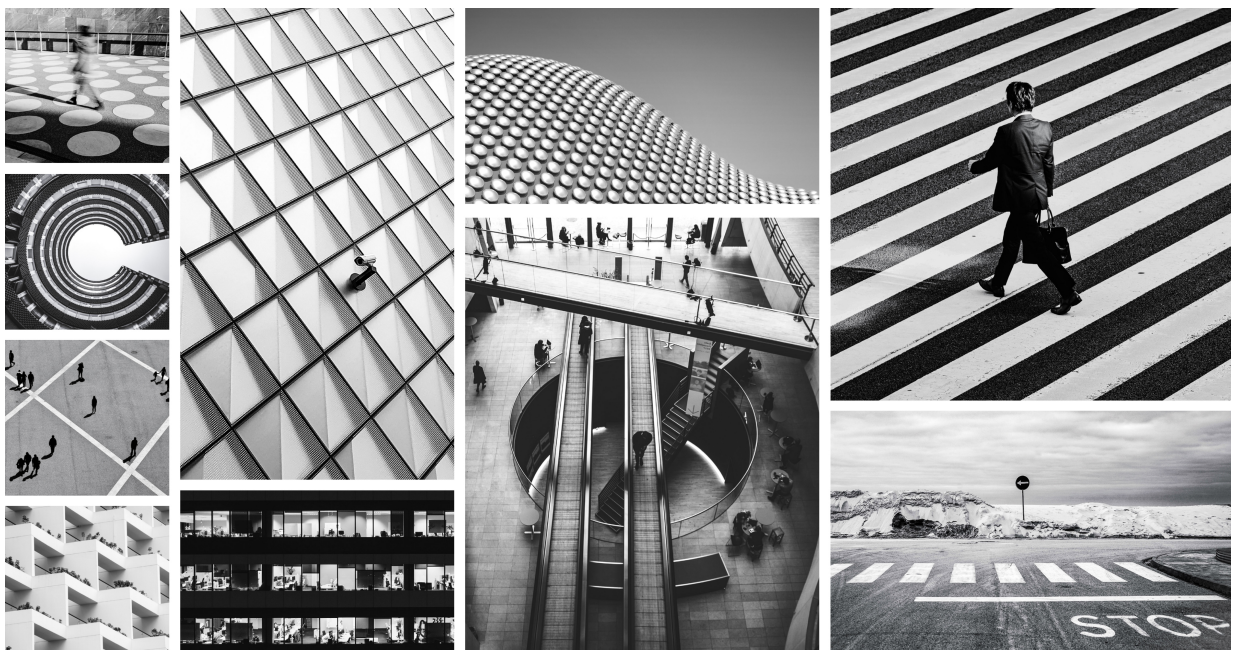




# Illumio Edge User Guide

---

2024



## Table of Contents

Legal Notice .....	3
Illumio Edge What's New .....	4
About This Release .....	4
Product Versions .....	4
General Advisories .....	4
Announcements .....	5
What's New and Changed in Edge 22.31.0 .....	5
Maintenance Release .....	5
Enhanced Illumio Managed Services Portal .....	5
What's New and Changed in 22.31.0 .....	5
What's New in Previous Releases of Edge .....	5
Illumio Edge User Guide .....	15
Overview of Illumio Edge .....	15
Benefits of Using Edge .....	15
How Edge Works .....	15
Getting Started with Illumio Edge .....	16
Edge Users .....	18
Customize Edge Settings .....	21
Policy Creation Process in Edge .....	23
How Policy Creation Works in Edge .....	23
About Inbound Policy .....	24
About Outbound Policy .....	24
Network Profiles .....	25
Edge User Groups .....	25
Create Policy Objects in Edge .....	29
Inbound Policy in Edge .....	32
Outbound Policy in Edge .....	36
Provision Policy in Edge .....	39
Agent Installation in Edge .....	40
Ways to Install Agents .....	40
VEN Library .....	40
Add VENs to a Group .....	41
Install and Activate .....	42
Upgrade VENs .....	42
Requirements for Agent Installation in Edge .....	43
Endpoints and VENs in Edge .....	44
About Admin Access in Edge .....	48
Network-level Access Control Using PKI Certificates .....	48
Benefits of Admin Access .....	48
How Admin Access Works .....	49
View Admin Groups .....	49
Configure Admin Access in Edge .....	50
PKI Certificates for Admin Access in Edge .....	54
Analyze Traffic with Explorer in Edge .....	55
Troubleshooting Tips in Edge .....	57
Access Configuration for Illumio Edge .....	61
Active Directory Single Sign-on .....	61
Azure Single Sign-on .....	91
Okta Single Sign-on .....	97
OneLogin Single Sign-on .....	99
Ping Identity Single Sign-on .....	101

## Legal Notice

Copyright © 2024 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied of Illumio. The content in this documentation is subject to change without notice.

### Resources

- [Legal information](#)
- [Trademarks statements](#)
- [Patent statements](#)
- [License statements](#)
- [Open Source Licensing Disclosures](#)

### Contact Information

- [Contact Illumio](#)
- [Contact Illumio Legal](#)
- [Contact Illumio Documentation](#)

# Illumio Edge What's New

## About This Release

This documentation portal describes the new features, enhancements, platform support for the Illumio Edge 22.31.0 release.

## Product Versions

PCE Version: 22.31.0

## Release Types and Numbering

Illumio release numbering uses the following format: "a.b.c-d+e"

- "a.b": Standard or LTS release number, for example "22.31.0"
- ".c": Maintenance release number, for example ".1"
- "-d": Optional descriptor for pre-release versions, for example "preview2"

## General Advisories

The information in this section provides general advisories about important aspects of this release. To ensure proper operation of the system after upgrade, you might need to take account on these advisories.

## Supported Operating Systems

The 22.31.0 PCE and 22.11.0 VEN are supported on operating systems detailed on the Illumio Support portal.

See [Edge VEN OS Support and Package Dependencies](#).

## Open Source Package Updates

Illumio updated several open source packages for the PCE in this release.

## Before Upgrading VENs to This Release

Before upgrading, review all changes from your current version to version 22.31.0.

To ensure readiness, Illumio strongly encourages you to review the prior release notes, from your currently installed VEN version to version 22.11.0.



## Announcements

### Changes to Teredo Tunnel Interfaces

Teredo tunnel interfaces are no longer reported from Windows endpoints. The change is to fix an issue with the interface's IP addresses changing very frequently. The Teredo interface is used for IPv6 connectivity, and is disabled by default.

## What's New and Changed in Edge 22.31.0

Familiarize yourself with these new and modified features in Edge 22.31.0.

### Maintenance Release

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Edge 22.31.0 solved software and security issues to refine the software and improve its reliability and performance.

### Enhanced Illumio Managed Services Portal

In this release, the Edge supports the enhanced Illumio Managed Services Portal. When managed services providers navigate to the Illumio Edge web UI from the enhanced Illumio Managed Services Portal, they see a link in the Edge web UI to take them back to their Managed Services Portal.

### What's New and Changed in 22.31.0

This section explains for Illumio Edge customers running earlier releases of Illumio Edge what is new in Illumio Edge 22.31.0.

### What's New in Previous Releases of Edge

If you are running earlier releases of Illumio Edge, learn what is new and what features are enhanced in the Illumio Edge in each release.

## Illumio Edge 22.11.0

### Tenant Management for MSPs

My Managed Tenants allows Managed Services Providers (MSPs) to onboard their customers into Illumio Edge (SaaS) and then manage and administer Edge on their behalf. Users with the Global Organization Owner role can:

- Add client tenants for their customers.
- View all their customer tenants from the **My Managed Tenants** page in their Illumio PCE.
- Navigate to their customer's Illumio tenant login page from the Illumio Edge login page or from a link on their **My Managed Tenants** page.

- Remove a tenant.

### Support for removing a Group in Edge

Beginning with this release, you can remove a Group in Edge. The **Remove Group** option appears in the drop-down menu next to the **Add VENs button** (**Illumio Edge > Groups**). For details, see [Remove a Group](#).

### Consolidated tallys for displaying errors and warnings

Beginning with this release, the VENs List page features a new pattern of consolidated tallys for displaying all errors and warnings. The new pattern avoids the need to display separate cascading banners for multiple errors or warnings that occur simultaneously.

## Illumio Edge 21.2.0

### Outbound Policy Enforcement

Prior to Illumio Edge 21.2.0, you could only control access to your managed endpoints with inbound policy enforcement. All traffic from each endpoint with Edge installed was allowed to reach your corporate applications.

In this release, you can now control egress traffic from your endpoints.

Using Illumio Edge, you can create outbound policy for your endpoints to control how they connect with external resources; specifically, your corporate data center, other cloud services, the Internet, and other devices on their home networks. When you install an Illumio Edge VEN on an endpoint, you can allow the endpoint to reach the Internet through its default gateway or router while at the same time controlling which corporate assets that endpoint can reach. Using Illumio Edge for endpoint control allows you to implement user segmentation from endpoints for assets in the corporate environment.

For the steps to configure outbound policy for your endpoints, see [Outbound Policy](#).

### Organization Policy

You set up outbound policy at the organization level so that the same outbound policies are applied to all endpoints on which you have installed the Illumio Edge agent (known as the VEN). This way, you do not need to replicate outbound rules to all Edge groups. Managing outbound policy is efficient because you do it at the organizational level.

When you view outbound policy for a specific group, the tab displays the rules as read-only. When you update your Organization Policy, you only need to provision the changes once because the changes are provisioned to the PCE as one set of rules.

For more information about Organization Policy, see [About Organization Policy](#).

### Network Profiles

You can specify the network profile for inbound and outbound policies. By using network profiles, you can separate your security policies by the type of network that the endpoints are connected to; namely, Corporate versus External network profiles. When you configure policy, you can specify whether it applies to the Corporate, External, or both ("All") profiles.

For more information about Network Profiles, see [Network Profiles](#).

## Domain Names in Policy

In Illumio Edge 21.2.0, you can now use domain names to control allowed traffic for your endpoints. Domain names can be fully-qualified domain names (FQDNs) or domain name patterns using wildcards (for example, \*.google.com).

Specifically, you can specify FQDNs in the destination IP ranges for outbound policy.

For more information, see [Policies Using Domain Names](#).

## User Groups

In 21.2.0, Illumio Edge introduces the ability to use User Groups in policy.

User Groups in Illumio Edge allow you to leverage Microsoft Active Directory (AD) User Groups in your Illumio Edge outbound policy. With this feature, you can create user groups in the Illumio Edge that map directly to your AD groups. You can then create policy with these groups so that you can control outbound access on specific endpoints (the destination of the outbound policy) based on the group membership of the user logged in to that endpoint.

For more information, see [Add User Group](#).

## Illumio Edge 21.1.0

### New Feature in Edge 21.1.0

Admin Access and Admin Groups

In Illumio Edge, you control which inbound connections your endpoints are allowed to accept. You have two ways to specify which inbound connections are allowed. In the previous release, you could only control which inbound connections your endpoints accepted by creating standard Illumio Edge groups containing endpoints. The groups included incoming services and specified IP ranges. You still have the ability to create standard Illumio Edge Groups. See these topics for information:

- [Edge Groups](#)
- [Inbound Policy](#)

Illumio Edge 21.1.0 expands the capability to control incoming connections to endpoints by adding the new Admin Access feature. The Admin Access feature allows you to control access by configuring network-level access control using PKI certificates.

The Admin Access feature has many benefits, including allowing administrators to access endpoints in other groups for troubleshooting and maintenance purposes. It is independent of IP ranges, which can change or overlap. Because endpoints use certificate-based identity of the connecting endpoints to verify their authenticity before allowing them to connect, the Admin Access feature reduces possible vulnerabilities related to IP address spoofing.

For more information about this new feature, see [Admin Access](#) in this guide.

## What's Changed in Edge 21.1.0

### Software Issues and Performance

Illumio provides regular updates for reported bugs and security issues, and to add support for new operating system versions.

Illumio Edge 21.1.0 solved software and security issues to refine the software and improve its reliability and performance. See [Illumio Edge Release Notes 21.1.0](#) for information.

### Open Source Package Updates

Illumio updated several open source packages for Illumio Edge in this release. See the “Change History” in [Illumio Edge Open Source Licensing Disclosures 21.1.0](#) for information.

## Enhancements in Edge 20.3.0

### Option to Increase Traffic Update Rate

‘Increase Traffic Update Rate’ button is available on workloads pages. Clicking this button triggers an action on workload to report flow information for selected workloads every 30 seconds for the next 10 minutes.

### Workload Renamed to Endpoint

In the Illumio Edge UI and documentation, the resource that you installed VENS on was previously known as a “workload.” In this release, this resource is known as an “endpoint.” This terminology update appears in the web console and in all product guides.

## Enhancement in Edge 20.2.1

### Support for IPv6 on the Services Page

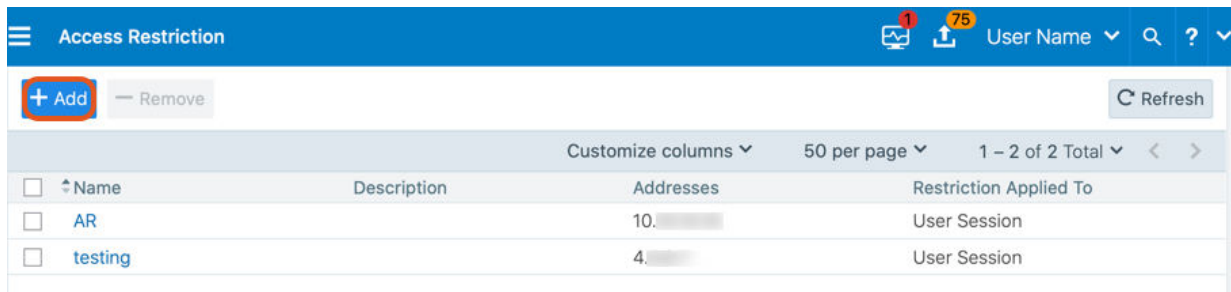
The Edge UI now supports the IPv6 encapsulation protocol service object. While creating a service object, you can specify the IPv6 encapsulation protocol in the “Port and/or Protocol” field by updating the “Service Definitions” information. You can use Explorer to filter for the IPv6 encapsulation protocol from the “Services” drop-down menu by choosing “Policy Services”.

## Illumio Edge 20.2.0

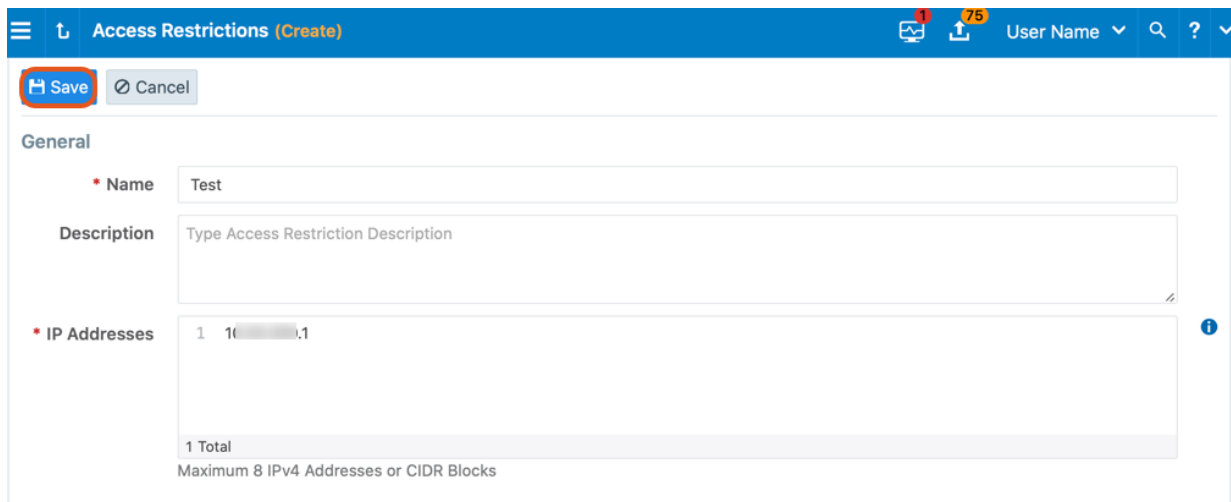
### New Features in Edge 20.2.0

#### Access Restrictions

Access restrictions are configurable entities and contain a list of up to 8 IPv4 IP addresses or CIDR blocks that specify the source IP addresses of the allowed clients. Only the Global Organization Owner can manage access restrictions in the organization while other roles cannot edit or view them. From the main menu, click Access Management > Access Restriction to edit the access restrictions.



<input type="checkbox"/>	Name	Description	Addresses	Restriction Applied To
<input type="checkbox"/>	AR		10.	User Session
<input type="checkbox"/>	testing		4.	User Session



**Save** **Cancel**

**General**

**Name** Test

**Description** Type Access Restriction Description

**IP Addresses**


1	10.0.0.1
---	----------


1 Total  
Maximum 8 IPv4 Addresses or CIDR Blocks

For more information, see [Access Restrictions for Users](#).

## Reversible Source and Destination Columns

Previously, the UI would display the Source column on the left and the Destination column on the right with an arrow pointing from left to right. The Source & Destination Order feature on the Policy Settings page provides an option to reverse the column display order. You can now decide whether you want the Source or Destination column to be displayed first in the UI.

 **Policy Settings**

 Edit

---

**Provisioning**



Require Provision Note    No

---

**Source & Destination Order**

UI Column Order    Display Source Column First

Source → Destination

  **Policy Settings (Edit)**

✓ Save    ⌕ Cancel

---

**Provisioning**

Require Provision Note    ☐ Yes  
☒ No

---

**Source & Destination Order**

UI Column Order    ☐ Display Destination Column First  
Destination ← Source

☒ Display Source Column First  
Source → Destination

For more information, see [Configure Edge Settings](#).

## Enhancements in Edge 20.2.0

Workload Enforcement States

The workload enforcement states have been updated from Build/Test to Enforced and Visibility Only modes. Illumio Edge includes three policy states for workloads:

- **Idle**

Illumio Edge does not take control of the workload's native OS firewall and no traffic is blocked in this state. In this mode, you get 'Limited' visibility and the snapshots of flows from the workload is collected periodically.

- **Visibility Only**

Illumio Edge does not block any traffic. In this mode, you can only select the 'Blocked + Allowed' option and Illumio Edge logs and displays traffic information for allowed and potentially blocked traffic.

- **Enforced**

Rules are enforced for all inbound services. Illumio Edge blocks traffic not allowed by a rule. In this mode, you can select any of three visibility levels to define how much data the VEN collects from the workload:

- Off: Illumio Edge does not collect traffic information.
- Blocked: Illumio Edge logs and displays traffic information for blocked traffic.
- Blocked + Allowed: Illumio Edge logs and displays traffic information for blocked and allowed traffic.

Workloads and VENs - Workloads

Workloads

VENs

1 Workload in Suspension

+ Add

Move to Group

Enforcement

Visibility

Select properties to filter view

1 Selected

Idle

Enforced

<input type="checkbox"/>	Connectivity	Policy Sync	Group	Last Applied Policy	Enforcement	Customize columns	50 per page
<input type="checkbox"/>	Online	Suspended	Domain_Grp29	11/23/2020, 16:46:28	Visibility Only	Blocked + Allowed	Name
<input checked="" type="checkbox"/>	Online	Active (Syncing)	Domain_Grp29	11/23/2020, 16:55:47	Visibility Only	Blocked + Allowed	Name
<input type="checkbox"/>	Offline		Domain_Grp29	11/23/2020, 16:47:12	Visibility Only	Blocked + Allowed	Name

Workload – W10

8H

Summary

Processes

Rules

Blocked Traffic

Edit

General

Name

W10

8H

Description

Enforcement

Visibility Only

Illumio Edge does not block any traffic

Visibility

Blocked + Allowed

Illumio Edge logs and display traffic information for allowed and potentially blocked traffic

VEN

W10

8H

Connectivity

Online

Policy Sync

Active (Syncing)

Policy Last Applied

11/23/2020 at 16:55:47

Group

Group

Ryan

Attributes

VEN Version

20.2.0-308

Hostname

W10

8H

OS

win-x86\_64-server

Release

18362.1.amd64fre.19h1\_release.190318-1202 (Windows 10 Enterprise)

Uptime

77 Days, 2 Hours, 59 Minutes

Heartbeat Last Received

11/24/2020, 21:10:37

Interfaces

eth32769: 10.

10.8.0.1 (domain)

eth32769: fe80::d01

:3b92/64 (domain)

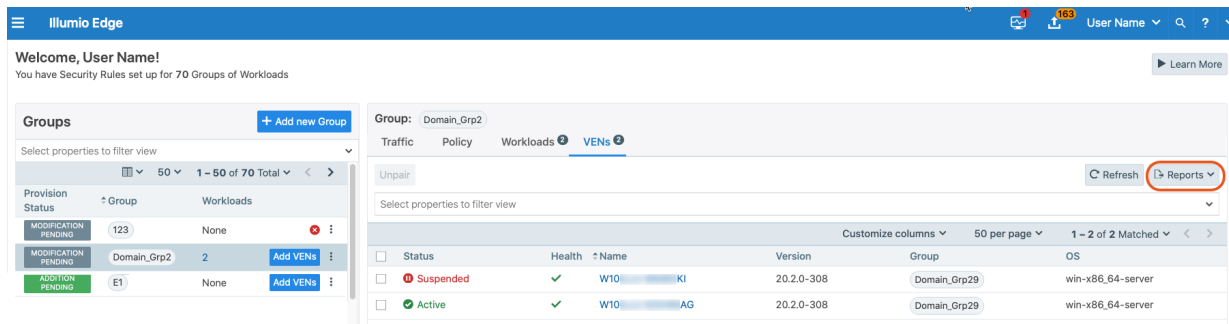
## IPv6 Support

The Windows VENs support IPv6 rules.

## Export Report on Groups Page

From the Groups page, you can generate Export Reports (CSV and JSON) that include the policies applicable to the selected group.

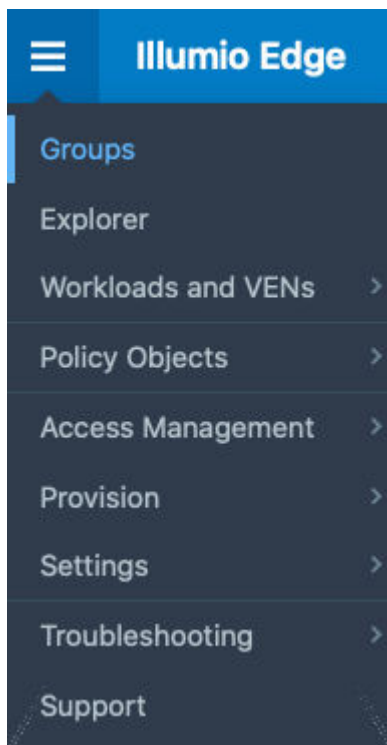




## Enhancements in Edge 20.1.3

Home Page Name Updated to Groups

For better visibility and navigation, the 'Home' page is renamed as 'Groups'. This enables you to easily navigate to Group view from any page.



## Adding Multiple IPLists per Service

Previously, you could add only one IPList to a service. Without nested IPLists or the ability to add more than one IPList to a service, you would need to create IPLists per services. You can now add more than one IPList to a service. As multiple IP Ranges for the same service is now allowed, you may define multiple IP ranges with smaller CIDR blocks or IP Range.

## Enhanced Explorer

Previously, Explorer would only filter based on Transmission type or Exclude Servers or IP Ranges. Explorer feature has now been enhanced to include its full functionality with filtering

options. You can now use Explorer to find data about a certain port and protocol or find information for a specific flow over a certain period.

### Selector for Static Categories

The MultiGroupMultiItemSelector selector is enhanced to support multi-item select with check boxes for static categories.

## New Features in Edge 20.1.2

### VEN Connections via Proxy Servers

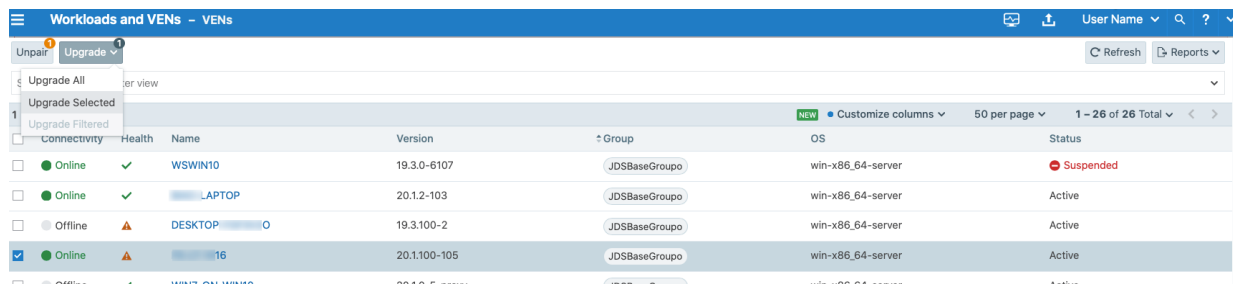
This release of Illumio Edge supports a VEN to PCE connection through proxy servers:

- The default proxy configuration on the OS is used and proxy configuration may or may not be required.
- Only non-authenticated proxy is supported, which may require you to add an exception for the PCE address.
- Only HTTP proxy is supported. The VEN will detect the proxy automatically and configuration or mode change will not be required.

See [VEN Connections via Proxy Servers](#) for more information.

### Upgrade VENs from the PCE UI

You can now upgrade one or more VENs from the VENs page in the PCE UI. You can upgrade all VENs, upgrade a selected subset of VENs, or upgrade all VENs that match a set of filters. After you confirm an upgrade from the UI, the VEN will download the new VEN image from the PCE and upgrade itself. If the VEN does not successfully upgrade within a certain amount of time (approximately 24 hours), the upgrade will time out and the PCE will put the VEN in a warning state. To clear this warning, just start another upgrade on the VEN. The VEN versions available in the UI will be uploaded by Illumio.



Connectivity	Health	Name	Version	Group	OS	Status
<input type="checkbox"/>	Online	WSWIN10	19.3.0-6107	JDSBaseGroup0	win-x86_64-server	Suspended
<input type="checkbox"/>	Online	LAPTOP	20.1.2-103	JDSBaseGroup0	win-x86_64-server	Active
<input type="checkbox"/>	Offline	DESKTOP	19.3.100-2	JDSBaseGroup0	win-x86_64-server	Active
<input checked="" type="checkbox"/>	Online	WIN7-ON-WIN10	20.1.100-105	JDSBaseGroup0	win-x86_64-server	Active
<input type="checkbox"/>	Offline	WIN7-ON-WIN10	20.1.0-5-100	JDSBaseGroup0	win-x86_64-server	Active

# Illumio Edge User Guide

## Overview of Illumio Edge

Endpoint segmentation is as important as data center segmentation because malware can spread when endpoints communicate with each other. Edge provides strong endpoint security by delivering visibility and segmentation to the endpoint. It delivers endpoint protection that eliminates malicious lateral connections by effectively blocking the east-west traffic. It proactively prevents the spread of breaches even before they are detected.

## Benefits of Using Edge



### IMPORTANT

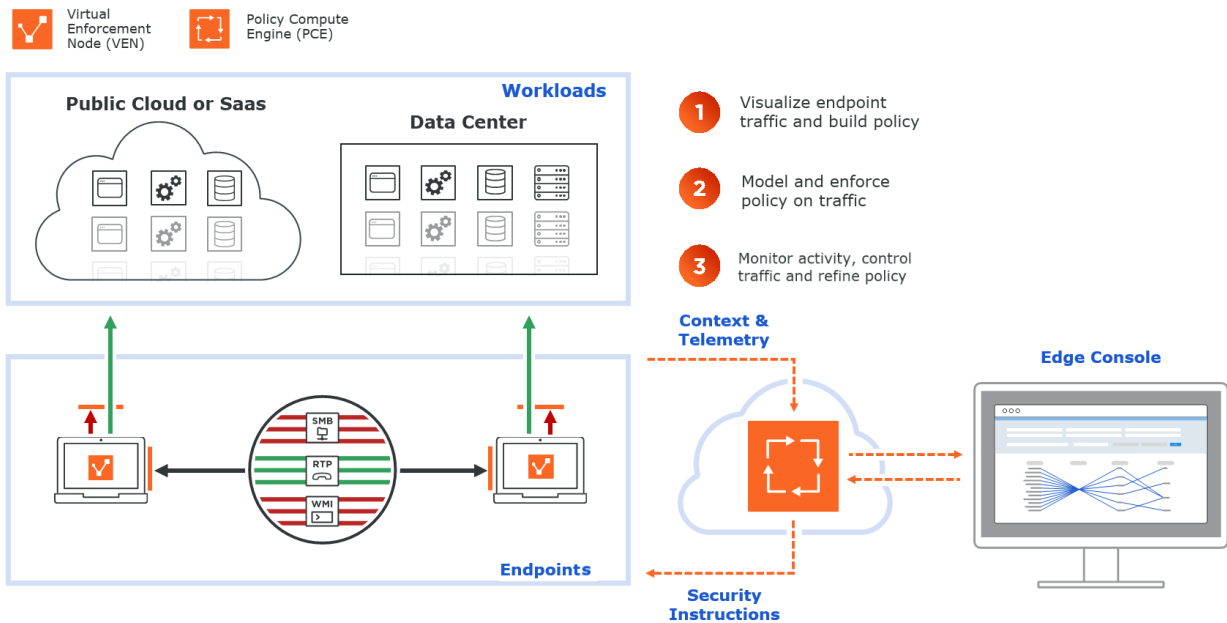
Edge is supported for Illumio Cloud (SaaS) customers only and available only for Windows endpoints.

Edge has the following key features:

- Blocks inbound traffic by default.
- Allows outbound traffic by default.
- Inbound rules allow traffic from subnets or core services to specific ports.
- Works remotely on wireless networks.
- Provides the ability to model policy in test and enforced modes.
- Enables firewall coexistence mode by default.
- Allows you to create separate policies for each endpoint's domain-connected network versus their external or home networks.

## How Edge Works

The following diagram details how Illumio Edge provides endpoint control.



## Getting Started with Illumio Edge

This topic provides important information to new customers, including how to [create an account \[17\]](#) in Illumio Edge.

- For information about creating your first group after creating your account, see [Edge Groups \[25\]](#).

## Availability of Illumio Edge

Illumio provides an uptime Service Level Agreement (SLA) of 99.8% for Illumio Edge.

For information about the SLA, see your Illumio Purchase Order and the Illumio Master Subscription Agreement (<https://www.illumio.com/eula>).

## Recommended Skills

Before continuing, make sure you're familiar with:

- Your organization's security goals
- User endpoint applications

## Requirements and Limitations



### IMPORTANT

Illumio Core is supported for Illumio Cloud (SaaS) customers only and available only for Windows endpoints.

Illumio Edge has the following requirements and limitations:

- Only on-premises Active Directory (AD) is supported.
- Laptops joined with Azure AD *only* are not supported. Laptops must be on-premises domain joined or on-premises Azure AD-hybrid joined.
- Edge is not compatible with hypervisors such as Windows Hyper-V. The connectivity to or from virtual machines may be blocked in Enforced mode.
- HTTP proxy is not supported.

## Interoperability

Illumio Edge works with the following software without needing special configuration:

- Symantec
- TrendMicro
- Cisco AnyConnect

The Illumio Edge agent software uses Windows PowerShell to implement features such as the activation script, agent installer, agent software upgrade, and support report generation. Your anti-virus software may interpret PowerShell to be a threat and block it, even if the scripts it's implementing are signed with Windows authenticode. To prevent this from occurring, Illumio recommends that you configure your anti-virus software to exempt the Illumio Edge agent from scanning and behavioral analysis. If the agent features aren't working properly, examine the anti-virus software logs and alerts to determine whether it is interfering with the functionality of the Illumio Edge agent.

## Create Illumio Edge Account

When you sign-up with Illumio Edge, you receive an email invitation to create your account and access Illumio Edge. The invitation link is valid for **7** days. After you create an account and log in for the first time, the "Welcome to Illumio Edge" page appears. Click **Get Started** to launch a wizard that'll walk you through the steps to set up Illumio Edge.

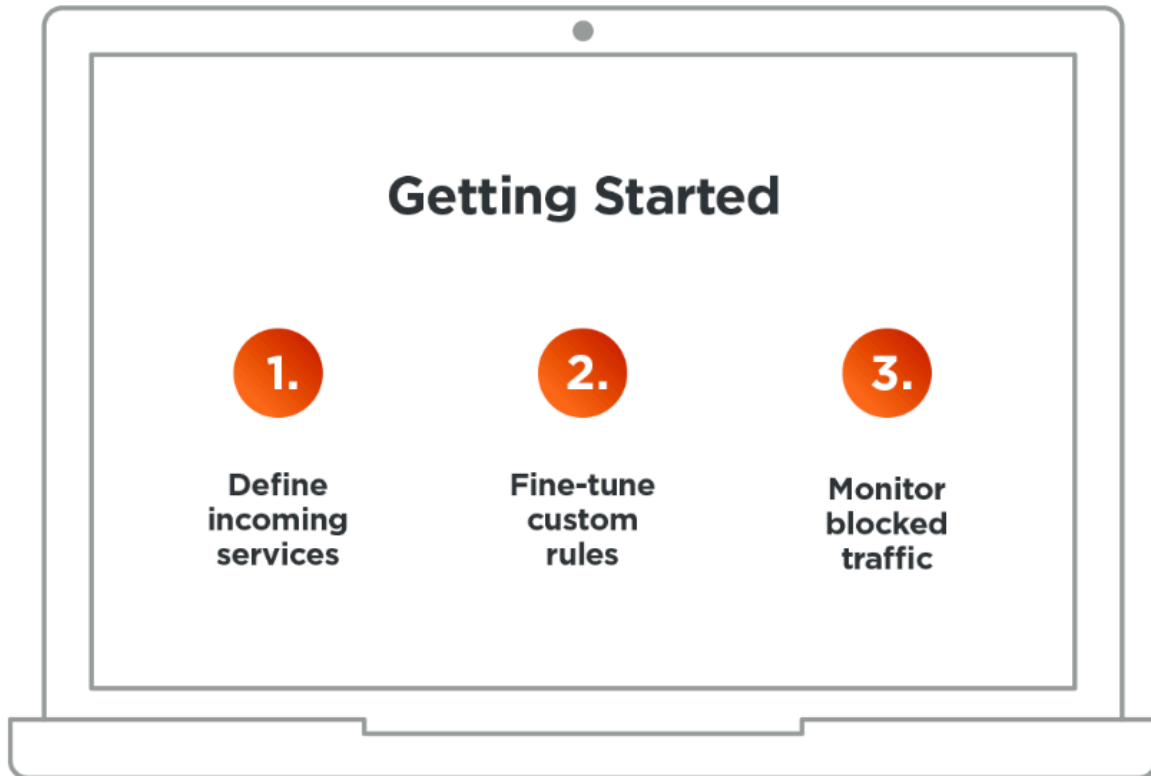
First time login

# Welcome to Illumio Edge

Click **Get Started** to create your first group and define security rules for a set of workloads.

▶ Learn More

Get Started



The wizard guides you through creating your first group for endpoints and configuring inbound policy for that group, including selecting incoming services and configuring IP ranges. For information about the wizard workflow, see [Inbound Policy \[32\]](#).

Once you've created an account, you're presented the Illumio Edge dashboard (Groups page) each time you log in.

## Edge Users

Illumio Edge includes four built-in Global Roles that allow users to perform specific operations. You can assign one or more roles to a single user, combining roles as needed to provide granular levels of permissions according to the needs of your organization.

## Global Roles

To view the Global Roles, go to **Access Management > Global Roles**.

Access permissions for each role are described in this table:

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 setting.
Global Read Only	View any resource or organization setting: can't perform any operations.
Global Policy Object Provisioner	Provision rules containing IP ranges, services, and groups: cannot provision rules, or add, modify, or delete existing policy objects.

<p>Role Global Organization Owner</p> <p>Granted Access <a href="#">^ Hide</a></p> <table> <tr><td>Groups</td><td>View, Add, Modify, Provision</td></tr> <tr><td>Workloads and VENS</td><td>View, Add, Modify, Delete</td></tr> <tr><td>Explorer</td><td>View, Add, Modify, Provision, Delete</td></tr> <tr><td>Users</td><td>View, Add, Modify, Delete</td></tr> <tr><td>Services</td><td>View, Add, Modify, Provision, Delete</td></tr> <tr><td>IP Ranges</td><td>View, Add, Modify, Provision, Delete</td></tr> <tr><td>Blocked Traffic</td><td>View, Delete</td></tr> <tr><td>Security Settings</td><td>View, Modify</td></tr> <tr><td>My Profile</td><td>View, Modify</td></tr> <tr><td>SSO Config</td><td>View, Modify</td></tr> </table>	Groups	View, Add, Modify, Provision	Workloads and VENS	View, Add, Modify, Delete	Explorer	View, Add, Modify, Provision, Delete	Users	View, Add, Modify, Delete	Services	View, Add, Modify, Provision, Delete	IP Ranges	View, Add, Modify, Provision, Delete	Blocked Traffic	View, Delete	Security Settings	View, Modify	My Profile	View, Modify	SSO Config	View, Modify	<p>Role Global Viewer</p> <p>Granted Access <a href="#">^ Hide</a></p> <table> <tr><td>Groups</td><td>View</td></tr> <tr><td>Workloads and VENS</td><td>View Scope</td></tr> <tr><td>Explorer</td><td>View Scope</td></tr> <tr><td>Users</td><td>View</td></tr> <tr><td>Services</td><td>View</td></tr> <tr><td>IP Ranges</td><td>View</td></tr> <tr><td>Blocked Traffic</td><td>View Scope</td></tr> <tr><td>Security Settings</td><td>View</td></tr> <tr><td>My Profile</td><td>View, Modify</td></tr> <tr><td>SSO Config</td><td>None</td></tr> </table>	Groups	View	Workloads and VENS	View Scope	Explorer	View Scope	Users	View	Services	View	IP Ranges	View	Blocked Traffic	View Scope	Security Settings	View	My Profile	View, Modify	SSO Config	None
Groups	View, Add, Modify, Provision																																								
Workloads and VENS	View, Add, Modify, Delete																																								
Explorer	View, Add, Modify, Provision, Delete																																								
Users	View, Add, Modify, Delete																																								
Services	View, Add, Modify, Provision, Delete																																								
IP Ranges	View, Add, Modify, Provision, Delete																																								
Blocked Traffic	View, Delete																																								
Security Settings	View, Modify																																								
My Profile	View, Modify																																								
SSO Config	View, Modify																																								
Groups	View																																								
Workloads and VENS	View Scope																																								
Explorer	View Scope																																								
Users	View																																								
Services	View																																								
IP Ranges	View																																								
Blocked Traffic	View Scope																																								
Security Settings	View																																								
My Profile	View, Modify																																								
SSO Config	None																																								
<p>Role Global Administrator</p> <p>Granted Access <a href="#">^ Hide</a></p> <table> <tr><td>Groups</td><td>View, Add, Modify, Provision</td></tr> <tr><td>Workloads and VENS</td><td>View, Add, Modify, Delete</td></tr> <tr><td>Explorer</td><td>View, Add, Modify, Provision, Delete</td></tr> <tr><td>Users</td><td>View</td></tr> <tr><td>Services</td><td>View, Add, Modify, Provision, Delete</td></tr> <tr><td>IP Ranges</td><td>View, Add, Modify, Provision, Delete</td></tr> <tr><td>Blocked Traffic</td><td>View, Delete</td></tr> <tr><td>Security Settings</td><td>View, Modify</td></tr> <tr><td>My Profile</td><td>View, Modify</td></tr> <tr><td>SSO Config</td><td>None</td></tr> </table>	Groups	View, Add, Modify, Provision	Workloads and VENS	View, Add, Modify, Delete	Explorer	View, Add, Modify, Provision, Delete	Users	View	Services	View, Add, Modify, Provision, Delete	IP Ranges	View, Add, Modify, Provision, Delete	Blocked Traffic	View, Delete	Security Settings	View, Modify	My Profile	View, Modify	SSO Config	None	<p>Role Global Policy Object Provisioner</p> <p>Granted Access <a href="#">^ Hide</a></p> <table> <tr><td>Groups</td><td>View</td></tr> <tr><td>Workloads and VENS</td><td>View</td></tr> <tr><td>Explorer</td><td>View</td></tr> <tr><td>Users</td><td>View, Provision</td></tr> <tr><td>Services</td><td>View, Provision</td></tr> <tr><td>IP Ranges</td><td>View, Provision</td></tr> <tr><td>Blocked Traffic</td><td>View</td></tr> <tr><td>Security Settings</td><td>View</td></tr> <tr><td>My Profile</td><td>View, Modify</td></tr> <tr><td>SSO Config</td><td>None</td></tr> </table>	Groups	View	Workloads and VENS	View	Explorer	View	Users	View, Provision	Services	View, Provision	IP Ranges	View, Provision	Blocked Traffic	View	Security Settings	View	My Profile	View, Modify	SSO Config	None
Groups	View, Add, Modify, Provision																																								
Workloads and VENS	View, Add, Modify, Delete																																								
Explorer	View, Add, Modify, Provision, Delete																																								
Users	View																																								
Services	View, Add, Modify, Provision, Delete																																								
IP Ranges	View, Add, Modify, Provision, Delete																																								
Blocked Traffic	View, Delete																																								
Security Settings	View, Modify																																								
My Profile	View, Modify																																								
SSO Config	None																																								
Groups	View																																								
Workloads and VENS	View																																								
Explorer	View																																								
Users	View, Provision																																								
Services	View, Provision																																								
IP Ranges	View, Provision																																								
Blocked Traffic	View																																								
Security Settings	View																																								
My Profile	View, Modify																																								
SSO Config	None																																								

## External Groups

Illumio Edge integrates with the user groups maintained in your corporate IdP so that you can manage user authentication centrally. When a user who is a member of an external group logs into Illumio Edge, the corporate IdP authenticates the user and returns the list of groups of which the user is a member.

## External Users

Note the following about external users:

- **If usernames aren't email addresses** - Illumio Core can't send email invitations to users whose username isn't maintained in the form of an email address in your external corporate Identity Provider (IdP). Make sure to send these users a login URL that they can use to set up their Edge accounts and log in to the web console.
- **Removing an external user** - Removing an external user from Illumio Core removes them from the External Users tab and from all of their role memberships. The user's authentication continues to be managed by your corporate IdP.

## Local Users

You can view a list of local users in the Local Users tab. Local users are created in the PCE (they are not managed by an IdP). You can create additional local users as a backup in case your external IdP goes offline or the SAML server is inaccessible.

To add a local user:

1. From the Edge main menu, choose **Access Management > Local Users**.
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 have duplicate names for local users but you cannot have duplicate email addresses.
4. Select a role for the user (see [Global Roles \[18\]](#)):
  - None (Users without a role have Read Only access when this access is enabled.)
  - Global Organization Owner
  - Global Administrator
  - Global Read Only

## User Activity

This page displays a list of all the users in your organization along with details such as, name, email address, status (online, offline, or invited), and their last login date and timestamp.

## Authentication

When you use a third-party SAML-based IdP to manage user authentication in your organization, you can configure that IdP to work with the PCE.

## Manage access restrictions for users

Access restrictions are configurable entities and contain a list of up to 8 IPv4 IP addresses or CIDR blocks that specify the source IP addresses of the allowed clients. Only the Global Organization Owner can manage access restrictions in the organization. Other roles can't edit or view them.

In Illumio Edge, you can apply access restrictions to user sessions.



### NOTE

You must have the Global Organization Owner role to view or edit access restrictions.

To add an access restriction:

1. Log in to the Illumio Edge web console as a user with the Global Organization Owner role.
2. Navigate to **Access Management > Access Restrictions**.  
The **Access Restriction** page appears showing the allowed IP addresses and where restrictions are applied.



3. Click **Add**.
4. Enter the required attributes:
  - Name
  - Description (optional)
  - IP Addresses (you can list up to eight IPv4 addresses or CIDR blocks)
5. Click **Save**.  
The new restriction appears on the **Access Restriction** page.

To remove an access restriction:

1. Log in to the Illumio Edge web console as a user with the Global Organization Owner role.
2. Navigate to **Access Management > Access Restrictions**.  
The **Access Restriction** page appears showing the allowed IP addresses and where restrictions are applied.
3. Select the check-box next to the restriction you want to remove and then click **Remove**.
4. Click **Remove** to confirm removal.

## Customize Edge Settings

This topic provides information about how you can customize the Illumio Edge UI for your organization.

### Require Provision Notes

Provision notes allow users to describe the provisioning settings they implement. This provides context that may be helpful to support your organization's workflow. For example, you might want your users to populate the Provision Note field with a project number or a link to your internal bug tracking system.



#### NOTE

Illumio Edge doesn't validate the content entered in the Provision Note field.

You can require administrators to add a note before new or updated provisioning rules take effect. Until text is entered in the Provision Note field, provisioning updates aren't implemented and the **Confirm & Provision** button is grayed out.

To require a Provision Note:

1. Navigate to **Settings > Policy Settings**. The Policy Settings page appears. By default, this option is set to **No**.
2. Click **Edit**.
3. Change the *Require Provision Note* option to **Yes**.
4. Click **Confirm**.
5. Click **Save**.

## Event Settings

By default, the auditable events are enabled in the PCE and cannot be disabled, in accordance with Common Criteria compliance.

You can change the following event-related settings by navigating to the **Settings > Event Settings** page:

- **Event Severity:** Set the severity level (Error, Warning, or Informational) 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, the default period is 30 days.
- **Event Format:** Set the message output to one of the three formats, JavaScript Object Notation (JSON), Common Event Format (CEF), or Log Event Extended Format (LEEF).

**Event Settings**

Edit

**Events**

<b>Event Severity</b>	Informational
	Only audit events of this severity or higher are saved
<b>Retention Period</b>	30 days
	Audit events older than this are purged
<b>Event Format</b>	JSON

## Reversible Source and Destination Columns

On the Policy Settings page, you can decide the order in which you want the Source or Destination column to be displayed in the UI. Previously, the UI would display the Source column on the left and the Destination column on the right with an arrow pointing from left to right.

To define the order of the columns:

1. Navigate to **Settings > Policy Settings**. The Policy Settings page appears.
2. Click **Edit**.

Policy Settings (Edit)

✓ Save

⊗ Cancel

---

### Provisioning

Require Provision Note ☒ Yes ☐ No

---

### Source & Destination Order

UI Column Order ☐ Display Destination Column First

Destination

← Source

☒ Display Source Column First

Source →

Destination

3. Choose the **UI Column Order**.

4. Click **Save**.

Depending on your selection, the Source and Destination columns will be displayed. Here's an example:

Reported Policy Decision	Source	Destination	Destination Port/Process [User]	Destination Groups	Flows/Bytes	First Detected	Last Detected
Allowed by Destination	fe80:fe221d:ced4:3a35	Deleted Workload	ICMPv6	System [NT AUTHORITY\SYSTEM]	4 flows	11/03/2020 02:49:44	11/03/2020 03:06:51
Allowed by Destination	fe80:fd28:d483:36ca:9d17	Deleted Workload	ICMPv6	System [NT AUTHORITY\SYSTEM]	4 flows	11/10/2020 01:09:33	11/10/2020 01:13:40
Allowed by Destination	fe80:fd28:d483:36ca:9d17	Deleted Workload	ICMPv6	System [NT AUTHORITY\SYSTEM]	4 flows	11/18/2020 06:20:41	11/18/2020 06:20:41

## Policy Creation Process in Edge

At a high level, security policies are configurable sets of rules that protect network assets from threats and disruptions. Illumio Edge uses security policies to secure communications.

### How Policy Creation Works in Edge

In Illumio Edge, security policy is defined at the group level. Then, when you add endpoints to the groups, the endpoints are protected by the policies defined for those groups. A group can have three types of policies:

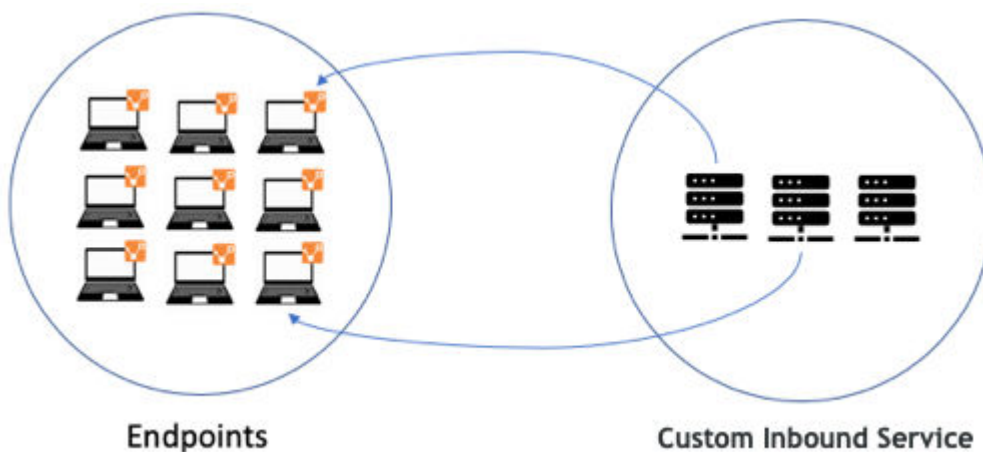
- Inbound policy  
For the steps to create inbound policy, see [Inbound Policy \[32\]](#).
- Outbound policy  
For the steps to create outbound policy, see [Outbound Policy \[36\]](#)

The process for creating policy for groups and installing the Illumio Edge agent (the VEN) on endpoints is separate. However, the wizard to create a group and configure the inbound policy for the group ends with the option to add endpoints to the group. See [Agent Installation \[40\]](#) for more information.

## About Inbound Policy

In most cases, you need to consider inbound service rules. The core services that communicate inbound to the endpoints such as, McAfee EPO, Qualys, SNMP, or other management services should be explicitly allowed. If you have inbound services that are unique to your organization, you will have to create a policy to suit your needs.

Inbound Services Communication



For more information about creating inbound policy, see [Configure Inbound Policy \[32\]](#).

## About Outbound Policy

Using Illumio Edge, you can create outbound policy for your endpoints to control how they connect with external resources; specifically, your corporate data center, other cloud services, the Internet, and other devices on their home networks. When you install an Illumio Edge VEN on an endpoint, you can allow the endpoint to reach the Internet through its default gateway or router while at the same time controlling which corporate assets that endpoint can reach. Using Illumio Edge for endpoint control allows you to implement user segmentation from endpoints for assets in the corporate environment.

Relying on a VPN connection to protect corporate assets doesn't provide the same level of security that Illumio Edge can provide. Relying on a VPN connection alone won't ensure zero-trust network access (ZTNA) for an endpoint to the corporate data center when that endpoint is compromised.

When creating outbound policy for endpoints, you should consider your corporate security, compliance, and IT auditing requirements. Usually, you start by defining what your organization's endpoints can communicate with. By default, Illumio Edge is configured to allow all outbound traffic from your endpoints. Finally, determine what corporate assets you need to control access to from your endpoints.

For more information about creating outbound policy, see [Configure Outbound Policy \[36\]](#).

## Network Profiles

You can specify the network profile for inbound and outbound policies. By using network profiles, you can separate your security policies by the type of network that the endpoints are connected to; namely, Corporate versus External network profiles. When you configure policy, you can specify whether it applies to the Corporate, External, or both ("All") profiles.

The Corporate network profile is reserved for interfaces that are domain authenticated, such as an endpoint's VPN interface or any interface connected to a Microsoft Active Directory (AD) domain. The External network profile should be used for all other networks that the endpoint connects to, such as home wireless networks or public networks. These networks are not domain authenticated. On Windows endpoints, both public or private interfaces map to the External network profile. Endpoints on home networks can communicate with many types of IoT devices, such as printers, Google Home, and Amazon Alexa.

Being able to segregate policies by network profile helps lock down security so that your organization isn't vulnerable to lateral migration of threats from an endpoint's home network to the corporate network because a device on the home network was exposed to a security threat.

In Illumio Edge, the network profile is attached to policy (rules) and not endpoints. The details pages for Endpoints and VENs - Endpoints shows "(Corporate)" or "(External)" next to each interface. For example:

eth32774: 192.168.125.86/24 (Corporate)

eth32775: 192.168.79.1/24 (External)

Illumio Edge users who have permission to create policy have the necessary permission to designate which network profile the policy applies to. The Edge UI does not provide a default setting. You must explicitly choose which network profile to use.

## Edge User Groups

This topic explains how Illumio Edge uses groups as part of endpoint security and how to add and manage the groups you create.

## About Illumio Edge Groups

In Illumio Edge, groups are logical collections of endpoints. You create groups for departments in your organization (for example, Finance, HR, and Engineering) or to logically organ-

ize your endpoints based on other criteria. You create inbound policy by group, which means that an endpoint must be in a group to be controlled by inbound policy. Also, an endpoint can be in only one group at a time. Outbound policy is also controlled by group; however, a global policy, called Organization Policy, is used universally by every group of endpoints.

The Outbound Policy tab for each group is read-only and displays the organization outbound rules that apply to the selected group. For example, the global Organization Policy includes 25 outbound rules and only 5 apply to the selected group (either because a rule applies to all groups or only to the selected group), then the Outbound Policy tab for that selected group will display only those 5 rules.

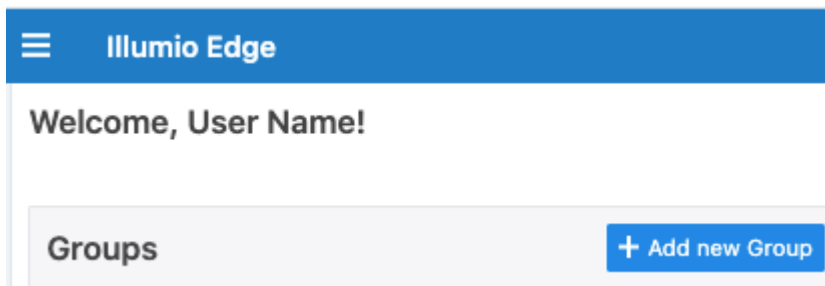
When you add a new group to Illumio Edge, it launches a wizard that walks you through the process of configuring inbound policy for that group; therefore, every group will always have inbound policy set up. You can update a group at any time by editing its inbound policy, providing Admin Access to that group, or by adding and removing endpoints from the group.

The Groups page (main menu > **Groups**) offers quick insight into all active inbound services seen across your groups. In the “Visibility” mode, you can confirm policies by reviewing potentially blocked traffic before enforcement. You can quickly understand the policy decision on all traffic via the green, yellow, and red traffic lines. You can sort the data based on port, traffic flows, and sources. Clicking any of the traffic lines under the Policy column, opens the Explorer page.

## Add a Group

You define a group and select your incoming services and IP ranges. Every time you add a group, Illumio Edge launches a wizard that walks you through the process of configuring the inbound policy.

1. From the Illumio Edge main menu, choose **Groups**.
2. Above the Groups panel, click the **Add new Group** button.



3. Enter a name for the group in the **Name of Group** field, for example *HR*. The group you have selected is the group of endpoints that the policy will be applied to.
4. Continue with the wizard to select the incoming services for the group and define the permitted IP ranges. See [Configure Inbound Policy \[32\]](#) for information.

## View Traffic for Groups

The color of the traffic lines indicates the following status:

- **Green:** Allowed
- **Yellow:** Potentially Blocked (in the Visibility mode, the traffic that does not conform to policy is displayed as potentially blocked)
- **Red:** Blocked

**Welcome, User!**  
You have Security Rules set up for 1 Group of Endpoints

**Groups** [+ Add new Group](#)

Select properties to filter view

Provision Status [Group](#) Endpoints

Finance 4 [Add VTEs](#)

Group: Finance

Traffic Inbound Policy Outbound Policy Admin Access Endpoints VENs

Ports	Total Flows	Blocked Flows	Top Sources	Policy
445 TCP System	10	10	ILLUMIO-LT-002 ILLUMIO-LT-001	
137 UDP System	6	6	ILLUMIO-LT-002 ILLUMIO-LT-001	
ICMP System	4	4	ILLUMIO-LT-002 ILLUMIO-LT-001	
4916 UDP jami.exe	10.9K	10.9K	51.91.75.152 51.222.10.40 54.36.178.20 +73 more	
51247 TCP jami.exe	1	1	ILLUMIO-LT-002	
50000 TCP lmc.exe	1	0	ILLUMIO-LT-001	
50380 TCP jami.exe	1	0	ILLUMIO-LT-001	
3389 UDP svchost.exe	1	0	AD Servers	
3389 TCP svchost.exe	1	0	AD Servers	

The Traffic tab also has an “Unknown” category. The Unknown category can appear for flows permitted by FQDN policies, because FQDN policy can encounter a traffic calculation delay.

You can **Refresh** the Groups page to see new traffic, add filters, and view policies. The “Inbound Traffic for Group” on the Groups page displays the traffic flow of endpoints in the group along with the port and protocol, process name, and Windows service name. You can view the policy, endpoints, and VENs associated with the selected group and also generate Export Reports (CSV and JSON) that include the policies applicable to the selected group.

## Manage Groups

You can manage all your groups from the Groups page. In the Groups panel, each group has a quick access menu that you can use to modify the selected group.

To the right of the group you want to manage, click the dots.

## Groups

+ Add new Group

Select properties to filter view

50

1 – 50 of 122 Total

<

>

Provision Status	Group	Endpoints
	a1	None <div>Add VENs</div>
	a2	None <div>Add VENs</div>
	aa	

Edit Group

Mark as Admin Group

Stop Pairing

Edit Install Script

Revoke Existing Install Script

A menu appears that provides options for the common group management tasks. For information about marking a group as an Admin Group, see [Admin Access](#).



### NOTE

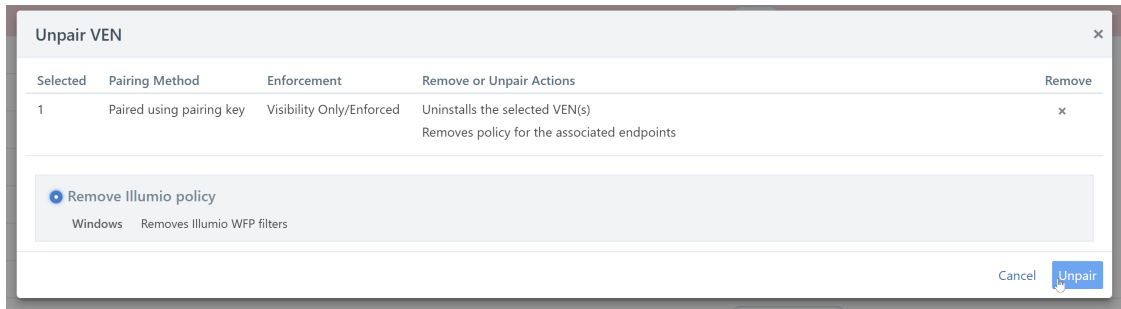
You cannot delete Illumio Edge groups. To modify a group so that its policy no longer impacts endpoints, remove all endpoints from that group.

You remove a VEN from a group by unpairing it, which uninstalls the VEN.

To remove a VEN from a group:

1. From the Illumio Edge main menu, choose **Endpoints and VENs > VENs**.
2. Select the endpoints you want to remove from the group and stop managing.
3. Click the **Unpair** button.  
A dialog box appears providing information about the impact of unpairing those VENs.





4. Click **Unpair**.  
The endpoint is no longer managed by Illumio Edge.

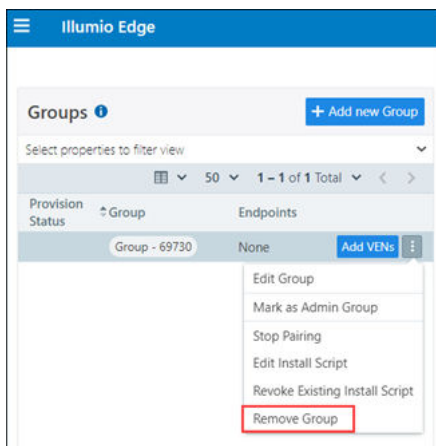
## Remove a Group

When you remove a group:

- The removal appears in the event logs along with the name of the user who removed the group.
- The removal is provisioned automatically and is reflected on the Policy Versions page (**Provision > Policy Versions**).
- Removing a group can't be undone.
- Services, IP ranges, and other policy objects used in the group are unaltered and can still be used by other groups.
- Following removal, flow data from the group may still be visible briefly in Explorer.
- Removing a group doesn't affect the endpoint estate in any way.

## Procedure

1. Prepare for Group Removal.
2. Provision all of the above actions.
3. Remove the group.  
Go to **Illumio Edge > Groups**, click the three vertical dots next to the **Add VENs** button, and then click **Remove Group**. Note the following:



## Create Policy Objects in Edge

You can create reusable policy objects (namely, services, IP ranges, and user groups) ahead of time and add them to the policies you create. Alternatively, you can create them while creating policy. The wizard for creating inbound policy, for example, has buttons to create policy objects while selecting services and IP ranges.

## Add Service

- From the main menu, choose **Policy Objects > Services**. The list of inbound services you have previously defined appears.

Provision Status	Name	Port/Protocol	Last Modified On	Last Modified By	Description
<input type="checkbox"/>	All Services	ALL	11/27/2019, 10:31:07	Unknown	
<input type="checkbox"/>	ICMP	ICMP, ICMPv6	11/27/2019, 10:31:07	Unknown	
<input type="checkbox"/>	Kollektive	Delivery Manager Service	06/08/2020, 22:06:19	illumio.com	Kollektive, formerly known as Kontiki, is a pe...
<input type="checkbox"/>	LMC	50000 TCP	06/09/2020, 08:31:38	illumio.com	Custom p2p Messaging
<input type="checkbox"/>	RDP	3389 TCP, 3389 UDP	06/09/2020, 10:05:33	illumio.com	
<input type="checkbox"/>	SMB	445 TCP	06/09/2020, 08:32:21	illumio.com	
<input type="checkbox"/>	Zoom	ZoomCptService	06/08/2020, 22:06:18	illumio.com	A collaboration application that can be confi...

- Click the **+Add** button to create a custom service. The Services page appears.

**Services (Create)**

**General**

**Name**

**Description**

**Service Definitions** **+ Add** **- Remove**

Port and/or Protocol	Process	Windows Service
<input type="checkbox"/> E.g. 22, 514 UDP, ICMP	<input type="text" value="E.g. c:\windows\myprocess.exe"/>	<input type="text" value="E.g. myprocess"/>

- Complete the settings for the new service and click **Save**.

## Add IP Range

- From the main menu, choose **Policy Objects > IP Ranges**. The list of IP ranges you have previously defined appears.

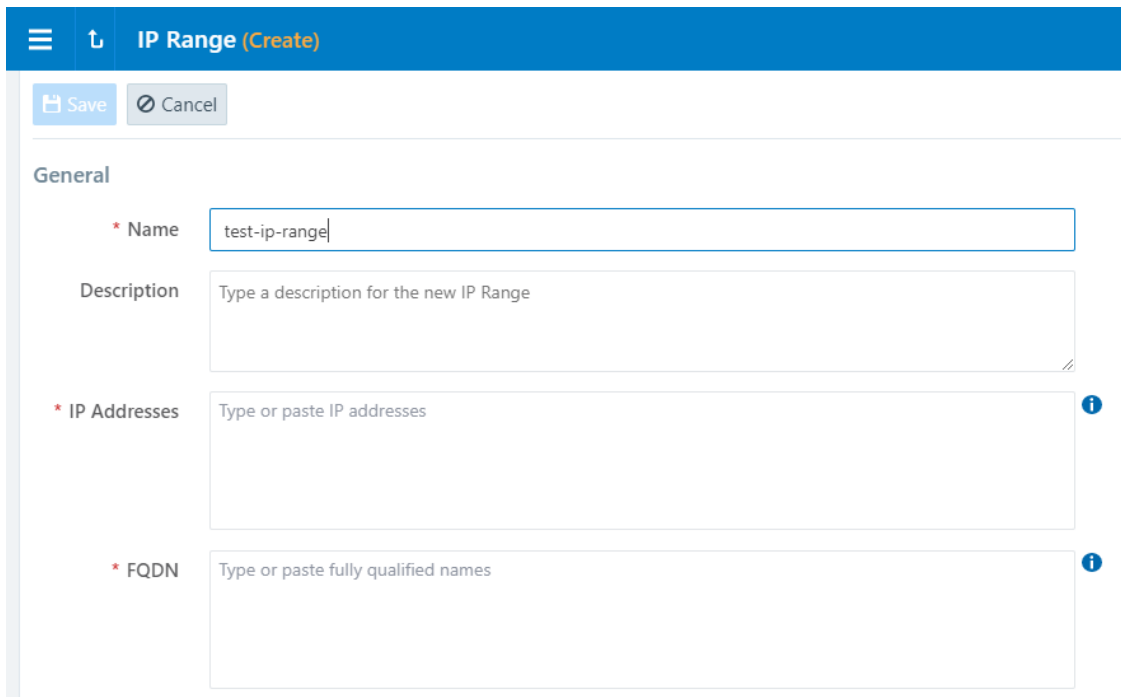
Provision Status	Name	Addresses	Last Modified On	Last Modified By
<input type="checkbox"/>	AD Servers	10.10.10.1-7	06/09/2020, 08:20:20	illumio.com
<input type="checkbox"/>	Any (0.0.0.0/0 and ::/0)	0.0.0.0/0 +1 more	11/27/2019, 10:31:07	System
<input type="checkbox"/>	Local	10.10.10.1/8	06/09/2020, 08:31:09	illumio.com



### NOTE

You can also add FQDN or an FQDN pattern in the IP Ranges page.

- Click the **+Add** button to add a custom IP range.



For information about specifying an FQDN for the IP range, see [Policies Using Domain Names \[38\]](#).

3. Complete the settings for the new IP range and click **Save**.

## Add User Group

User Groups in Illumio Edge allow you to leverage Microsoft Active Directory (AD) User Groups in your Illumio Edge outbound policy. With this feature, you can create user groups in the Illumio Edge that map directly to your AD groups. You can then create policy with these groups so that you can control outbound access on specific endpoints (the destination of the outbound policy) based on the group membership of the user logged in to that endpoint.

If you combine setting up user groups and including FQDNs in outbound policy, you can write rules that control which AD groups can access corporate applications or public Internet resources that are identified by those FQDNs. For example, you might want to allow only employees in the Sales user group to access the ERP application, but not users in HR. You might want to allow HR users to only access HR applications, but not all internal resources.

To add a user group:

1. From the Illumio Edge main menu, choose **Policy Objects > User Groups**.  
The User Group page appears.
2. Click **Add**.
3. In the Add User Group page, enter a name, system identifier (SID), and description for the AD group.
4. Click **Save**.  
The new user group appears in the User Groups list. You can now use the user group in allow rules for outbound endpoint policy to control access to specific applications.

## Inbound Policy in Edge

You can configure inbound policy for a new group or update the policy for an existing group. For information about how Illumio Edge defines inbound policy at the group level, see [Edge Groups \[25\]](#).

Illumio Edge includes a wizard that walks you through the steps to select services and source IP ranges for inbound policy, and then preview and provision the policy.

## Process-Based Rules in Inbound Policy



### TIP

When services have dynamic ports, consider creating a policy that is tied to the process or Windows service and allow all ports. This way, the host firewall will control access only on those ports on which that application is listening.

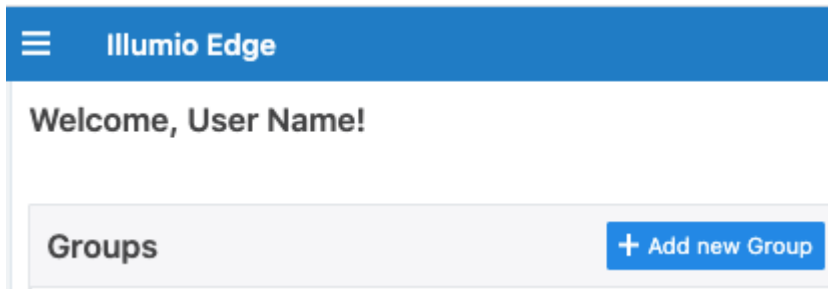
The Windows process-based type of service is used by Windows endpoints and defined by specifying ports and protocols, processes, or Windows service name. The process paths can contain:

- Windows OS defined system environments variables such as, %SystemDrive%, %SystemRoot%, %WINDIR%, %ProgramFiles(x86)%, %ProgramFiles%, and %ProgramData%.
- Windows OS defined per-user environments variables such as, %APPDATA%, %HOMEPATH%, and %USERPROFILE% are not supported.
- Drive letters other than C: such as, X: and Z: are supported, provided they exist in the endpoint.
- Network UNC path in the "\\server\folder" format is supported.
- Driver letter mapping to a UNC path is supported
- Path containing NTFS mount point is supported.
- A process path need not exist in the endpoint at time of policy provisioning.

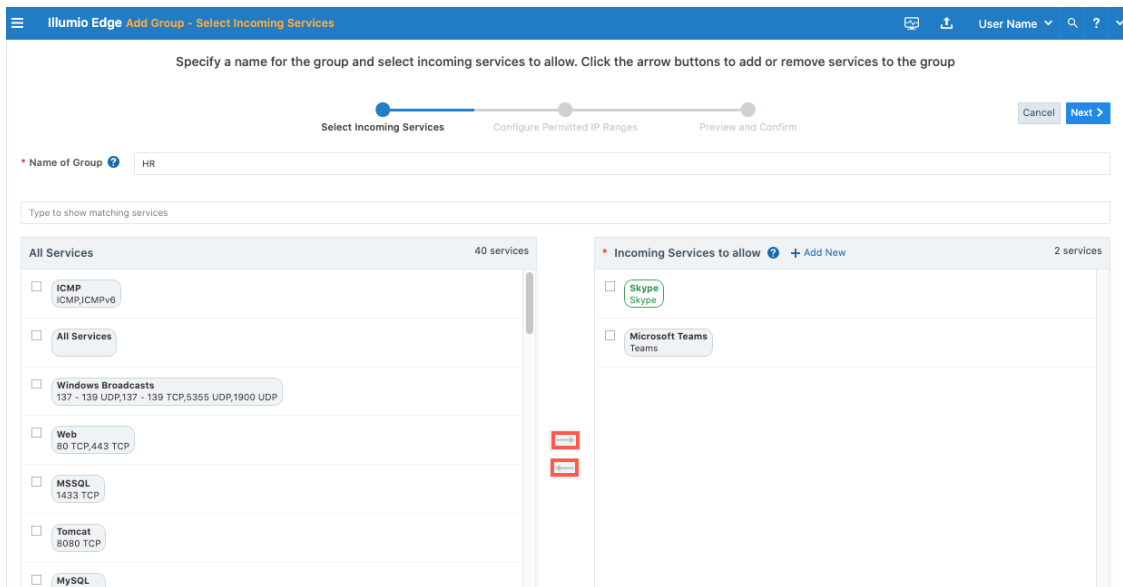
## Select Incoming Services

A service is an incoming peer-to-peer service that you would want to include while writing your policy. It can be a port and protocol, a process, or a Windows service. Illumio Edge provides a list of common applications and you can select which items you want. This topic describes how to select the Incoming Services to allow for peer-to-peer communication.

1. From the Illumio Edge main menu, choose **Groups**.
2. To define inbound policy for an existing group, click the group in the Groups pane > **Inbound Policy** tab > **Edit Group** button.  
Or  
To add a new group, click **Add new Group**.



3. The wizard starts that guides you through configuring inbound policy. In the **Name of Group** field, enter or update the name for the group; for example, *HR*. The group you have selected is the group of endpoints that the policy is applied to.
4. Select the incoming services. By default, Illumio Edge provides approximately 30 services in the All Services list. Start entering a service name in the “Type to show matching services” field to filter service in the All Services list. Select the service you want and use right/left arrows to add or remove them from the “Incoming Services to allow” list. For example, you can add *Skype* and *Microsoft Teams* to be allowed for this HR group.



### TIP

In the next step of the wizard, you can add multiple IP ranges for the same service, thereby allowing you to specify smaller CIDR blocks and IP ranges. See [Configure IP Ranges \[34\]](#).

5. (Optional) Click the **Service** name to view or edit it.

6. To use a custom peer-to-peer application that is not in the provided All Services list, click **Add New** and define that service. Enter a **Name**, **Description**, and **Service Definitions** (port and/or protocol, process, and Windows service) and click **Save**. You have the option to select the “All Operating Systems: Port-Based” and the “Windows: Process/Service-Based.”

The new service is added to the list.

You have now defined your incoming services, which means you have confirmed the selected services to be authorized for the specified group.

7. Click **Next** to continue the wizard and configure source IP ranges for the inbound policy.

## Configure IP Ranges

An IP range is a range of IP addresses that is permitted to communicate using an incoming service. It could consist of a single IP address, a CIDR block, or an IP range.

You configure the authorized IP ranges that are allowed to communicate on the services you have defined. For example, in the case of *Skype*, the IP range can be *Any* because you want all the laptops of employees that belong to the HR group to communicate with each other via Skype. By default, Illumio Edge provides a few IP range options, such as *Any* and *RFC 1918*, which you cannot edit.

1. From the Source IP Ranges drop-down menu, select an incoming IP range that is permitted to communicate for each of the incoming services you added.

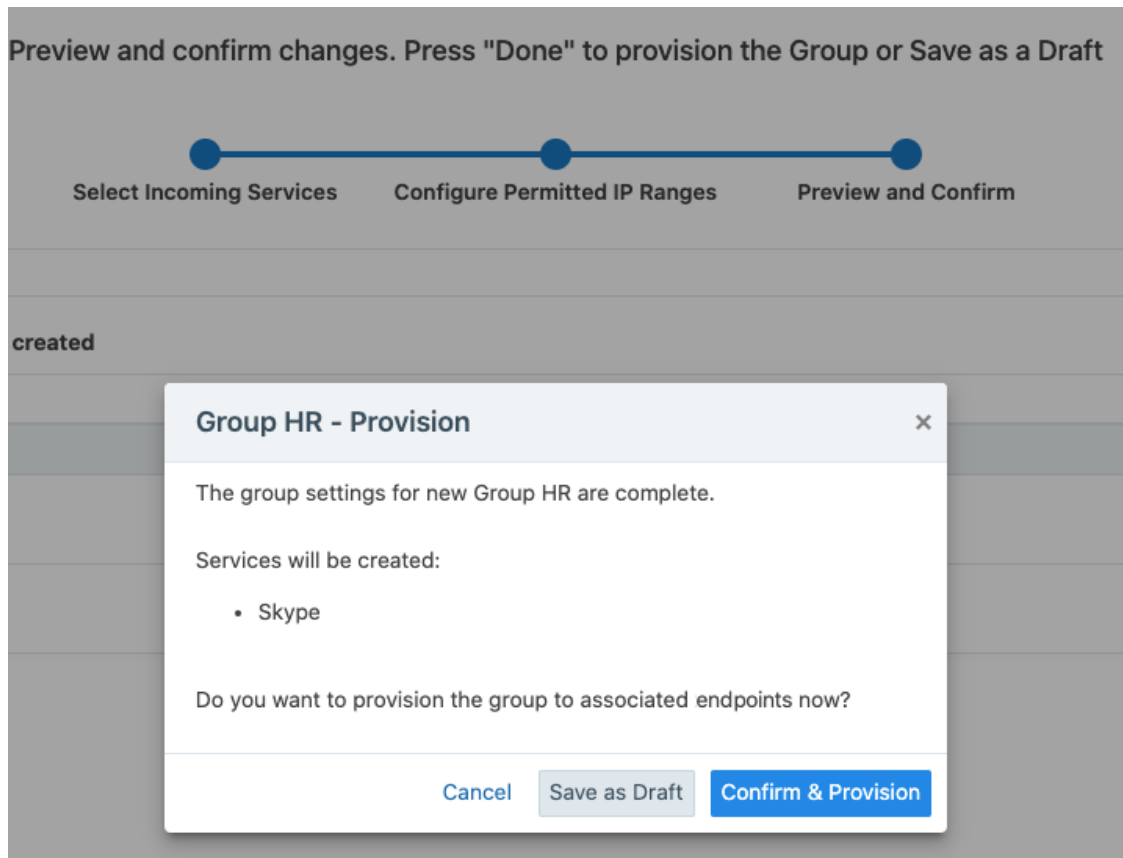


### TIP

To apply an IP range to more than one service, select those services and click Apply IP Range.

2. (Optional) To create a new custom IP range, click **Add New**. Click the **i** icon to see the examples.

3. Specify the network profile for each service and its source IP range. See [Network Profiles \[25\]](#) for information.
4. After choosing the IP ranges, click **Next** to view the summary of your Rules, which displays the list of incoming services and permitted IP ranges.
5. Click **Done** to provision the rules or save them as a draft.
6. Verify the information in the pop-up and click **Confirm & Provision** to provision the rule to the associated endpoints.



If you selected **Save as Draft**, see the Draft Changes section.

7. After successful provisioning, the **Illumio Edge Groups** are displayed, with the groups, their provision status, and the number of VENs that are associated with that group (number of paired endpoints) displayed in the left panel. If you want to add additional endpoints, click the '+' button located next to the number of VENs as described in the [Agent Installation \[40\]](#) section.  
The inbound traffic configured for that group is displayed in the right panel. For information, see the [Explorer \[55\]](#) section.

## Outbound Policy in Edge

This section describes how you create outbound policy for your endpoints by configuring the global Organization Policy in Illumio Edge.

### About Organization Policy

In Illumio Edge, you set up outbound policy at the organization level so that the same outbound policies are applied to all endpoints on which you have installed the Illumio Edge agent (known as the VEN). This way, you do not need to replicate outbound rules to all Edge groups. Managing outbound policy is efficient because you do it at the organizational level.

When you view outbound policy for a specific group, the tab displays the rules as read-only. When you update your Organization Policy, you only need to provision the changes once because the changes are provisioned to the PCE as one set of rules.

### Elements of Outbound Policy Rules

In outbound policy, each rule includes the following elements:



- Source Groups
  - Illumio Edge groups (which are groups of endpoints)
  - User groups (Active Directory groups)

You can specify a single group, multiple groups, or all groups.

- Destination IP Ranges
  - IP addresses, CIDR blocks, IP ranges
  - Exclude IP addresses, CIDR blocks, IP ranges
  - FQDNs, including with wildcard characters
- Destination Services
  - Port and protocol

You can specify multiple services per rule.



#### NOTE

Illumio Edge includes a list of 100+ service definitions and you can use in policy or you can define your own services.

- Network Profile
  - Corporate
  - External

You can use the destination services to create very granular outbound security policy. For example, you could have services on a server that you want to control access to. You specify the ports and protocols or Windows processes/services in your Organization policy that only specific endpoint groups can access.

## Rule Evaluation for Outbound Policy

Organization policy for outbound control consists of three parts:

- Allow rules
- Deny rules
- A default rule

Illumio Edge evaluates and applies policy in the following order:

1. If you haven't defined a global Organization Policy, a default rule allowing all outbound policy.
2. When you have defined Organization Policy, rules in the following order:
  - a. All allow rules
  - b. Deny rules
  - c. The default rule that all outbound traffic is allowed  
You cannot edit or delete the default rule.

As soon as Illumio Edge finds a match with an outbound rule, that rule controls the outbound traffic and the evaluation process stops.

For endpoints, this is usually how you start creating global outbound policy for the Corporate network profile. Namely, this profile has a default allow for all traffic; then, you can start to define policies based on corporate security, compliance, or audit requirements. Lastly, you define different policies for what users can or cannot connect to outbound from their endpoints.

## Policies Using Domain Names

In Illumio Edge, you can use domain names to control allowed traffic for your endpoints. Domain names can be fully-qualified domain names (FQDNs) or domain name patterns using wildcards (for example, \*.google.com).

Specifically, you can specify FQDNs in the destination IP ranges for outbound policy.



### NOTE

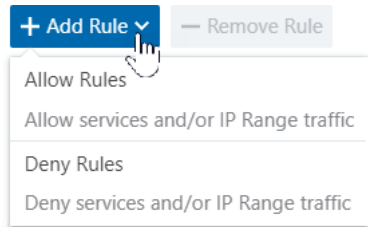
You can add FQDNs *only* to IP ranges for allow rules. They are not supported in outbound deny rules.

Adding FQDNs in policy is especially useful for allowing traffic to your corporate applications. For example, you could create an outbound policy by adding an allow rule for your Engineering team to connect to `jira.samplecompany.io` so they can access your Jira application running in your corporate data center or in your colo hosted in a public cloud.

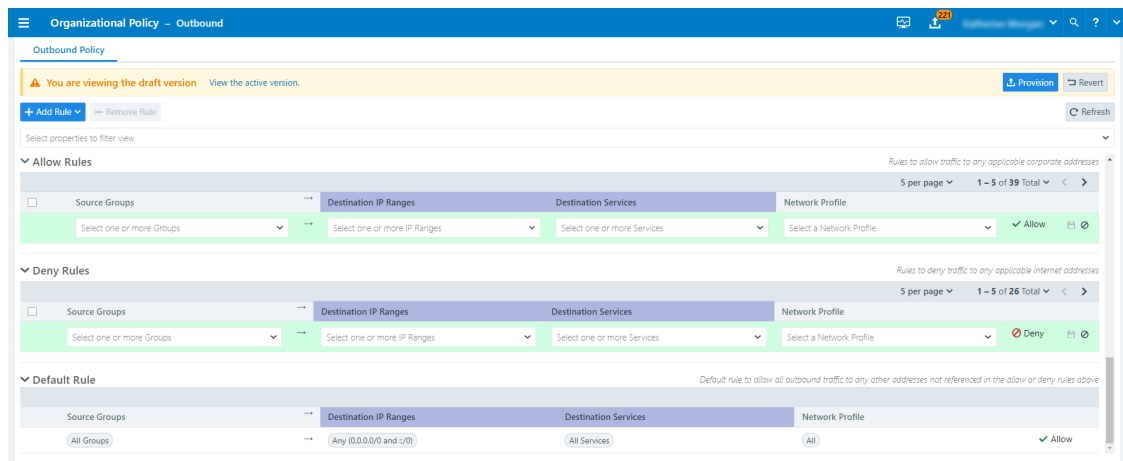
Illumio Edge provides the same support for FQDNs in policy that Illumio provides for Illumio Core. See [FQDN-Based Rules](#) in the *Illumio Core Security Policy Guide* for more information.

## Configure Organization Policy

1. From the main menu, choose **Organization Policy**. The Organization Policy – Outbound page appears.
2. Click **Add Rule** and choose either allow rule or deny rule.



A new row appears in the table in either the Allow Rules or Deny Rules section depending on the type of rule you are adding.



The structure of each type of rule is the same – source groups, destination IP ranges, destination services, and network profile.

3. Complete the settings for the allow or deny rule that you are adding. See [About Organization Policy \[36\]](#) for more information.
4. Click the Save icon (💾) for the new rule at the end of the row.  
The new outbound policy is saved as a draft. To provision the policy changes, click Provision. See [Provision Policy \[39\]](#) for information.

## Provision Policy in Edge

Provisioning means the policies you have defined are sent to the VENs that are installed on the endpoints.

### Draft Changes

Any changes you make to groups, IP ranges, services, or policy need to be provisioned. When your PCE has changes that need to be provisioned, the orange badge on the Provision button indicates the number of changes that need to be provisioned. When you select the check-box and click **Provision**, the PCE recalculates the changes and transmits those changes to the VENs installed on your endpoints. All of the changes you make to those items are considered to be in a "draft" state (un-versioned) until you provision them. After the provisioning is complete your changes, those changes become "active" and current.

Draft Changes

User Name

Provision

1

Revert

1

1 IP Range

Refresh

Select properties to filter view

1 Selected

Customize columns

50 per page

1 - 1 of 1 Total

Change

Name

Item

Last Modified By

Last Modified On

DELETION PENDING

\*ec2.

.com

IP Range

@illumio.com

01/08/2020, 11:52:03

When you confirm provisioning by clicking **Confirm & Provision**, the Provisioning progress indicator displays the number of endpoints that need to be synchronized with the latest provisioned policy changes and the progress for applying the policy changes to those endpoints.

Provision selected items					
Change	Name	Item	Last Modified By	Last Modified On	Remove
<div>DELETION PENDING</div>	*ec2.	.com	IP Range	@illumio.com	01/08/2020, 11:52:03
Summary					
1 Total : 1 IP Range					
Provision Note					
Provision Note					
<div> <div>The PCE recalculates policy and sends it to impacted VENs when you provision.</div> </div>					
<div> <div>Cancel</div> <div>Confirm &amp; Provision</div> </div>					

On the Provisioning page, you can:

- View the previous policy change by clicking View the last commit.

- View the list of policy versions by clicking View Policy Versions.

## Policy Versions

Select Provision > Policy Versions from the top-left main menu [☰] on the left or from the top-right provision menu [⬆]. The policy versions are displayed under the Version column.

Policy Versions

Provision

Revert

Refresh

Customize columns

50 per page

1 – 35 of 35 Total

Version	Group	Services	Provisioned By	Note
	IP Ranges		Provisioned On	
1	Group 1 IP Range	2 Services	System 07/19/2019, 13:21:37	System created default
2	Groups 7 IP Ranges	10 Services	<div></div> @illumio.com 10/24/2019, 12:28:10	Duplication from <div></div> .io
3	Groups 7 IP Ranges	10 Services	<div></div> illumio.com 10/24/2019, 17:50:06	
4	Groups 7 IP Ranges	10 Services	<div></div> @illumio.com 11/05/2019, 18:51:48	

## Agent Installation in Edge

An agent installation script is generated for every Group. You can use any of the deployment options to deploy the agent on your endpoints.

## Ways to Install Agents

You can deploy Illumio Edge agents in several ways:

- Use Microsoft Endpoint Configuration Manager [formerly System Center Configuration Manager (SCCM)]
- Use group policy to push out an executable
- Systems manager or master data management (MDM)
- EXE bundle
- Any software deployment tool that you currently use



### IMPORTANT

You need to be a member of your organizations' desktop administration team with the required permissions to deploy Illumio Edge.

## VEN Library

The PCE can act as a repository for distributing, installing, and upgrading the VEN software. The PCE can host multiple VEN versions, allowing you to evaluate and certify new versions of the VEN while continuing to deploy older versions in production. The VEN Library page is available after you have loaded a VEN software bundle. From this page, you can download individual VEN packages and also view the dependencies and supported OS versions.

VEN Library					
<div>  Refresh            Dependencies            Supported OS Versions         </div>					
Select properties to filter view					
<div>  Customize columns           50 per page           1 – 50 of 97 Total         </div>					
Default	Release	VEN Filename	Distribution Architecture	OS Version	Download
✓	20.1.2-103	illumio-edge-20.1.2-103.win.x86.exe	Windows x86		
✓	20.1.2-103	illumio-edge-20.1.2-103.win.x64.exe	Windows x64		
	19.3.100-2	illumio-hven-19.3.100-2.win.x86.msi	Windows x86		
	19.3.100-2	illumio-hven-19.3.100-2.win.x64.msi	Windows x64		
	19.3.0-	illumio-ven-19.3.-686.rpm	CentOS i686	6	
	19.3.0-	illumio-ven-19.3.-x86_64.rpm	CentOS x86_64	6	
	19.3.0-	illumio-ven-19.3.0-x86_64.rpm	Amazon	1	

## Add VENs to a Group

From the Groups list, click **Add VENs** for the endpoint on which you want to install a VEN.

**Illumio Edge**

### Welcome, User Name!

You have Security Rules set up for 14 Groups of Endpoints

**Groups**

Select properties to filter view

Customize columns
 50 per page
 1 – 14 of 14 Total

Provision Status	Group	Endpoints	
MODIFICATION PENDING	Domain_Grp2	None	

Click the up arrow on the Install Script page to view the Endpoints and VENs page.

## Install and Activate

```
illumio-edge-20.2.0-310.win.x64.exe /install /quiet /norestart /log C:\Windows\temp\Illu
```



The `quiet`, `norestart`, and `log` commands are all optional.

## Upgrade VENs

42

Connectivity	Health	Name	Version	Group	OS	Status
<input type="checkbox"/>	Online	WSWIN10	19.3.0-6107	JDSBaseGroup0	win-x86_64-server	Suspended
<input type="checkbox"/>	Online	LAPTOP	20.12-103	JDSBaseGroup0	win-x86_64-server	Active
<input type="checkbox"/>	Offline	DESKTOP	19.3.100-2	JDSBaseGroup0	win-x86_64-server	Active
<input checked="" type="checkbox"/>	Online	16	20.1.100-105	JDSBaseGroup0	win-x86_64-server	Active
<input type="checkbox"/>	Offline	WIN7-ON-WIN10	20.1.0-5-server	JDSBaseGroup0	win-x86_64-server	Active

## Requirements for Agent Installation in Edge

The following requirements and prerequisites must be met to install the Illumio Edge agent (the VEN) on endpoints.

### Requirements

In order to deploy Illumio Edge, you require:

- Illumio SaaS PCE login credentials
- Windows 7 or Windows 10 machines

### Prerequisites

Illumio Edge requires Visual C++ runtime libraries, which is provided by Microsoft as a redistributable package. If the Visual C++ runtime is not available on your system, Illumio Edge will pre-install it during the installation process. The Visual C++ runtime is a system component, so you may choose to install it separately from Illumio Edge.

You may download the latest Visual C++ runtime from:

<https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads>

## VEN Connections via Proxy Servers

Illumio Edge supports a VEN to PCE connection through proxy servers:

- The default proxy configuration on the OS is used and proxy configuration may or may not be required or available on the VEN. See configuration details below.
- Only non-authenticated proxy is supported, which may require you to add an exception for the PCE address.
- Only HTTP proxy is supported. The VEN will detect the proxy automatically and configuration or mode change will not be required.

The configuration details are as follows:

- If the network environment supports WPAD protocol, the Edge VEN will automatically use WPAD to discovery proxies and no special configuration is required.
- If proxy configuration is done via a PAC file, you will have to import Internet Explorer's (IE) proxy setting with the PAC file URL to the LocalSystem user (S-1-5-8). The VEN only supports `http://` PAC file URL. It does not support `file://` URLs.

- If proxies are statically configured, you can configure using one of the following two methods:
  - Using `netsh winhttp set proxy` command. This method takes precedence. For `netsh winhttp` usage, refer to [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731131\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731131(v=ws.10)).
  - Importing IE setting with static proxies setting to the LocalSystem user. For importing IE settings for the VEN, refer to <https://serverfault.com/questions/34940/how-do-i-configure-proxy-settings-for-local-system>.



## NOTE

Both IE-based proxy setting and `netsh winhttp` can be pushed to the endpoints (PCs) using Group Policy.

## Endpoints and VENs in Edge

After you pair endpoints, you can view details by clicking a single endpoint. Only groups that the endpoint is in are displayed. Each endpoint, last received, group. You can **Edit** the endpoint description, policy state and managed interfaces. The VENs page displays a list of all the VENs. If you click on a VEN it opens the corresponding endpoint. You can unpair, generate support reports, and suspend a VEN. Clicking the Add button located next to the Policy State button, displays the Group's Install Script page.

## VENs Page

[ADD INTRO]

Endpoints and VENs – VENs

1

75

User Name

Endpoints

VENs

Unpair

Upgrade

2 Active

1 Suspended

Refresh

Reports

Select properties to filter view

Customize columns

50 per page

1 – 3 of 3 Total

<input type="checkbox"/>	Status	Health	Name	Version	Group	OS
<input type="checkbox"/>	<div>Suspended</div>	✓	W...KI	20.2.0-308	Domain_Grp29	win-x86_64-server
<input type="checkbox"/>	<div>Active</div>	✓	W...H	20.2.0-308	Non-Domain_Grp1	win-x86_64-server
<input type="checkbox"/>	<div>Active</div>	✓	W...AG	20.2.0-308	Domain_Grp29	win-x86_64-server

## Endpoints Page

[ADD INTRO]



Connectivity	Policy Sync	Group	Last Applied Policy	Enforcement	Visibility	Name
Online	<span style="color: red;">Suspended</span>	Domain_Grp29	11/23/2020, 16:46:28	Visibility Only	Blocked + Allowed	W10IL...<I
Online	<span style="color: green;">Active</span>	Non-Domain_Grp1	11/23/2020, 16:55:47	Enforced	Blocked	W10IL...3H
Offline		Domain_Grp29	11/23/2020, 16:47:12	Visibility Only	Blocked + Allowed	W10IL...G

Endpoints have the following attributes:

- Endpoint enforcement and visibility state
- Connectivity and policy sync state
- Endpoint labels
- Attributes

## Endpoint Enforcement States

Policy state determines how the rules affect a endpoint's network communication. Illumio Edge includes three policy states for endpoints:

### • Idle

The Idle state is used for installing and activating VENs on endpoints without changing the endpoints' firewalls. Illumio Edge does not take control of the endpoint's native OS firewall. The VEN uses the endpoint's network analysis to provides relevant details to Illumio Edge. No traffic is blocked in this state. In this mode, you get 'Limited' visibility and the snapshots of flows from the endpoint is collected periodically. A pairing profile can be used to pair endpoints in the idle state.

### • Visibility Only

In the Visibility Only state, the VEN inspects all open ports on an endpoint and reports the flow of traffic between it and other endpoints to Illumio Edge. In this mode, you can only select the 'Blocked + Allowed' option and Illumio Edge logs and displays traffic information for allowed and potentially blocked traffic. 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.

### • Enforced

Used to enforce the policies. The policies written are now active. In the enforced state, you can select any of three visibility levels to define how much data the VEN collects from the endpoint and sends to the PCE:

- Off: The VEN does not collect or display any information about traffic connections.
- Blocked: Illumio Edge logs and displays traffic information for blocked traffic. 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.
- Blocked + Allowed: Illumio Edge logs and displays traffic information for allowed and blocked traffic. The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections.

**Endpoints and VENs – VENs**

1 Workload in Suspension

+ Add Move to Group Enforcement Visibility Increase Traffic Update Rate Refresh Reports

Select properties to filter view

1 Selected

Connectivity	Policy Sync	Group	Last Applied Policy	Enforcement	Visibility	Name
<input type="checkbox"/> Online	<span style="color: red;">Suspended</span>	Domain_G	11/23/2020, 16:46:28	Visibility Only	Blocked + Allowed	W1 KI
<input checked="" type="checkbox"/> Online	Active (Syncing)		11/23/2020, 16:55:47	Visibility Only	Blocked + Allowed	W1 8H

[UPDATE SCREENSHOT]

**Endpoint – W10 KI (Edit)**

Summary Processes Rules Blocked Traffic

Save Cancel

**General**

Name W10 /KI

Description

Enforcement Enforced

Visibility

- ☐ Off  
Illumio Edge does not log and display traffic information
- ☐ Blocked  
Illumio Edge logs and display traffic information for blocked traffic
- ☒ Blocked + Allowed  
Illumio Edge logs and display traffic information for allowed and blocked traffic

**Group Assignment**

Group Domain\_Grp29 Select Group

**Network Interfaces**

Managed interfaces will be included in policy configuration provided by PCE  
Ignored interfaces will NOT be included in policy configuration provided by the PCE. Traffic will continue to flow through the interface uninterrupted.

Interface Name	Subnet(s)	PCE Action
----------------	-----------	------------

The recommended flow of policy state cycle is to start with the Idle mode and then move to the Visibility mode to refine and provision your policies. After confirming that the policies suit your organization needs, move to the Enforced mode and select the detail level based on the amount of traffic details you want the VEN to report to the Illumio Edge.

## Endpoint Summary

Endpoint summary provide detailed information such as the hostname, the VEN software version, and other attributes. If an endpoint belongs to a particular group, it will receive the rules defined for that group after the ruleset is provisioned.

- The name of the endpoint
- A description (if provided)
- The endpoint's enforcement states

- The visibility the VEN uses
- The dates when the policy was revised and last applied
- The endpoint's VEN connectivity status
- The endpoint's VEN policy sync status
- Group name
- Endpoint system attributes (such as, VEN version number, hostname, and uptime)

[UPDATE SCREENSHOT]

↑

Endpoint - W108H

3H

Summary

Processes

Rules

Blocked Traffic

✎ Edit

General

Name

W108H

Description

Enforcement

Visibility Only

Illumio Edge does not block any traffic

Visibility

Blocked + Allowed

Illumio Edge logs and display traffic information for allowed and potentially blocked traffic

VEN

W108H

Connectivity

● Online

Policy Sync

↻ Active (Syncing)

Policy Last Applied

11/23/2020 at 16:55:47

Group

Group

Ryan

Attributes

VEN Version

20.2.0-308

Hostname

W108H

OS

win-x86\_64-server

Release

18362.1.amd64fre.19h1\_release.190318-1202 (Windows 10 Enterprise)

Uptime

77 Days, 2 Hours, 59 Minutes

Heartbeat Last Received

11/24/2020, 21:10:37

Interfaces

eth3276 10.8.0.1 (domain)

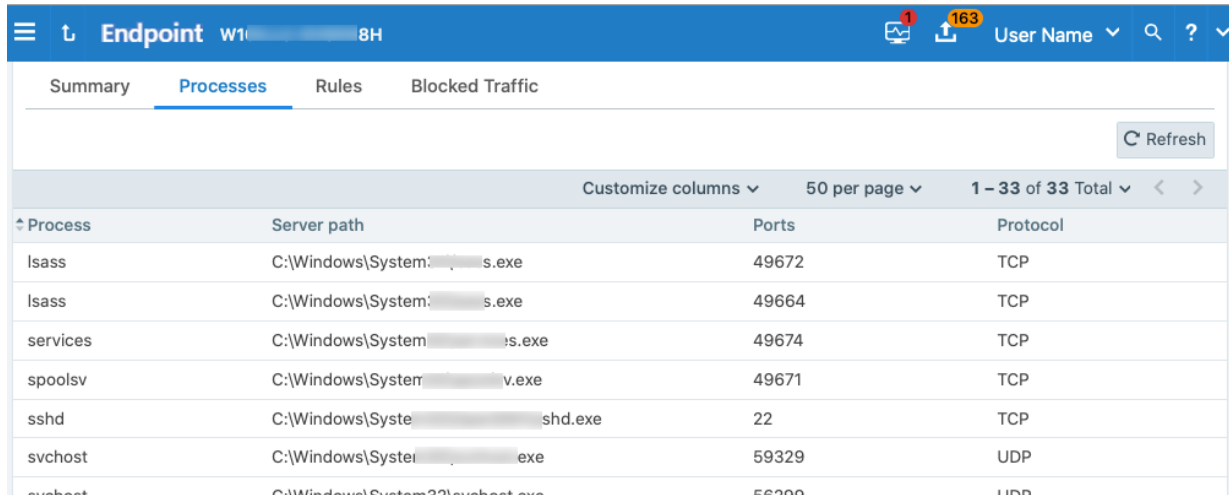
eth3276 10.8.0.12/64 (domain)

## Endpoint Processes

In the Endpoint Processes tab, you can view the processes currently running on the endpoint. For each process running on the endpoint, the following information is listed:

- Process name
- Server path
- Ports used by the process
- Protocol (for example, TCP or UDP)

[UPDATE SCREENSHOT]



Process	Server path	Ports	Protocol
lsass	C:\Windows\System32\lsass.exe	49672	TCP
lsass	C:\Windows\System32\lsass.exe	49664	TCP
services	C:\Windows\System32\services.exe	49674	TCP
spoolsv	C:\Windows\System32\spoolsv.exe	49671	TCP
sshd	C:\Windows\System32\sshd.exe	22	TCP
svchost	C:\Windows\System32\svchost.exe	59329	UDP
svchost	C:\Windows\System32\svchost.exe	56799	UDP

## About Admin Access in Edge

In Illumio Edge, you control which inbound connections your endpoints are allowed to accept. You can set up standard Illumio Edge groups to control access to endpoints. See [About Edge Groups \[25\]](#) for information. Alternatively, you can use the Admin Access feature to control endpoint access.

### Network-level Access Control Using PKI Certificates

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

Using Admin Access, you can control access to network resources based on Public Key Infrastructure (PKI) certificates. Because the feature bases identity on cryptographic identity associated with the certificates and not IP addresses, mapping users to IP addresses (common for firewall configuration) is not required. When using Admin Access, an endpoint can use the certificate-based identity of the connecting endpoint to verify its authenticity before allowing it to connect.

For more information, see [Configure Admin Access in Illumio Edge \[50\]](#).

### Benefits of Admin Access

Choosing to allow inbound access to endpoints by configuring Admin Access has the following benefits:

- Allows administrators to access endpoints in other groups for troubleshooting and maintenance purposes and access by other endpoints is disallowed.
- Is independent of IP ranges that can change or overlap.
- Is easy to deploy because it is completely software based.

## How Admin Access Works

To delegate endpoint management, you create Admin Groups in Illumio Edge. An administrator marks a group as an Admin Group. A member of that Admin Group can access and manage endpoints in other groups (target groups). You configure the target groups to allow access from the specific Admin Groups you have designated.

For example, if you want the IT department to manage two other departments, such as Engineering and Marketing, first designate the IT group as an Admin Group. Then, in those target groups, authorize the IT Admin Group access to them. IT administrators will be able to administer services for any endpoint belonging to either of those groups.

## IPsec Operation for Admin Access

Illumio Edge utilizes IPsec configuration to endpoints with IKE ID sets. IPsec configuration is required for this feature, but only for authenticating endpoints. You can choose to encrypt the connections between the Admin Groups and the endpoints in standard groups, but this is completely optional. Endpoints that can successfully authenticate using IKE are allowed to connect with each other.

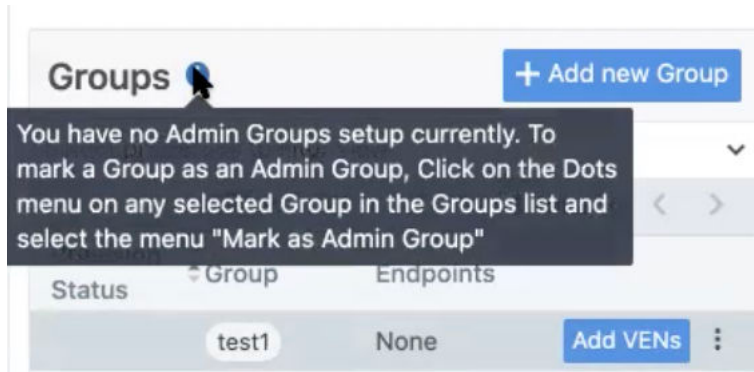
## Requirements for Using Admin Access

To use the Admin Access feature for your endpoints, you must meet the following requirements:

- Be a member of the Global Organization Owner or Global Administrator role so that you can mark groups as Admin Groups. See [Access Management \[18\]](#) for information.
- Are running the Illumio Edge 21.1.0 VEN or later on the endpoints that will accept connections from Admin Groups. See [Agent Installation \[40\]](#) for information.
- Have configured an IKE certificate in Illumio Edge. See [Configure Admin Access in Illumio Edge \[50\]](#) for information.
- Have deployed the PKI certificates on the endpoints that will use the Admin Access feature. See [PKI Certificates for Admin Access \[54\]](#) for information.

## View Admin Groups

Before you begin setting up an Admin Group, you will see a message when you hover over the information button next to the Groups heading. This message states that no Admin Groups have been set up:



After you have designed some Admin Groups, you can identify them in the Groups page in the following ways:

- A colored bubble to the left of the group's name in the left navigation pane.
- A badge appears to the right of the Group in the top pane.
- The badge, "Admin Group" appears on the top right-hand corner for that group.
- Next to "Admin Group," you will see the number of groups that are managed by that admin. If you click on 'Used by X Groups', you will see the names of the group that it will manage. In this case, the Admin Group, test1, will manage group, test123



## Configure Admin Access in Edge

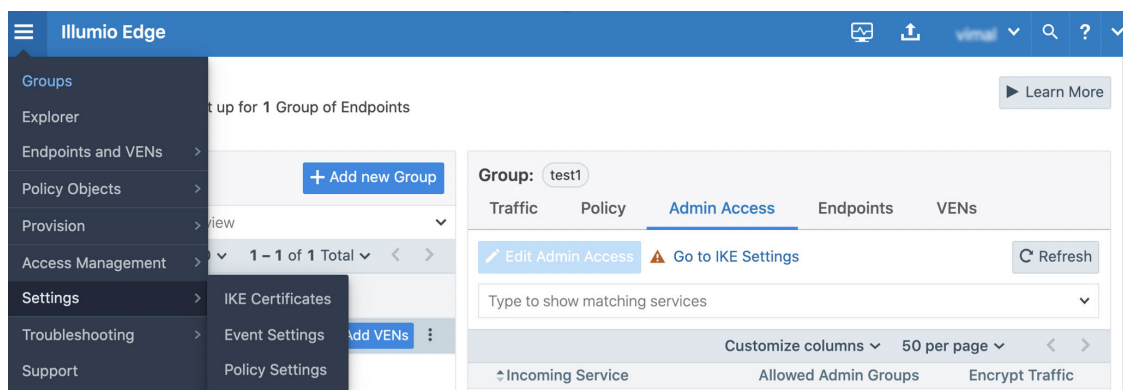
To configure Admin Access in Illumio Edge, perform the following tasks:

1. Configure an IKE certificate in Illumio Edge by specifying the details of the organization's PKI certificate.
2. Mark a group as an Admin Group.
3. Allow the Admin Group to access groups within your organization for group administration and management needs.

## Configure Certificate Issuer

IKE uses the control channel (UDP 500) to exchange certificates and a subset of the IPsec protocol called Encapsulating Security Payload (ESP) as the protocol on which data flows.

1. From the main menu, choose **Settings** > **IKE Certificate**. (Alternatively, you can click **Go to IKE Settings** in the Groups page.)



- The IKE Certificates page appears.
2. Click **Edit**.
  3. In the Certificate Issuer field, specify the details of the IKE certificate issuer's name. The name typically has the following format:  
C=Country-Name, O=Organization-Name, OU=Org-Unit-Name, CN=common-name@company.com  
For example, C=US, O=Illumio, OU=Engineering, CN=user@illumio.com.

4. Click **Save**.

## Mark a Group as an Admin Group

### Requirement

Before you mark a group an Admin Group, you must configure an IKE certificate. If you haven't configured a certificate, an error message appears when marking the group:

You will also see the error message on the Admin Access tab for that group:

To mark a group as an Admin Group:




### TIP

If you want to create a new group and designate it as an Admin Group, see [About Edge Groups \[25\]](#) for information.

1. From the Groups dashboard, locate the group that will serve as the Admin Group. In case the list of groups is long, use a filter to search for the group you want to mark as an Admin Group.
2. Click the 3 dots to the right of the group name to display a drop-down menu and choose **Mark as Admin Group**.

The screenshot shows the 'Groups' dashboard. At the top, there's a header with 'Groups' and an info icon, and a blue button '+ Add new Group'. Below the header is a filter bar with 'Select properties to filter view' and a dropdown arrow. Underneath is a table with columns: 'Provision Status', 'Group', and 'Endpoints'. The first row shows 'test1' under 'Group' and 'None' under 'Endpoints'. To the right of 'None' is a blue button 'Add VENs' and a three-dot menu icon. The dropdown menu is open, showing options: 'Edit Group', 'Mark as Admin Group', 'Stop Pairing', 'Edit Install Script', and 'Revoke Existing Install Script'.

3. Confirm that you want to mark that group.  
A blue badge [  test1 ] appears to indicate that the group has been designated as an Admin Group.

## Enable Admin Access in Target Groups

1. From the Groups dashboard, click the name of a target group that you want to enable admin access for. The details for that group appear.
2. Select the **Admin Access** tab.
3. Click **Edit Admin Access** to launch the Admin Access wizard.  
A page appears that displays All Services for that group.



Admin Access - Select Incoming Services - test123 Edit

Specify a name for the group and select incoming services to allow for Admin Access. Click the arrow buttons to add or remove services to the group

Select Incoming Services Allowed Admin Groups Preview and Confirm

\* Name of Group ? test123

RDP

All Services 13 Matched

Incoming Services to allow ? + Add New 0 Matched

Select an Incoming Service to begin

4. In the *All Services* column, select the services that will allow access from the Admin Group and click the right arrow to move them to the allowed column.
5. Click the next arrow. The Allowed Admin Groups step of the wizard appears. For each incoming service, you must indicate the Admin Group you want to grant access privileges to.
6. Click the checkbox for the incoming service to grant access to; then, choose the Admin Group (or groups) from the Select Admin Groups drop-down menu in that row.

Alternatively, you can select multiple incoming services and click **Apply Groups**. Choose the Admin Groups from the pop-up dialog box.

Apply Admin Groups to Selected Services?

Select Admin Groups to allow

☒ Add Admin Groups for selected services

☐ Replace Admin Groups for selected services

Cancel Apply

7. (Optional) To encrypt communication between the Admin Group and this group for a particular incoming service, select the Encrypt Traffic checkbox in that row. Selecting this option enables the use of IPsec encryption. If you do not select this checkbox, all authentication capabilities remain effective, but the traffic flows between the two groups will not be encrypted. Alternatively, you can select multiple incoming services and encrypt traffic for all those services by selecting the services and clicking **Encrypt Traffic**.
8. Click the next arrow. The Confirm and Preview step of the wizard appears.
9. Choose to save the Admin Access changes as a draft [📄] or provision [📥] them.
10. If you chose to provision the changes, enter a note (optional) and click **Confirm and Provision** in the "Provision selected items" dialog box.

You are done configuring Admin Access for the selected groups and incoming services.

## PKI Certificates for Admin Access in Edge

Configuring Admin Access in Illumio Edge enables IKE authentication and IPsec communication between Windows endpoints. In Illumio Edge, you enable IPsec communication by specifying the details of your IKE certificate, such as the distinguished name from the issuer field. See [Configure Certificate Issuer \[50\]](#) for information.

Additionally, you must set up the client-side PKI certificates on your Windows endpoints for Admin Access to work.

## Prerequisites and Limitations for PKI Certificates

The following prerequisites and limitations apply when configuring Admin Access to use PKI certificates:

- You must have a PKI infrastructure to distribute, manage, and revoke certificates for your workloads. The Illumio Edge does not manage certificates or deliver them to your endpoints.
- Illumio Edge supports configuring only one global Certificate Authority ID (CA ID) for your organization.
- The VEN on an endpoint uses a CA ID to authenticate and establish a secure connection with other endpoints.
- Endpoints must have CA identity certificates signed by the same root certificate authority. When endpoints on either end of a connection use different CA IDs, the IKE negotiation between them will fail and the endpoints will not be able to communicate with each other.
- The certificates you deploy for PKI or IPsec must have the following properties:
  - Version 3
  - Subject Name DN must contain the Common Name
  - SubjectAltName (must be the same as the Common Name)
  - CN and SubjectAltName must be in one of the following formats:
    - Email Address
    - DNS
  - Must contain key usage with:
    - Digital Signature
    - Key Encipherment
    - Data Encipherment
    - Key Agreement
  - Must contain Extended key Usage with:
    - IPSec End System
    - IPSec User
    - TLS Web Server Authentication (optional for mac OS x compatibility)
  - Must contain Authority Key Identifier

## PKI Certificate Setup on Endpoints

If you have a certificate management infrastructure in place, you can leverage it for IKE authentication between Windows endpoints managed by Illumio Edge. To use your PKI certificates with Admin Access, you must independently set up the certificates on your Windows endpoints.

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

## File Requirements

File	Requirements
Issuer's certificate	The global CA certificate, either root or intermediate, in PEM or DER format
pkcs12 container	<p>Archive containing the public key, private key, and identity certificate generated for the endpoint.</p> <p>Sign the identity certificate using the global root certificate.</p> <p>You can password protect the container and private key but do not password protect the public key.</p>

## Installation Locations

Windows Store

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

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

## Verify PKI Certificates in Illumio Edge

If you do not have a PKI certificate on both endpoints, the IKE certificate negotiation exchange process will fail. If one of the endpoints does not have a valid certificate, when you view an endpoint, the Policy Sync status will show up in an Error state.

To verify that you have an IKE certificate on an endpoint:

1. From the main menu, choose **Endpoints and VENS > Endpoints**.
2. In the endpoint list, click an online or active endpoint to display the details for the endpoint.

The Admin Access entry is displayed in the PKI Certificate details.

## Analyze Traffic with Explorer in Edge

Explorer allows you to analyze traffic flows for auditing, reporting, and troubleshooting purposes. You can access the Explorer feature from multiple locations in the UI as listed below.

- From the top-left main menu, select **Explorer**.
- By clicking on the traffic flow on the Groups page or by clicking the **View All Traffic** button located on the Groups page.

On the Explorer page, you can filter either Global (all groups) or per Group, Time, and Transmission mode. The transmission mode defaults to Unicast. You can select Broadcast or Multicast.

- **Source:** The origin IP address or endpoint for the selected flow.
- **Destination:** The destination IP address or endpoint for the selected flow.
- **Source Group:** The origin endpoint group for the selected flow.
- **Destination Group:** The destination endpoint group for the selected flow.

Explorer

Group

Global

Time

Last Hour

Transmission Mode

Unicast x

Select Traffic...

Reported View

Export

Format

Table

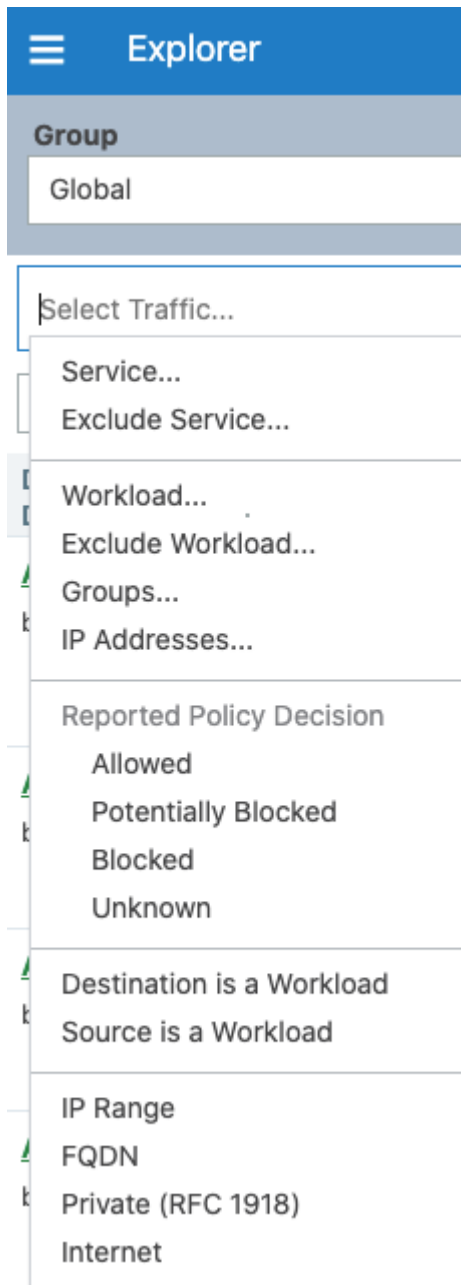
1 – 50 of 1,159 Matched

Reported Policy Decision	Source	Source Group	Destination	Destination Group	Port/Process [User]	Flows	First Detected	Last Detected
Allowed by Source	<div>SV-LT-1415</div> <div>192.168.1.76</div>		<div>54.159.142.08</div> <div>dzt-mcs-amzn-us-west-2-<div>phos.com</div></div> <div>Unicast</div> <div>Internet</div>		443 TCP mcsclient.exe [NT AUTHORITY\LOCAL SERVICE]	7	06/11/2020 13:34:34	06/11/2020 14:06:38
Allowed by Source	<div>SV-LT-1415</div> <div>192.168.1.11</div>		<div>52.144.162.62</div> <div>s.outlook.com</div> <div>Unicast</div> <div>Internet</div>		443 TCP outlook.exe [ILLUMIO\...]	10	06/11/2020 13:36:22	06/11/2020 14:06:24
Allowed by Source	<div>SV-LT-1415</div> <div>192.168.1.1</div>		<div>216.146.122.02</div> <div>www.googleapis.com</div>		443 UDP chrome.exe [ILLUMIO\...]	25	06/10/2020 18:18:54	06/11/2020 14:06:09

You can also sort based on Reported or Draft (All, Blocked, or Allowed) Views and Export the data.

- Draft View: View policies without provisioning them.
- Reported View: View policies by actually provisioning them.

For more in-depth and targeted filtering, you can select specific traffic criteria displayed on clicking in the **Select Traffic...** field.



On selecting the Parallel Coordinates format, the Explorer displays traffic flows as a vertical list of Source and Destination applications, and the port being used in the flows. You can also sort the results to view based on port number or number of traffic flows and also by process name or number of flows.

The Explorer feature has been enhanced to include its full functionality with filtering options along with filter based on Transmission type or Exclude Servers or IP Ranges. You can also use Explorer to find data about a certain port and protocol or find information for a specific flow over a certain period.

## Troubleshooting Tips in Edge

This section describes how to troubleshoot common issues while using Illumio Edge.

## Blocked Traffic

It displays all the blocked inbound traffic for the selected endpoint.

The Blocked Traffic page shows you all traffic that attempted to communicate with your endpoint but was blocked due to policy. Blocked traffic alerts provide information such as the source and destination IP, source and destination group, the total number of flows, and the time last detected.

Blocked Traffic							
Traffic is <b>Potentially Blocked</b> when a Endpoint is in <b>Visibility Only</b> mode. Traffic is <b>Blocked</b> when a Endpoint is in <b>Full Enforcement</b> mode. If the Endpoint is in <b>Selective Enforcement</b> , traffic is <b>Blocked</b> or <b>Potentially Blocked</b> depending on the Selective Enforcement Rule.							
1 - 50 of 459 Total							
Select properties to filter view				Last Hour		Go	
Traffic Type	Source	Source Group	Service	Destination	Destination Group	Total Flows	Last Detected
Blocked	66.151.147.212 Internet		63858 UDP zoom.exe	SV-LT-1415 192.168.125.26 Unicast	Base-Group	154	06/10/2020 13:30:28
Blocked	66.151.147.212 Internet		63857 UDP zoom.exe	SV-LT-1415 192.168.125.26 Unicast	Base-Group	130	06/10/2020 13:30:24
Potentially Blocked	192.168.0.194 RFC1918		57621 TCP spotify.exe	No Name 192.168.0.144 Unicast		1	06/10/2020 12:56:40
Potentially Blocked	192.168.0.194 RFC1918		57621 TCP spotify.exe	BIAO-PC 192.168.0.144 Unicast	Base-Group	1	06/10/2020 19:26:12
Potentially Blocked	192.168.0.194 RFC1918		50343 TCP spotify.exe	No Name 192.168.0.144 Unicast		49	06/10/2020 12:56:50
Blocked	10.14.0.201 RFC1918		49664 UDP swi_service.exe	SV-LT-1415 192.168.125.26 Unicast	Base-Group	1	06/10/2020 13:09:27

You can narrow down the view by filtering based on Group name, Traffic Status (Blocked or Potentially Blocked), name of the endpoint, and time filter (last hour, day, week, or month). You can sort the Source and Destination columns and choose to view Names or IP Addresses.

Traffic Status: Potentially Blocked		Select properties to filter view		Last Week		Go	
Traffic Type	Source	Source Group	Service	Destination	Destination Group	Total Flows	Last Detected
Potentially Blocked	SV-LT-1585 192.168.20.16		67 UDP	192.168.20.1 Unicast RFC1918		2	06/08/2020 04:44:53
Potentially Blocked	SV-LT-1585 192.168.20.16		67 UDP	192.168.20.1 Unicast RFC1918		1	06/06/2020 12:19:12
Potentially Blocked	192.168.20.1 RFC1918		1900 UDP svchost.exe SSDPSRV	SV-LT-1585 239.255.255.250 Multicast		360	06/10/2020 19:50:04
Potentially Blocked	192.168.20.15 RFC1918		5353 UDP chrome.exe	SV-LT-1585 224.0.0.251 Multicast		288	06/10/2020 19:49:12
Potentially Blocked	10.0.0.33 RFC1918		5353 UDP svchost.exe	DESKTOP-NVIO930 224.0.0.251 Multicast	Base-Group	2378	06/10/2020 19:46:15

## Events

The Events page displays a list of events based on the activities performed. You can export all events or export a filtered list of organization events to a CSV file. You can also do faster filtering via the browser.

Events

Export All

Export Filtered

Refresh

Select properties to filter view

	«		Customize columns	50 per page	1 – 50 of ~452,427 Total	<	>
by Event	▼	Event	Description	Severity	Status	Timestamp	Generated By
		user.logout	User logout	Informational	Success	06/10/2020, 20:05:02	System
by Severity	▼	system_task.agent_offline_check	VEN marked offline	Informational	Success	06/10/2020, 20:03:44	System
by Timestamp	▼	workload_service_report.update	Workload service reports updated	Informational	Success	06/10/2020, 19:57:15	
by Generated	▼	workload_service_report.update	Workload service reports updated	Informational	Success	06/10/2020, 19:52:08	
		user.login	User login	Informational	Success	06/10/2020, 19:49:03	@illumio.com
		user.logout	User logout	Informational	Success	06/10/2020, 19:44:35	System
		user.pce_session_terminated	PCE user session terminated	Informational	N/A	06/10/2020, 19:40:44	System
		user.logout	User logout	Informational	Success	06/10/2020, 19:40:40	System
		user.logout	User logout	Informational	Success	06/10/2020, 19:39:24	System
		permission.create	RBAC permission created	Informational	Success	06/10/2020, 19:33:50	@illumio.com
		auth_security_principal.create	RBAC auth security principal created	Informational	Success	06/10/2020, 19:33:50	@illumio.com
		user.create	User created	Informational	Success	06/10/2020, 19:33:50	System
		user.login	User login	Informational	Success	06/10/2020, 19:33:11	@illumio.com
		request.authentication_failed	Request authentication failed	Error	Failure	06/10/2020, 19:33:01	System

## Export Reports

You can generate reports for endpoints, VENs, services, and IP ranges in JSON or CSV formats from the **Reports** drop down option on the corresponding page and then download the report from the **Troubleshooting > Export Reports** page.

Services

+ Add

Provision

Revert

Remove

Refresh

Reports

Select properties to filter view

Provision Status

Name

Port/Protocol

Last Modified On

Last Modified By

ICMP

ICMP, ICMPv6

07/19/2019, 13:21:37

All Services

ALL

07/19/2019, 13:21:37

Windows Broadcasts

137 - 139 UDP , 137 - 139 TCP , 5355 UDP , 1900 UDP

12/30/2019, 11:48:07

@illumio.com

Web

80 TCP , 443 TCP

10/24/2019, 12:26:19

@illumio.com

MSSQL

1433 TCP

10/24/2019, 12:26:19

@illumio.com

Customize columns

50 per page

1 - 11 of

Generate as JSON

Generate as CSV



All Export Reports





Export Reports							
<a href="#">+ New Report</a> <a href="#">Remove</a> <a href="#">Download</a>		<a href="#">Refresh</a>					
		Customize columns v 50 per page v 1 - 1 of 1 Total v					
<input type="checkbox"/>	File name	Containing All	Generated By	Generated At	Status	Retry	Download
<input type="checkbox"/>	Services_CSV_2020-06-10_20-14-55	Services	@illumio.com	06/10/2020, 20:14:55	Done	<a href="#">Regenerate</a>	<a href="#">Download</a>

## Support Reports

If you need to troubleshoot any issue with your VENs, click **Generate Support Report** on the VEN's summary page. It may take up to 10 minutes to generate the report. After the report

is generated, you can download it from the **Troubleshooting > Support Reports** page and send it to Illumio support for any assistance.



**VEN – DESKTOP-6QJTO7H**

 **Edit**
 **Unpair**
 **Generate Support Report**
 **Mark as Suspended**



---

### Node

<b>Name</b>	DESKTOP-6QJTO7H
<b>Description</b>	
<b>Hostname</b>	DESKTOP-6QJTO7H
<b>Enforcement Node Type</b>	Virtual Enforcement Node (VEN)
<b>Version</b>	1.7
<b>Activation Type</b>	Pairing Key

---

### Status

<b>Connectivity</b>	 Offline
<b>Status</b>	Active
<b>Condition</b>	 <b>Healthy</b>
<b>Last Heartbeat Received</b>	01/07/2020 at 12:54:18

---

### Host

<b>Location</b>	Unnamed Datacenter, Unknown Location
<b>OS</b>	win-x86_64-server
<b>Release</b>	18362.1.amd64fre.19h1_release.190318-1202 (Windows 10 Pro)

---

### Endpoint

<b>Name</b>	<a href="#">DESKTOP-6QJTO7H</a>
<b>Policy State</b>	Build Build Rules without events
<b>Policy Sync</b>	Syncing
<b>Policy Last Received</b>	01/07/2020 at 11:39:25
<b>Interfaces</b>	wlan32 10.3.12.1
<b>Public IP Address</b>	12.34.56.78
<b>Group</b>	Base-Group



## Access Configuration for Illumio Edge

This section describes how to configure Illumio Edge to control access using identify providers (IdPs).

### 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 for Illumio Edge.

### Overview of AD FS SSO Configuration

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

- NameID
- Surname
- Given Name

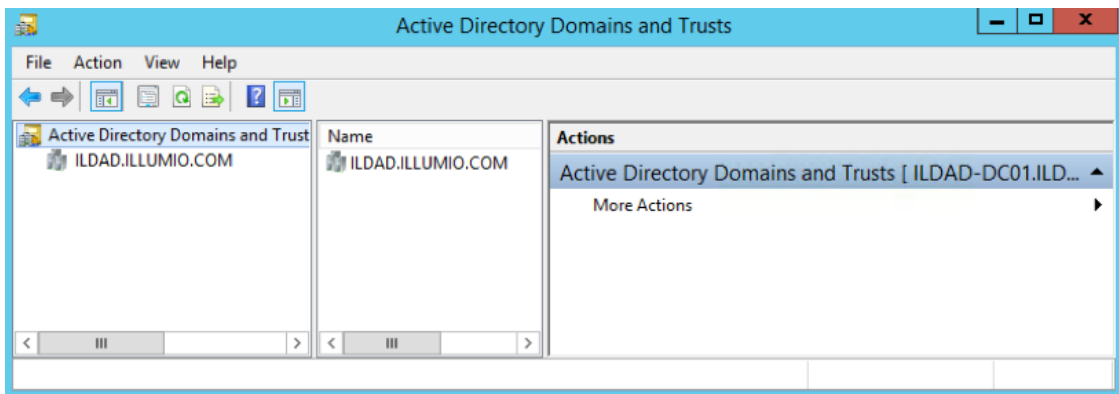
There are two ways for AD FS to produce the NameID claim for an SSO user. The first uses the email field in an Active Directory user account for the NameID.

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

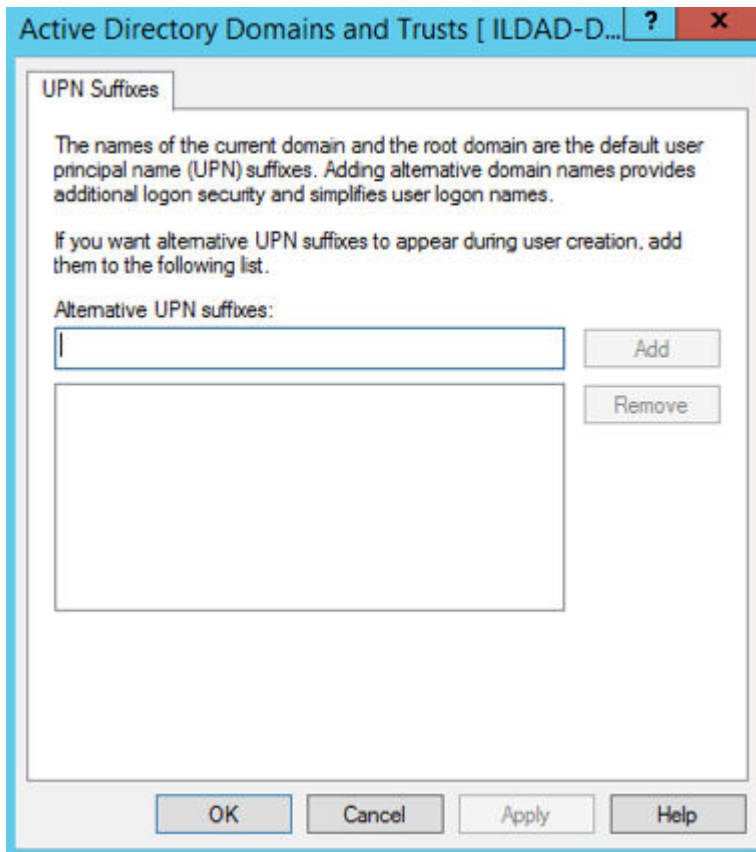
### Configure AD Users to Use Different UPN Suffixes

To configure different UPN suffix as the source for NameID:

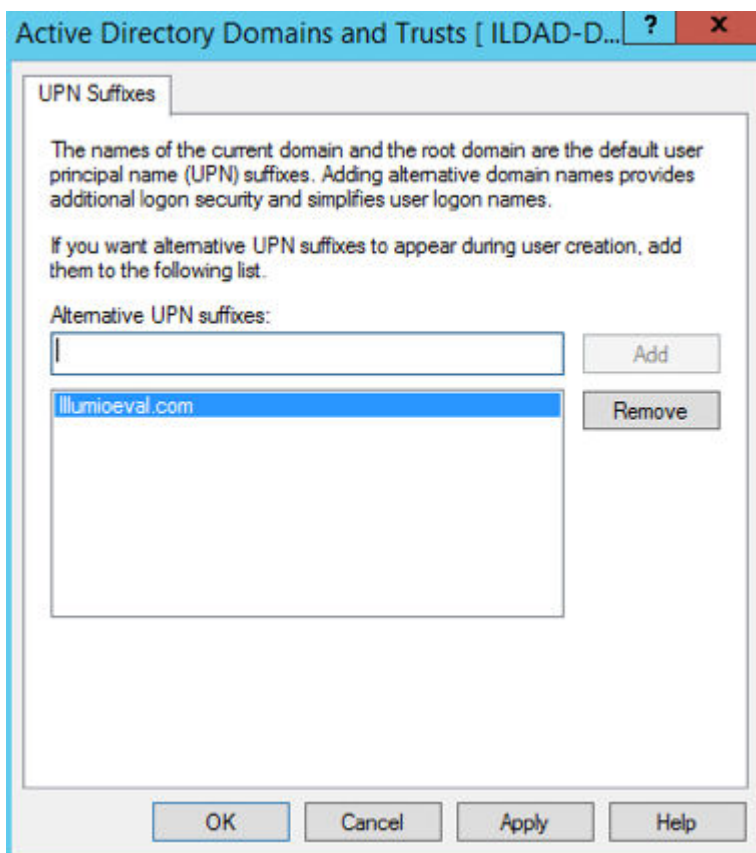
1. Add a UPN suffix. On your system under Server Manager Tools, click **Active Directory Domains and Trusts**.



2. From the left side of the window, right-click Active Directory Domains and Trusts, and select **Properties**. In this dialog, you can create new suffixes for Active Directory usernames.



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



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

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

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

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

## Initial AD FS SSO Configuration

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

To configure AD FS:

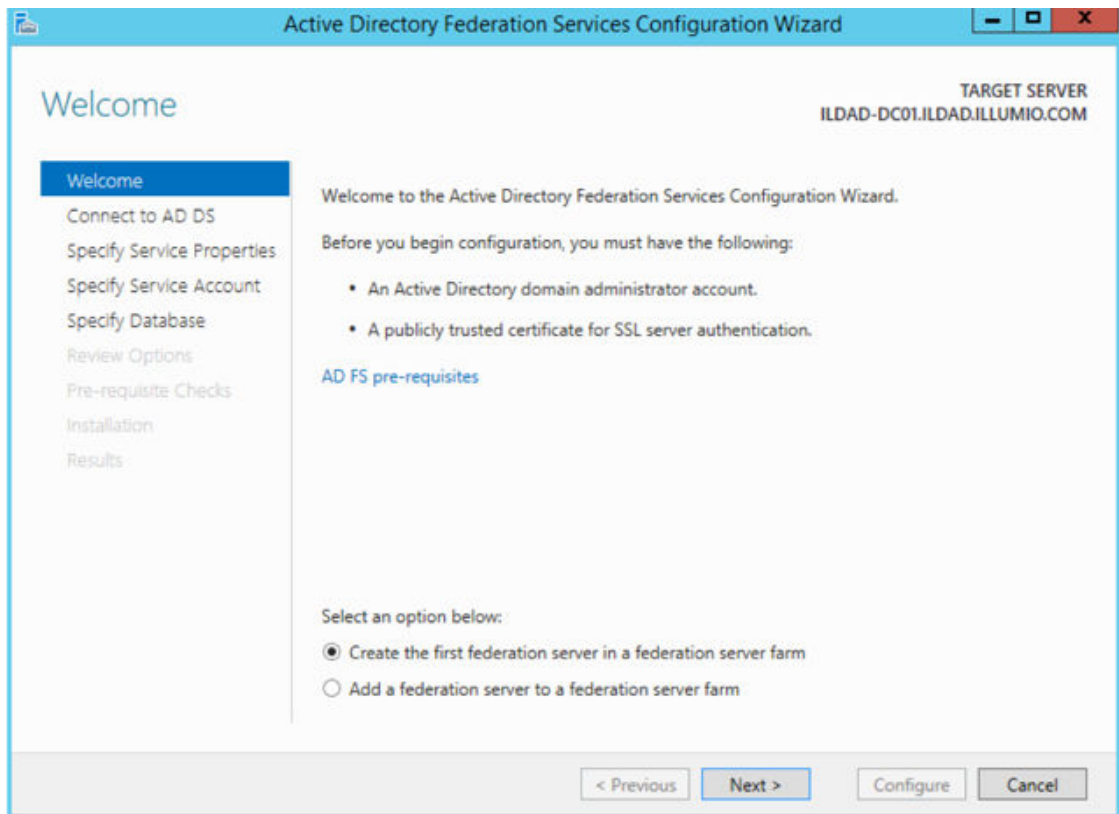
1. Open Microsoft Server Manager and click the notification icon.



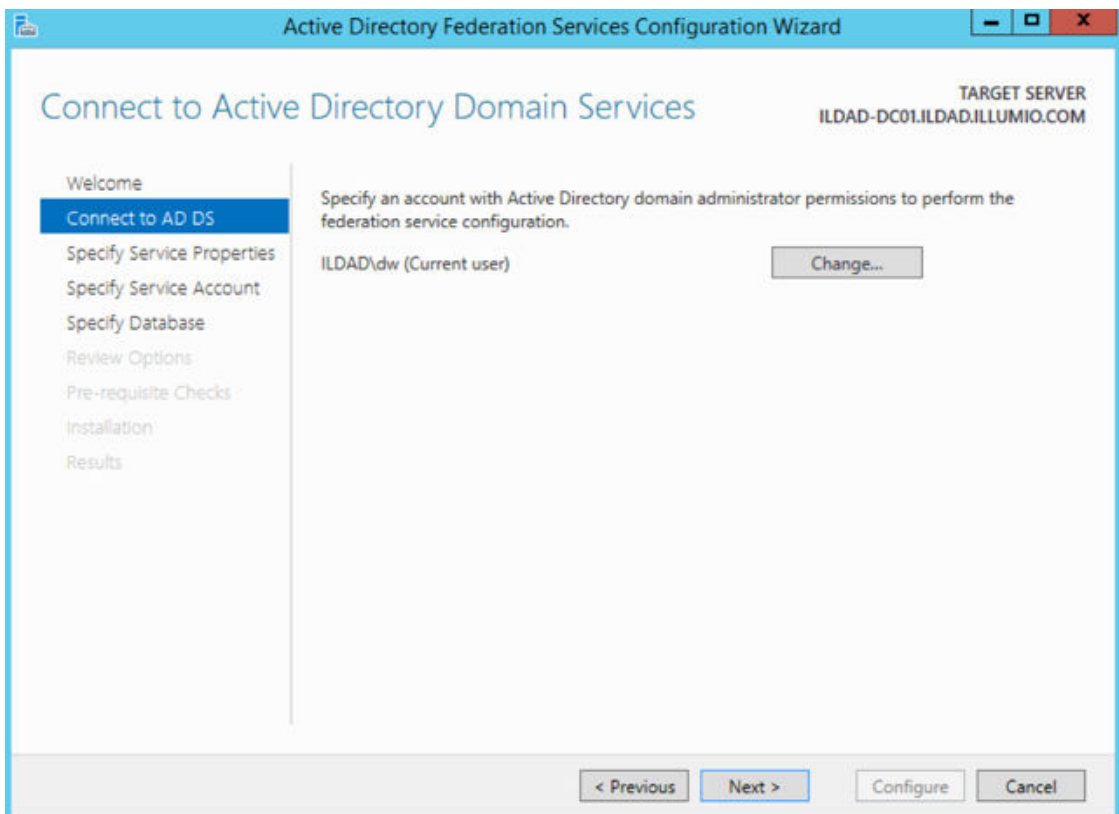
2. Click the "Configure the federation service on this server" link.



3. Select 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.

Active Directory Federation Services Configuration Wizard

TARGET SERVER  
ILDAD-DC01.ILDAD.ILLUMIO.COM

### Specify Service Properties

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

SSL Certificate:  [View](#)

Federation Service Name:  *Example: fs.contoso.com*

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

< Previous Next > Configure Cancel

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

Active Directory Federation Services Configuration Wizard

TARGET SERVER  
ILDAD-DC01.ILDAD.ILLUMIO.COM

### Specify Service Properties

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

SSL Certificate:  [View](#)

Federation Service Name:  *Example: fs.contoso.com*

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

< Previous Next > Configure Cancel

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

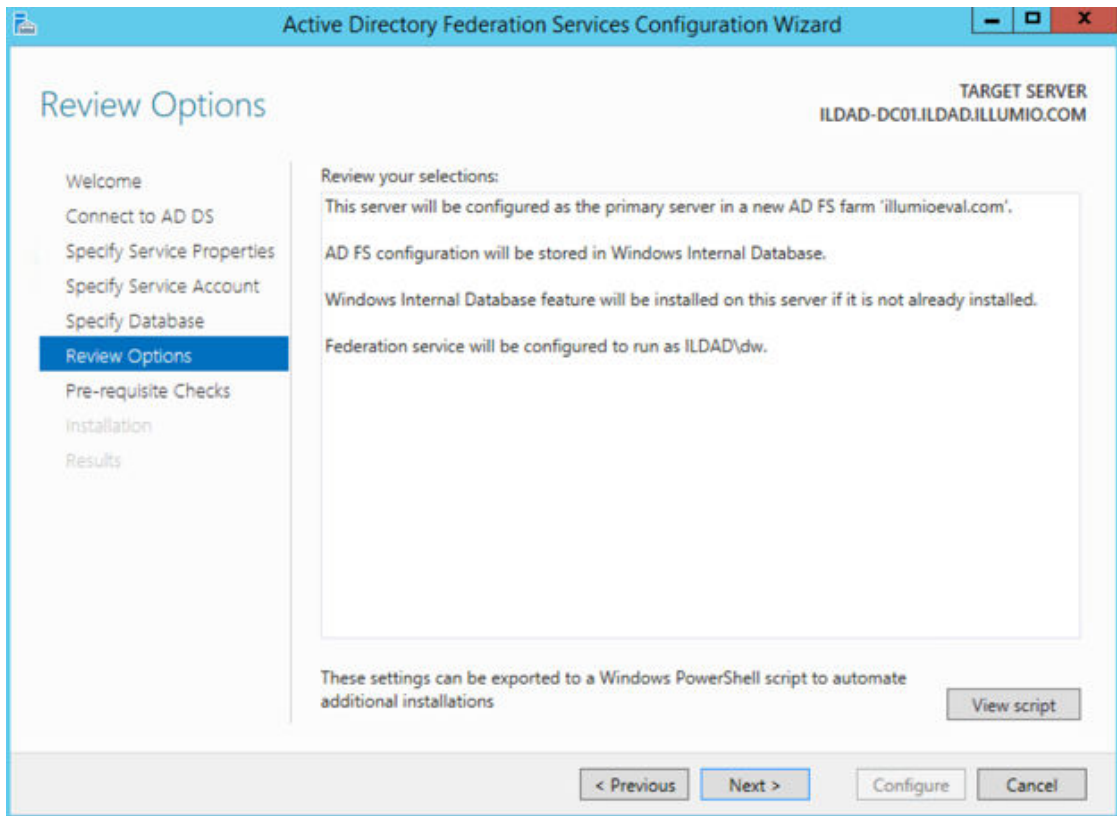
The screenshot shows the 'Specify Service Account' step of the 'Active Directory Federation Services Configuration Wizard'. The wizard's title bar is blue with the Microsoft logo and the text 'Active Directory Federation Services Configuration Wizard'. The main title 'Specify Service Account' is in blue. The target server is 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. On the left, a navigation pane lists steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account (highlighted), Specify Database, Review Options, Pre-requisite Checks, Installation, and Results. The main area has the heading 'Specify a domain user account or group Managed Service Account.' with two radio buttons: 'Create a Group Managed Service Account' (unselected) and 'Use an existing domain user account or group Managed Service Account' (selected). Below, the 'Account Name' is 'ILDAD\dw' with a 'Clear' button and a 'Select...' button. The 'Account Password' is masked with dots. At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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

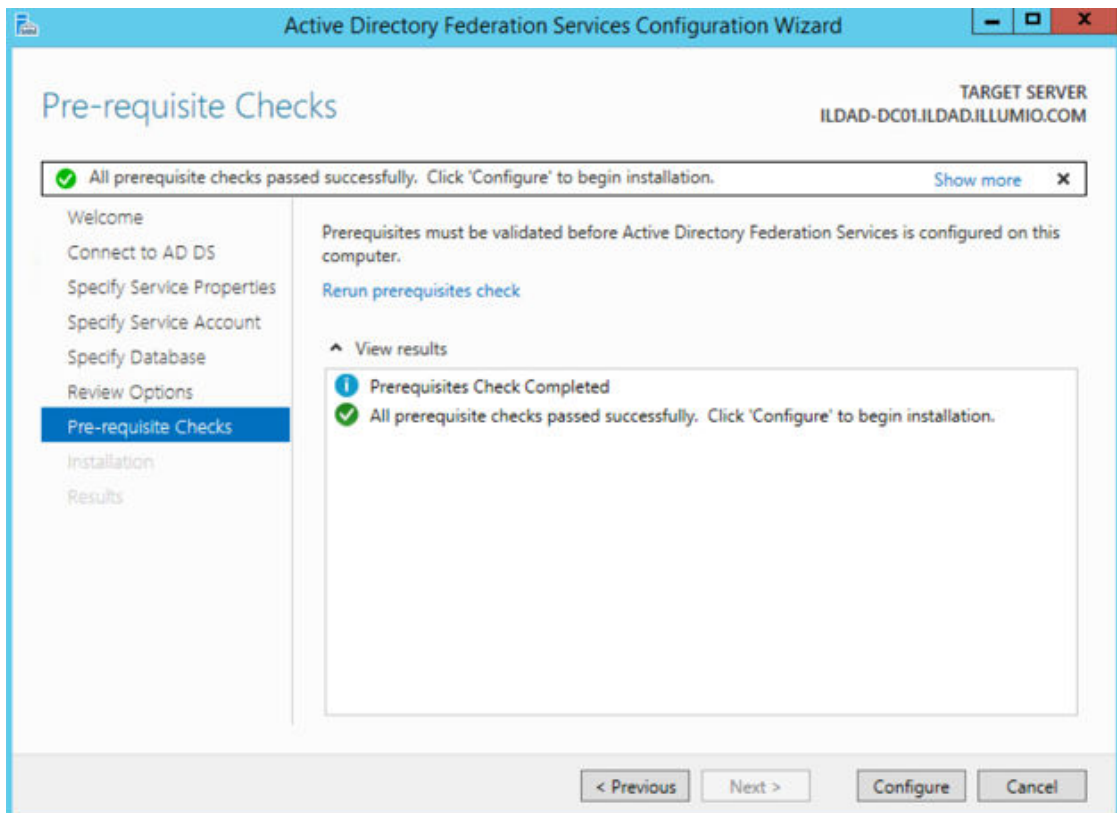
The screenshot shows the 'Specify Configuration Database' step of the 'Active Directory Federation Services Configuration Wizard'. The wizard's title bar is blue with the Microsoft logo and the text 'Active Directory Federation Services Configuration Wizard'. The main title 'Specify Configuration Database' is in blue. The target server is 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. On the left, a navigation pane lists steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account, Specify Database (highlighted), Review Options, Pre-requisite Checks, Installation, and Results. The main area has the heading 'Specify a database to store the Active Directory Federation Service configuration data.' with two radio buttons: 'Create a database on this server using Windows Internal Database.' (selected) and 'Specify the location of a SQL Server database.' (unselected). Below, the 'Database Host Name' and 'Database Instance' fields are empty. A note below the instance field says 'To use the default instance, leave this field blank.' At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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





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

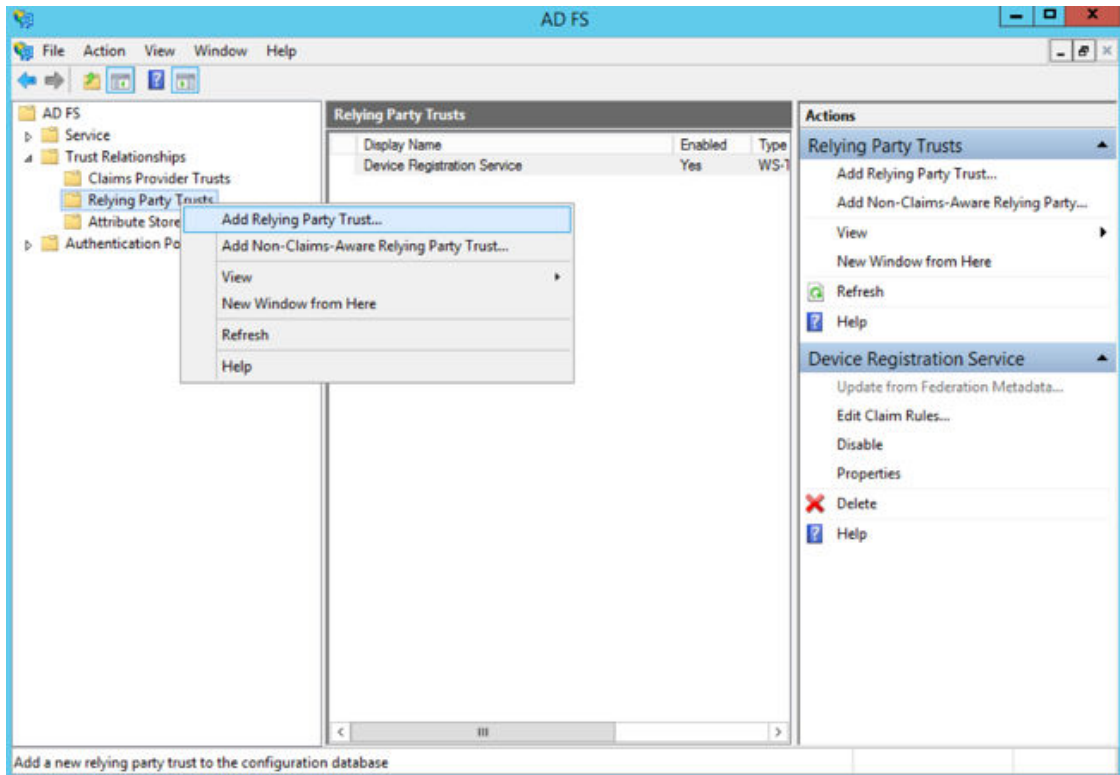


11. In the results screen, click **Close**.  
AD FS is now installed with the basic configuration on this host.

## Create a Relying Party Trust

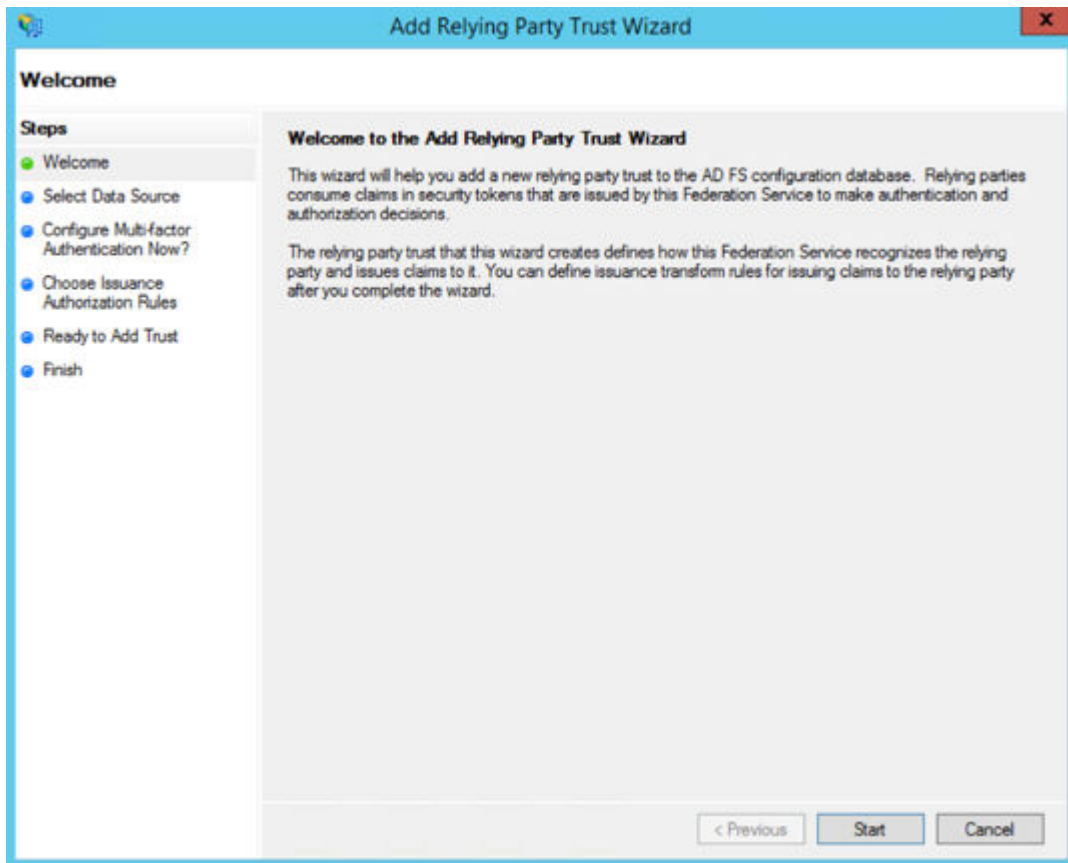
To start configuring AD FS for SSO with the PCE, you need to create a Relying Party Trust for your Illumio PCE.

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



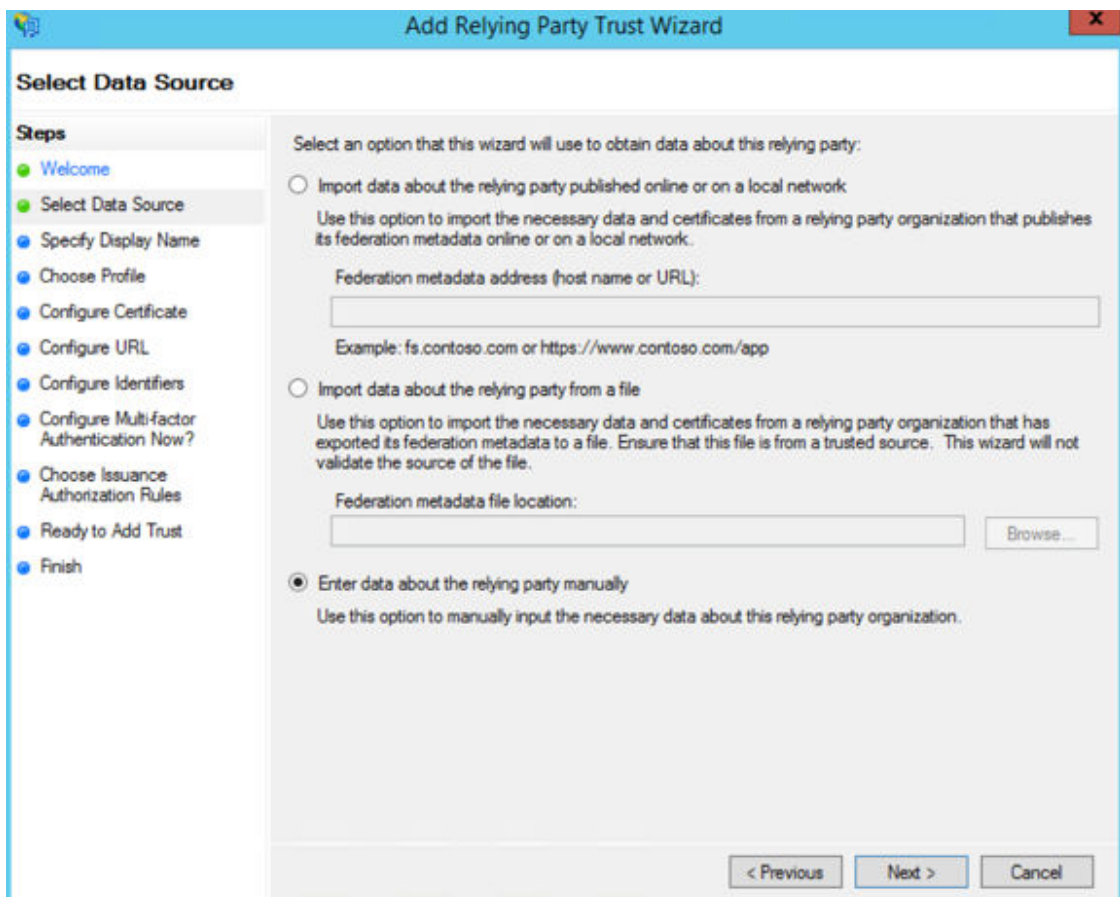
The Add Relying Party Trust Wizard appears.





3. Click **Start**.

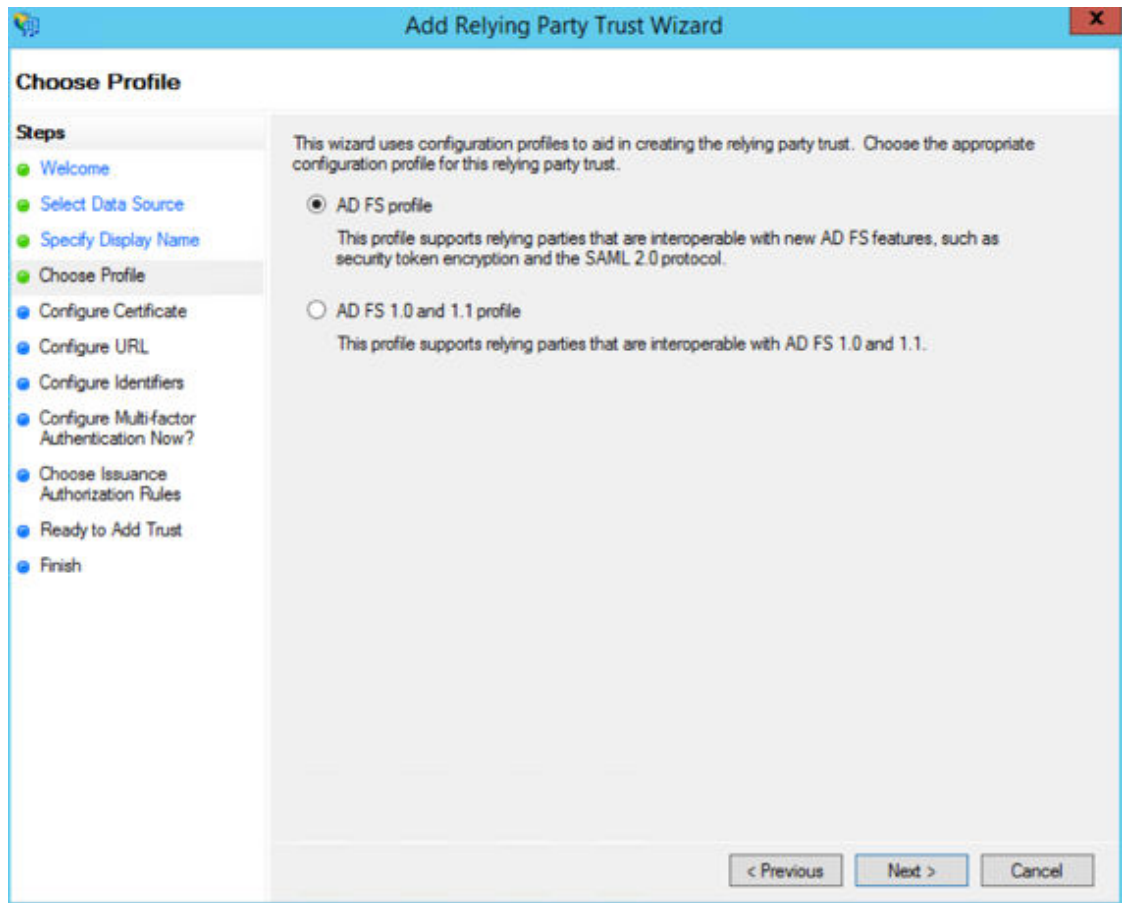
4. Select the “Enter data about the relying party manually” option and click **Next**.



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

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main window has a light gray background. On the left, there is a 'Steps' pane with a list of steps: 'Welcome' (green dot), 'Select Data Source' (green dot), 'Specify Display Name' (green dot and highlighted), 'Choose Profile' (blue dot), 'Configure Certificate' (blue dot), 'Configure URL' (blue dot), 'Configure Identifiers' (blue dot), 'Configure Multi-factor Authentication Now?' (blue dot), 'Choose Issuance Authorization Rules' (blue dot), 'Ready to Add Trust' (blue dot), and 'Finish' (blue dot). The main area of the wizard is titled 'Specify Display Name' and contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label and a text box containing 'Illumio PCE'. Below the text box is a 'Notes:' label and a large text area for notes. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

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



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

**NOTE**

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

**Add Relying Party Trust Wizard**

**Configure Certificate**

**Steps**

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

Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse...

Issuer:  
Subject:  
Effective date:  
Expiration date:

View... Browse... Remove

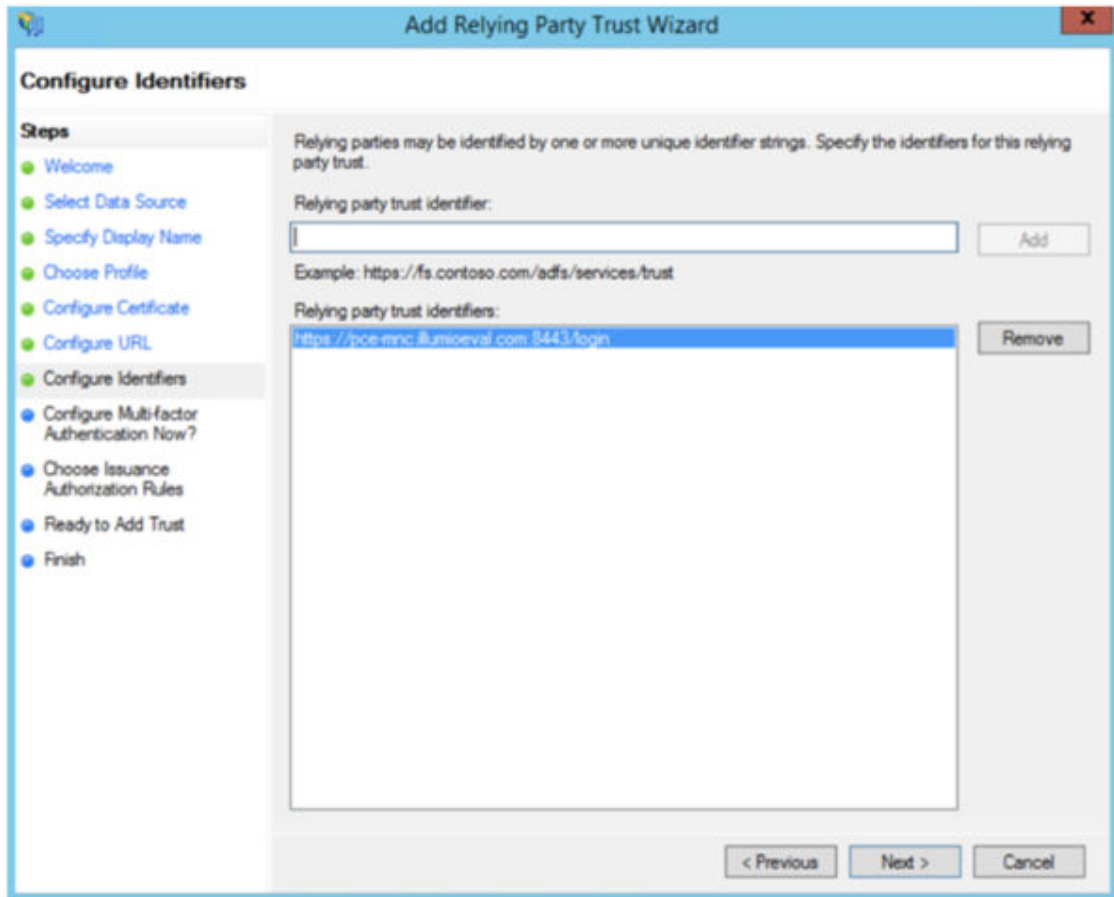
< Previous Next > Cancel

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

To locate the “Assertion Consumer URL,” go to **Settings > Authentication > Information for Identity Provider** in the PCE web console:

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

- 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**.

**Add Relying Party Trust Wizard**

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

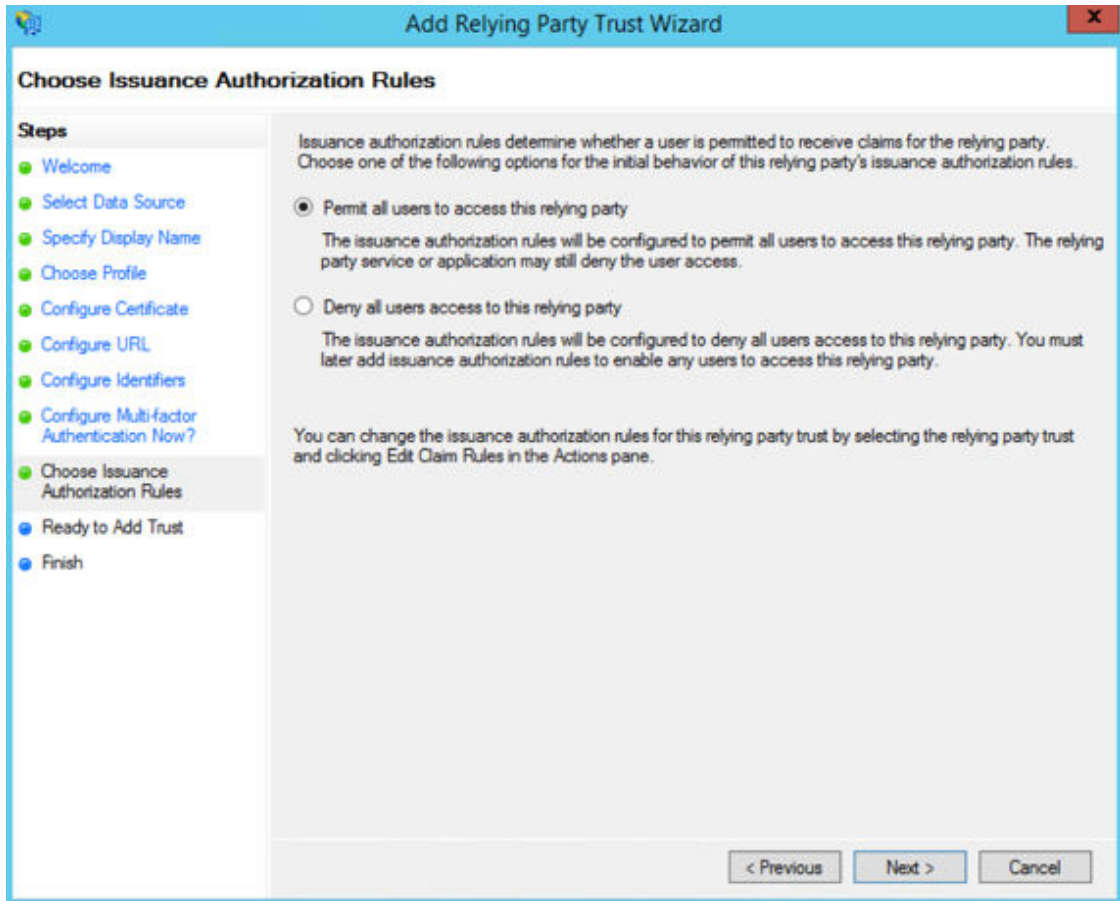
☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.

☐ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous   Next >   Cancel

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



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



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the Illumio logo and the text 'Add Relying Party Trust Wizard'. The window has a sidebar on the left with a 'Steps' list: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust (highlighted), and Finish. The main area has a heading 'Ready to Add Trust' and a message: 'The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.' Below this is a tabbed interface with tabs: Monitoring (selected), Identifiers, Encryption, Signature, Accepted Claims, Organization, Endpoints, and Note. The 'Monitoring' tab contains the text 'Specify the monitoring settings for this relying party trust.' followed by a text box for 'Relying party's federation metadata URL:'. Below this are two checkboxes: 'Monitor relying party.' (unchecked) and 'Automatically update relying party.' (unchecked). Further down are two lines of text: 'This relying party's federation metadata data was last checked on: < never >' and 'This relying party was last updated from federation metadata on: < never >'. At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'.

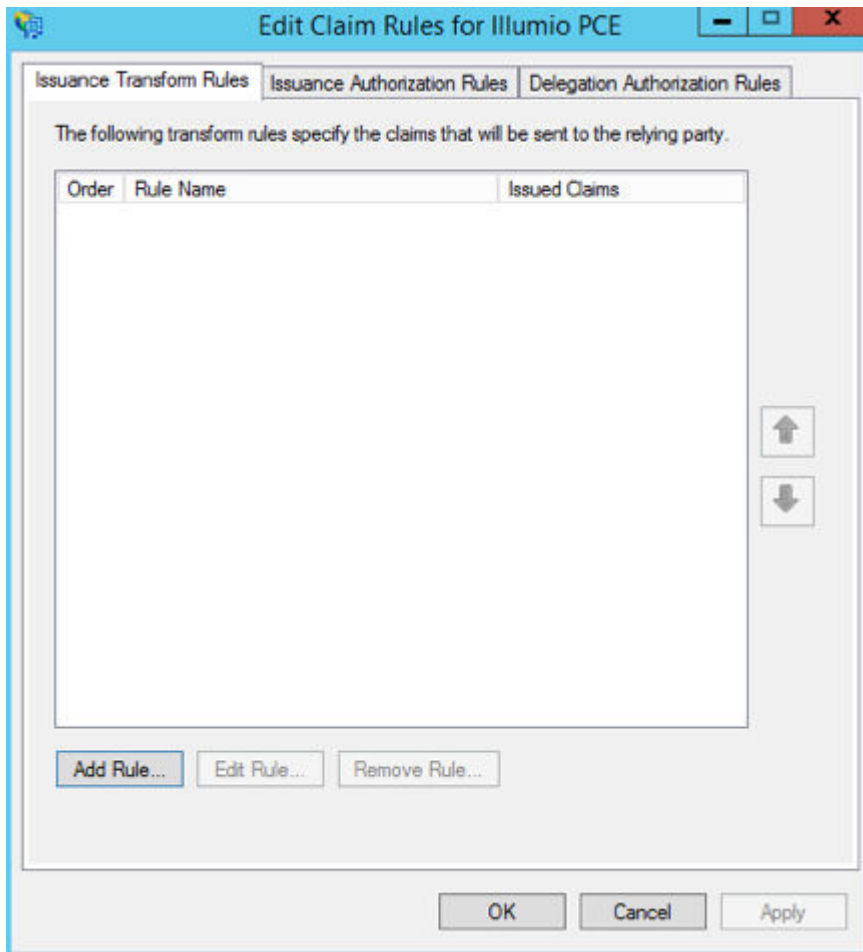
13. Leave the Open the Edit Claim Rules checkbox selected and click **Close**.

The screenshot shows the 'Add Relying Party Trust Wizard' window at the 'Finish' step. The title bar is blue with the Illumio logo and the text 'Add Relying Party Trust Wizard'. The sidebar on the left has the 'Steps' list, with 'Finish' highlighted. The main area has a heading 'Finish' and a message: 'The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.' Below this is a checkbox labeled 'Open the Edit Claim Rules dialog for this relying party trust when the wizard closes', which is checked. At the bottom right is a 'Close' button.

## Create Claim Rules

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

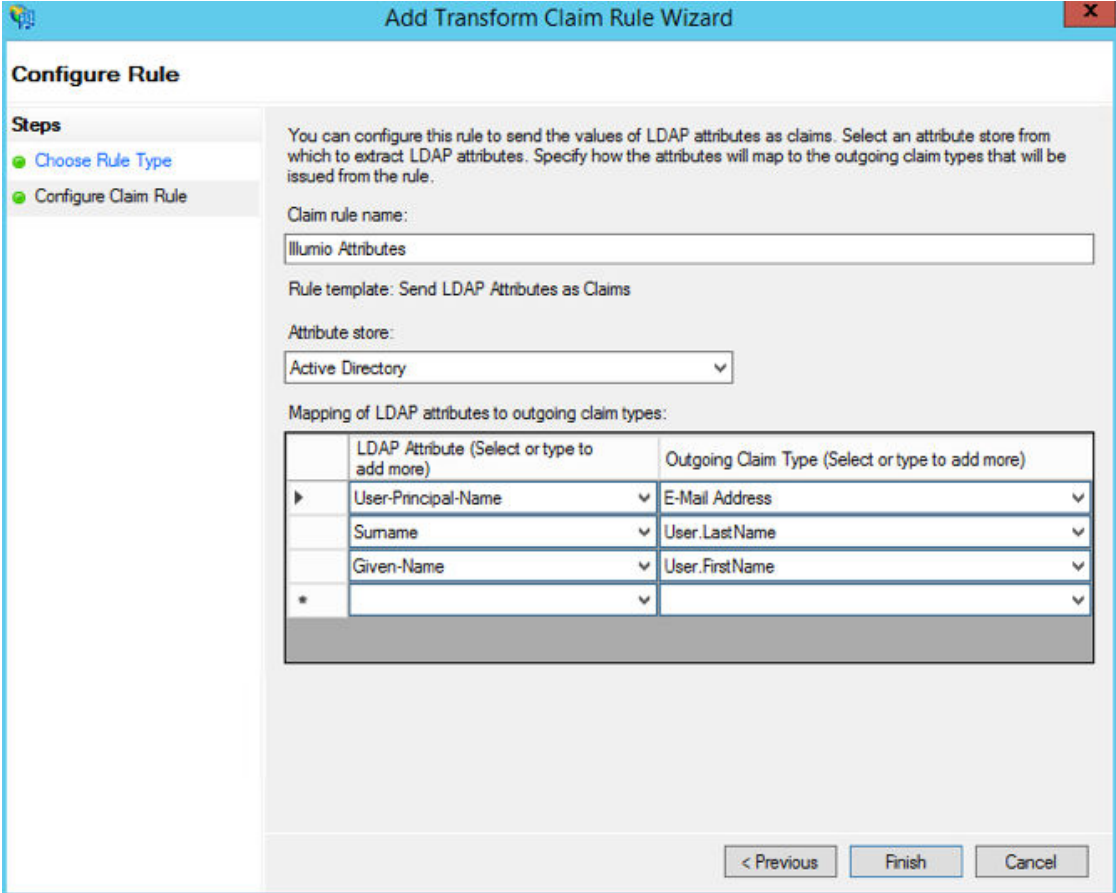
1. In the Edit Claim Rules dialog, click **Add Rule**.



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

The screenshot shows a window titled "Add Transform Claim Rule Wizard" with a close button in the top right corner. The window is divided into two main sections. On the left, under the heading "Steps", there are two steps: "Choose Rule Type" (marked with a green dot) and "Configure Claim Rule" (marked with a blue dot). The right section contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a label "Claim rule template:" followed by a dropdown menu showing "Send LDAP Attributes as Claims". Underneath the dropdown is a label "Claim rule template description:" followed by a text box containing the following description: "Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template." At the bottom right of the window are three buttons: "< Previous", "Next >", and "Cancel".

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



**Add Transform Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

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

Claim rule name:  
Illumio Attributes

Rule template: Send LDAP Attributes as Claims

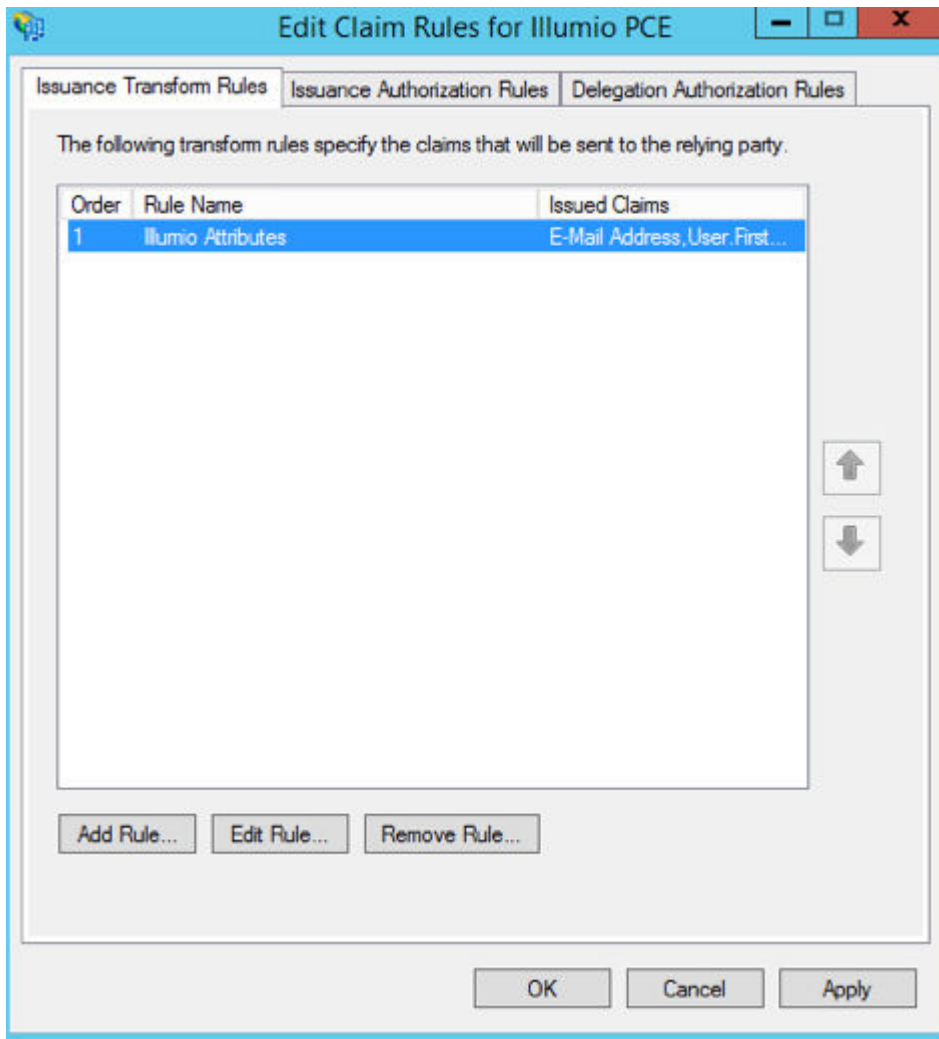
Attribute store:  
Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

< Previous Finish Cancel

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



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

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

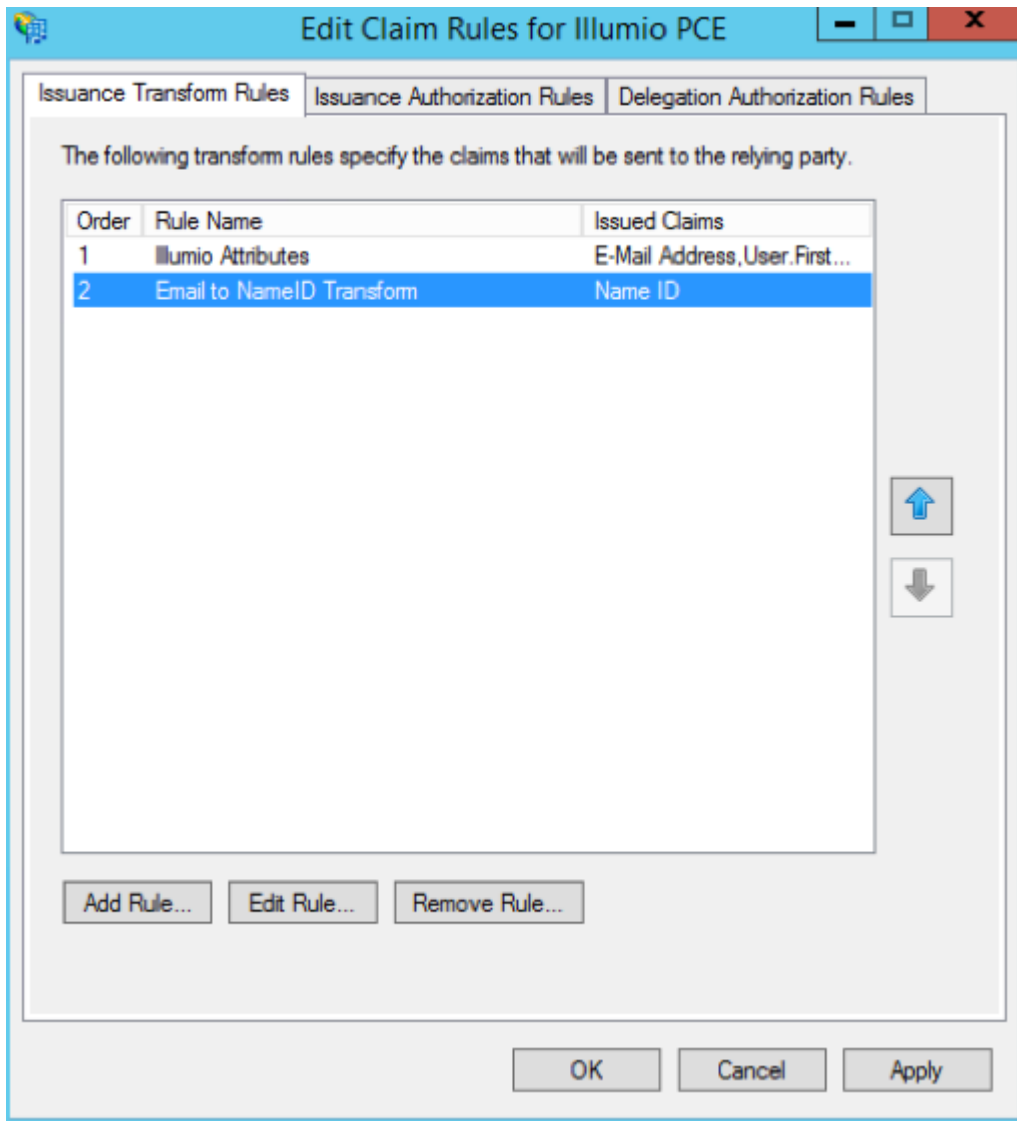
6. Name the rule "Email to NameID Transform" and change the incoming claim type to "E-Mail Address." Set the Outgoing claim type to "Name ID" and the Outgoing name ID format to "Email" and click **Finish**.

The screenshot shows a window titled "Add Transform Claim Rule Wizard" with a close button in the top right corner. The window is divided into two main sections. On the left is a "Steps" sidebar with two items: "Choose Rule Type" (highlighted with a green dot) and "Configure Claim Rule" (also with a green dot). The main area on the right is titled "Configure Rule" and contains the following elements:

- Instructions:** "You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value."
- Claim rule name:** A text input field containing "Email to NameID Transform".
- Rule template:** A dropdown menu set to "Transform an Incoming Claim".
- Incoming claim type:** A dropdown menu set to "E-Mail Address".
- Incoming name ID format:** A dropdown menu set to "Unspecified".
- Outgoing claim type:** A dropdown menu set to "Name ID".
- Outgoing name ID format:** A dropdown menu set to "Email".
- Options:**
  - ☒ **Pass through all claim values**
  - ☐ **Replace an incoming claim value with a different outgoing claim value**
    - Incoming claim value:** An empty text input field.
    - Outgoing claim value:** An empty text input field with a "Browse..." button to its right.
  - ☐ **Replace incoming e-mail suffix claims with a new e-mail suffix**
    - New e-mail suffix:** An empty text input field with the example "Example: fabrikam.com" below it.

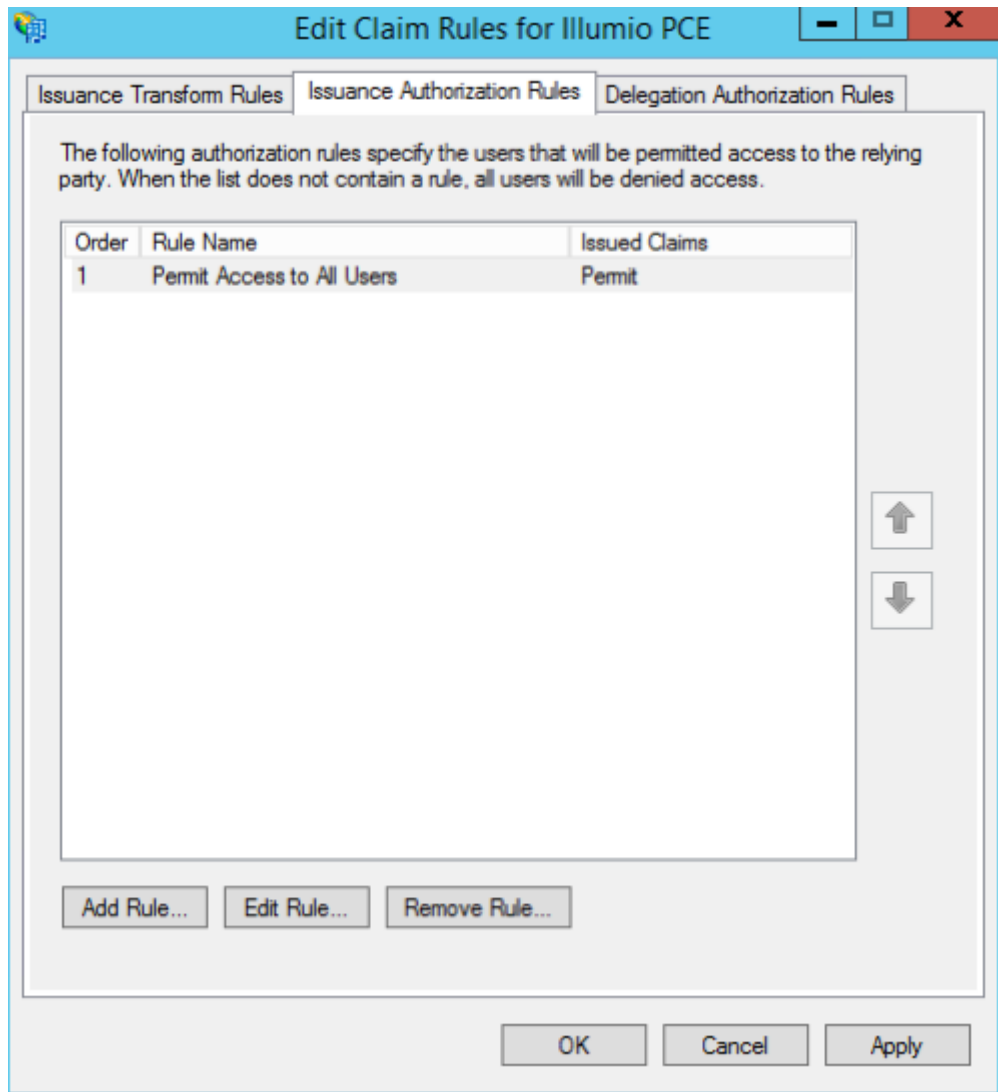
At the bottom right of the window are three buttons: "< Previous", "Finish", and "Cancel".

The Edit Claim Rules window opens.



7. (Windows 2016 and Windows 2019) Skip to step 12.  
The Edit Claim Rules window has three tabs. You have already filled out the first tab. The other two tabs are not available in Windows 2016 or Windows 2019. Therefore, skip steps 8 - 11.
8. Select the Issuance Authorization Rules tab.
9. To allow all your Active Directory Users to access the PCE, leave the "Permit Access to All Users" as is. Otherwise, you should restrict access to a single group or groups of users.





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

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

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

**Add Issuance Authorization Claim Rule Wizard**

**Configure Rule**

**Steps**

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to permit or deny users based on an incoming claim. Specify the incoming claim type, claim value, and whether the users should be permitted or denied access to the relying party.

Claim rule name:  
AD FS Users

Rule template: Authorize Users Based on an Incoming Claim

Incoming claim type:  
Group SID

Incoming claim value:  
ILDAD\ADFS Users Browse...

Select one of the following options to indicate whether users with this claim will be permitted or denied access to the relying party.

☒ Permit access to users with this incoming claim

☐ Deny access to users with this incoming claim

< Previous Finish Cancel

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

Edit Rule - Groups
X

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

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

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

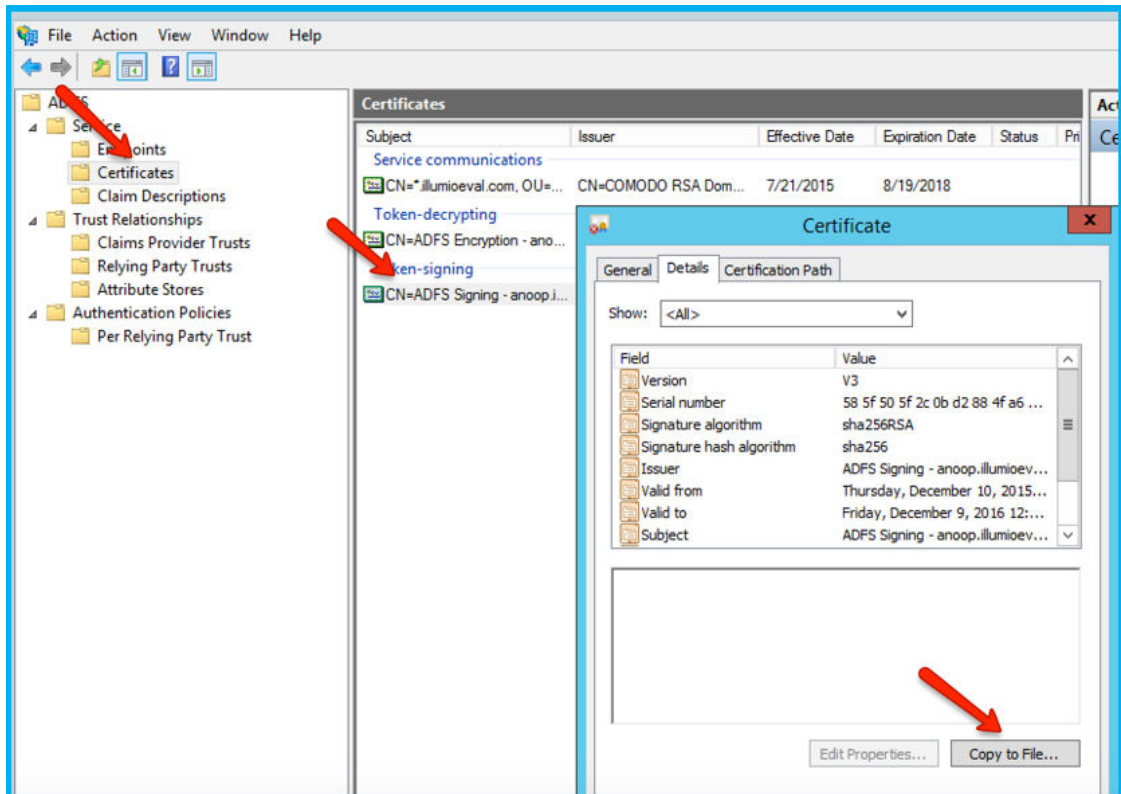
## Obtain ADFS SSO Information for the PCE

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

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

To obtain the AD FS SSO information for the PCE:

1. To find the certificate in your AD FS configuration, log into the AD FS server and open the management console.
2. Browse to the certificates and export the Token-Signing certificate.
3. Right-click the certificate and select **View Certificate**.
4. Select the **Details** tab.
5. Click **Copy to File**.



6. When the Certificate Export Wizard launches, click **Next**.
7. Verify that the "No - do not export the private key" option is selected and click **Next**.
8. Select Base 64 encoded binary X.509 (.cer) and click **Next**.
9. Select where you want to save the file, name the file, and click **Next**.
10. Click **Finish**.
11. After exporting the certificate to a file, open the file with a text editor. Copy and paste the contents of the exported x.509 certificate, including the BEGIN CERTIFICATE and END CERTIFICATE delimiters in to the SAML Identity Provider Certificate field.
12. To find the **Remote Login URL** (which AD FS calls "Sign-On URL"), download and open the following metadata file from your AD FS server by navigating to <https://server.mydomain/FederationMetadata/2007-06/FederationMetadata.xml> and search for SingleSignOnService.

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

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

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

```
https://<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 \[88\]](#).



### NOTE

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

To configure the PCE for AD FS:

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



### NOTE

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

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

## Azure Single Sign-on

This section describes how to configure Azure Active Directory (AD) for SSO authentication with the PCE for Illumio Edge.

### Prerequisites

Before you begin configuration:

- Log in to the PCE as a Global Organization Owner.
- Navigate to the **Settings > Single Sign-On** page.
- Copy the following URLs, which you will need to complete the Azure configuration:
  - Issuer: `https://pce.xxxx:8443/login`
  - NameID Format: `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - Assertion Consumer URL: `https://pce.xxxx:8443/login/acs/16884d35-036e-48c2-a685-c33f5458f407`
  - Logout URL: `https://pce.xxxx:8443/login/logout/16884d35-036e-48c2-a685-c33f5458f407`

## Configure Azure



### NOTE

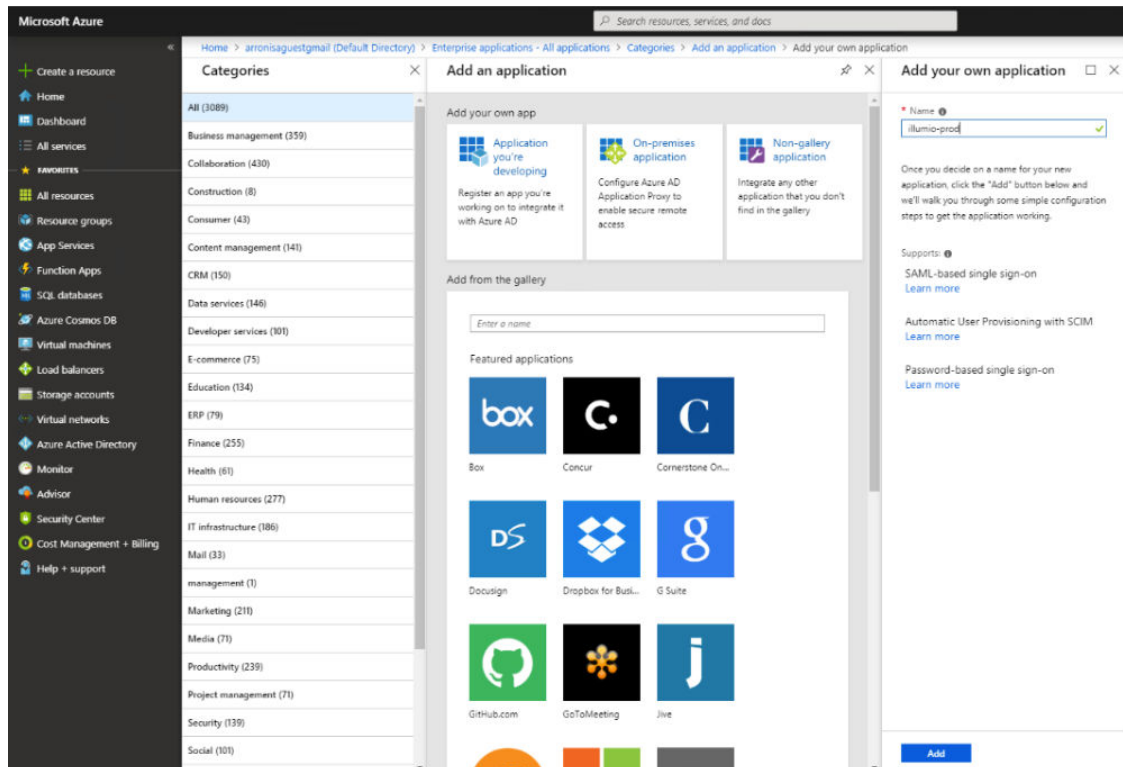
Only an Azure 'Application Administrator' can configure Azure AD.

To configure Azure AD:

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

NAME	GROUP TYPE	MEMBERSHIP TYPE
AD_Illumio_admins	Security	Synced
AD_Illumio_readonly	Security	Synced

- Navigate to **Azure Active Directory > Enterprise Applications > New application**.
- Select **Non-gallery application** and enter a name, for example 'illumio-prod', and click **Add**.



4. From the 'Getting Started' option, select **Configure single sign-on (required)** and select **SAML** from the list of single sign-on methods.



### Configure single sign-on (required)

Configure your instance of illumio-prod to use Azure AD as its identity provider.



### SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

5. In **Basic SAML Configuration**, enter the URLs that you had noted down in step 3 of [Prerequisites \[91\]](#).
  - Identifier (Entity ID) = Issuer
  - Reply URL (Assertion Consumer URL) = Assertion Consumer URL



**1**

### Basic SAML Configuration

Identifier (Entity ID)	https://pce.	:8443/login
Reply URL (Assertion Consumer Service URL)	https://pce.	:8443/login/acs/16884d35-036e-48c2-a685-c33f5458f407
Sign on URL	Optional	
Relay State	Optional	

6. Click the Edit button and enter the **User Attributes & Claims** configuration values.

**2**

### User Attributes & Claims

User.MemberOf	user.assignedroles
Given Name	user.givenname
Surname	user.surname
Unique User Identifier	user.mail

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

**3**

### SAML Signing Certificate

Status	Active
Thumbprint	0F55803323.
Expiration	1/29/2022, 1:15:56 PM
Notification Email	@.co.uk
App Federation Metadata Url	https://login.microsoftonline.com/9469879a-44b4-...
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

8. Download **Login URL** and **Logout URL**.

**4**

### Set up illumio-prod

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

Login URL	https://login.microsoftonline.com/9469879a-44b4-...
Azure AD Identifier	https://sts.windows.net/9469879a-44b4-491a-997a-...
Logout URL	https://login.microsoftonline.com/common/wsfede...

[View step-by-step instructions](#)

9. Create the 'Roles' that will have access to the illumio-prod application.
- Navigate to **Azure Active Directory > App registrations** and select the illumio-prod application.
  - Click 'Manifest' to open the .json manifest:

<b>illumio-prod</b>		
Registered app		
Settings          Manifest          Delete		
Display name	Application ID	
illumio-prod	a779f017-e7e5-4c57-9fc6-97b5964323eb	
Application type	Object ID	
Web app / API	e82f44c4-a1fc-43fc-9076-73ebdbd6b3c8	
Home page	Managed application in local directory	
<a href="https://account.activedirectory.windowsaz...">https://account.activedirectory.windowsaz...</a>	<a href="#">illumio-prod</a>	

- Locate the `appRoles` section of the manifest and enter:
  - `displayName`: A display name.
  - `id`: The Azure object ID for the group you are going to use.
  - `description`: A description.
  - `value`: A value for the Illumio role.

```

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

```

10. Add the required users or groups to the `illumio-prod` application and assign the necessary roles.

- Navigate to Azure Active Directory > Enterprise Applications > `illumio-prod` > Users and groups.
- Click Add and select the Azure user or group you want to add and assign a role.

The screenshot shows the Azure Active Directory 'Users and groups' interface. On the left, there are two dropdown menus: 'Users and groups' (None Selected) and 'Select Role' (None Selected). The main area displays a search bar with the text 'AD\_illumio\_admins' and a green checkmark. Below the search bar, there is a list of results, including 'AD\_illumio\_admins'. Below this, the 'Select Role' dropdown is set to 'illumio admins role'. The main area shows a search bar with the text 'admin' and a list of results, including 'illumio admins role'.

## Configure PCE for Azure



### NOTE

Only an Illumio PCE 'Global Organizational Owner' can configure the PCE.

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

- Certificate (Base64). See step 7 of [Configure Azure](#). [91]
- Azure Login URL and Logout URL. See step 8 of [Configure Azure](#). [91]

To configure the PCE for Azure AD:

1. Configure the Illumio PCE Single Sign-on SAML settings (information from the Identity Provider):
  - a. Log in to the Illumio PCE web console.
  - b. From the left navigation menu, select **Settings > Authentication**.
  - c. Click **Configure** that is located next to 'SAML'.
  - d. On the Single Sign-on Configuration page, click **Edit**.
  - e. Enter the following information:
    - SAML Identity Provider Certificate: Paste your Azure Base64 certificate.
    - Remote Login URL: Enter the Azure Login URL.
    - Logout Landing URL: Enter the Azure Logout URL.

SSO method SAML

---

Information from Identity Provider

SAML Identity Provider Certificate	-----BEGIN CERTIFICATE----- [Redacted Base64 Certificate Data] -----END CERTIFICATE-----
Remote Login URL	<a href="https://login.microsoftonline.com/9469879a-44b4-491a-997a-268d04ddab31/saml2">https://login.microsoftonline.com/9469879a-44b4-491a-997a-268d04ddab31/saml2</a>
Logout Landing URL	<a href="https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0">https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0</a>

2. Configure the Illumio PCE Single Sign-on SAML settings (information for the Identify Provider):
  - a. Select the authentication method from the drop-down list:
    - Unspecified: Uses the IdP default authentication mechanism.
    - Password Protected Transport: Requires the user to log in with a password in a protected session.
  - b. To require users to re-enter their login information to access Illumio (even if the session is still valid), select the **Force Re-authentication** checkbox (disabled, by default). This allows users to log in to the PCE using login credentials different than their default computer login.
  - c. Click **Save**.



#### NOTE

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

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

- a. From the menu, select **Role-Based Access > External Groups**.
- b. Click **Add**.
- c. Enter a **Name**.
- d. Enter an **External Group** name. This groups name must match the value you entered in step 8 (value: A value for the Illumio role) in [Configure Azure](#). [91]
- e. Click **Save**.
- f. Repeat for additional groups.

### Add External Group

**\* Name**

**\* External Group**

Illumio Administrator Users

R-illumio-admins

Cancel
Save

☰ Users and User Groups – External Groups

External Groups
External Users
Local Users

+ Add
– Remove

Filter by External Group

<input type="checkbox"/> ^Name	External Group
<input type="checkbox"/> Illumio Administrator Users	R-illumio-admins
<input type="checkbox"/> Illumio Read Only Users	R-illumio-readonly

- g. Select a group you created in the above step.
  - Select **Add Role > Add Global Role** or **Add Scoped Role**.
  - Select a **Role** and click **Grant Access**.
  - Repeat for additional groups.

**Role-Based Access – Access Wizard**

**Scope** All Applications All Environments All Locations

**Name** Illumio Administrator Users

**Email or Username** R-illumio-admins

**1 Select Roles**

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

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

## Okta Single Sign-on

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

### Prerequisite for Okta SSO

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

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



#### NOTE

Your PCE user account must have Owner or Admin privileges to perform this task.

## Configure the PCE for Okta SSO

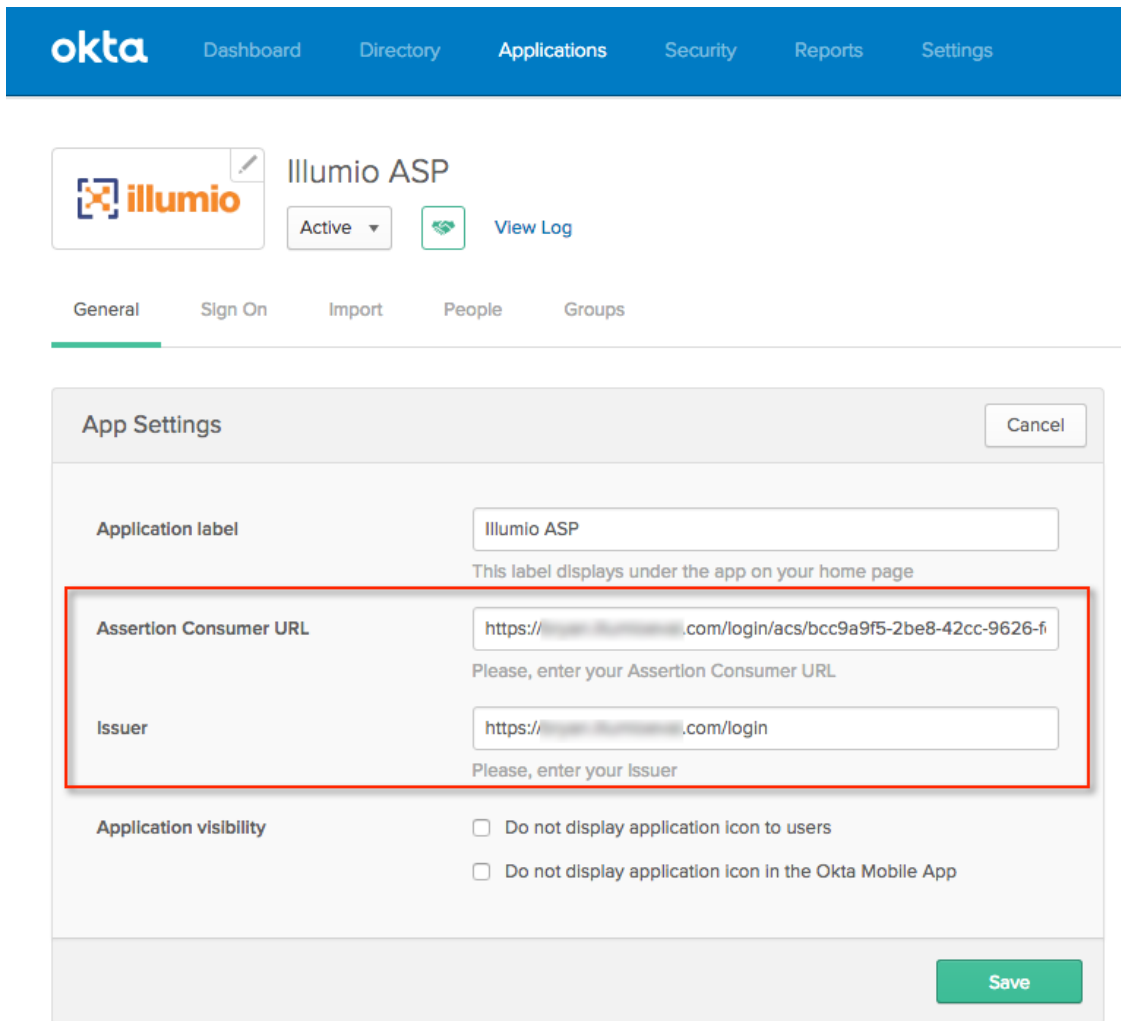
1. From the PCE web console menu, choose **Access Management > Authentication**.
2. On the Authentication Settings screen, locate the SAML configuration panel and click **Configure**.

3. Enter the following information:
  - **SAML Identity Provider Certificate:** Paste your Okta x.509 certificate (in PEM text format):
  - **Remote Login URL:** Enter the Okta Remote Login URL.
  - **Logout Landing URL:** Enter the Okta Logout Landing URL.
4. In the Information for Identity Provider section, choose the Access Level for the users who will use Okta to authenticate with the PCE. When you select No Access, SSO users from your Okta account will have to be added manually before they can log into the PCE. (For more information on user permissions, see [Edge Users \[18\]](#).)
5. In the Information for Identity Provider section, make note of the following fields:
  - Issuer
  - Assertion Consumer URL
6. Select the authentication method from the drop-down list:
  - **Unspecified:** Uses the IdP default authentication mechanism.
  - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
7. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log into the PCE using a different login than their default computer login and is disabled by default.

**NOTE**

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

8. Click **Save**.
9. Log into your Okta account.
10. Select the Illumio Core app, select the General tab, and click **Edit**.
11. Enter the values you copied from the Information for Identity Provider section of the PCE SSO Configuration page.



The screenshot shows the Okta Admin Console interface. At the top, there's a blue navigation bar with the Okta logo and links to Dashboard, Directory, Applications, Security, Reports, and Settings. Below this, the 'Illumio ASP' application is selected, showing its status as 'Active' and a 'View Log' link. The 'General' tab is active, and the 'App Settings' modal is open. Inside the modal, the 'Application label' is 'Illumio ASP'. The 'Assertion Consumer URL' and 'Issuer' fields are highlighted with a red box. The 'Assertion Consumer URL' is 'https://[redacted].com/login/acs/bcc9a9f5-2be8-42cc-9626-f[redacted]' and the 'Issuer' is 'https://[redacted].com/login'. Below these, there are checkboxes for 'Application visibility'.

12. Click **Save**.  
Your PCE is now configured to use Okta SSO for authenticating users with the PCE.

## OneLogin Single Sign-on

This section describes how to configure SSO for OneLogin for Illumio Edge.

### Configure SSO for OneLogin

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

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

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

**NOTE**

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

To configure the PCE for OneLogin SSO:

1. From the PCE web console menu, choose **Settings > SSO Config**.
2. Click **Edit**.
3. Select the Enabled checkbox for SAML Status.
4. Enter the following information:
  - **SAML Identity Provider Certificate:** Paste your OneLogin x.509 certificate (in PEM text format).
  - **Remote Login URL:** Enter the OneLogin SAML 2.0 Endpoint (HTTP) URL.
  - **Logout Landing URL:** Enter the OneLogin SLO Endpoint (HTTP) URL.
5. In the Information for Identity Provider section, choose the Access Level for the users who use OneLogin to authenticate with the PCE. When you select No Access, SSO users from your OneLogin account will have to be added manually before they can log in to the PCE. (For more information on user permissions, see [Edge Users \[18\]](#).)
6. In the Information for Identity Provider section, make note of the following fields:
  - Issuer
  - Assertion Consumer URL
  - Logout URL

You will enter this information into your OneLogin SSO configuration.
7. Select the authentication method from the drop-down list:
  - **Unspecified:** Uses the IdP default authentication mechanism.
  - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
8. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log in to the PCE using a different login than their default computer login and is disabled by default.

**NOTE**

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

9. Click **Save**.
10. Log in to your OneLogin account.
11. Select the Illumio Core app, and then click the Configuration tab.
12. Enter the values copied from the Information for Identity Provider section of the PCE SSO configuration page.



USERS APPS ACTIVITY SETTINGS

← Illumio ASP MORE ACTIONS SAVE

Info **Configuration** Parameters Rules SSO Access Users

**Application Details**

Issuer

Assertion Consumer URL

Logout URL

**Enter PCE  
'Information for  
Identity Provider'  
here**

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

13. Click **Save**.  
 Your PCE is now configured to use OneLogin SSO for authenticating users with the PCE.

## Ping Identity Single Sign-on

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

### Configure SSO for Ping Identity

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

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



#### NOTE

Your PCE user account must have Owner or Admin privileges to perform this task.

To configure the PCE for Ping Identity SSO:

1. From the PCE web console menu, choose **Settings > SSO Config**.
2. Click **Edit**.
3. Select SAML from the Select SSO method drop-down list and click **Configure**.
4. Enter the following information:
  - **SAML Identity Provider Certificate**: Paste your Ping Identity x.509 certificate (in PEM text format).
  - **Remote Login URL**: Enter the Ping Identity Remote Login URL.

5.
  - **Logout Landing URL:** Enter the Ping Identity Logout Landing URL.

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

  - Issuer
  - NameID Format
  - Assertion Consumer URL
  - Logout URL
6. Select the authentication method from the drop-down list:
  - **Unspecified:** Uses the IdP default authentication mechanism.
  - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
7. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log in to the PCE using a different login than their default computer login and is disabled by default.

**NOTE**

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

8. Click **Save**.
9. Log in to your Ping Identity account.
10. Select the Applications tab and add the Illumio app.
11. Click **Edit** and enter the following values you just noted from Illumio:
  - **ACS URL:** Enter the value from the Assertion Consumer URL field in the PCE web console.
  - **Entity ID:** Enter the value from the Issuer field in the PCE web console.
  - **Single Logout Endpoint:** Enter the value from the Logout URL field in the PCE web console.
  - **Single Logout Response Endpoint:** Enter the value from the Logout URL field in the PCE web console.

Welcome, [Admin Pelham](#)

[Dashboard](#) [Applications](#) [Users](#) [Setup](#) [Account](#) [Help](#)

[My Applications](#) [Application Catalog](#)

## My Applications

[Applications](#) / [My Applications](#)

Applications you've added to your account are listed here.

- Active applications are enabled for single sign-on (SSO).
- Details displays the application details.

Application Name	Type	Status	Enabled
Illumio ASP	SAML	Incomplete	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <a href="#">Remove</a>

### 1. Configure your connection

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

Upload Metadata [Select File](#) [Or use URL](#)

ACS URL  \*

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

Entity ID  \*

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

Target Resource

Single Logout Endpoint  \*

Single Logout Response Endpoint  \*

Verification Certificate [Choose File](#) No file chosen

Force Re-authentication ☐

PingOne dock URL

Default PingOne dock URL  \*

☐ Use Custom URL

NEXT: Attribute Mapping

[Cancel](#) [Continue to Next Step](#)

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

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

Advanced Attribute Options

### Advanced Attribute Options for SAML\_SUBJECT

#### Advanced Attribute Options

NameIDFormat ⓘ

Name ID Format to send to SP:

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

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

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

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

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

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

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

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

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

#### Attribute Mapping

You can build an attribute mapping using

An example of a possible SAML\_SUBJECT

firstName + "." + lastName + "

SAML\_SUBJECT = SAML\_SUBJECT

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

Close

Save

14. Click **Save**.

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