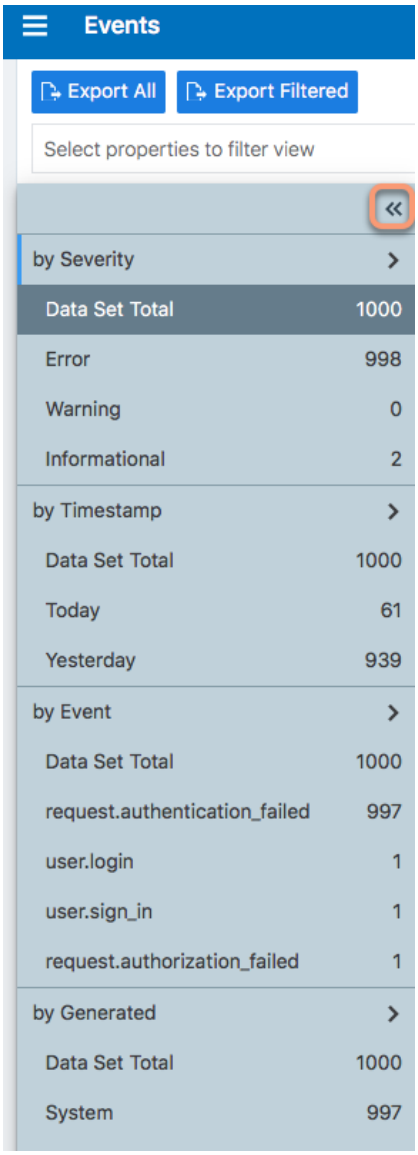
To export events:

1. From the PCE web console menu, choose **Troubleshooting** > **Events**.

   You see a list of events based on the activities performed.
2. Click **Export** > **Export All** to export all Organization events.
3. To export a filtered list of events, filter the list and then click **Export** > **Export Filtered** to export only the filtered view.
4. To search for events based on event ID, severity, status, timestamp, and who generated them, use the search filter:



5. For a faster filtering via the browser, use the following field:



Startup and Shutdown Events

The PCE leverages the operating system's syslog function to log audit events. As syslog is part of the operational environment, there is no mechanism to enable and disable the audit feature. The PCE starts sending audit events when it is started. The PCE stops sending audit events when it is stopped. The corresponding events are `pce.application_started` and `pce.application_stopped`. These events are registered internally in the log file `illumio-pce.log`. They are also registered as audit events that are sent to the audit server.

Audit Server and Active Sessions

This section explains how to determine the remote audit server status and discusses the types of active sessions for logged in PCE users.

Determining Remote Audit Server Status

From the “Events Configuration” screen of the PCe web console, one can check the configuration of each audit server. The current reachability status of the syslog server can be found by searching for “remote_syslog_reachable” or “remote_syslog_unreachable” events via the Events Viewer.

Figure 17: Remote Audit Server Reachable

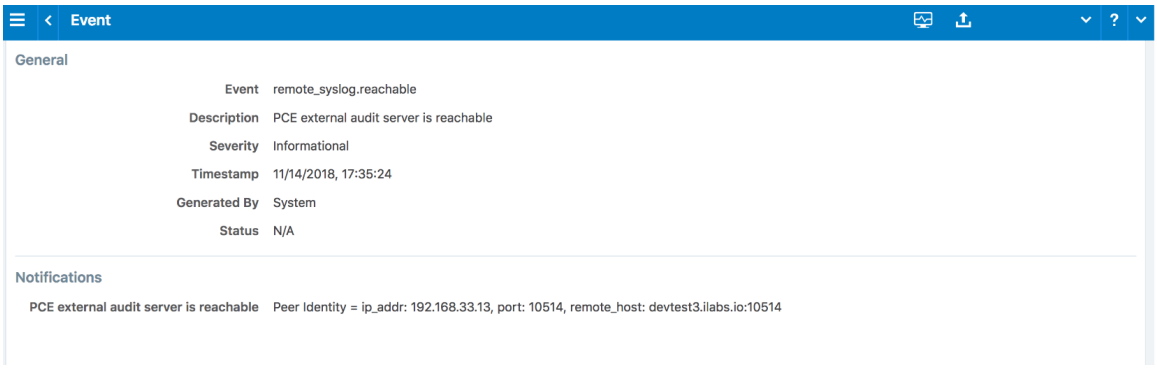
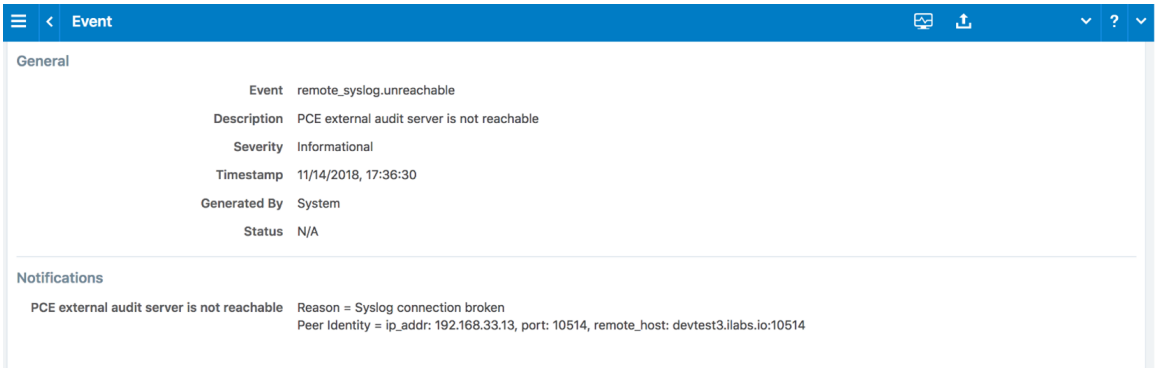


Figure 18: Remote Audit Server Unreachable



Understanding Login Sessions and Agent Manager Sessions

A logged in PCE user has two active sessions – one active session is with the Login service and another active session is with the Agent Manager service:

Login service: Manages sessions related to users and user authentications. The Login service maintains user login sessions.

Agent Manager service: Manages PCE sessions related to policy objects, labels, managed workloads, unmanaged workloads and related PCE services.

Given the two user sessions noted above, the following scenarios are useful in understanding expected audit event messages related to user sessions:

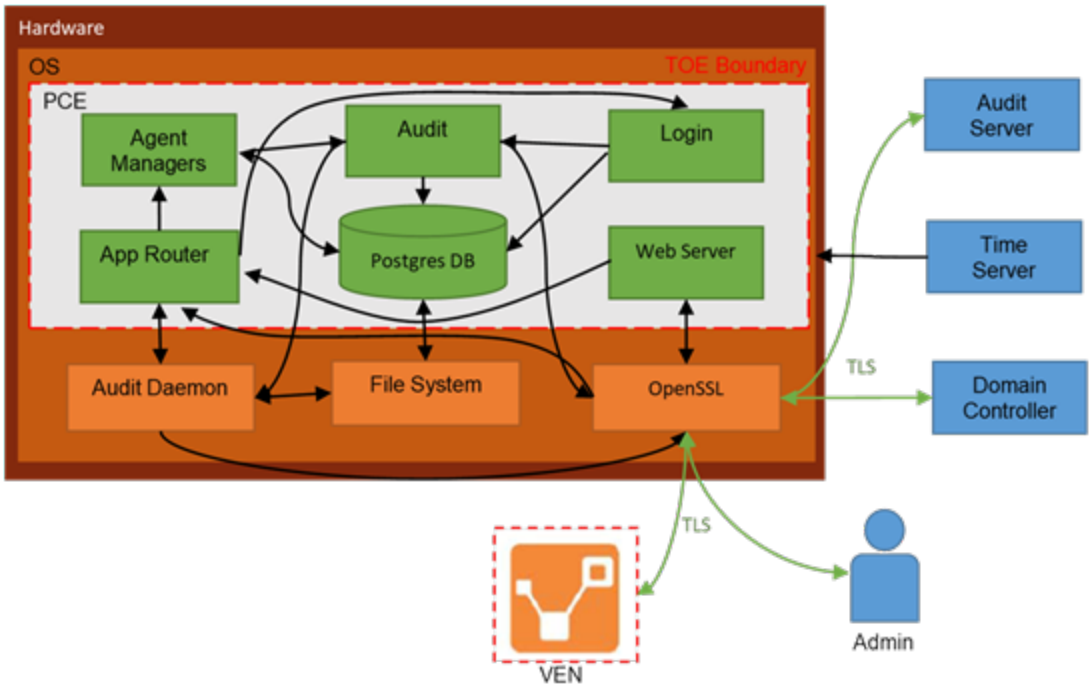
Scenario 1: Both Agent Manager and Login Sessions Expired

When a user takes an action (e.g. first time logging in, refreshes a page) and the session is expired in the Agent Manager, the authentication failure is logged as an event and the user's browser is redirected to the login service for authentication. If the session on the login service has expired too, the user will be prompted to log in and a successful login will result in two session created events corresponding to the two active sessions.

Scenario 2: Agent Manager Expired and Login Session Still Active

When a user takes an action and the session is expired in the Agent Manager, the authentication failure is logged as an event and the user's browser is redirected to the login service for authentication. If the user's session on the login service is still current, the user's browser is redirected back to the Agent Manager (with no interaction from the user) and a new session is created for him, resulting in a single session created event for the Agent Manager session.

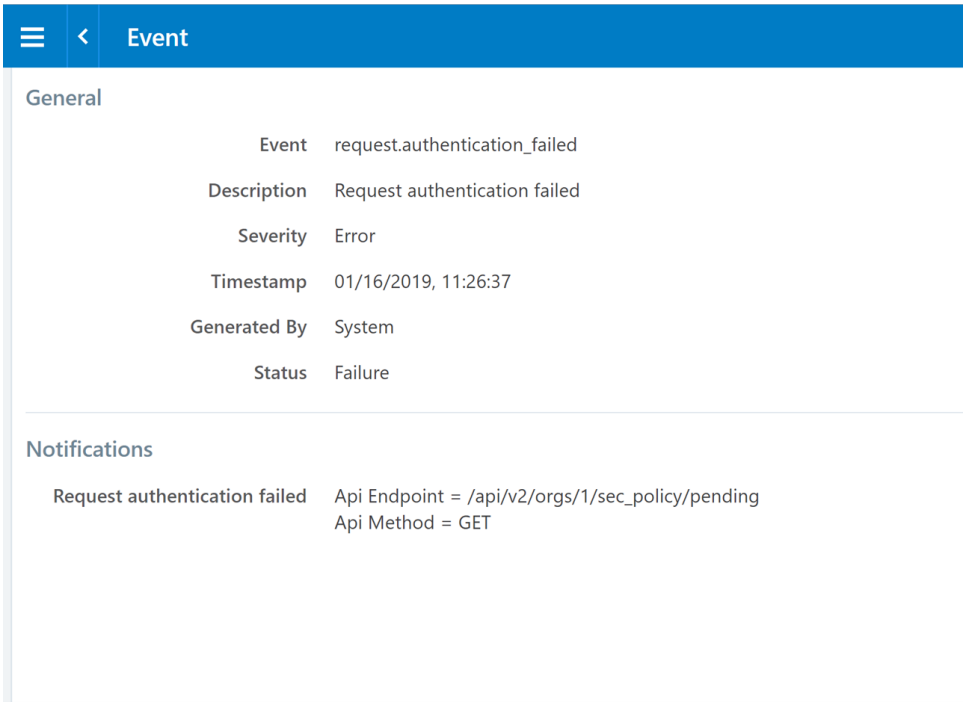
Figure 19: Login Service and Agent Manager Service



The Agent Manager session can generate events by either a user performing an action or the system performing a task. An example of a “system generated” event is a user authenticated failure

event in which a user types in an incorrect password. This results in a “request.authentication_failed” event being generated by the system. (See example below)

Figure 20: User Authentication Failure Event



An example of a “user generated” event is when a user creates a new security policy. The resulting event captures the information related to the newly created security policy including a unique identifier listed in the “Resource” field for the event. See example audit message below with unique identifier “version .after=3”:

Figure 21: Event Message Unique ID

Common Criteria Only Events

The following table lists the types of JSON events that are generated and their descriptions.

For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `agent.update` is `agent.update.success` and the failure event is `agent.update.failure`.

Auditable Event	Description
`pce.application_started`	PCE application started
`pce.application_stopped`	PCE application stopped
`remote_syslog.reachable`	Remote syslog destination reachable
`remote_syslog.unreachable`	Remote syslog destination not reachable
`tls_channel.establish`	TLS channel established

Auditable Event	Description
`tls_channel.terminate`	TLS channel terminated

Management Functions

The following table describes management activities of the evaluated security functionality. All management activities require the role Global Organization Owner.

Requirement	Management Activities
ESM_ACD.1	Creation of policies
ESM_ACT.1	Transmission of policies
ESM_ATD.1	Definition of object attributes Association of attributes with objects
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1	Configuration of authentication failure threshold value Configuration of actions to take when threshold is reached Execution of restoration to normal state following threshold action (if applicable)
FIA_SOS.1	Verification of secrets
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)
FMT_MTD.1	Management of user authentication data
FMT_SMR.1	Management of the users that belong to a particular role
FTA_TAB.1	Maintenance of the banner
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

Chapter 4

Authentication

This section introduces you to the how authentication works in the Illumio Core for Illumio Core 22.2.30.

Login Lockout for Invalid Credentials

This section describes how the PCE can lockout PCE users for invalid credentials and how to view them in the PCE web console Events page.

How and When the PCE Locks Out Users

By default, the PCE enforces the following login lockout behavior:

- Lockout value after invalid login attempts

  After a user enters an invalid password 5 consecutive times while attempting to log into the PCE, the user's account is locked for 15 minutes. The login lockout feature resets the account after 15 minutes and does not require an Illumio administrator to unlock it. The number of unsuccessful authentication attempts can be configured by changing the default value of the runtime variable `max_failed_login_attempts` (default: 5; minimum: 1; maximum 256) in the configuration file `runtime_env.yml`. Similarly, the lockdown period can be configured by changing the default value of `account_lockout_duration_minutes` (default: 15; minimum: 1; maximum 256).

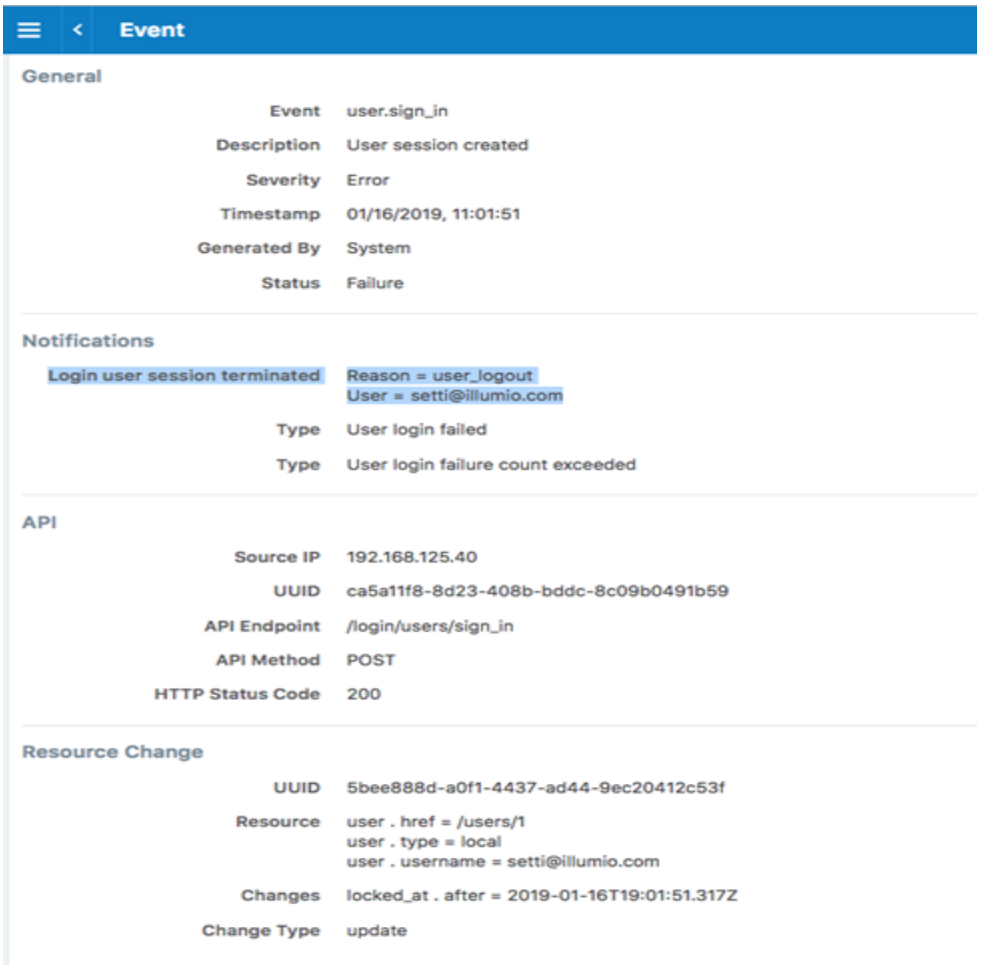
- Active browser token

  If a user successfully logs into the PCE and subsequently logs out but does not close the browser, the browser token remains active for 15 minutes. If the user then logs back into the PCE within that same 15 minute period, the user will be brought back to the last page the user visited on the PCE prior to logging out.

- Audit message for invalid login attempts

  If the user attempts to log in to the PCE but fails 5 times to enter a valid password, the PCE will generate an audit message with a reason code stating that the user has been “logged out” due to exceeding login failure count. See example audit message below.

  Figure 24: Login User Session Terminated



The PCE enforces unsuccessful authentication thresholds only for local users. For users who log in through a SAML SSO Provider (IdP), the PCE does not store passwords and relies on the SAML Identity Provider to enforce a configurable unsuccessful authentication threshold. Actions on exceeding unsuccessful authentication thresholds must be configured at the SAML IdP.

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 **Access Management> Authentication** menu options.

> NOTE:
> Organizations using SAML authentication can not use the PCE's Password Policy features to configure password policies. The PCE enforces the password policy only for local users created in the PCE. For users who authenticate to the PCE using SAML authentication, the PCE relies on the SAML Identity Provider to enforce the password policy. The PCE does not store the passwords for such external users. Hence, any password policy enforcement must be configured in the SAML Identity Provider.

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

Password Requirements

The password requirements you set are displayed to users when they are required to change their passwords. You can set the minimum character length, ranging from a minimum of 8 characters to a maximum of 64 characters. The default length is 8 characters. However, in the Common Criteria evaluated configuration, the administrator must set the minimum password length to 16 characters.

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

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

You have to select at least three of the above categories. The default password requirement is one number, one uppercase character, and one lowercase character. You can set the password to use either one or two characters from each category. In the evaluated configuration, the minimum password length must be set to 16 characters by the administrator.

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.

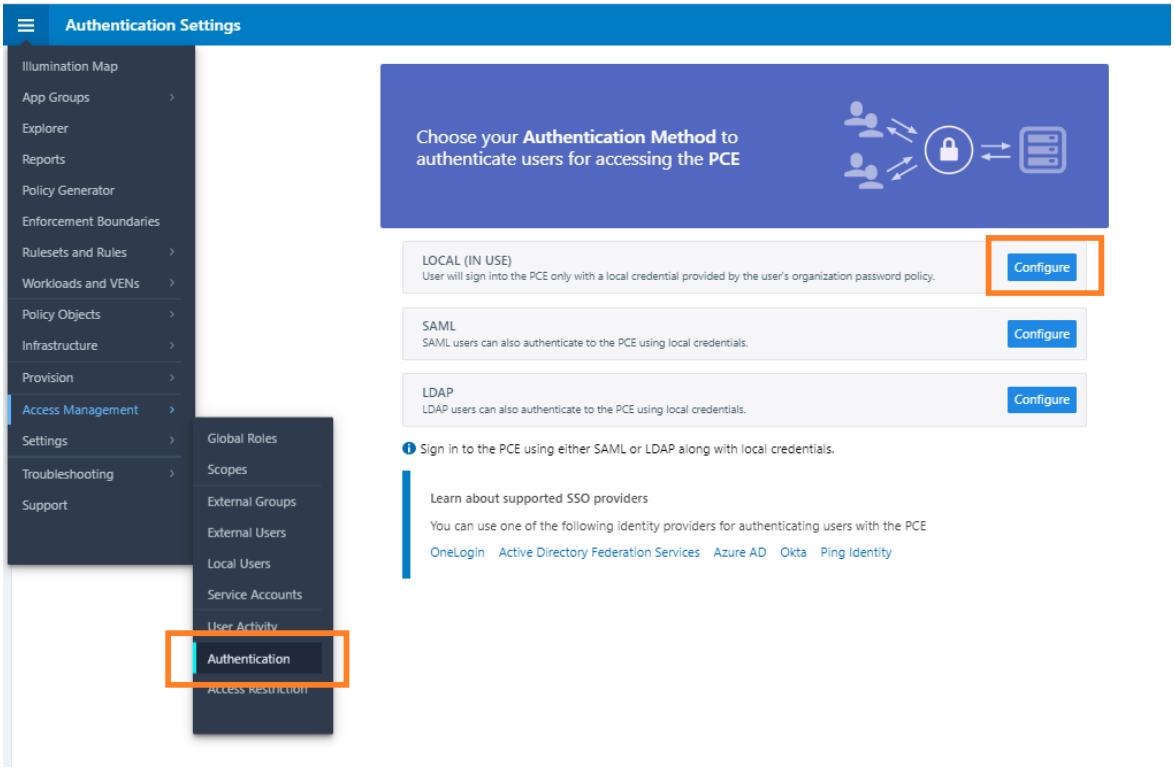
Allowable password reuse and password history can be set to from 1 to 24 passwords before reuse is allowed. The default setting for password reuse is five password changes before reuse is permitted.

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 must reset their passwords when they next log in.

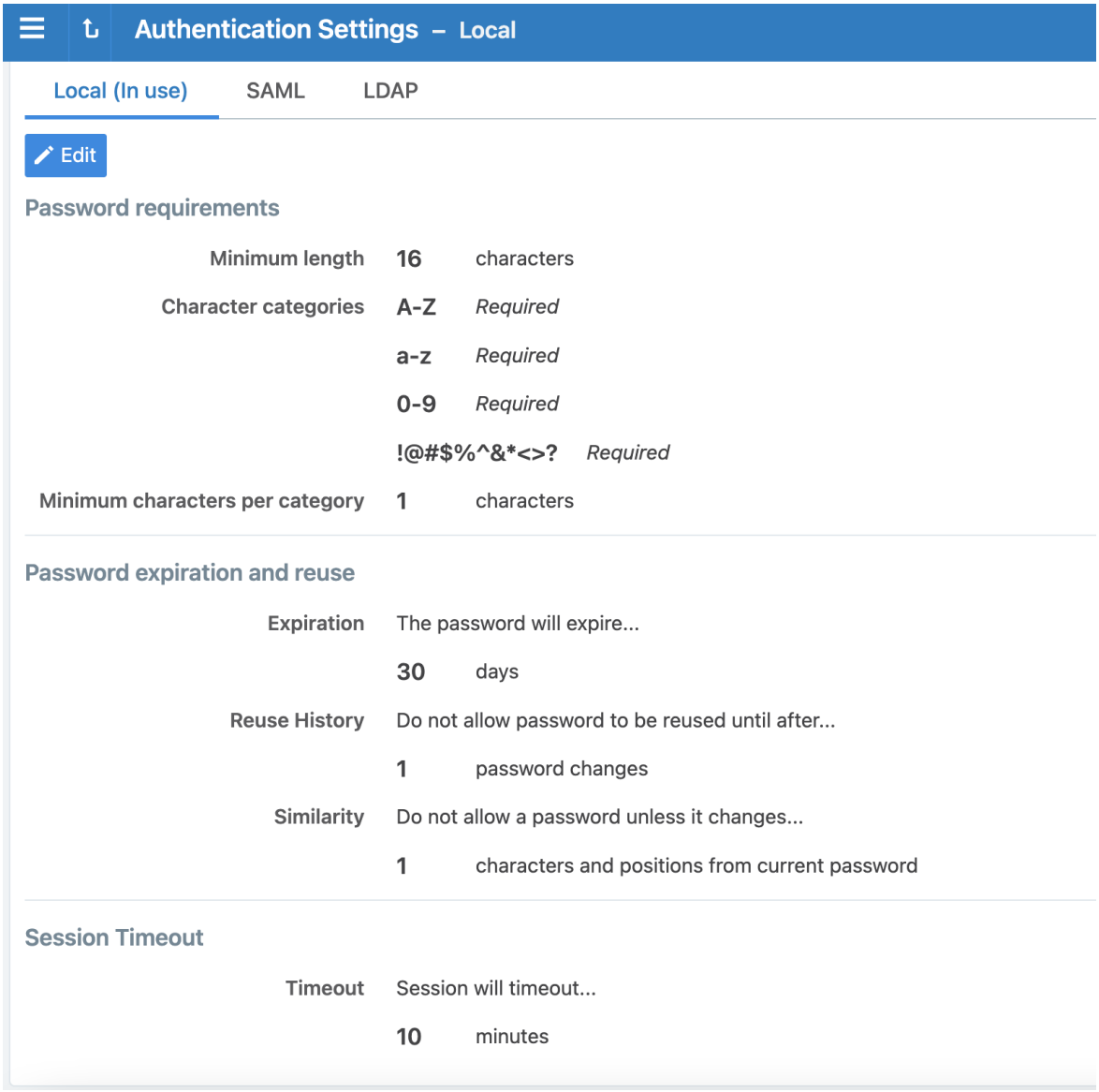
Change Password Policy Settings

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



3. Click **Edit**.

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

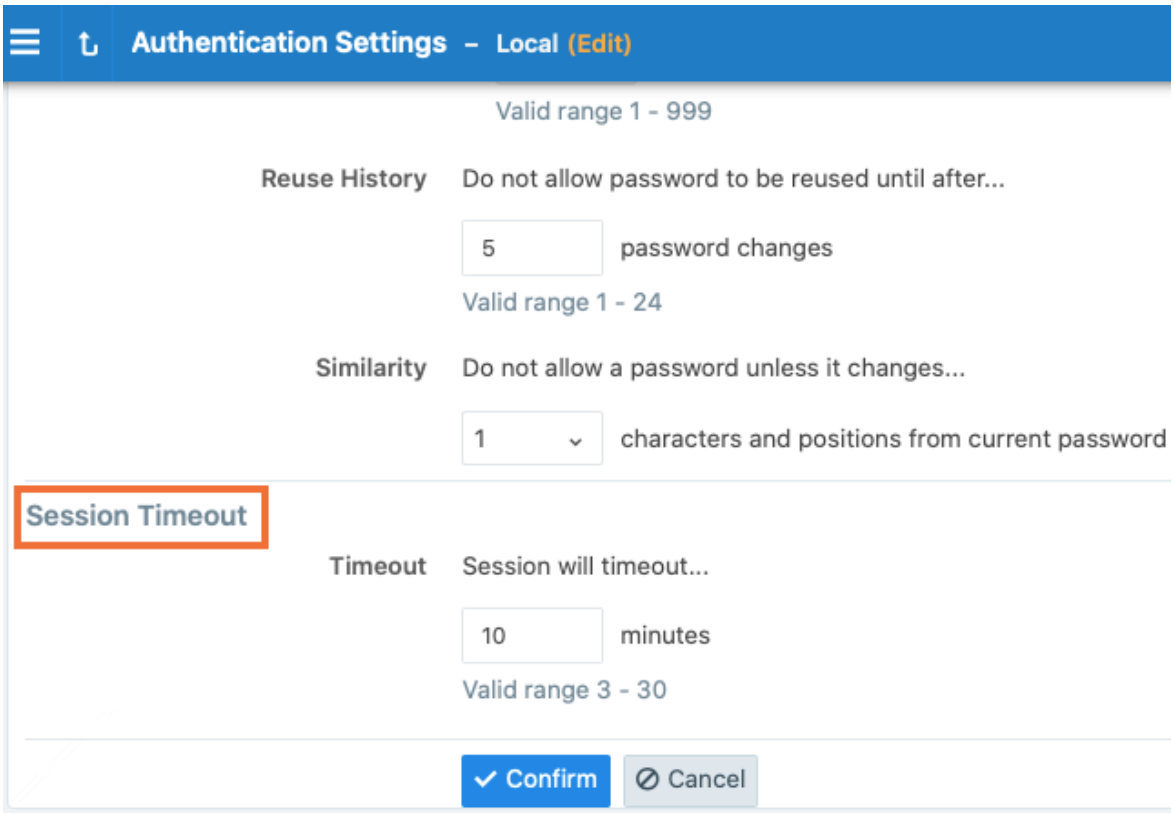


5. Click **Confirm** and then **Save** to save the password policy for your local users.

Configure Session Timeout

You can configure the session timeout value using the PCE web console. The session expiration timeout values must be set accordingly to balance security and usability so that your users can comfortably complete operations within the PCE web console without their session frequently expiring. The timeout value is dependent on how 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.

1. From the PCE web console menu, choose **Access Management** > **Authentication**.
2. Click **Configure** (Local).
3. Click **Edit**.
4. In the *Session Timeout* section, set a value between 3 minutes and 30 minutes. By default, the value is 10 minutes.



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

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

Authentication

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

SAML SSO Authentication

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

> NOTE:
> For users who authenticate to the PCE with SAML SSO, password policy enforcement must be configured at the SAML SSO Provider. PCE enforces the password policy only for local users created in the PCE.

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.

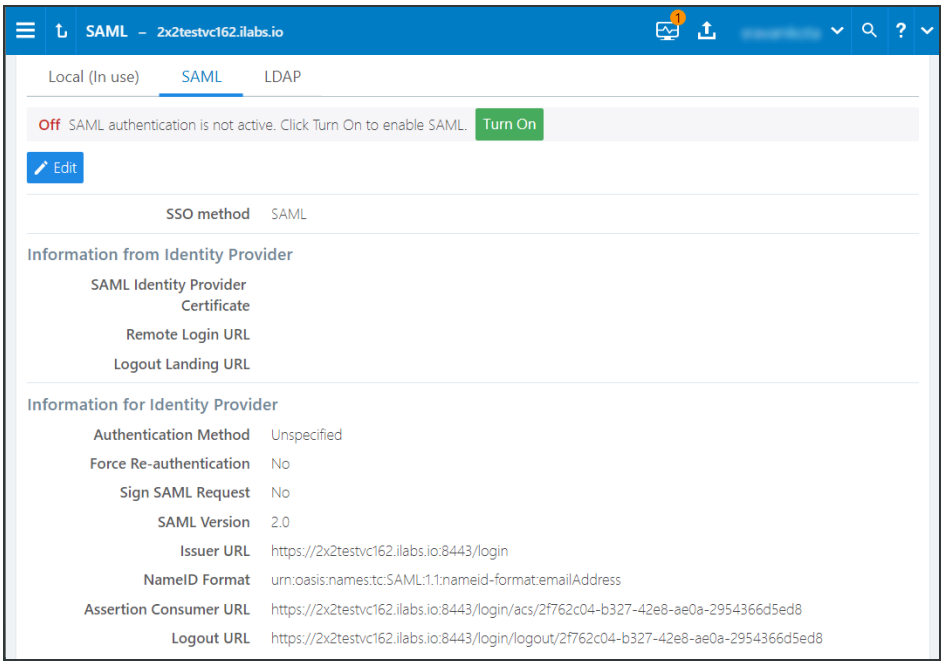
To obtain the SSO information from the PCE:

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.

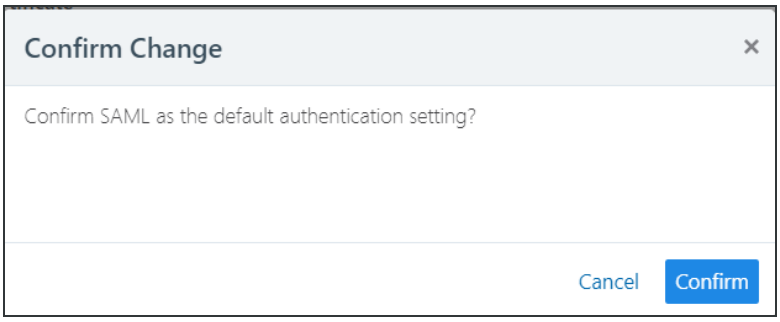
> NOTE:
> Even though the SAML NameID format specifies an emailAddress, the PCE can support any unique identifier such as, userPrincipalName (UPN), common name (CN), or samAccountName as long as the IdP is configured to map to the corresponding unique user identifier.

To enable SAML request signing:

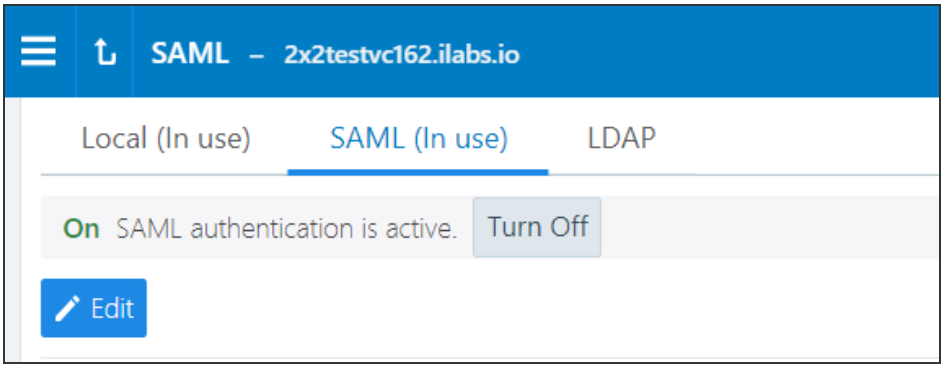
1. Using the Web Console, go to **Access Management > Authentication**.
2. In the *Authentication Setting* screen, select **Configure** button for SAML.
3. In the SAML screen, click **Turn On**.



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



The updated SAML screen shows that SAML authentication is active.



If necessary, you can disable it at any time.

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

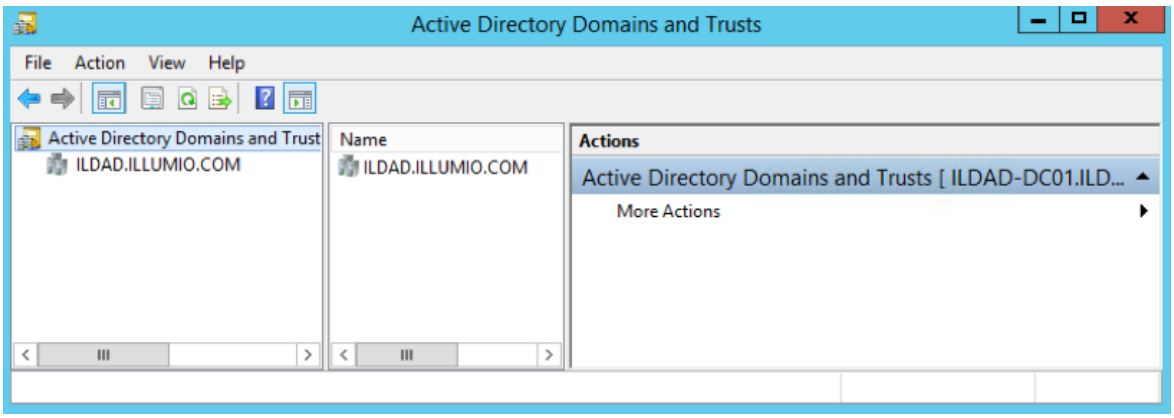
There are two ways for AD FS to produce the NameID claim for an SSO user. The first uses the email field in an Active Directory user account for the NameID.

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 ADUser-Name@yourADDomanName. For example, a user named "test" in an Active Directory domain called "testing.com" would have a UPN of test@testing.com.

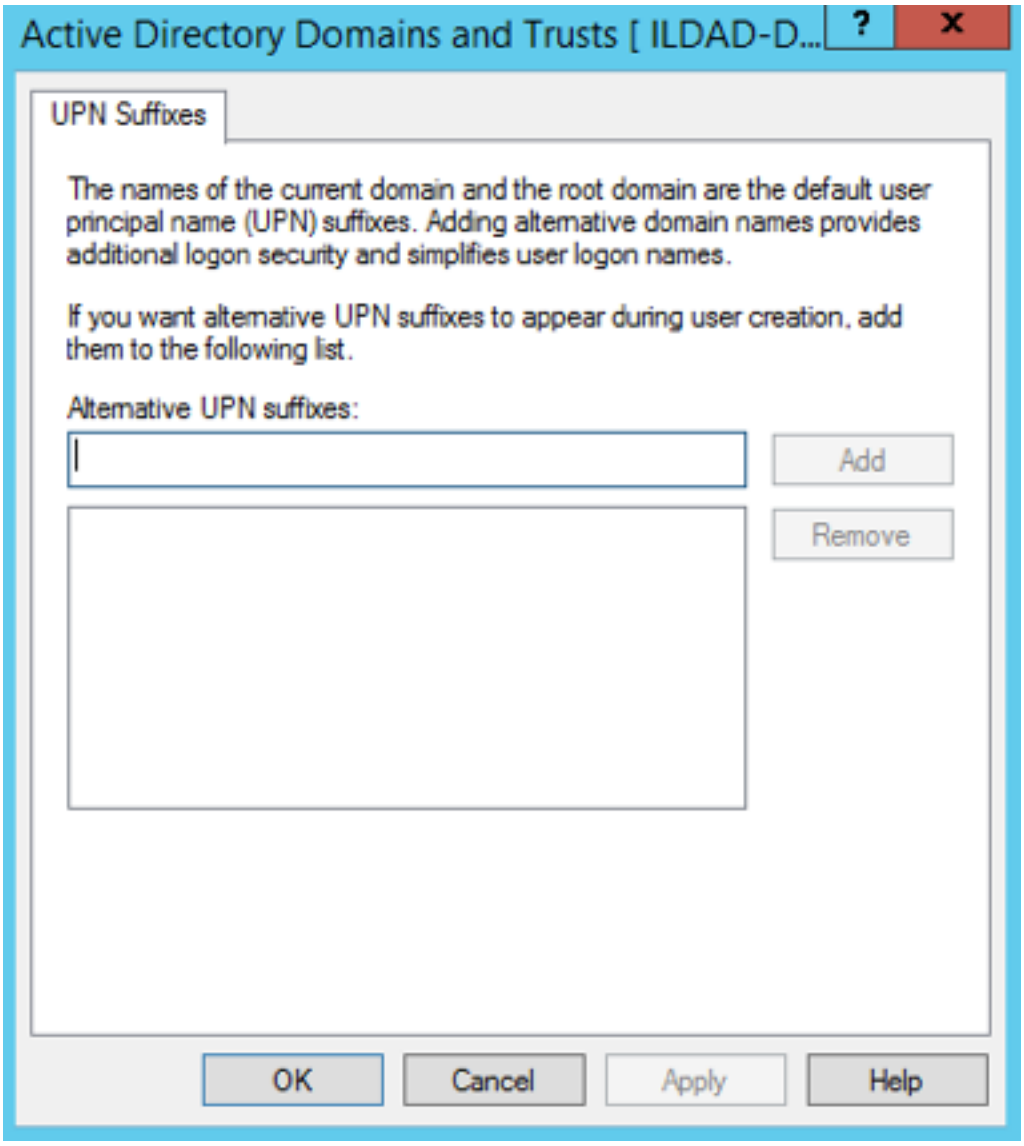
Configure AD Users to Use Different UPN Suffixes

To configure different UPN suffix as the source for NameID:

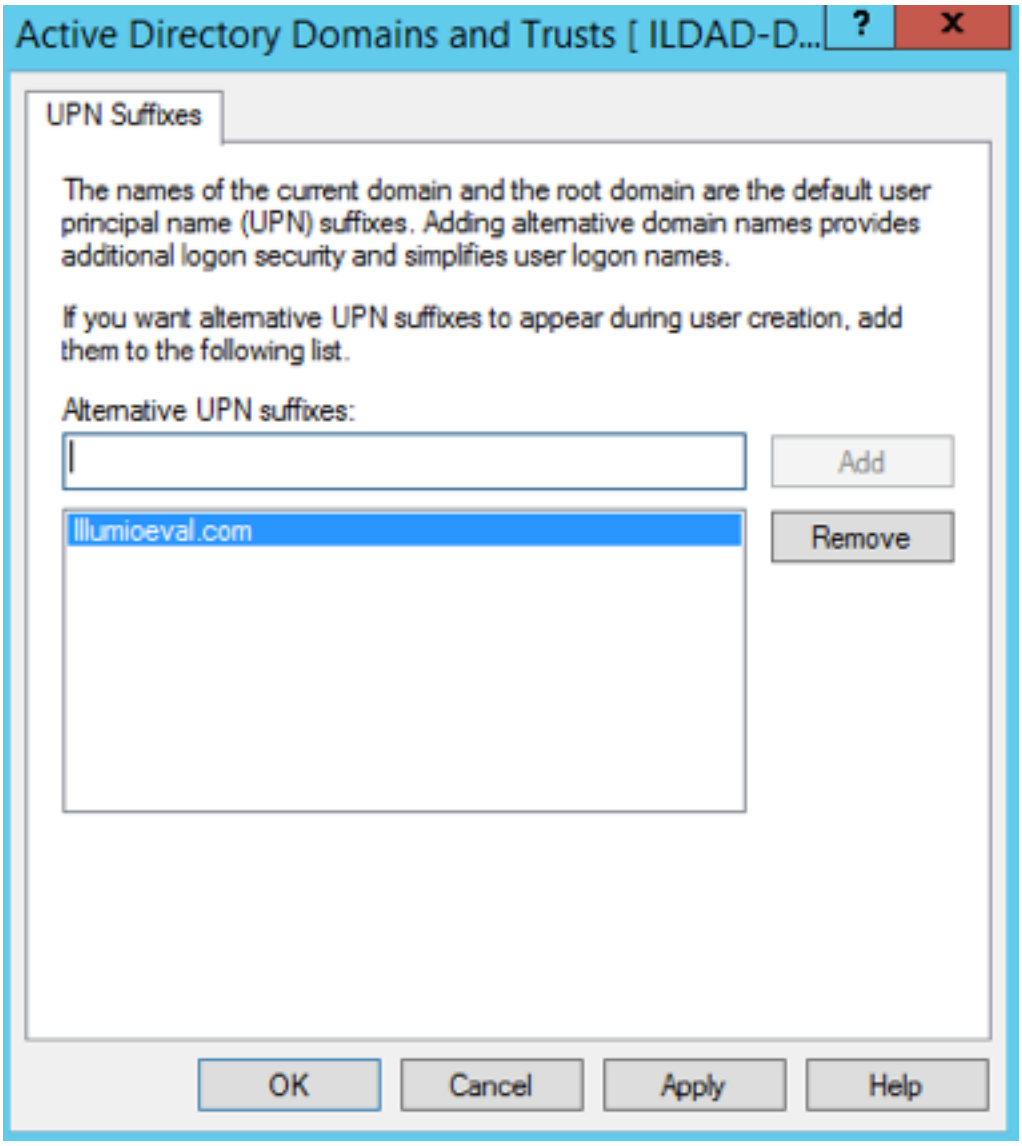
1. Add a UPN suffix. On your system under Server Manager Tools, click **Active Directory Domains and Trusts**.



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 user-names.

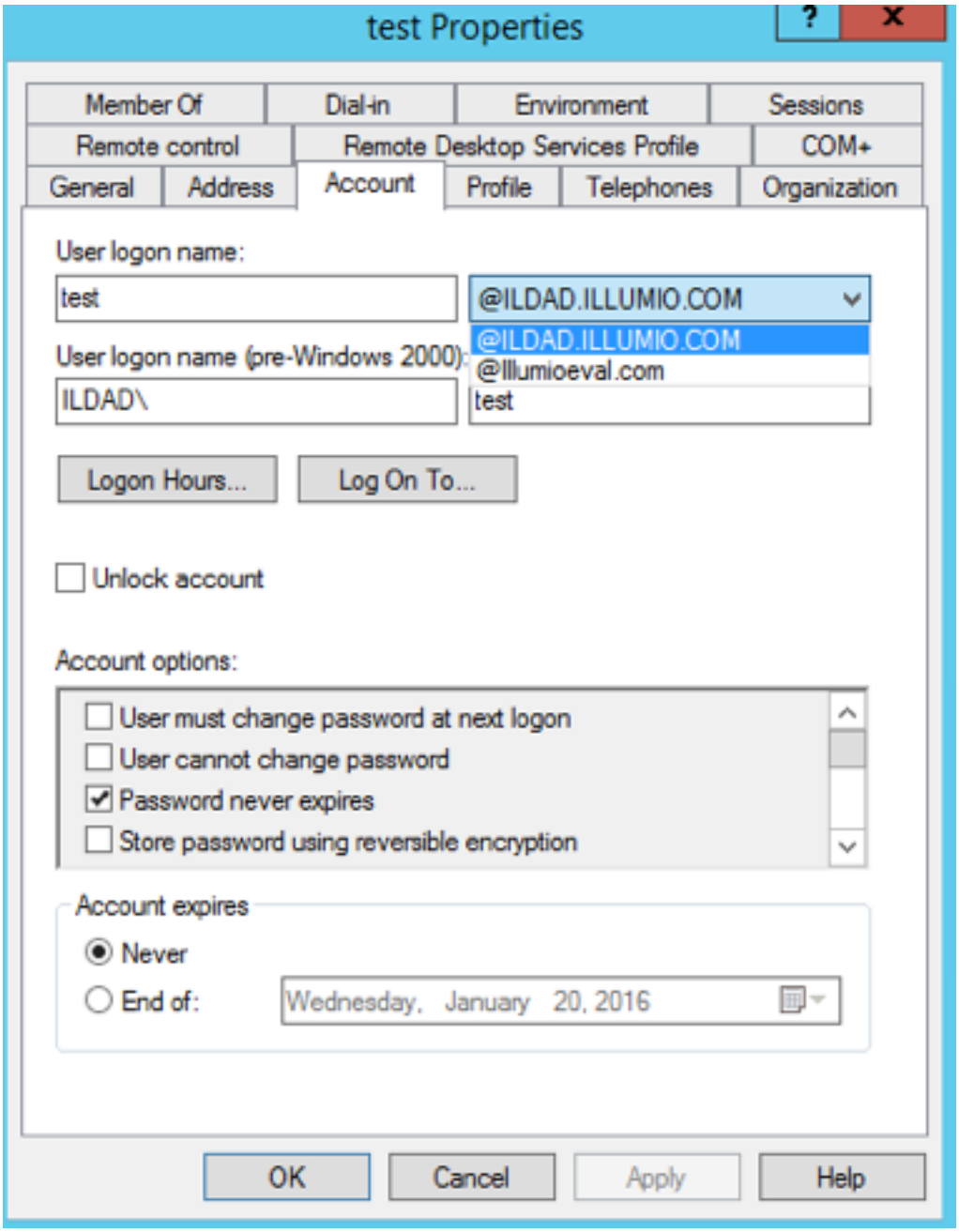


3. Create a suffix that matches the external namespace you'll be using and click **Add**.



You can now assign an Active Directory user your custom UPN for the SAML response.

4. You can add multiple UPNs if needed. As shown below, you can select the UPN created in the previous steps.



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

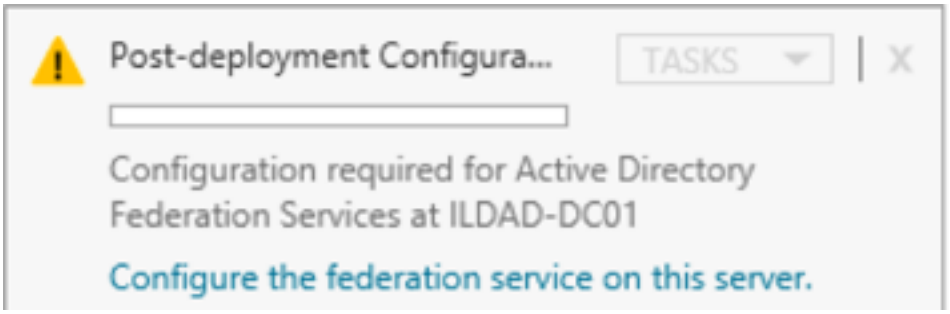
Initial AD FS SSO Configuration

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

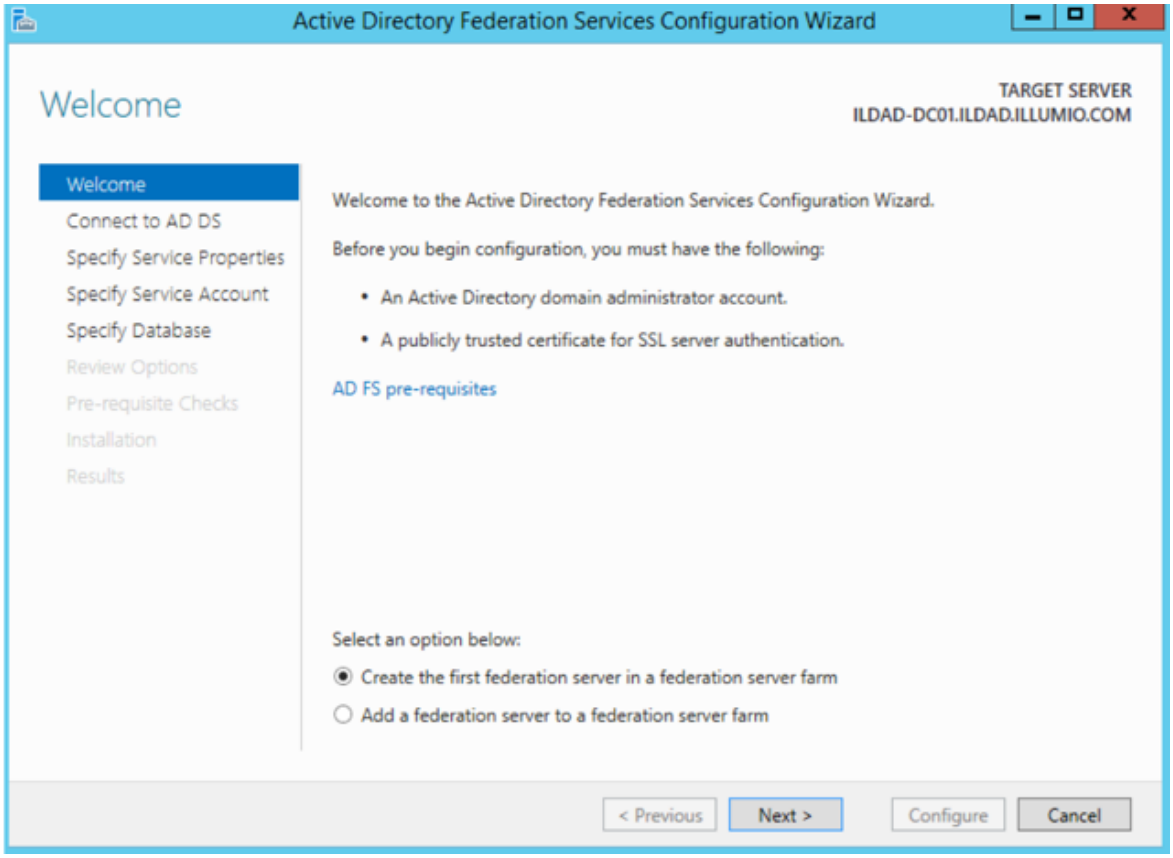
To configure AD FS:

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

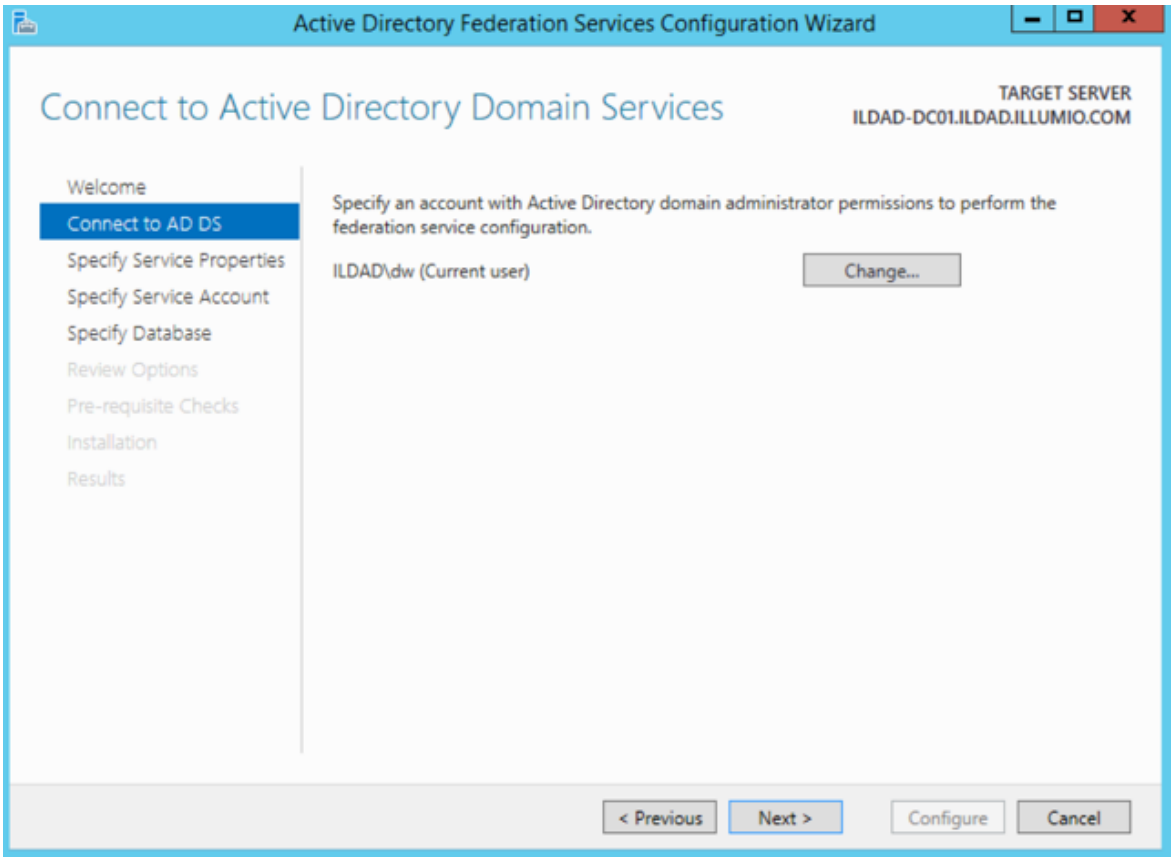
2. Click the “Configure the federation service on this server” link.



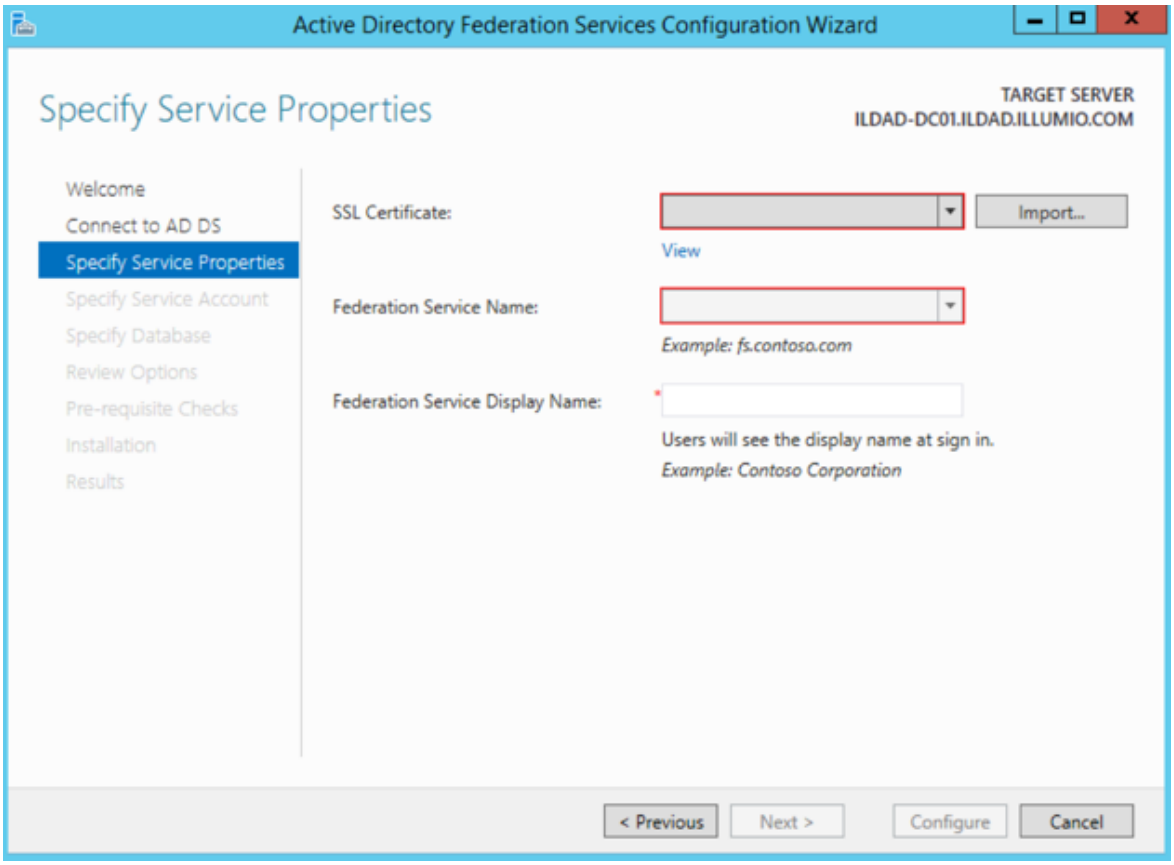
3. Select the “Create the first federation server in a federation server farm” option and click **Next**.



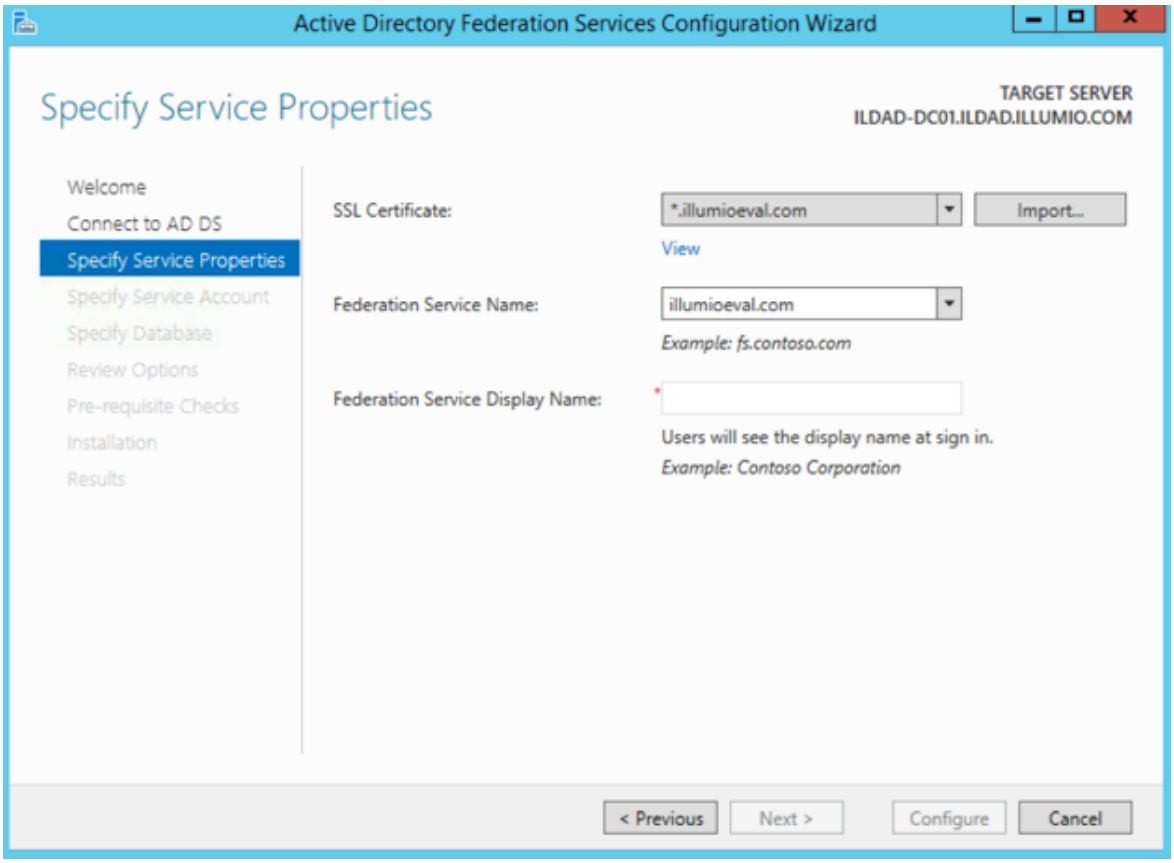
4. Specify a domain admin account for AD FS configuration.



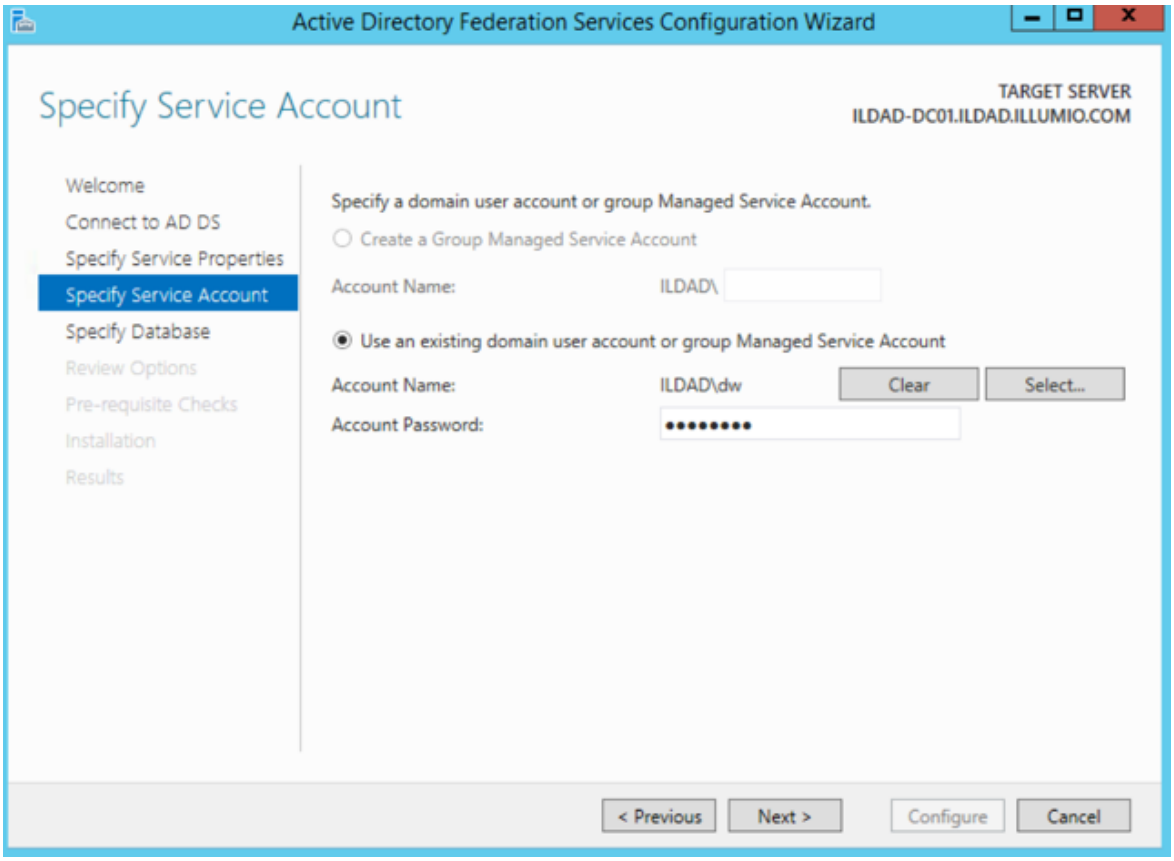
5. Select or import a certificate. This certificate can be a self-signed certificate.



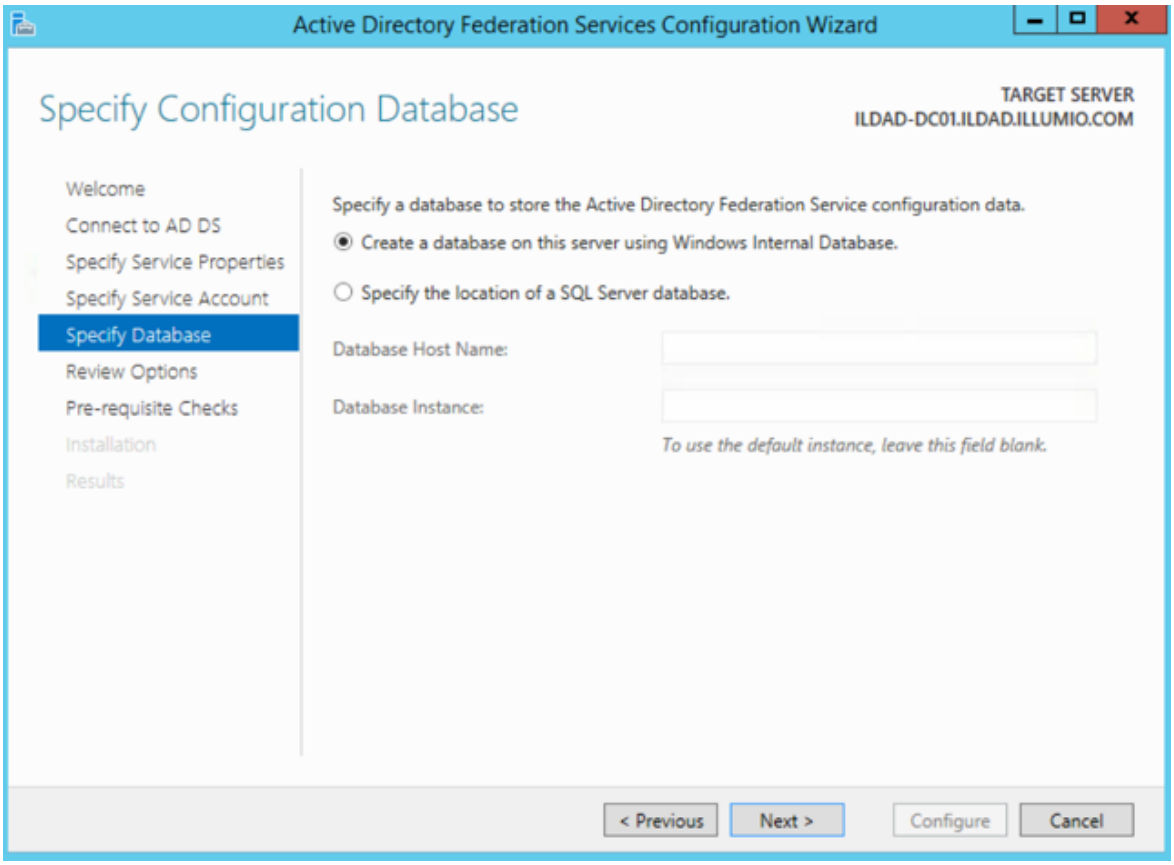
6. Specify your Federated Service Name, enter a display name for this instance of AD FS, and click **Next**.



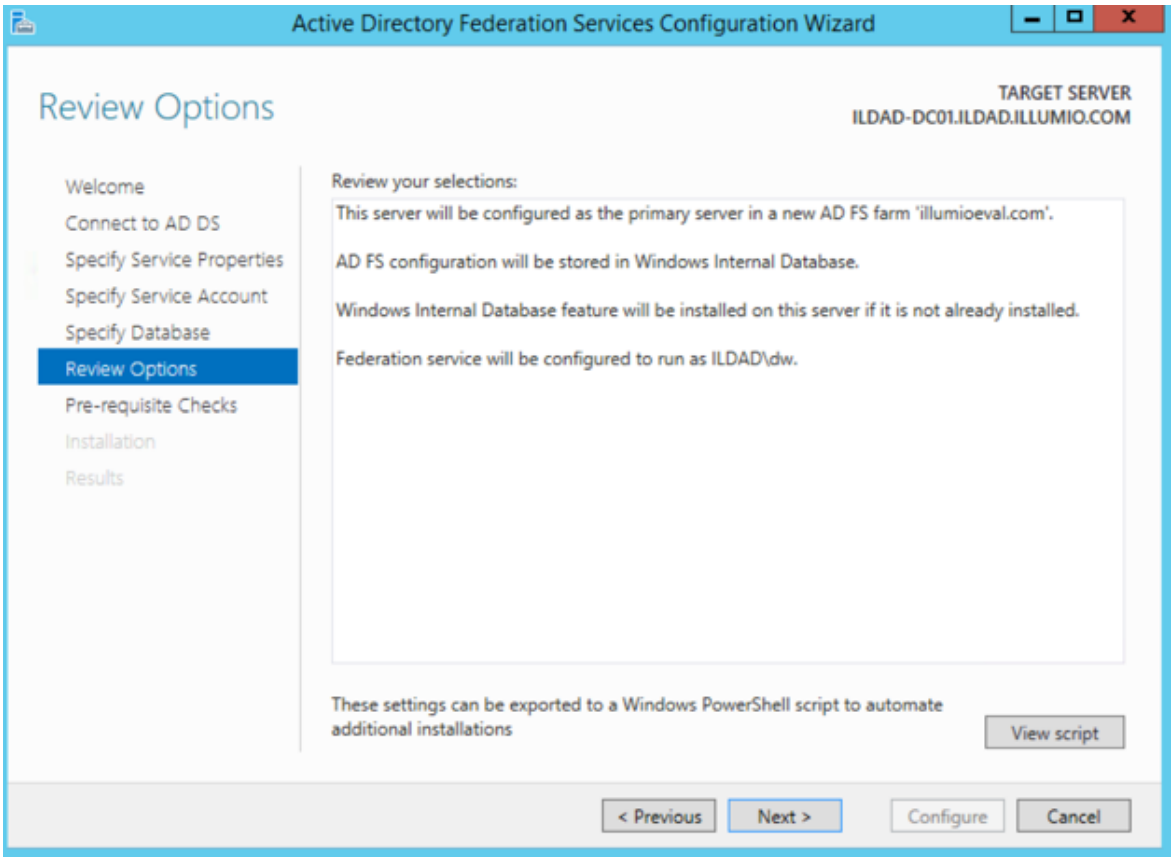
7. Specify your service account and click **Next**.



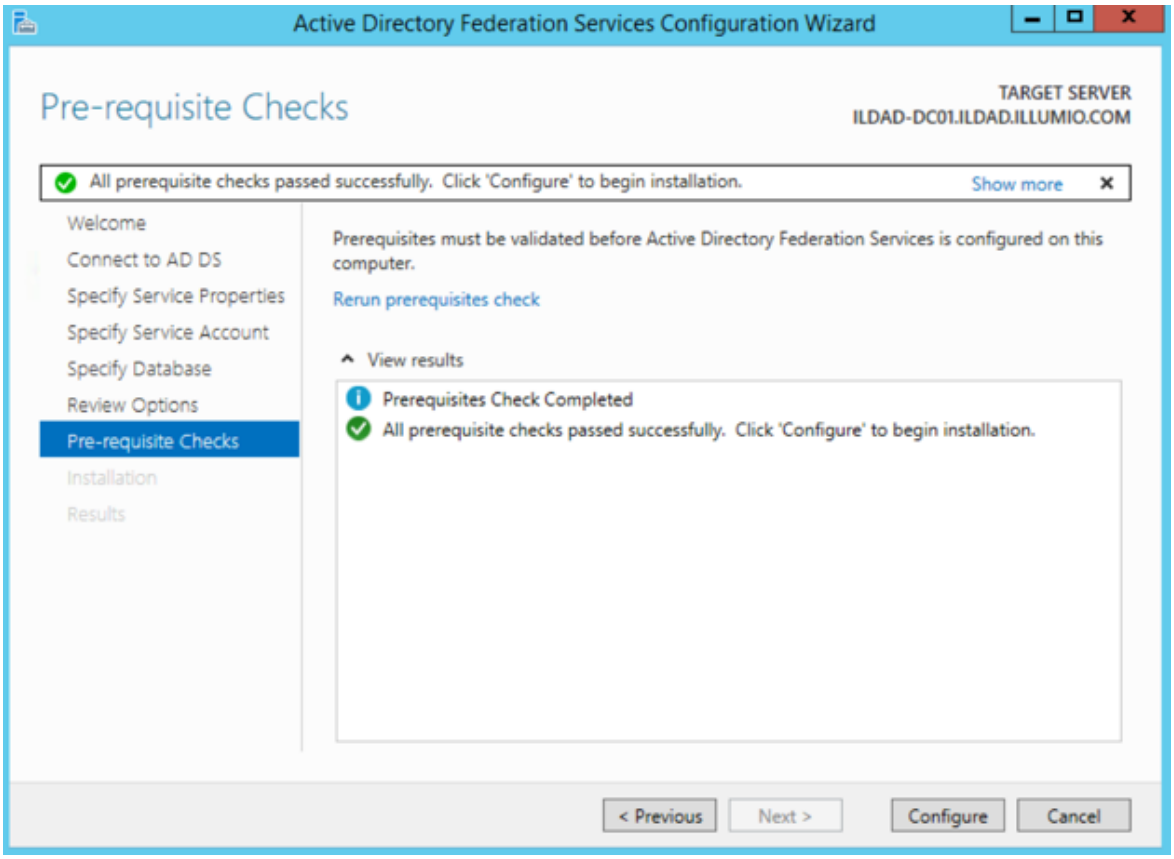
8. Select “Create a database on this server using Windows Internal Database” or choose the SQL server option, and click **Next**.



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



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



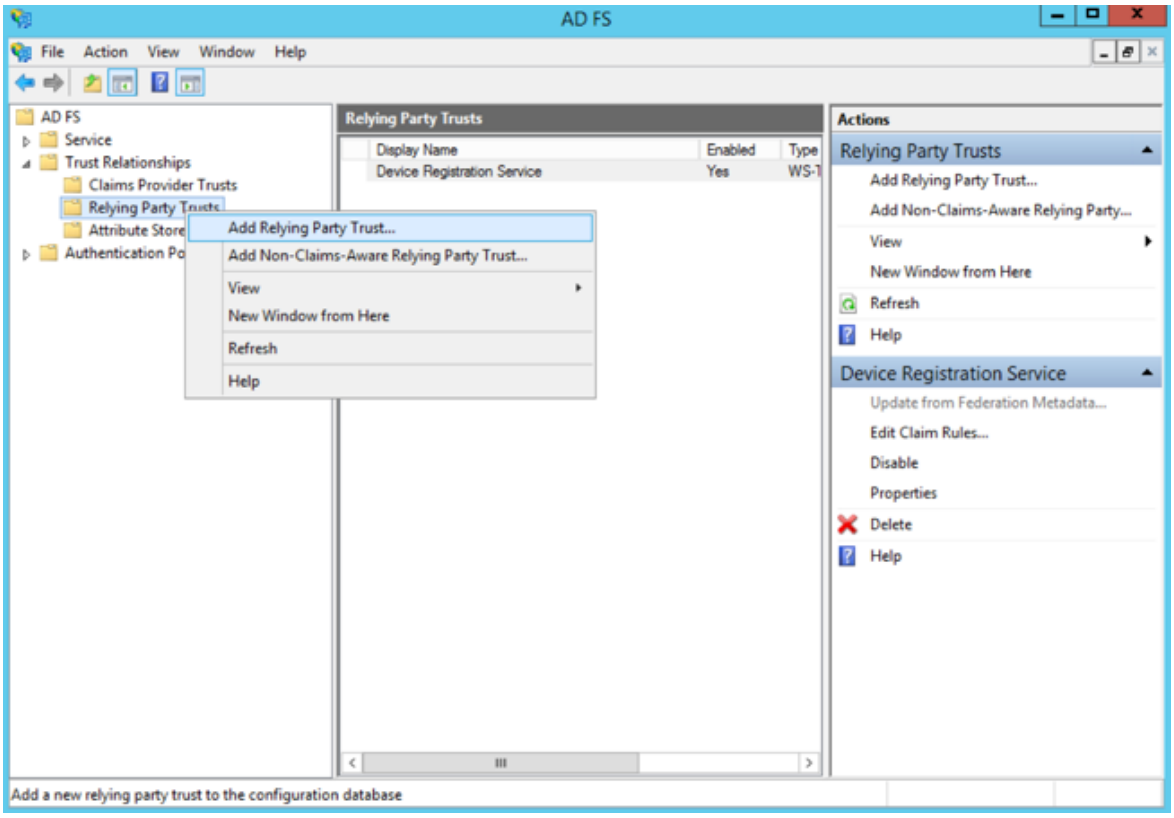
11. In the results screen, click **Close**.

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

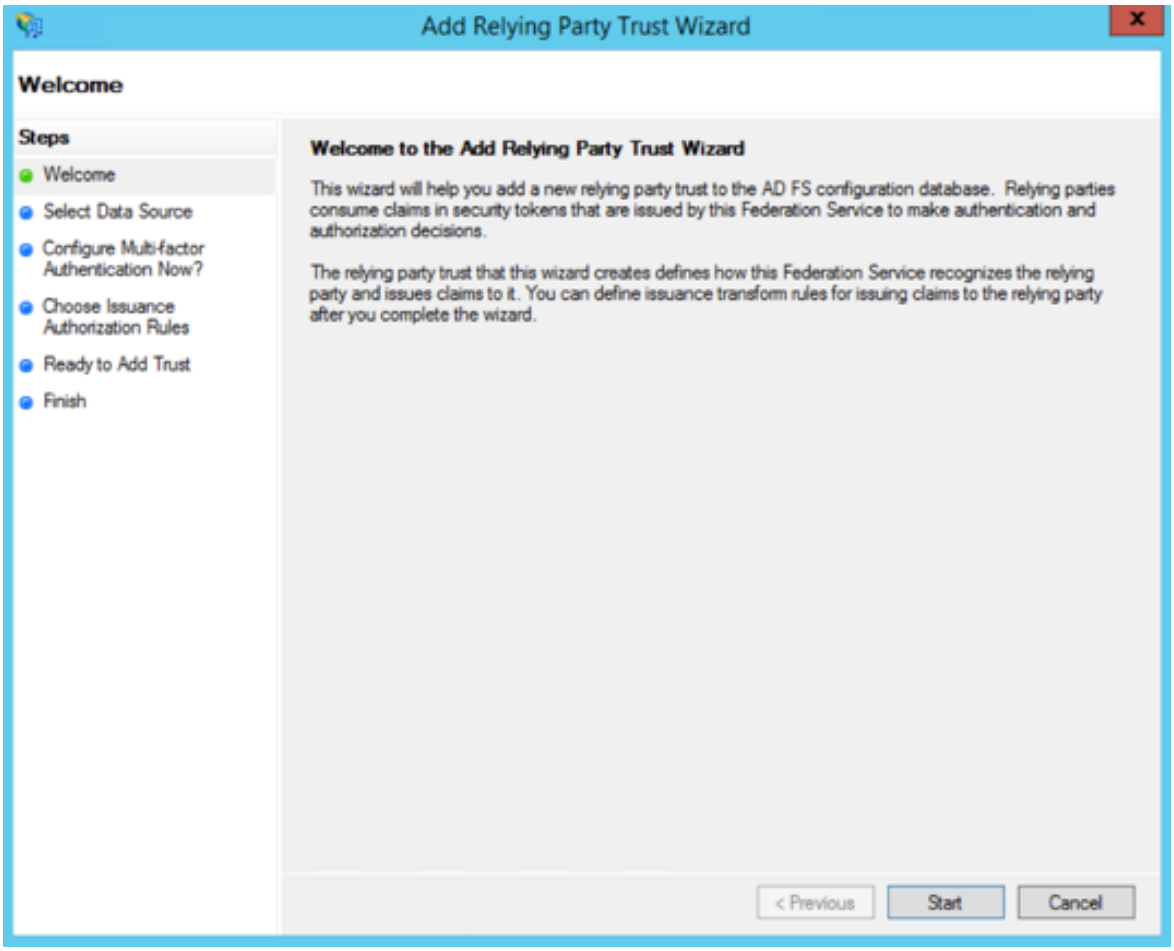
Create a Relying Party Trust

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

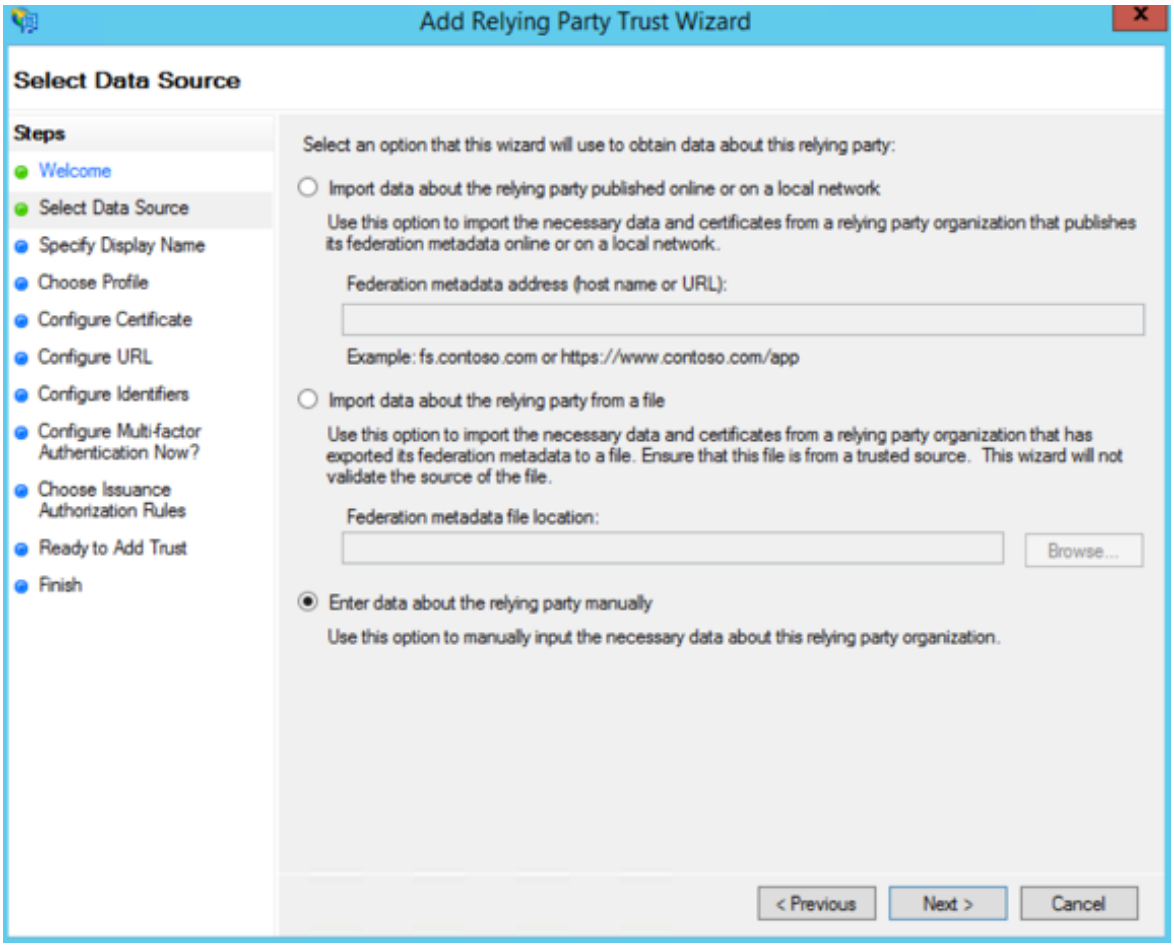
1. From Server Manager/Tools, open the AD FS Manager.
2. From the left panel, choose **Relying Party Trusts** > **Add Relying Party Trust**.



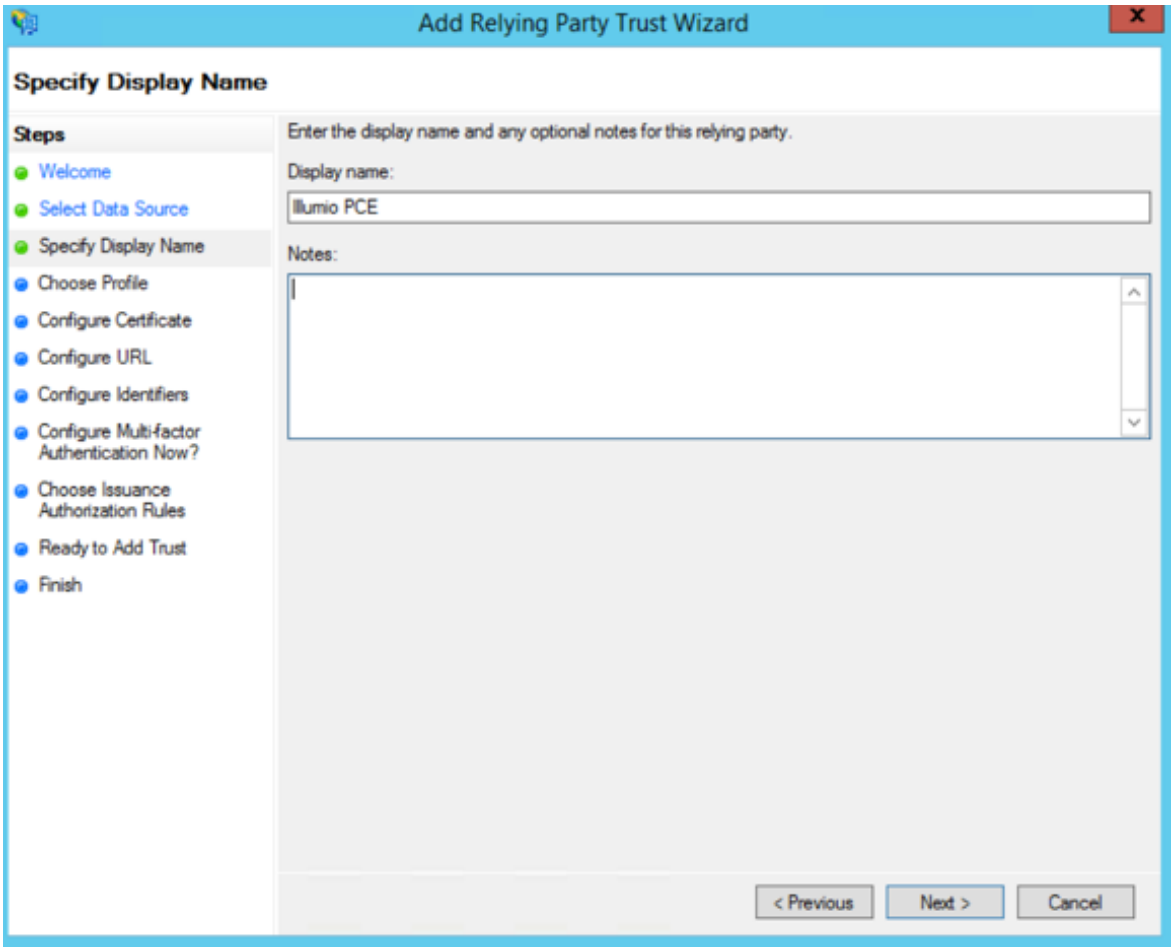
The Add Relying Party Trust Wizard appears.



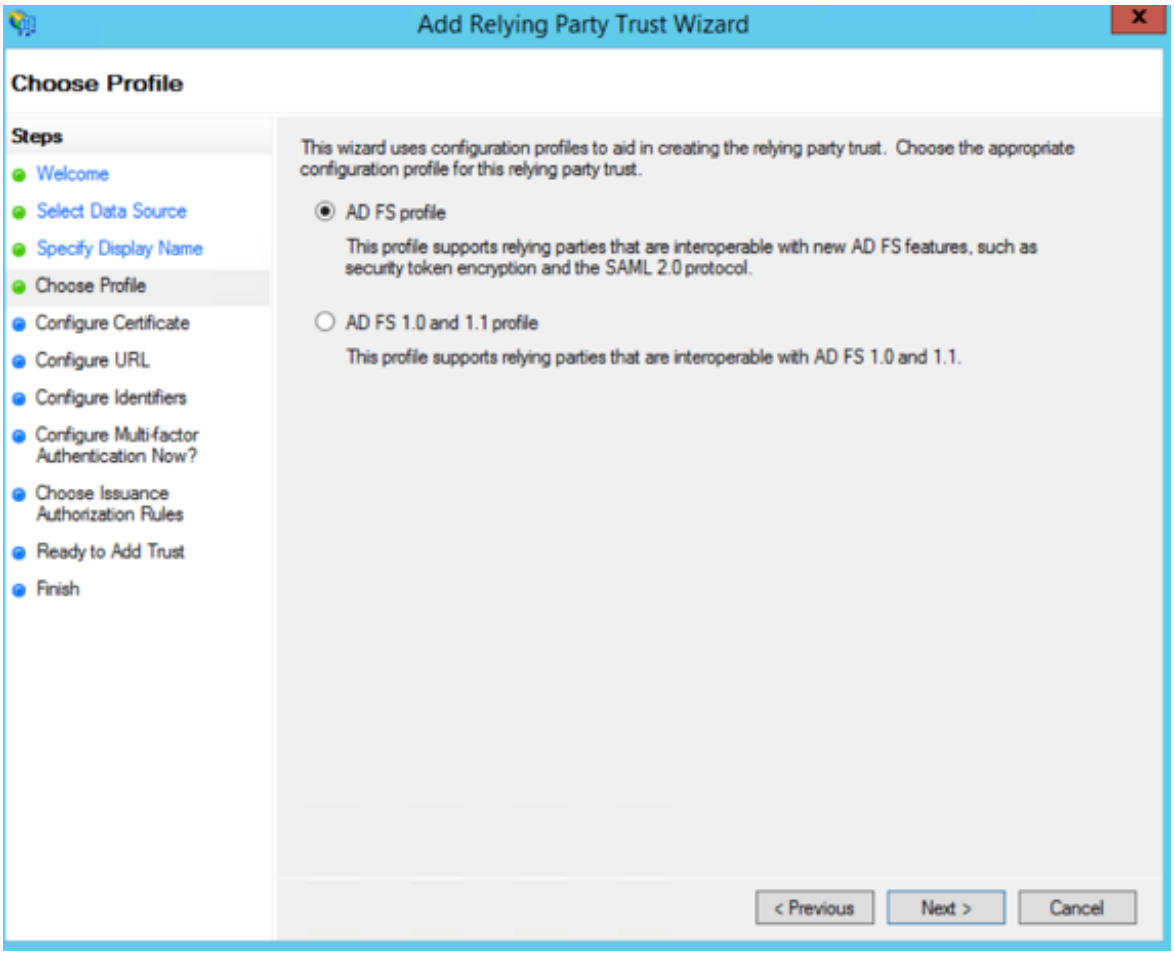
3. Click **Start**.
4. Select the “Enter data about the relying party manually” option and click **Next**.



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

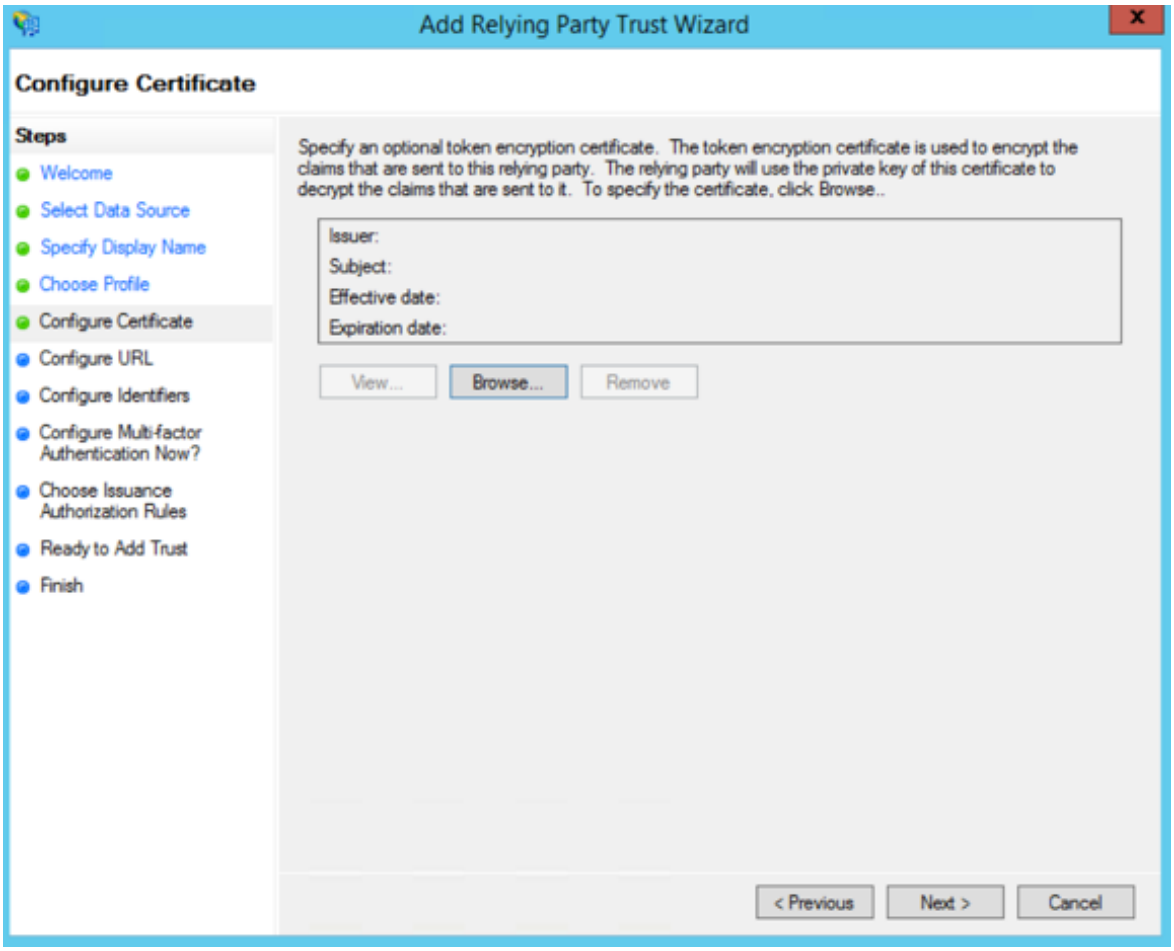


6. Select “ADFS profile” and click **Next**.

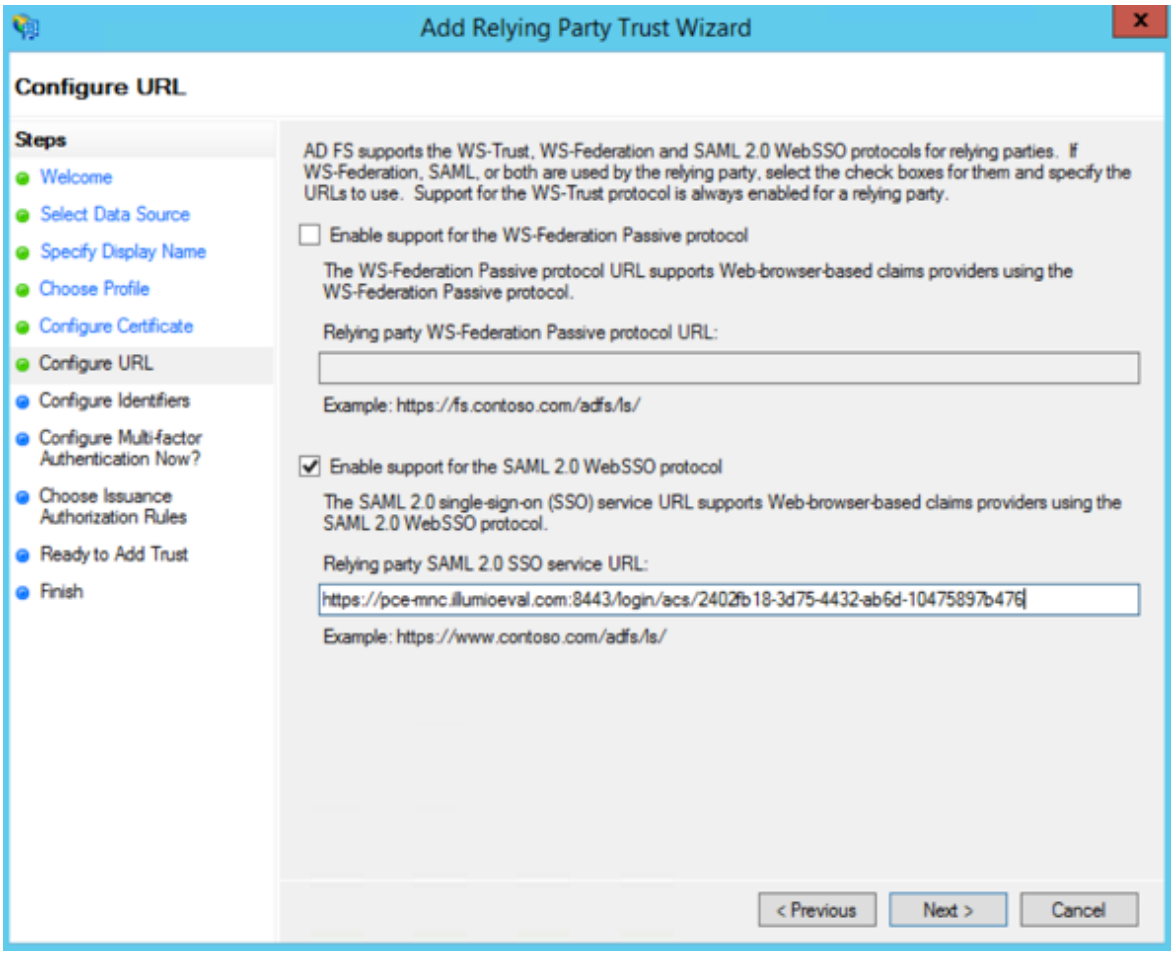


7. When you have a separate certificate for token encryption, browse to, select it, and click **Next**.

> NOTE:
> To use the standard AD FS certificate (created during AD FS installation) for token signing, don't select anything in this step and click **Next**.

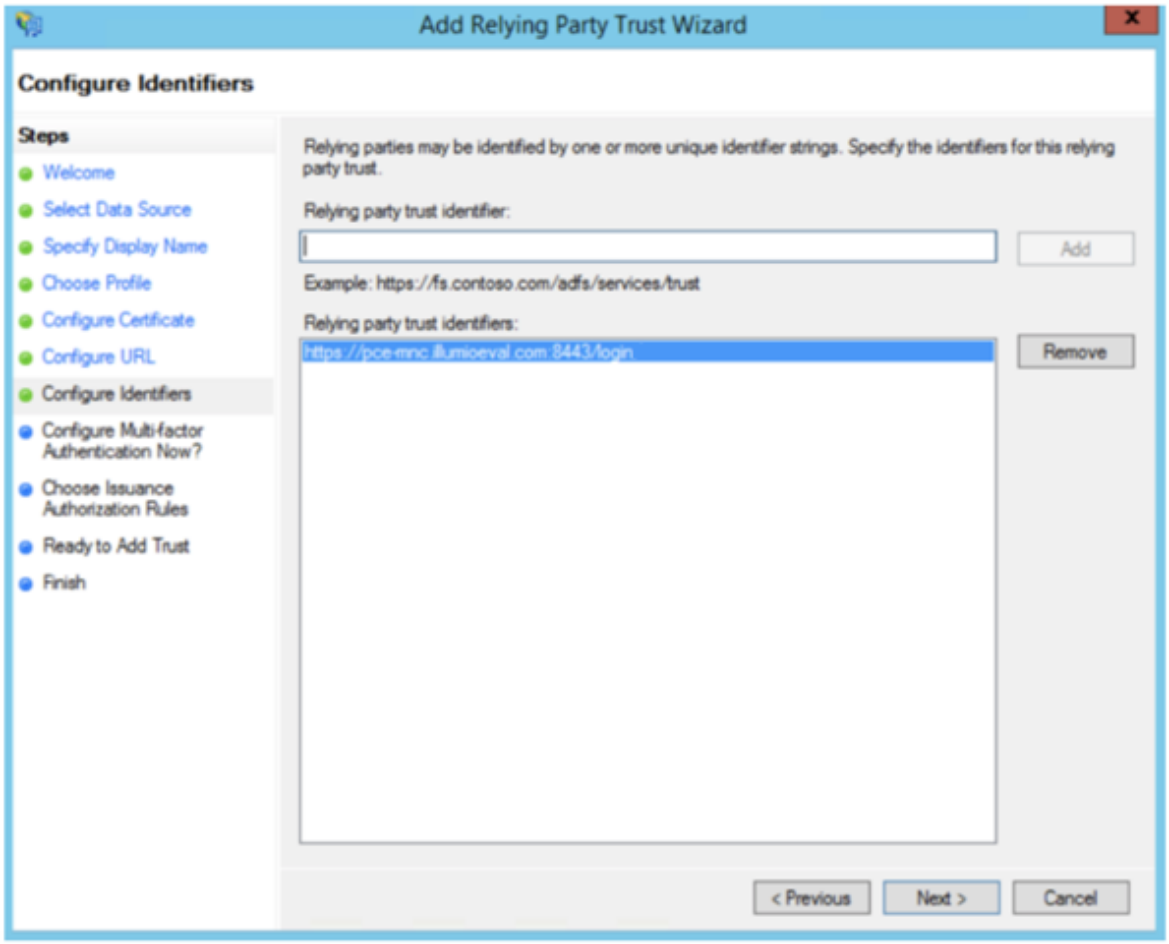


8. Select “Enable support for the SAML 2.0 WebSSO protocol.” In the *Relying party SAML 2.0 SSO service URL* field, add your “Assertion Consumer URL” (obtained from the PCE web console).

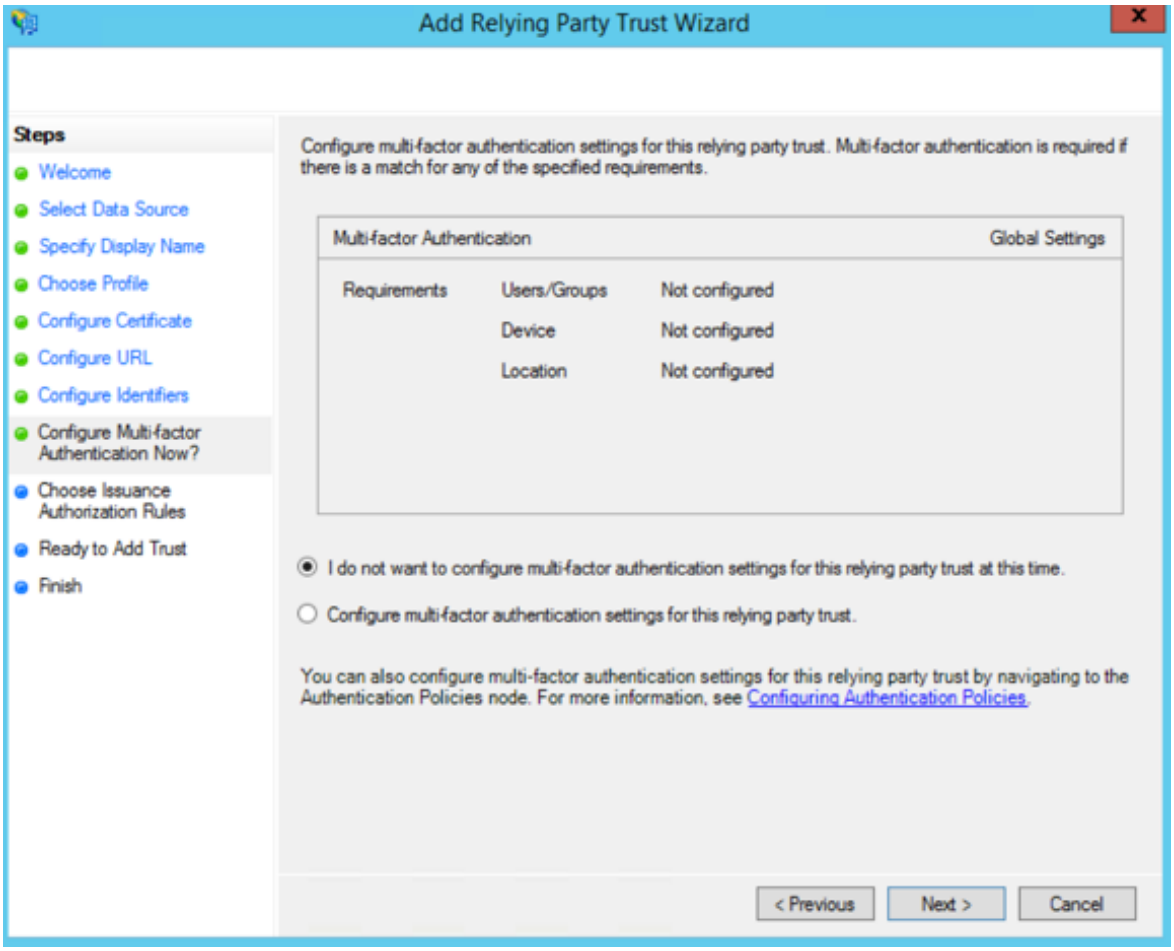


To locate the “Assertion Consumer URL,” in the PCE web console, go to **Access Management** > **Authentication** and click **Configure** in the SAML section. The URL is under **Information for Identity Provider**:

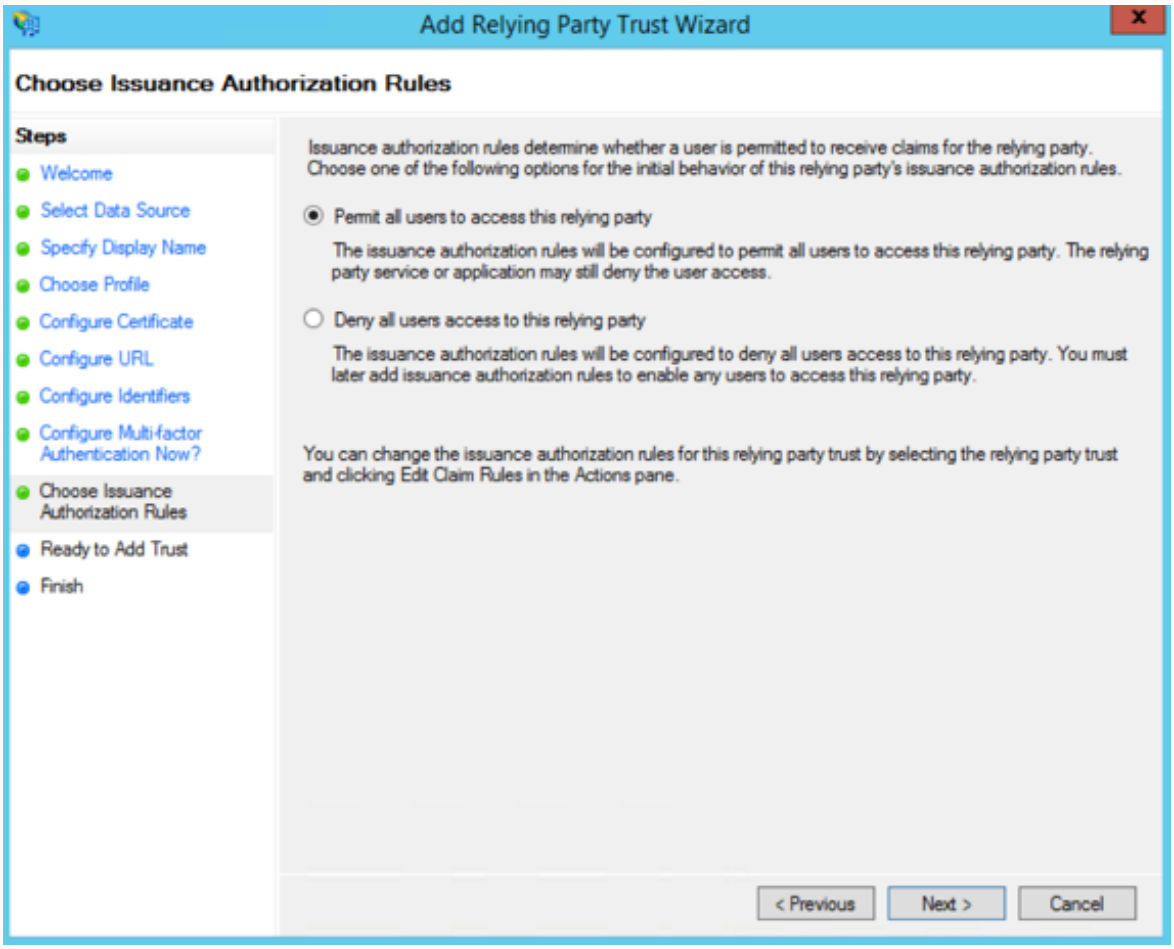
9. On the Configure Identifiers page, use the same URL for the Relying party trust identifier, without the `/acs/<randomNumbers>`. For example: `https://pce-mnc.illumioeval.com:8443/login`. Click **Next**.



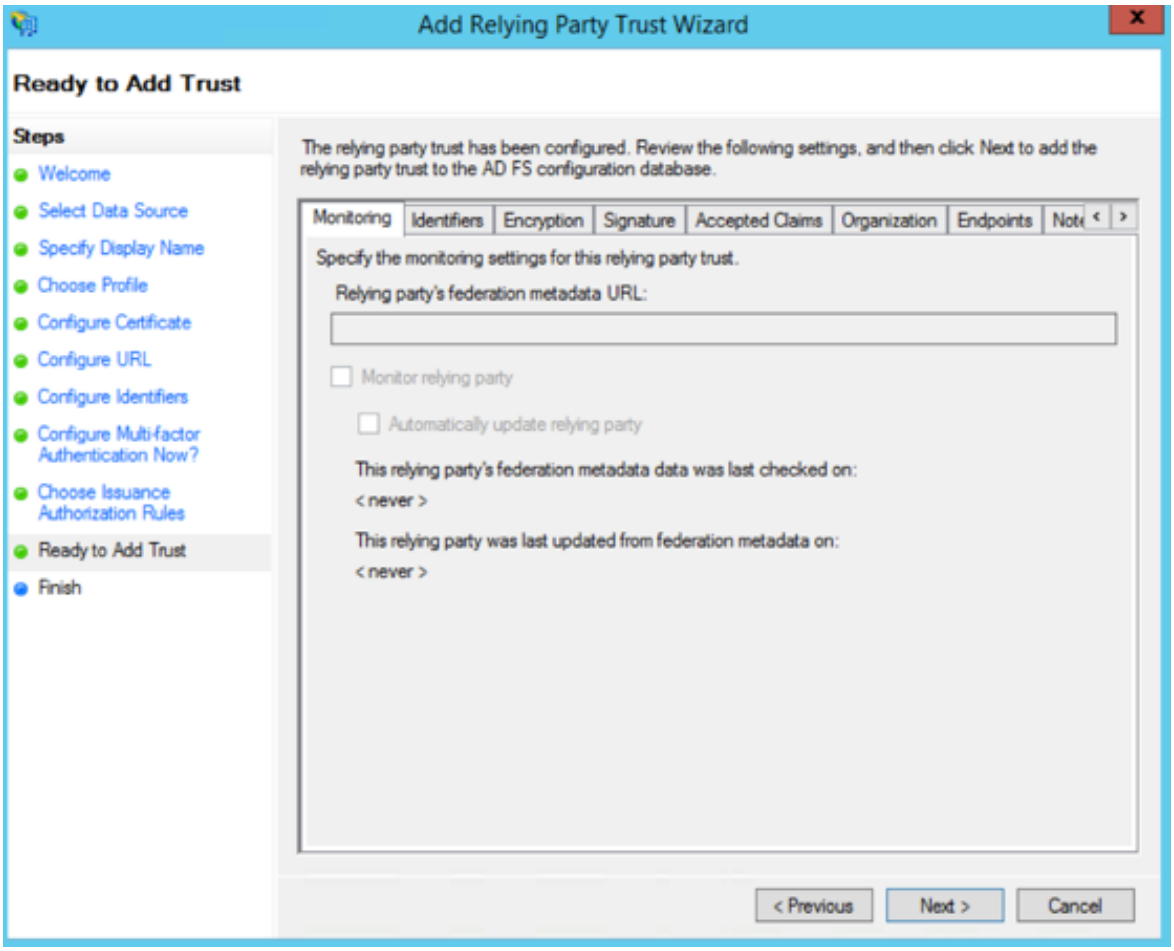
10. Select the “I do not want to configure multi-factor authentication...” and click **Next**.



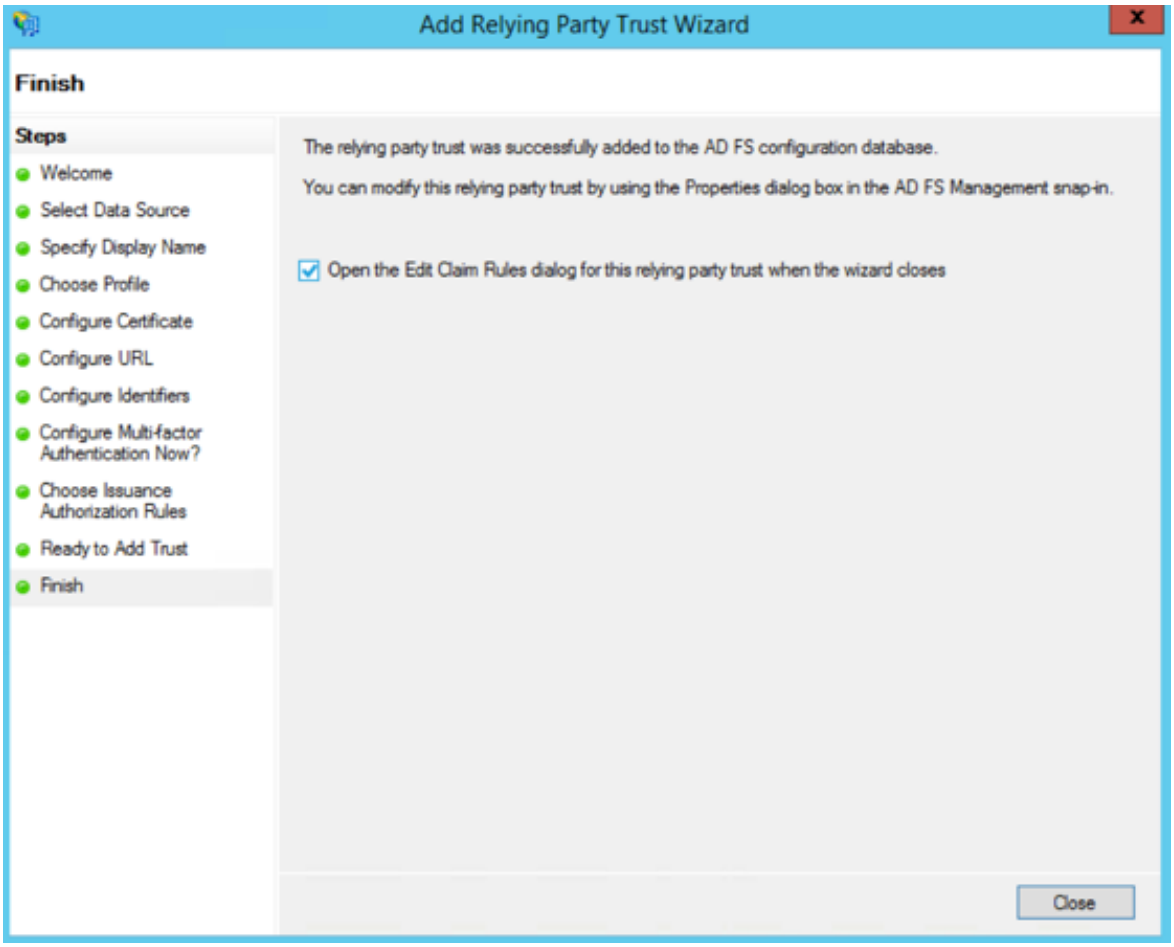
11. Select “Permit all users to access this relying party” and click **Next**.



12. On the Ready to Add Trust page, click **Next**.



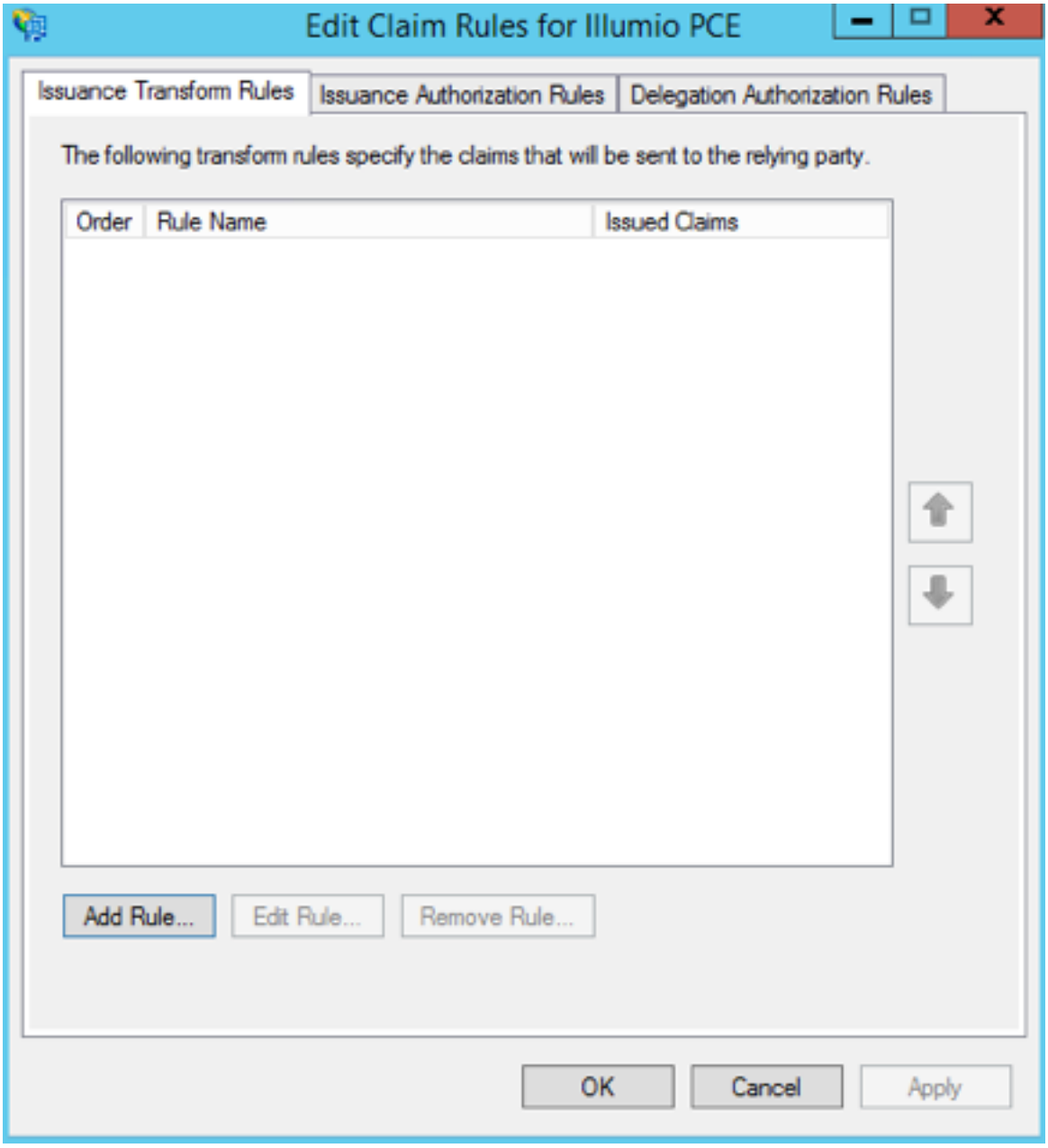
13. Leave the *Open the Edit Claim Rules* checkbox selected and click **Close**.



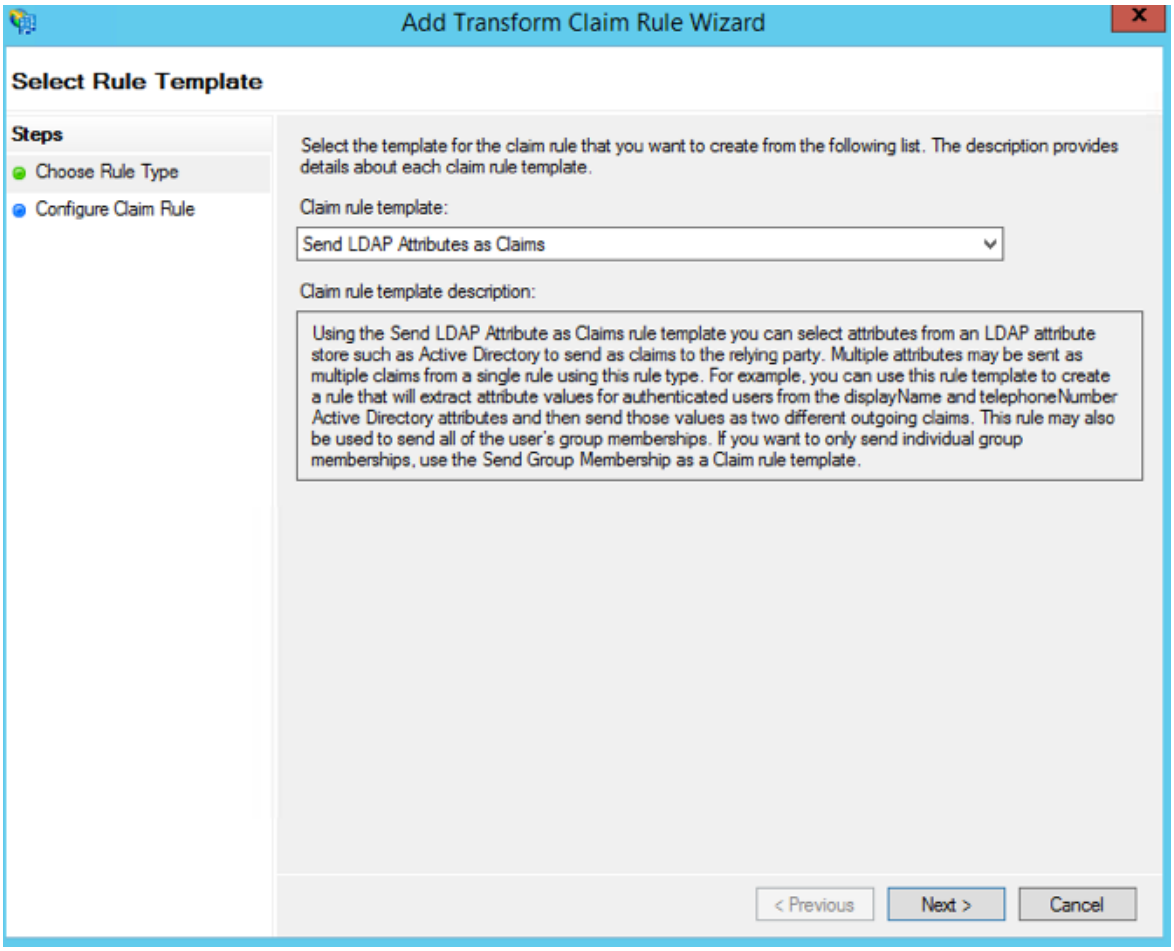
Create Claim Rules

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

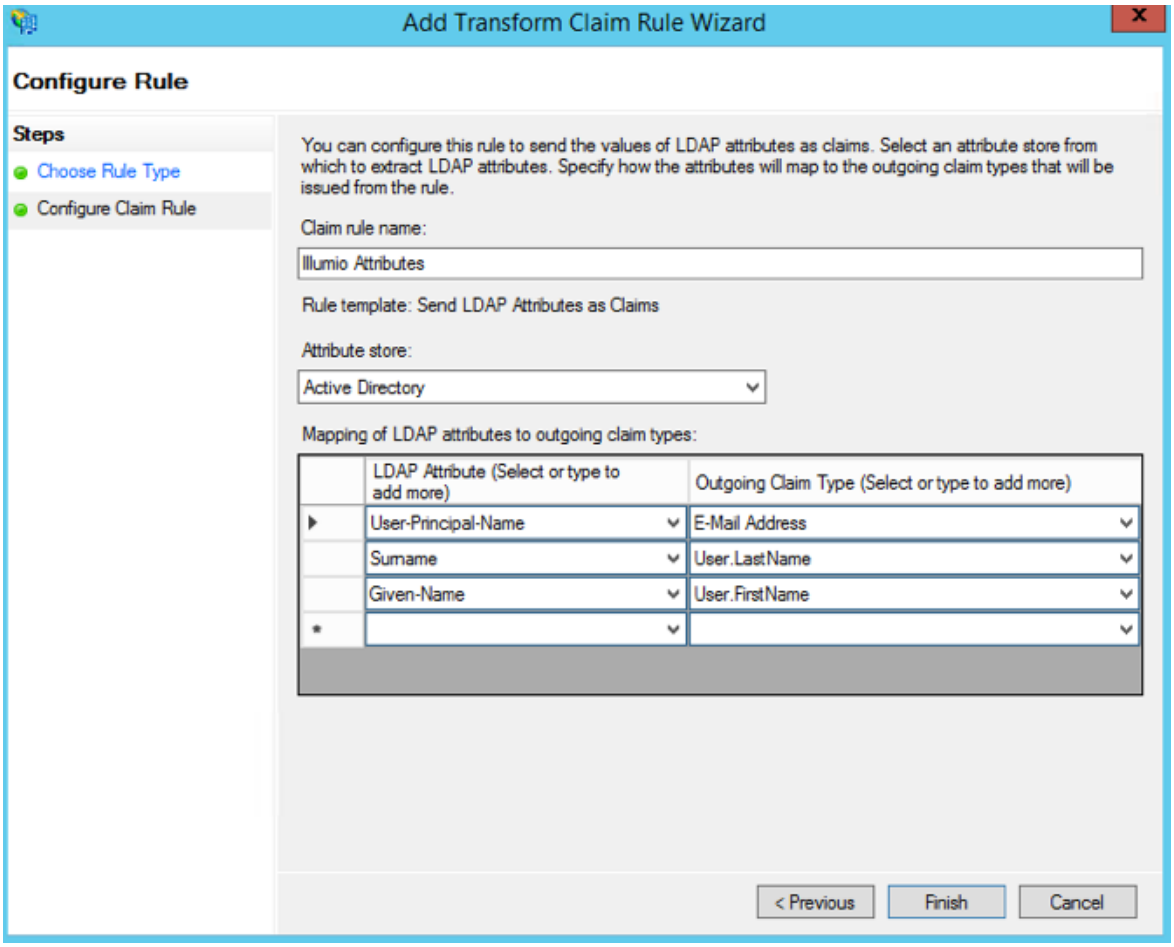
1. In the Edit Claim Rules dialog, click **Add Rule**.



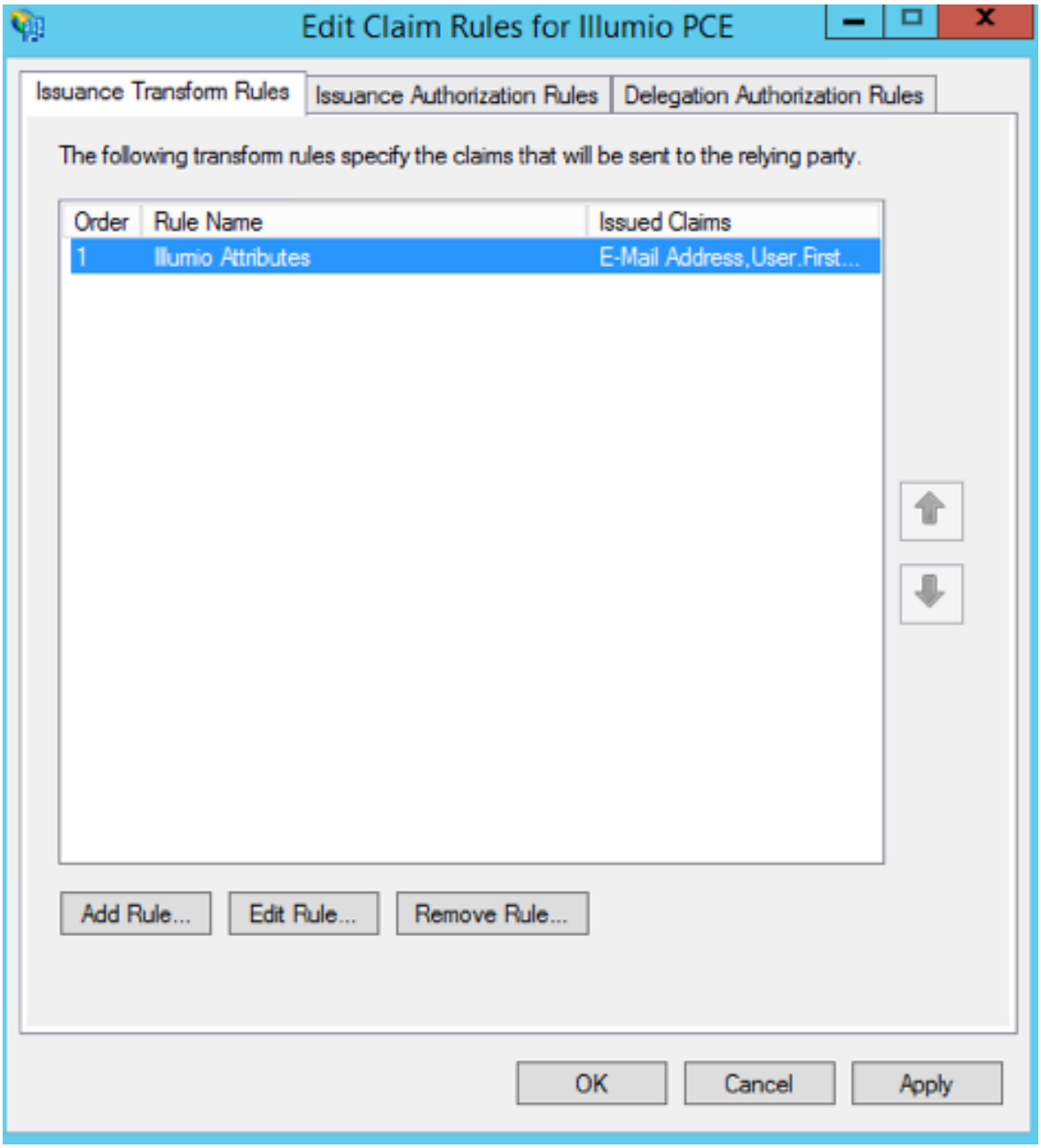
2. Under Select Rule Template, select “Send LDAP Attributes as Claims” and click **Next**.



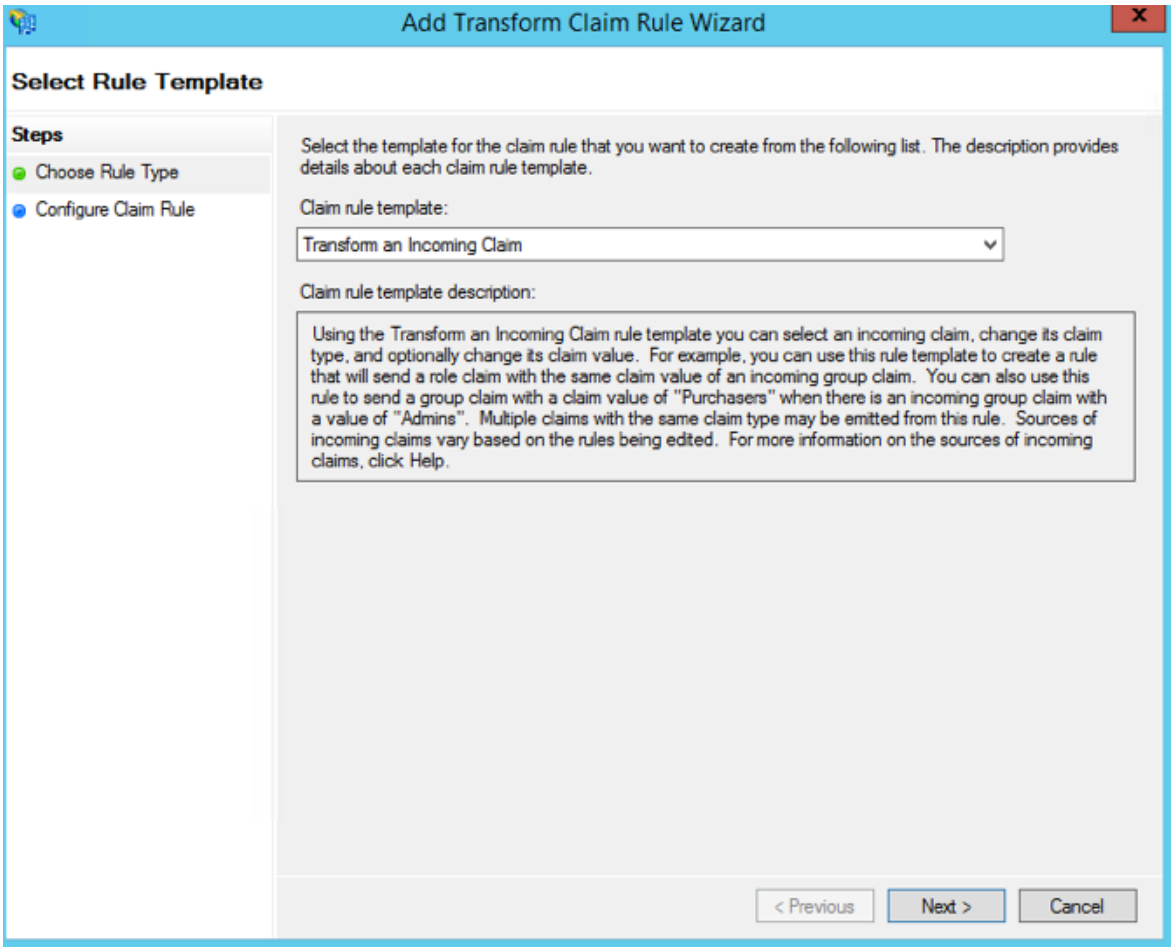
3. Name the Claim rule “Illumio Attributes” and select **Active Directory** as the Attribute store. Under the first attribute, select “User-Principal-Name” and “E-Mail Address” as the outgoing. Select “Surname” and type the custom field name of “User.LastName” in the outgoing field. Repeat the values for “Given-Name” and “User.FirstName” and click **Finish**.



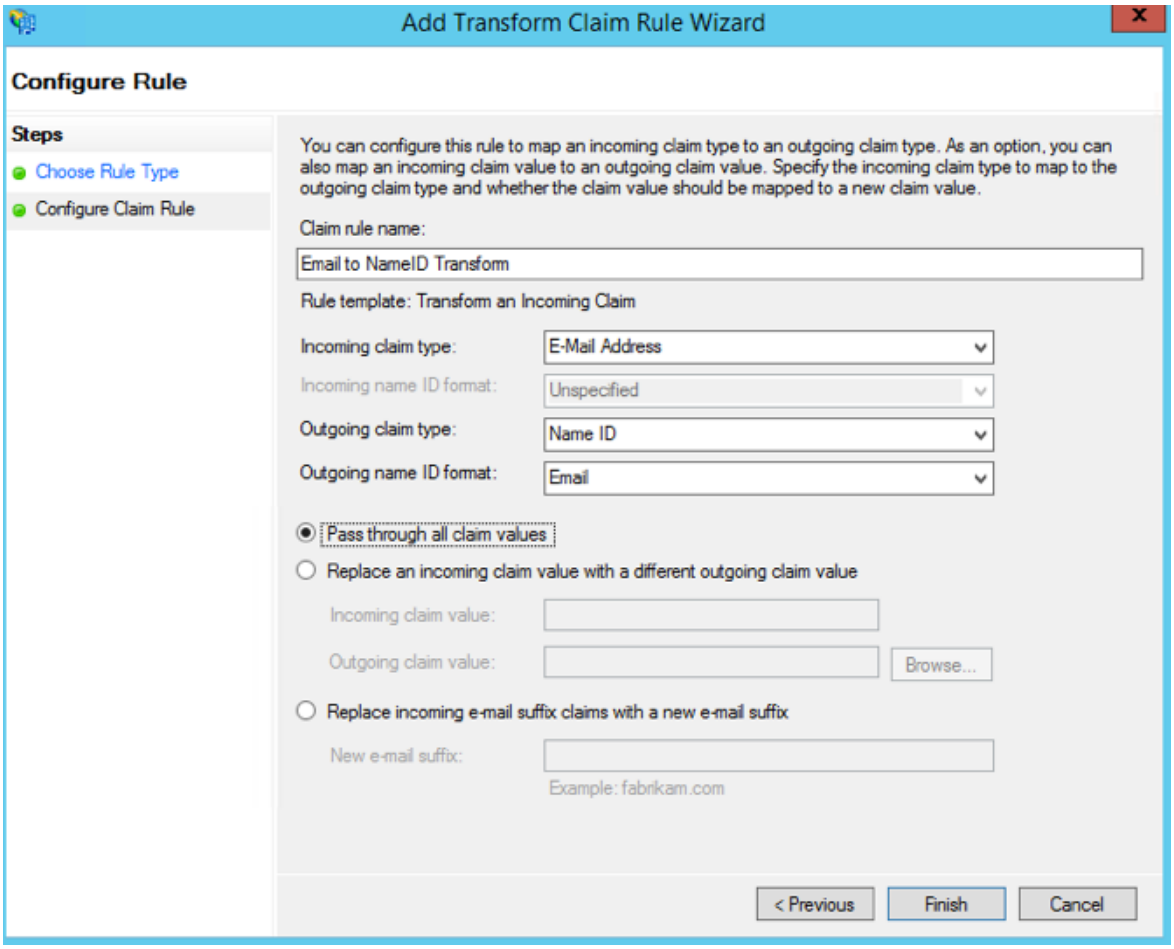
4. In the Edit Claim Rules dialog with your new rule added, click **Add Rule** to add the final rule.



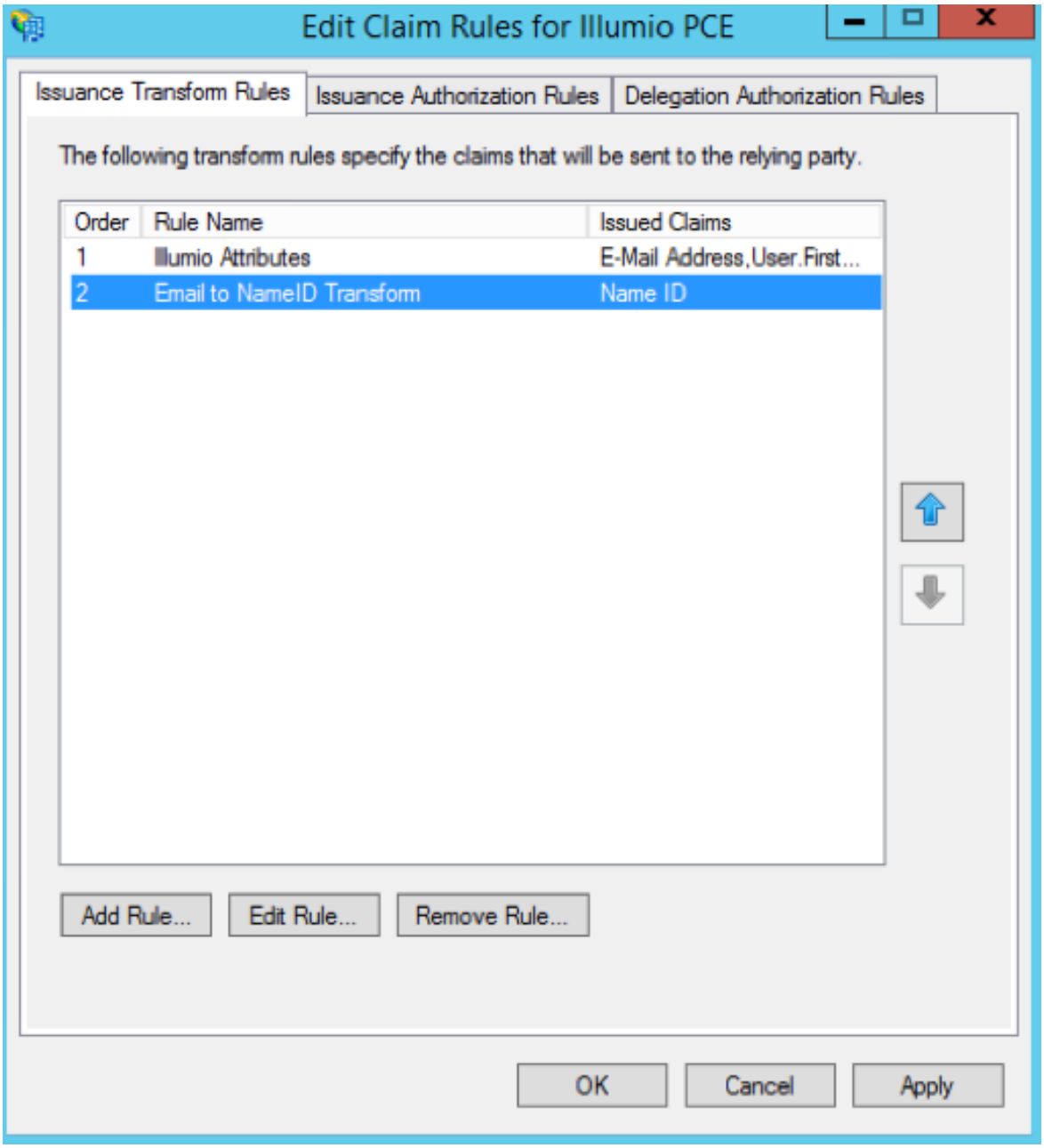
5. Under the Claim Rule Template, select “Transform and Incoming Claim” and click **Next**.



6. Name the rule “Email to NameID Transform” and change the incoming claim type to “E-Mail Address.” Set the Outgoing claim type to “Name ID” and the Outgoing name ID format to “Email” and click **Finish**.



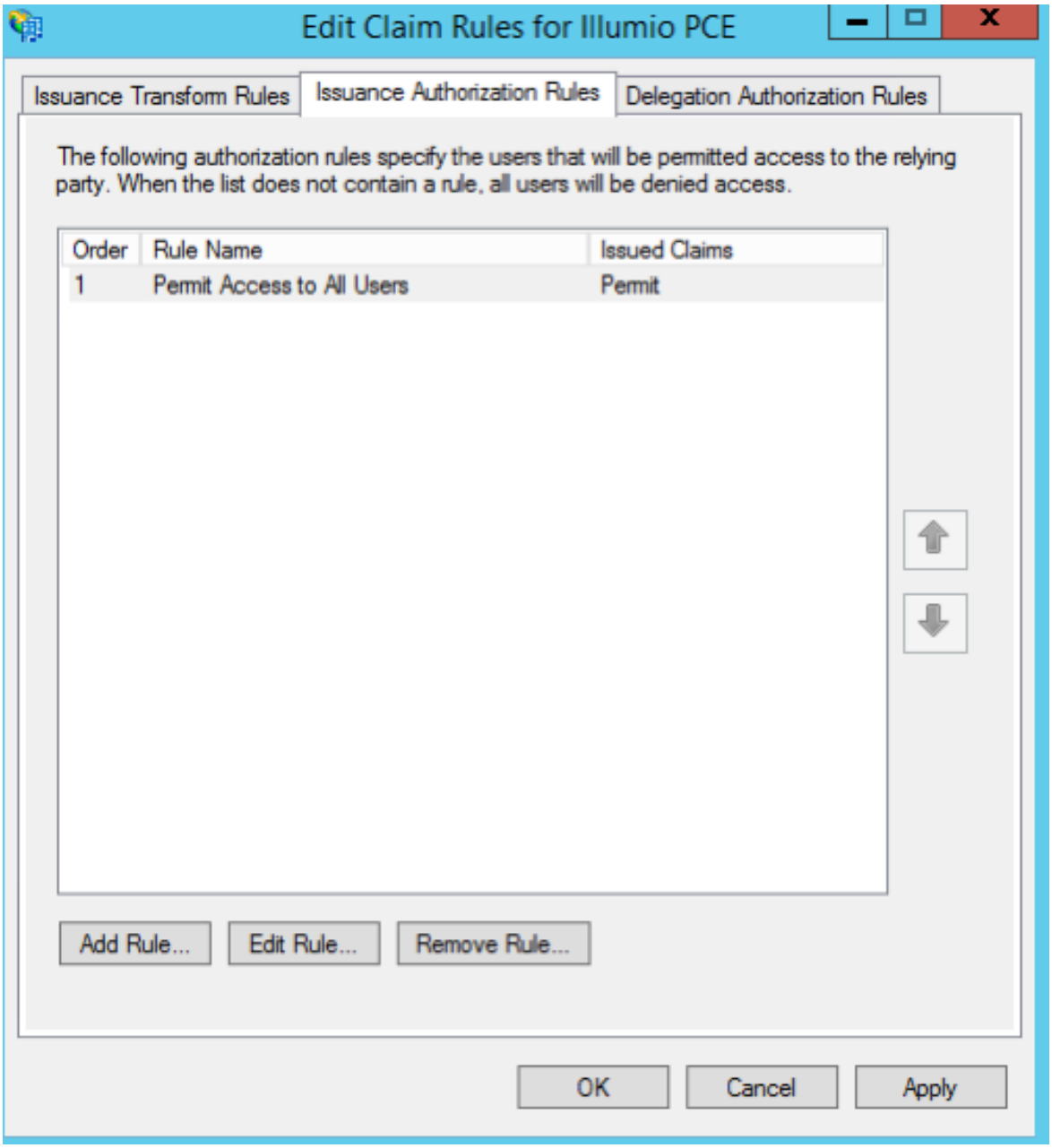
The Edit Claim Rules window opens.



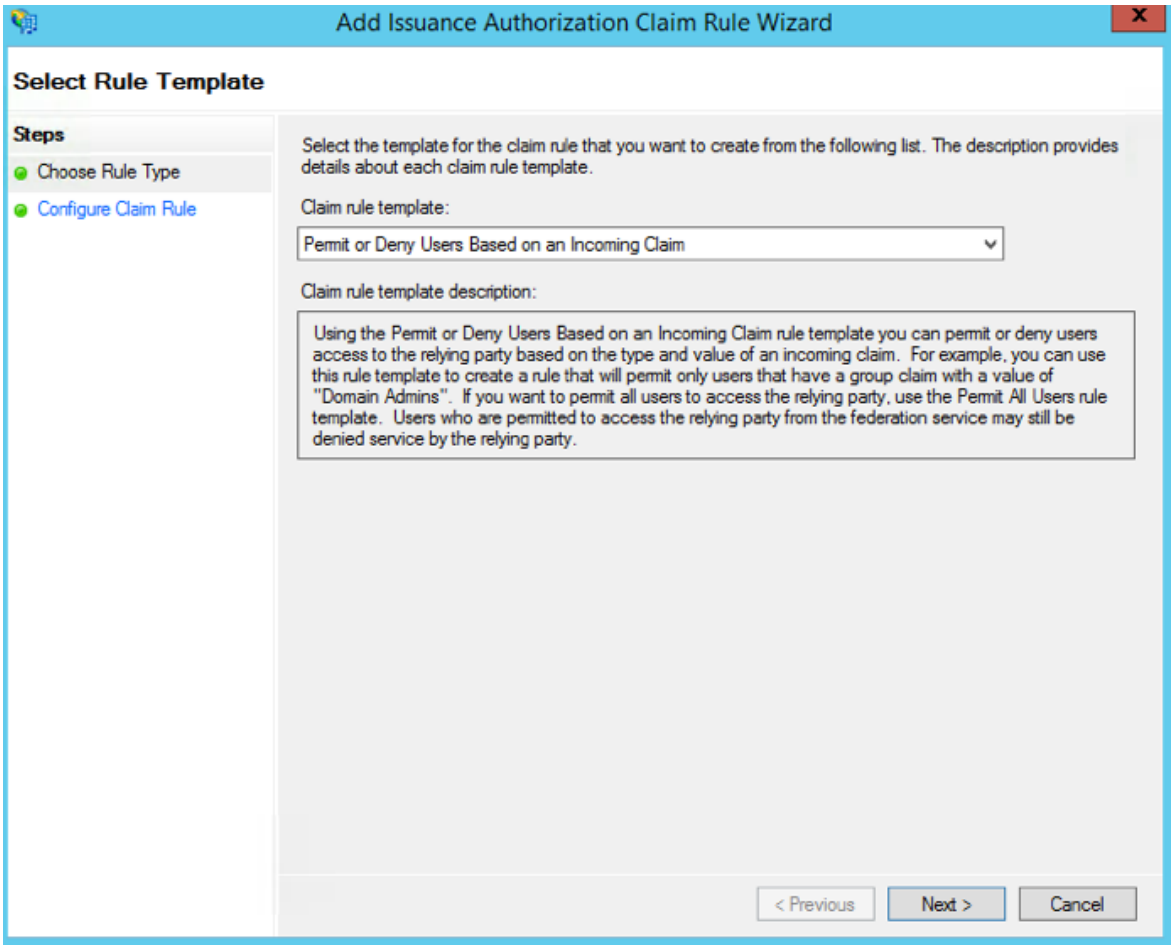
7. (Windows 2016 and Windows 2019) Skip to step 12.

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

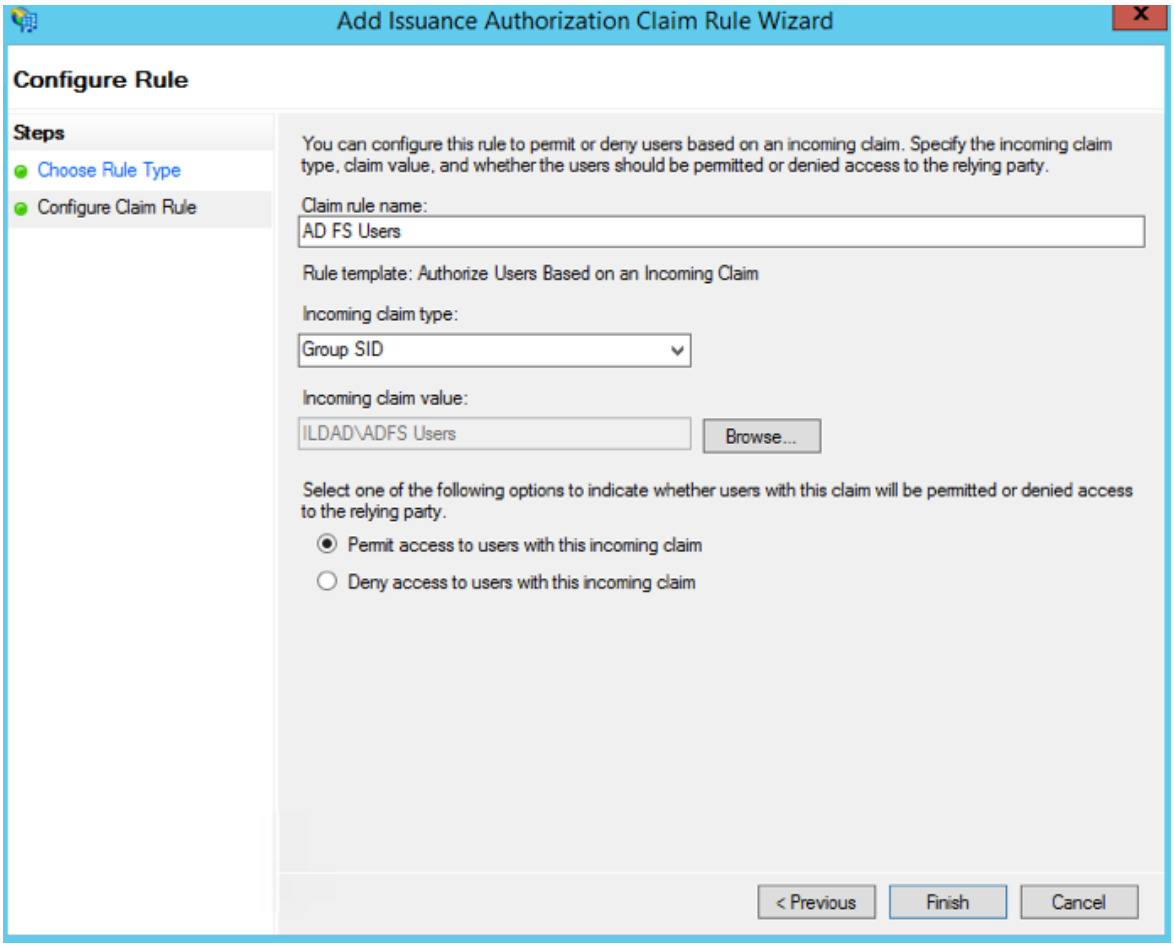
8. Select the Issuance Authorization Rules tab.
9. To allow all your Active Directory Users to access the PCE, leave the “Permit Access to All Users” as is. Otherwise, you should restrict access to a single group or groups of users.



10. Select “Permit or Deny Users Based on an Incoming Claim” and click **Next**.

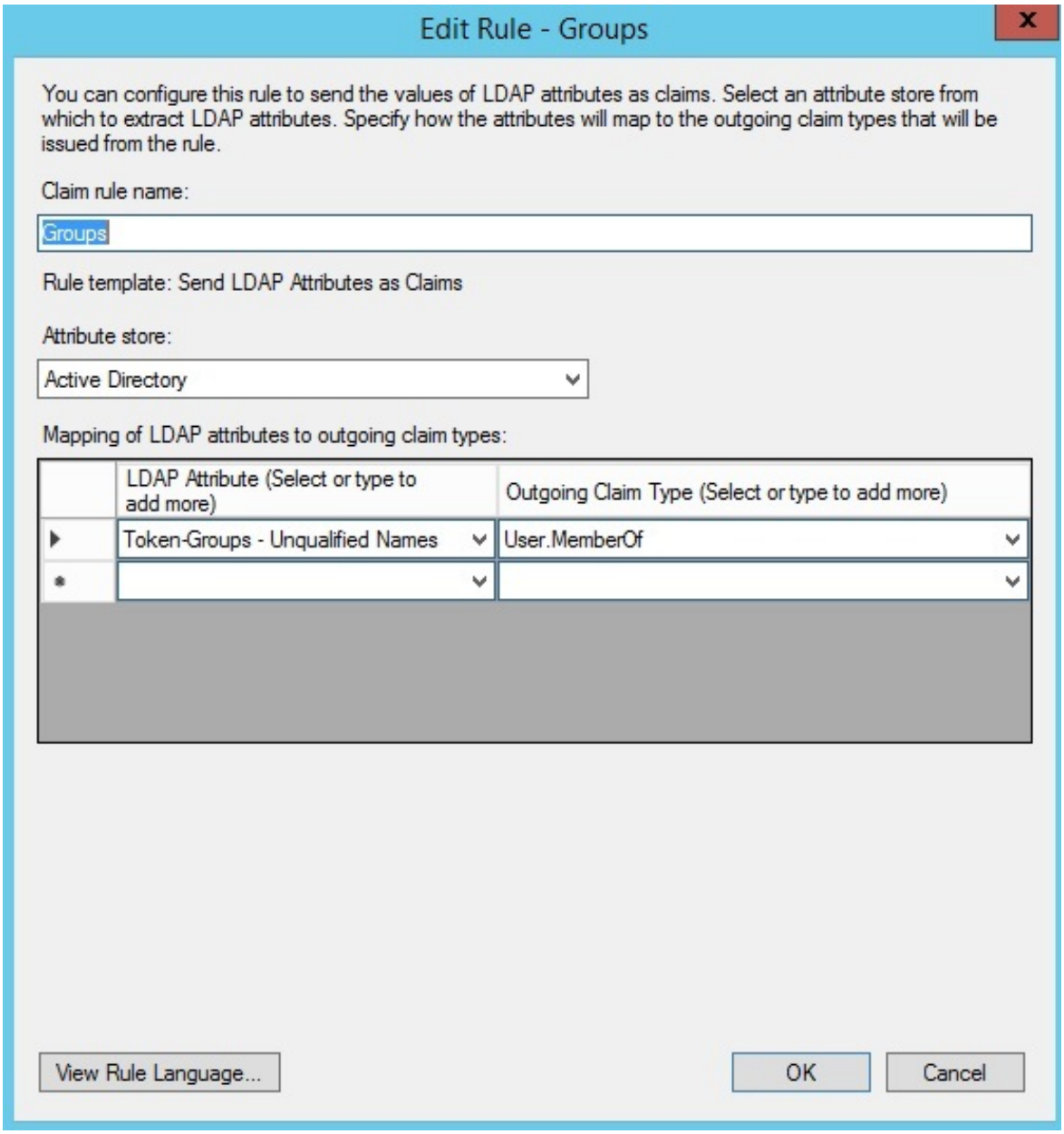


11. Name the rule “AD FS Users” and change the Incoming claim type to “Group SID” (you might have to scroll to find it). In Incoming claim value, browse to the group of users you want to give access. Make sure “Permit access” is selected and click **Finish**.



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

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



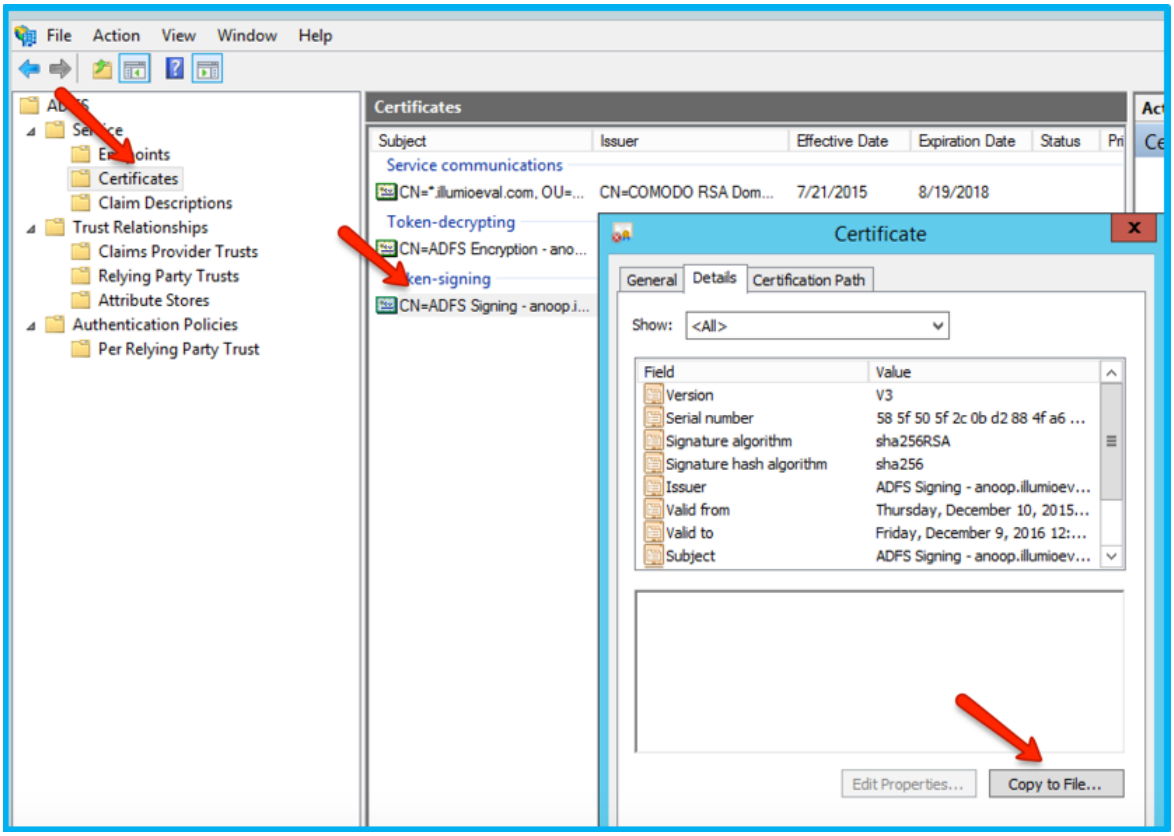
Obtain ADFS SSO Information for the PCE

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

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

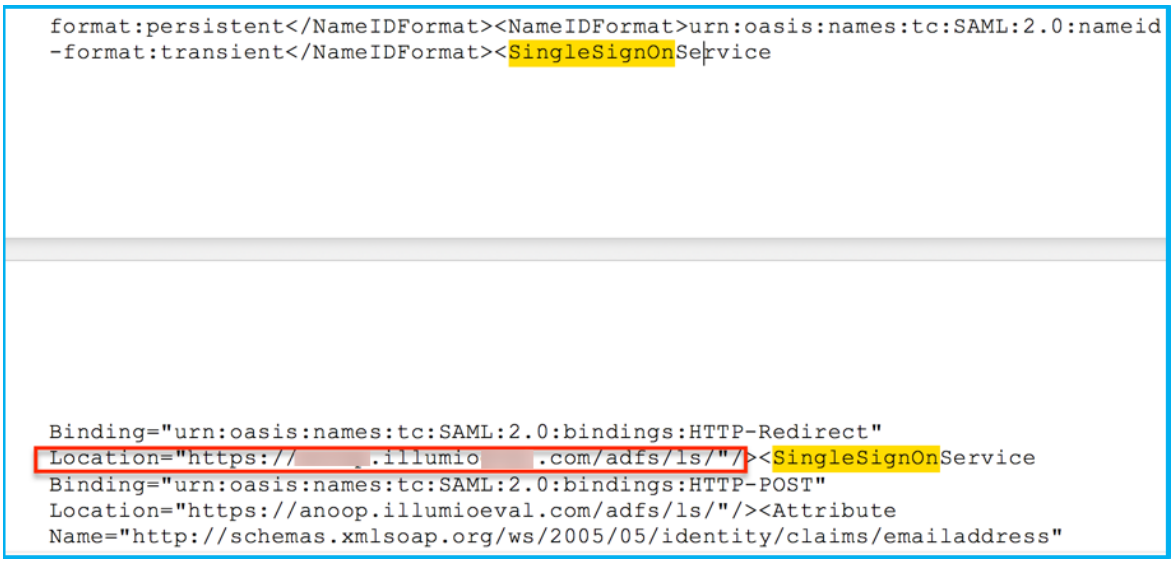
To obtain the AD FS SSO information for the PCE:

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`.



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

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

    Or, a generic logout URL of AD FS:

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

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

Configure the PCE for AD FS SSO

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

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

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

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

To configure the PCE for AD FS:

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

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

7. Click **Save**.

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

Chapter 5

PCE Management

This section describes how to manage the PCE software and how to manage PCE users.

Check the PCE Software Version

To check the installed version running on the PCE go to the PCE navigation menu and click on the down arrow at the very top, right side of the page. Next, select “About Illumio Core” to view the currently installed PCE version.

User Management

Local users are created in the PCE (they are not managed by an identity provider). When local users login to 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 identity provider goes off line or the SAML server is not accessible.

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.

PCE System Account

A system account called `ilo-pce` is used to operate the PCE. The `ilo-pce` account is a system account created when the PCE is installed. This is the only account used to operate the PCE, from starting and stopping to other PCE-related tasks such as backup and restore. This account can not be used to log in to the Linux OS, as it is a system account. This account can not control or install security policies in VENs. This account can not access the PCE Web Console UI and

has no direct access to the database. The `ilo-pce` account is the only system account used by the PCE, and no other accounts are used. The PCE and its services run under this account.

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 Viewer	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.

Roles with Custom Scopes

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

Role	Granted Access
Full Ruleset Manager	• Add, edit, and delete all rulesets within the specified scope. • Add, edit, and delete rules when the provider matches the specified scope. The rule consumer can match any scope. NOTE: You can choose the All Applications, All Environments, and All Locations scope with the Full Ruleset Manager role.
Limited Ruleset Manager	• Add, edit, and delete all rulesets within the specified scope. • Add, edit, and delete rules when the provider and consumer match the specified scope. • Ruleset Managers with limited privileges cannot manage rules that use IP lists, custom iptables rules, user groups, label groups, iptables rules as consumers, or have internet connectivity.

Role	Granted Access
	NOTE: You cannot choose the All Applications, All Environments, and All Locations scope with the Limited Ruleset Manager role.
Ruleset Viewer	• View rules that match the scope. • Can not edit rulesets or rules.
Ruleset Provisioner	Provision rulesets within specified scope. NOTE: You can choose the All Applications, All Environments, and All Locations scope and custom scopes with the Ruleset Provisioner role.
Workload Manager	Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources.
`ilo-pce`	The `ilo-pce` user is a system account created when the PCE is installed. This is the only account used to operate the PCE, from starting and stopping to other PCE-related tasks such as backup and restore.

Setup for Role-based Access Control

This section describes how to configure role-based access control (RBAC) for the PCE.

Add a Scoped Role

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

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

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

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

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

Manage a Local User

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

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

To add a local user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **Local Users** tab.
2. Click **Add**.
3. Enter a name and an email address.
   The email address must use the format xxxx@yyyy.zzzz and be 255 characters or less.
   You can add email addresses with an apostrophe (') in them.
   In the PCE, you can have duplicate names for local users but you cannot have duplicate email addresses.
   The PCE emails the user at the address you specify an invitation with a link to create their Illumio user account. The link in invitation email is valid only for 7 days after which it expires.
4. Select a role for the user:
   - None
   - Global Organization Owner
   - Global Administrator
   - Global Read Only

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:

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

3. Click **Remove**.

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

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

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

To edit a local user:

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

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

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

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

To convert a local user:

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

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

To invite a local user:

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

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

To lock or unlock a local user:

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

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

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

Add or Remove an External User

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

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

To add an external user:

1. From the PCE web console menu, choose **Role-Based Access** > **Users and Groups** > **External Users** tab.
2. Click **Add**.
3. Enter a name and an email address or username.
   Whether you enter an email address or username for the user depends on how you have configured your IdP to identify corporate users.
   The username can contain up to 225 alphanumeric and special characters (. @ / _ % + -).
   In the PCE, you can have duplicate names for external users but you cannot have duplicates email addresses or usernames.
   When your IdP is configured to identify users by using email addresses, the PCE emails the user at the address you specify an invitation with a link to create their Illumio user account.
   If your IdP is configured to use usernames, you must provide the user your Illumio PCE web console URL.

4. Select a role for the user:
    - None
    - Global Organization Owner
    - Global Administrator
    - 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:

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

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

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

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

Add or Remove an External Group

The RBAC feature in Illumio Core integrates with the user groups maintained in your corporate IdP so that you can manage user authentication centrally for the Illumio Core. In the PCE, you assign roles and scopes to the groups managed by your IdP to control the access that Illumio users have to their Illumio managed resources.

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

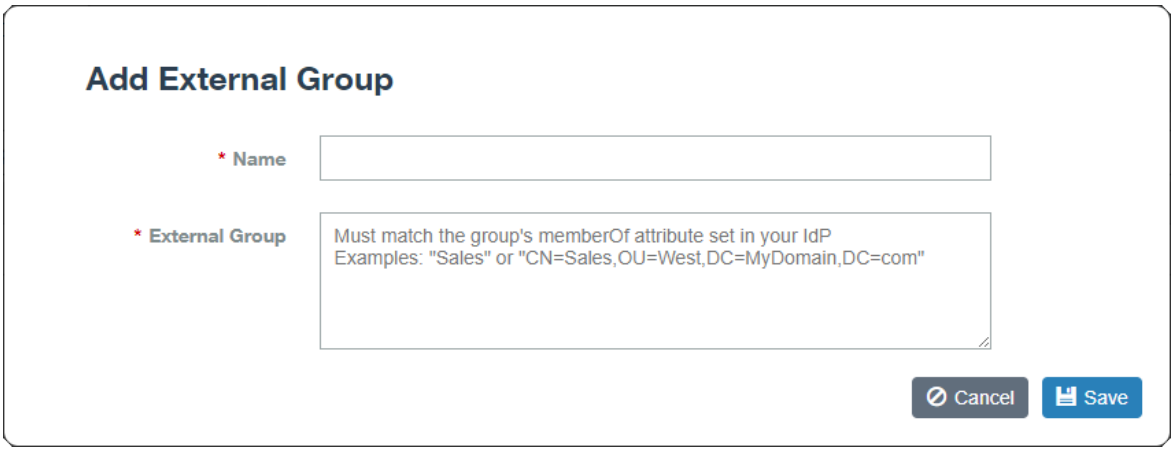
When a user who is a member of an external group logs into the PCE, the corporate IdP authenticates the user and returns the list of groups the user belongs to. For each of those groups, the

PCE determines what roles and scopes are assigned to the group. The user is granted access to the resources associated with the roles and scopes.

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

To add an external group:

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



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

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

5. Click **Save**.

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

To remove an external group:

1. From the PCE web console menu, choose **Access Management** > **External Groups**.
2. Select the external group you want to remove.
3. Click **Remove Group**.

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

If Read Only User access to the PCE is enabled, the external group members can still log into the PCE and view resources after you remove the group.

Change Users and Groups Added to Roles

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

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

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

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

Chapter 6

Common Criteria for the VEN

This section provides information about how to configure Common Criteria for the VEN.

FIPS Compliance for VEN

This section describes the operational requirements for compliance with Federal Information Processing Standard (FIPS) 140-2 for the VEN.

The candidate VEN version is Windows 10 Enterprise.

Enable Windows VEN FIPS Compliance

Windows 10 Enterprise must be configured conforming with Section 2 of the NIST Microsoft Windows FIPS 140 Validation Security Policy Document.

FIPS-related Government and Vendor Documentation

- Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules
- NIST Microsoft Windows FIPS 140 Validation Security Policy Document

Enable FIPS Compliance for Windows VENs

Windows VEN is FIPS compliant when installed on Windows 10 Enterprise.

1. Before activating the VEN, configure FIPS mode as described in the documentation provided by Microsoft. See "Step 3: Enable the FIPS security policy" in FIPS 140-2 Validation on the Microsoft Learn website.
2. Activate the VEN.

Pairing VENs

Illumio Core relies on authentication (role-based access control) to deliver security at enterprise scale. The PCE allows two roles to perform VEN pairing: the “Global Organization Owner” and “Global Administrator”. These roles 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.

Pairing is the process of installing a VEN on a workload.

When you pair a workload, you run a script that installs the VEN on the workload. The VEN then reports detailed workload information to the PCE, such as all services running on the workload, all of its open ports, details about the operating system, workload location, and more.

When you configure and then provision rules, the PCE calculates and configures policy for each paired workload.

When you pair workloads, you can choose to place those workloads in one of these policy states:

Enforcement Mode for Policy

You can choose one of the enforcement modes for workloads when you pair them:

- **Idle**: A state in which the VEN does not take control of the workload’s WFP, but uses workload network analysis to provides the PCE relevant details about the workload, such as the workload’s IP address, operating system, and traffic flows. This snapshot is taken every ten minutes.

  > NOTE:
  > SecureConnect is not supported on workloads in the Idle policy state. If you activate SecureConnect for a rule that applies to workloads that are in both Idle and non-Idle policy states, it could impact the traffic between these workloads.

- **Visibility:** In the Visibility Only state, the VEN inspects all open ports on a workload and reports the flow of traffic between it and other workloads to the PCE. In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the datacenter and the applications running in it. No traffic is blocked in this state. This state is useful when firewall policies are not yet known. This state can be used for discovering the application traffic flows in the organization and then generating a security policy that governs required communication.
- **Selective:** Segmentation rules are enforced only for selected inbound services when a workload is within the scope of a Selective Enforcement Rule.

- **Full:** Segmentation Rules are enforced for all inbound and outbound services. Traffic that is not allowed by a Segmentation Rule is blocked.

You can choose one of three modes for the traffic visibility for workloads:

- **Off (no detail)**: The VEN does not collect any details about traffic connections. This option provides no Illumination detail and utilizes the least amount of resources from workloads. This state is useful when you are satisfied with the rules that have been created and do not need additional overhead from observing workload communication.
- **Blocked:** The VEN only collects the blocked connection details (source IP, destination IP, protocol and source port and destination port), including all packets that were dropped. This option provides less Illumination detail but also demands fewer system resources from a workload than high detail.
- **Blocked + Allowed:** The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections. This option provides rich Illumination detail but requires some system resources from a workload.

Checking VEN Status

After you pair workloads, you can view details by clicking the name of a single workload. From the **Workload Summary** page, you can name the workload, write a description, and change the workload's policy state. To edit any of the workload's properties, click **Edit**.

To view or edit this information, select the **Workload Summary** page.

The **Workload Summary** displays information about the workload, including the user-specified attributes at the time of pairing and information that the Illumio Core has automatically detected about the workload.

If the connection to a VEN is unintentionally broken, the VEN connection is automatically retried after a timeout period.

Checking VEN Connection

To check the connection status of the VEN, click the Health icon at the top of the PCE web console. In the Application tab, check the VEN Heartbeat section. The VEN sends a regular heartbeat to the PCE every five minutes with the latest hostname and other properties of the workload. The VEN Heartbeat section of the Application tab shows the connection status of the VEN as revealed by its heartbeat. The VEN Heartbeat section shows the VEN's success, failure, or latency.

VEN Connectivity

The VEN connection status can be any of the following:

- Online: The workload is connected to the network and can communicate with the PCE.
- Offline: The workload is not connected to the network and cannot communicate with the PCE.
- Suspended: The VEN is in the suspended state and any rules programmed into the workload's IP tables (including custom iptables rules) or Windows filtering platform firewalls are removed completely. No Illumio-related processes are running on the workload.

VEN Heartbeats and Lost Agents

The VEN sends a heartbeat message every five minutes to the PCE to inform the PCE that it is up and running. If the VEN fails to send a heartbeat, check the workload where the VEN is installed and investigate any connectivity issues. If the VEN continues to fail to send a heartbeat, it eventually is marked Offline, which means it can no longer communicate with the PCE or other managed workloads.

PCE down or network issue and the VEN degraded state

If the VEN cannot connect to the PCE, either because the PCE is down or because of a network issue, the VEN continues to enforce the last known good policy while it tries to reconnect with the PCE.

After missing three heartbeats, the VEN enters the degraded state. In the degraded state, the VEN ignores all the asynchronous commands received as lightning bolts from the PCE, except the commands for software upgrades and support reports.

After connectivity to the PCE is restored, the VEN comes out of the degraded state after three successful heartbeats.

Workload Attributes

Workload attributes provide detailed information such as the hostname, the VEN software version, and other attributes.

In particular, workloads have the following attributes:

- Workload enforcement and visibility state
- Connectivity and policy sync state
- Workload labels
- Additional attributes, such as dates when the policy was revised and last applied, VEN version number, hostname, and uptime

The Location of the workload refers to the cloud service provider of the Workload, such as AWS, Rackspace, or Azure. If the workload is hosted in a private data center, then this is listed as Unknown.

VEN Support Reports

A workload's support report provides diagnostic information for selected workloads. To troubleshoot issues with your workloads, you can generate a support report and send it to Illumio support.

> NOTE:
> Your PCE user account must have the Organization Owner or Admin user role to perform this task and the workload should be an active, managed workload.

Generate Support Report from PCE

To generate a VEN support report from the PCE web console:

1. In the PCE web console, go to **Workloads and VENs**, then **VENs**. The page displays your installed VENs.
2. Click the **Workloads** tab.
3. Click a workload and scroll to the bottom of its **Summary** page.
4. Click **Generate Report**. This process can take up to 10 minutes.
5. To view the status of the report, click the **Support Reports** link, which opens the **Support Reports** page. Displays the 50 most recent reports that you have generated.
6. Click the **Download** to download a report.

Chapter 7

Creating Security Policy

This section describes the security policies, which are configurable sets of rules that protect network assets from threats and disruptions. Illumio Core relies on security policy to secure communications between workloads.

Introduction to Core Policy

This topic explains the components of Illumio Core security policy and how to visualize it in the PCE web console.

Visualizing Policy

> NOTE:
> This section is provided for informational purposes only. Visualizing policy is outside the scope of the Common Criteria evaluation. Also outside the scope is the translation of rules by the VEN. The scope of this evaluation includes policy definition and transmission of policies from PCE to VEN.

The PCE Illumination feature enhances policy writing by allowing administrators to visualize flows before they write policy. While PCE Illumination can improve rule writing, it is purely an enhancement that can simplify policy creation. Note that policies can also be created without using Illumination by directly creating Rulesets with Rules.

Policies are identified using unique policy ID numbers. The policy ID identifies the policy and (if applicable) the version of the policy. For more information, see Policy Versioning.

The PCE Illumination feature provides the following different ways to create policy.

Illumination Map

The Illumination map visualizes the workloads that form logical groups (based on labels attached to workloads) and provides an understanding of the traffic flows between workloads. The Illumination Map visualizes all the workloads and traffic in an entire data center. Within the Illumination Map, administrators can expand workloads inside groups and see the traffic links for each connection. After the workloads are visible, users can write rules to allow the traffic between selected workloads (or roles) within or across groups by clicking on the traffic links and selecting the **Add Rule** link.

App Group Maps

App Group Maps are very similar to Illumination Maps but can be used to logically group workloads associated with a common application instance. App Groups are generated using a combination of Application and Environment labels or a combination of Application, Environment, and Location labels. Policies can be created by clicking on traffic flows between App Groups and by converting them into Rules using the **Create Ruleset** option.

Explorer

The Explorer feature can be used to query the PCE's traffic database to search for traffic flows between workloads or hosts, labeled workloads, or IP addresses. Also, Explorer searches can be restricted to specific port numbers and protocols. Explorer can also be used to add rules for traffic flows by selecting traffic flows and then allowing the selected connections.

Policy Generator

The Policy Generator simplifies the policy creation process by recommending the optimal security policy for App Groups. Policy Generator is used to accelerate security workflows and reduce the risk of human error by automatically creating security policies.

Components of Core Policy

The Common Criteria evaluation includes rule definition and provisioning. It does not include the translation of firewall rules by the VEN.

You can use rulesets to write policy so the workloads in your application can communicate with each other. A ruleset consists of rules and scopes:

- Rules define which workloads are allowed to communicate.
- Scopes define which workloads that the rules are applied to.

If workloads share the same labels as a ruleset, then those workloads will receive the rules described in the ruleset.

Rules are an integral component of the Illumio security policy. A set of rules, known as a ruleset, specify the allowed traffic in your network. Create the rules using labels that identify your workloads.

Rules are created to define the allowed communication for two or more workloads. The PCE uses an allow-list policy model. This means that you must specifically define what traffic is allowed; otherwise, it is blocked by default. For example, if you have two workloads that compose a simple application — a web server and a database server — to allow these two workloads to communicate, you must write a rule that describes this relationship and allows the required traffic between the workloads.

Because the PCE employs an allow-list policy model, it is not possible for contradictory rules to be created. Before any rules are written, all traffic is denied by default. As you add rules, each rule allows some subset of traffic to occur. The effects of rules can only be additive: more traffic is allowed by each rule. Traffic allowed by one rule can not negate or conflict with the traffic allowed by another rule.

> NOTE:
> The order in which the rules are written or any possible overlap between rules does not affect the allow-list model, since each rule permits some traffic between workloads.

Access Control Policy Transmission

When the VEN starts up, the VEN requests policy from the PCE by using a REST API over a TLS connection. The API is authenticated and the PCE returns the policy for that particular VEN. Also, when a VEN is paired, it requests its policy from the PCE. During the time between the pairing and first policy application, the VEN is in Idle mode.

The VEN receives notifications about policy updates from the PCE in two ways:

- The VEN sends a heartbeat message every 5 minutes to the PCE, and the PCE responds to the message with any updates for the VEN (for example, a new policy update is waiting for the VEN).
- The VEN opens a persistent connection with the PCE (called Event Channel), and the PCE sends notifications over that channel.

When a VEN is configured from Idle to Enforcement or Visibility mode, the VEN uses whatever policy it receives from the PCE. It does not have any local policy. When a VEN is suspended, the VEN removes all its firewall rules. When a VEN is unpaired, it can be configured to set the new state of the firewall after the VEN is uninstalled. The VEN can be configured to leave the firewall

open (no rules), closed (only allow ssh and other critical connections), or saved (remove VEN-specific firewall rules and do not modify firewall rules belonging to other entities).

Policy Unique ID

New policies provisioned to the VEN include a unique ID to support the Common Criteria for Information Technology Security re-certification. With this ID, you can confirm the new policy version applied to the VEN is the same as the one currently provisioned on the PCE. To view the policy generation on the VEN, enter the following command:

```
${persistent_data_root}/etc/firewall/debug/sec_policy.generation
```

You can also see the logged policy version in ${persistent_data_root}/log/platform.log.

> NOTE:
> Persistent_data_root is used to express the location of the illumio data directory. By default, the data directory is C:/ProgramData/illumio.

Policy Versioning

An administrator can define policies in the PCE, but policies take effect only after they are provisioned in the PCE and applied by the VENs. The PCE assigns a unique version number to each provisioned policy. When a policy is provisioned, the PCE calculates a list of VENs to which the policy should be applied. All applicable VENs receive the provisioned policy. Each VEN gets the latest policy version that applies to that VEN.

Each time a policy is updated, the provisioned change gets a new version number. The PCE has one active version of the policy at one time. The older versions are considered historical versions. The PCE administrator can at any time restore a previous policy version by using the policy restore capability, which will provision the chosen policy version to the VENs. The administrator can also view a list of all historical policy versions and the incremental changes made by those policy versions.

Viewing the Policy Version

To view the policy version in the PCE Web Console:

1. Go to Troubleshooting > Events.
2. In the Select properties to filter view field, enter sec_policy.create and press Go.
3. Click on an event. Under Resource Change, see the Version number.

Workload Setup Using PCE Web Console

After you pair workloads, you can view details by clicking a single workload. From the Workload Summary page, you can name the workload, write a description, and change the workload's policy state.

Unmanaged Workloads

Unmanaged workloads extend rule-writing capabilities to network entities that are not paired with the PCE and do not have an installed VEN. Adding unmanaged workloads to the PCE allows you to write rules so that workloads that are paired with the PCE can communicate with those other entities. The policy between workloads with a VEN and unmanaged workloads is enforced using the outbound rules on the workloads where the VEN is running. For Unmanaged workloads, enforcement is displayed blank.

For example, when you want to ensure that a network file server belonging to an HRM application is only accessible from the database workloads of the HRM application, you can add unmanaged workloads for the file servers and use label-based rules to enforce the policy. The PCE uses the outbound rules on the database workloads running the VEN to ensure that only the databases labeled HRM are allowed to make outbound connections to the network file servers.

To view and edit unmanaged workloads, navigate to the Workloads page and select Unmanaged Workloads, and under the Attributes section edit the following parameters:

- Hostname
- OS family
- Public IP address

To edit the network traffic object go to the section titled Processes where the following attributes for the workload can be edited:

- Process name
- Port
- Protocol

Labels and Label Groups

The Illumio Core policy model is a label-based system, which means that the rules you write don't require the use of an IP address or subnet, like traditional firewall solutions. You control the range of your policy by using labels. This helps you categorize your workloads more quickly and makes it easier to set up your policy.

Label Workloads

The PCE policy model is a Label-based system, which means that the rules you write don't require the use of an IP address or subnet, like traditional firewall solutions. You control the range of your policy by using labels. This functionality helps you categorize your workloads more quickly and makes it easier to set up your policy. Illumio users assign four-dimensional labels to their workloads to identify functionality.

You apply labels to workloads to identify their function or purpose in an application (Role label), the application they belong to (Application label), their network environment (Environment label), and their location (Location label). After a workload is labeled, you can write rules using the labels you have applied to the workload.

After you Create a label, you can label a workload in two ways:

- Automatically label the workloads when you pair them by adding labels in the pairing profile.
- Add labels to the workload on the Workload Summary page. In the PCE web console, select **Workloads and VENs > Workloads** from the left navigation menu. Select a workload, and in the details panel click **Edit** to select any or all of the four label types to apply to the workload.

Configuring Label-based Policy

Once a workload is labeled, then you can write rules using the labels you have applied to workloads. Users specify labels in ruleset scopes and in the providers and consumers components of rules, which allows the workloads in their environments to communicate with each other. Together, labeling workloads and creating the corresponding rulesets and rules define the security policies for workloads. The PCE converts these label-based security policies into the appropriate rules for the OS-level firewalls of the workloads.

Label Groups

Label groups help you write your security policy more efficiently when you use the same labels repeatedly in rulesets. When you add those labels to a label group, the label group can be used in a rule or scope as a shortcut or an alias for multiple labels. The Label Groups list pages can contain up to 10,000 label groups and the individual Label Groups pages can contain up to 10,000 members. You can use filters to find labels or label groups.

Chapter 8

Reference: Auditable Events

This section describes audit events generated by the evaluated security functionality.

Event Syntax

The names of recorded auditable events have the following general syntax:

```
resource.verb[.success_or_failure]
```

Where:

- `resource` is a PCE and VEN object, such as PCE `user` or VEN `agent` component.
- `verb` describes the action of the event on that resource.
- In CEF and LEEF formats, the success or failure of the verb is included in the recorded event ID. This indicator is not needed in the JSON format.

Event Record Structure

Regardless of export format (JSON, CEF, or LEEF), the records and fields for all events share a common structure. This common structure of composite events makes post-processing of event data easier.

Bulk change operations on many resources simultaneously are recorded as individual operations on the resource within a single composite event. Failed attempts to change a configuration, such as incorrect authentication, are also collected.

Common Fields

Field Name	Description
`href`	Unique event identifier; contains a UUID.
`timestamp`	Exact time that the event occurred in RFC 3339 format with fractional seconds.
`pce_fqdn`	The fully qualified domain name of the PCE. Especially useful for Supercluster deployments or if there are multiple PCEs sending data to the SIEM server.
`created_by`	Identifies creator of the event. Could be a user, the system, or a workload.
`event_type`	ID of the auditable event. For more information, see the List of Auditable Events table.
`status`	"Success" or "failure." If the status is null, the event is for information only and doesn't indicate success or failure.
`severity`	"Informational," "warning," or "error" indicating the severity of the event.
`version`	Schema version for events.

Events Displayed in PCE Web Console

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

From the platform and API perspective, Organization events are referred to internally as `auditable_events` and are generated by the `auditable_events_service`.

You can use the filter at the top of the page to search for events by type of event, event severity level, and when the event occurred.

List of Auditable Events

The following table provides the types of JSON events generated and their description. For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `agent.activate` is `agent.activate.success` and the failure event is `agent.activate.failure`.

Each event can generate a variety of notification messages. See Notification Messages in Events.

Auditable Event	Description	Corresponding SFRs
agent.activate	Agent paired	ESM_ACT.1 FMT_SMF.1
agent.deactivate	Agent unpaired	
agent.goodbye	Agent disconnected	
agent.machine_identifier	Agent machine identifiers updated	
agent.refresh_policy	Success or failure to apply policy on VEN	
agent.suspend	Agent suspended	
agent.update	Agent properties updated	
auth_security_principal.create	RBAC auth security principal created	FMT_SMR.1 FMT_SMF.1
auth_security_principal.delete	RBAC auth security principal deleted	
auth_security_principal.update	RBAC auth security principal updated	
authentication_settings.update	Authentication settings updated	ESM_EAU.2
event_settings.update	Event settings updated	FAU_GEN.1.1
firewall_settings.update	Global policy settings updated	FMT_SMR.1 ESM_ACD.1
label.create	Label created	ESM_ATD.1 FMT_SMF.1
label.delete	Label deleted	
label.update	Label updated	
labels.delete	Labels deleted	
pairing_profile.create	Pairing profile created	
pairing_profile.create_pairing_key	Pairing profile pairing key created	
pairing_profile.delete	Pairing profile deleted	
pairing_profile.update	Pairing profile updated	
pairing_profile.delete_all_pairing_keys	Pairing keys deleted from pairing profile	
pairing_profiles.delete	Pairing profiles deleted	
password_policy.create	Password policy created	FIA_SOS.1 FMT_SMF.1
password_policy.delete	Password policy deleted	
password_policy.update	Password policy updated	
pce.application_started	PCE started	FAU_GEN.1
pce.application_stopped	PCE stopped	

Auditable Event	Description	Corresponding SFRs
permission.create	RBAC permission created	FMT_SMR.1 FMT_SMF.1
permission.delete	RBAC permission deleted	
permission.update	RBAC permission updated	
remote_syslog.reachable	Remote syslog reachable	FAU_ STG.EXT.1
remote_syslog.unreachable	Remote syslog unreachable	
rule_set.create	Rule set created	ESM_ACD.1 FMT_SMF.1
rule_set.delete	Rule set deleted	
rule_set.update	Rule set updated	
rule_sets.delete	Rule sets deleted	
saml_acs.update	SAML assertion consumer services updated	ESM_EAU.2 FMT_SMF.1
saml_config.create	SAML configuration created	
saml_config.delete	SAML configuration deleted	
saml_config.update	SAML configuration updated	
saml_sp_config.create	SAML Service Provider created	
saml_sp_config.delete	SAML Service Provider deleted	
saml_sp_config.update	SAML Service Provider updated	
sec_policy.create	Security policy created	ESM_ACD.1
sec_policy_pending.delete	Pending security policy deleted	
sec_policy.restore	Security policy restored	
sec_rule.create	Security policy rules created	
sec_rule.delete	Security policy rules deleted	
sec_rule.update	Security policy rules updated	
security_principal.create	RBAC security principal created	FMT_SMR.1
service.create	Service created	FMT_SMF.1 ESM_ACD.1
service.delete	Service deleted	
service.update	Service updated	
services.delete	Services deleted	
syslog_destination.create	syslog remote destination created	FMT_SMF.1
syslog_destination.delete	syslog remote destination deleted	
syslog_destination.update	syslog remote destination updated	
tls_channel.establish	TLS connection established	FTP_ITC.1
tls_channel.terminate	TLS connection terminated	

Auditable Event	Description	Corresponding SFRs
`user.accept_invitation`	User invitation accepted	ESM_EAU.2 FTP_TRP.1
`user.authenticate`	User authenticated	ESM_EAU.2 FTP_TRP.1
`user.create`	User created	FMT_SMR.1 FMT_SMF.1
`user.delete`	User deleted	
`user.invite`	User invited	
`user.login`	User logged in	ESM_EAU.2 FTP_TRP.1
`user.login_session_terminated`	User login session terminated	ESM_EAU.2 FTA_SSL.3
`user.logout`	User logged out	FTA_SSL.4
`user.reset_password`	User password reset	FMT_SMR.1 FMT_SMF.1
`user.sign_in`	User session created	ESM_EAU.2 FIA_AFL.1 FIA_SOS.1
`user.sign_out`	User session terminated	ESM_EAU.2 FTA_SSL.3 FTA_SSL.4
`user.update`	User information updated	FIA_AFL.1 FMT_SMR.1
`user.update_password`	User password updated	FIA_SOS.1 FMT_SMR.1
`user.use_expired_password`	User entered expired password	FMT_SMR.1 FMT_SMF.1
`user_local_profile.create`	User local profile created	
`user_local_profile.delete`	User local profile deleted	
`user_local_profile.reinvite`	User local profile reinvited	
`user_local_profile.update_password`	User local password updated	

Auditable Event	Description	Corresponding SFRs
ven_settings.update	VEN settings updated	ESM_ATD.1 FMT_SMF.1
workload.create	Workload created	
workload.delete	Workload deleted	
workload.online	Workload online	
workload.recalc_rules	Workload policy recalculated	
workload.redetect_network	Workload network redetected	
workload.update	Workload settings updated	FAU_SEL_EXT.1 ESM_ATD.1
workload_interface.create	Workload interface created	ESM_ATD.1 FMT_SMF.1
workload_interface.delete	Workload interface deleted	
workload_interface.update	Workload interface updated	
workload_interfaces.update	Workload interfaces updated For example, IP address changes, new interface added, and interface shut down.	
workload_settings.update	Workload settings updated	
workloads.apply_policy	Workloads policies applied	
workloads.remove_labels	Workloads labels removed	
workloads.set_labels	Workload labels applied	
workloads.unpair	Workloads unpaired	
workloads.update	Workloads updated	

Notification Messages in Events

Events can generate a variety of notifications that are appended after the event ID:

- agent.clone_detected
- agent.fw_state_table_threshold_exceeded
- agent.missed_heartbeats
- agent.missing_heartbeats_after_upgrade
- agent.policy_deploy_failed
- agent.policy_deploy_succeeded

- agent.process_failed
- agent.service_not_available
- agent.upgrade_requested
- agent.upgrade_successful
- agent.upgrade_time_out
- container_cluster.duplicate_machine_id
- container_cluster.region_mismatch
- container_workload.invalid_pairing_config
- container_workload.not_created
- database.temp_table_autocleanup_completed
- database.temp_table_autocleanup_started
- hard_limit.exceeded
- pce.application_started
- pce.application_stopped
- remote_syslog.reachable
- remote_syslog.unreachable
- request.authentication_failed
- request.authorization_failed
- request.internal_server_error
- request.invalid
- request.service_unavailable
- request.unknown_server_error
- sec_policy.restore
- soft_limit.exceeded
- system_task.event_pruning_completed
- system_task.hard_limit_recovery_completed
- user.csrf_validation_failed
- user.login_failed
- user.login_failure_count_exceeded

- user.login_session_created
- user.login_session_terminated
- user.pce_session_created
- user.pce_session_terminated
- user.pw_change_failure
- user.pw_changed
- user.pw_complexity_not_met
- user.pw_reset_completed
- user.pw_reset_requested
- virtual_service.not_created
- workload.duplicate_interface_reported
- workload.nat_rules_present
- workload.offline_after_ven_goodbye
- workload.online
- workload.oob_policy_changes
- workload.partial_policy_delivered
- workload.update_mismatched_interfaces
- workloads.flow_reporting_frequency_updated