



Illumio Edge[®]

Version 20.2.1

CrowdStrike Integration Guide

January 2021

57000-100-20.2.1

Legal Notices

Copyright © 2020 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.

Product Versions

PCE Version: Illumio Edge 20.2.1-512

UI Version: Illumio Edge 20.2.1.UI1-511

VEN Version: 20.2.0

CS-NEN Version: 1.0.6

Resources

Product information, see <https://www.illumio.com/products/edge>

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

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

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

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

Open source software utilized by Illumio Edge and their licenses, see [Open Source Licensing Disclosures](#)

Contact Information

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

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

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

Contents

Chapter 1 About Illumio Edge-CrowdStrike Integration	5
Overview of the Illumio Edge-CrowdStrike Integration	5
About the Integration	6
Workflow Diagram	7
About the Integration Architecture	7
Illumio Edge-CrowdStrike Integration Concepts	8
Prerequisites and Limitations	9
Recommended Skills	9
Prerequisites for Illumio Edge-CrowdStrike Integration	9
Limitations for Illumio Edge-CrowdStrike Integration	9
Policy Writing	9
Inbound Allow-List Policy	10
Outbound Policy	10
Services with Dynamic Ports	10
Chapter 2 Deployment	11
Get Started	11
Account Setup	11
Steps for Illumio Edge-CrowdStrike Integration	12
Select Incoming Services	15
Configure IP Ranges	17
Chapter 3 Edge Groups	22
Illumio Edge Groups and Explorer	22
Groups for Edge-CrowdStrike Integration	22
Explorer for Edge-CrowdStrike Integration	23
Workloads	27
Workloads Page	27
Workload Policy States	28
Workload Summary	28
Rules	29

Policy Objects for Edge-CrowdStrike Integration	30
Inbound Services	30
IP Ranges	31
Edit the Policy of a Group	32
Chapter 4 Management	34
<hr/>	
Access Management	34
View Global Roles	34
Add a Local User	36
External Groups and External Users	37
Authentication	37
User Activity	38
Access Restrictions	38
Provision	41
Draft Changes	41
Policy Versions	42
Settings	42
Event Settings	42
Policy Settings	43
Reversible Source and Destination Columns	44
Troubleshooting	46
Blocked Traffic	46
Events	46
Export Reports	47

About Illumio Edge-CrowdStrike Integration

This chapter contains the following topics:

Overview of the Illumio Edge-CrowdStrike Integration	5
Prerequisites and Limitations	9
Policy Writing	9

This section provides an overview of how Illumio® Edge® and CrowdStrike integrate, and lists a few limitations of the 20.2.0 generally available (GA) release.

Overview of the Illumio Edge-CrowdStrike Integration

This Illumio® Edge® and CrowdStrike® Integration Guide provides information on how to use Illumio Edge with the CrowdStrike agent, use the Illumio Edge UI to create groups, and write policies for endpoint protection. It also lists some troubleshooting steps and known limitations.

**IMPORTANT:**

This is an Illumio Secure Cloud only release.

About the Integration

About Illumio Edge

Endpoint segmentation is a very important security control and it is as important as data center segmentation. Illumio Edge gives you that security control by providing visibility and segmentation to the endpoint. Malware can spread when endpoints communicate with each other. Illumio Edge 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. The outbound connections from your machine will work, however, inbound connections will not work unless you write rules to allow them. So if an endpoint is compromised, it will not be able to spread the breach to other endpoints. Illumio Edge can be easily deployed and consumed thereby enabling you to quickly get the security benefits.

About CrowdStrike

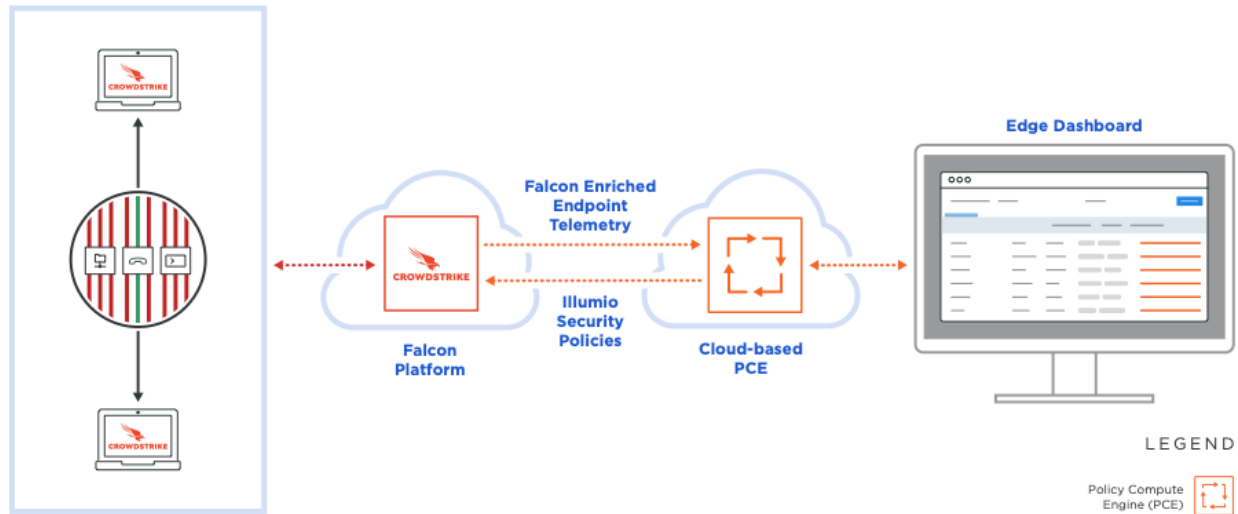
CrowdStrike is a SaaS endpoint management service that runs an agent on endpoints. CrowdStrike's agent (Falcon) sends a stream of events to the controller, and you can program the controller to define various types of policies to be applied to the agent.

The integration of Illumio Edge with CrowdStrike's ecosystem enables you to leverage Illumio Edge for securing your workloads. A modified version of Illumio Edge Policy Compute Engine (PCE) analyzes the traffic collected by the CrowdStrike agent and provides a mechanism to enforce firewall policy. This is helpful if you want to use existing agents and do not want to install new agents on your hosts. The CrowdStrike agent also programs firewall policy similar to Illumio's Virtual Enforcement Node (VEN).

By default, with Illumio Edge, all the workloads paired will be in the Coexistence mode. With the Illumio Edge and CrowdStrike integration you can use the Fal-

con agent in place of the VEN and still use Illumio Edge for endpoint segmentation.

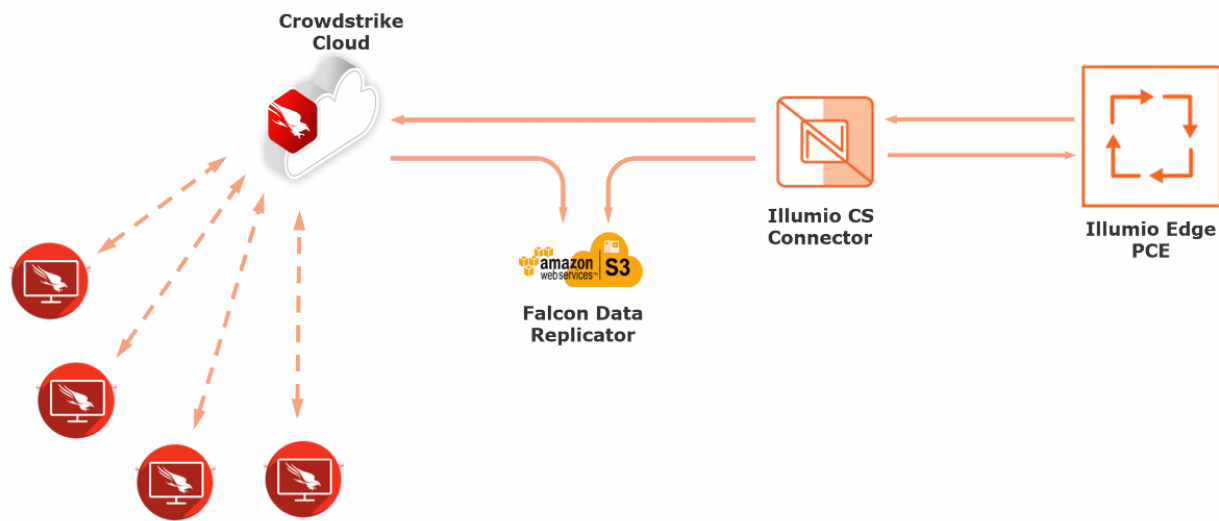
Workflow Diagram



About the Integration Architecture

CrowdStrike follows a model similar to Illumio. CrowdStrike agents (similar to Illumio's VENs) communicate with their cloud controller (similar to Illumio's PCE) and applies the rules for enforcement at the endpoints. CrowdStrike enters the telemetry from these agents in the Falcon Data Replicator for partners, such as Illumio to consume. Illumio's CrowdStrike (CS) Connector, gets the events from the Falcon Data Replicator and populates the visibility aspect of the Illumio Edge PCE. In the Edge Explorer, you can see the flow of events, the workloads, and so on. Once the policy is written on the Edge PCE, it gets sent to the Illumio CrowdStrike Connector which modifies it in to a form that CrowdStrike can understand and accordingly program its cloud. Illumio does not have a direct interaction with the CrowdStrike agent. Only CrowdStrike's cloud PCE and Illumio Edge PCE communicate with each other.

Architecture Diagram



Illumio Edge-CrowdStrike Integration Concepts

The concepts listed below are specific to the Illumio Edge-CrowdStrike integration:

- **Illumio CrowdStrike Connector:** Enables CrowdStrike agent integration with Illumio Edge PCE.
- **Hostgroup:** Is an arbitrary grouping of hosts. In this integration we consider only static hostgroups, where group membership is managed manually.
- **Illumio Edge PCE:** Provides mechanism to define groups, write and enforce policies.
- **Workload:** Are individual endpoints in your environment.
- **Groups:** Is a logical grouping of endpoints. A group can be a department (Finance, HR, Engineering, and so on), a phase (Phase1), or any other way to organize your endpoints.
- **Services:** Are the incoming (inbound or peer-to-peer) services that you want to include in your policy.
- **IP Ranges:** Is a range of IPs that is permitted to communicate for any given inbound service.
- **Rules:** Are policies allowing inbound services from specified IP ranges.

Prerequisites and Limitations

Recommended Skills

Illumio® recommends that you be familiar with:

- Your organization's security goals
- User endpoint applications
- CrowdStrike Falcon

Prerequisites for Illumio Edge-CrowdStrike Integration

- Illumio Edge 20.2.0 for CrowdStrike module
- Windows 7 or Windows 10 machines
- CrowdStrike Sensor version 5.10.x or later

Limitations for Illumio Edge-CrowdStrike Integration

The known limitations of this release are:

- Maximum number of hosts in preview is 100.
- A maximum of 10,000 rules can be configured in a hostgroup, which puts a capacity limitation on number of rules Illumio can generate.
- A separate SaaS PCE is required.
- Only on-premises Active Directory (AD) is supported. Azure AD is not supported.
- Is not compatible with hypervisors such as Windows Hyper-V, due to which connectivity to or from virtual machines may be blocked in the Enforced mode.
- Only supported on Windows OS.

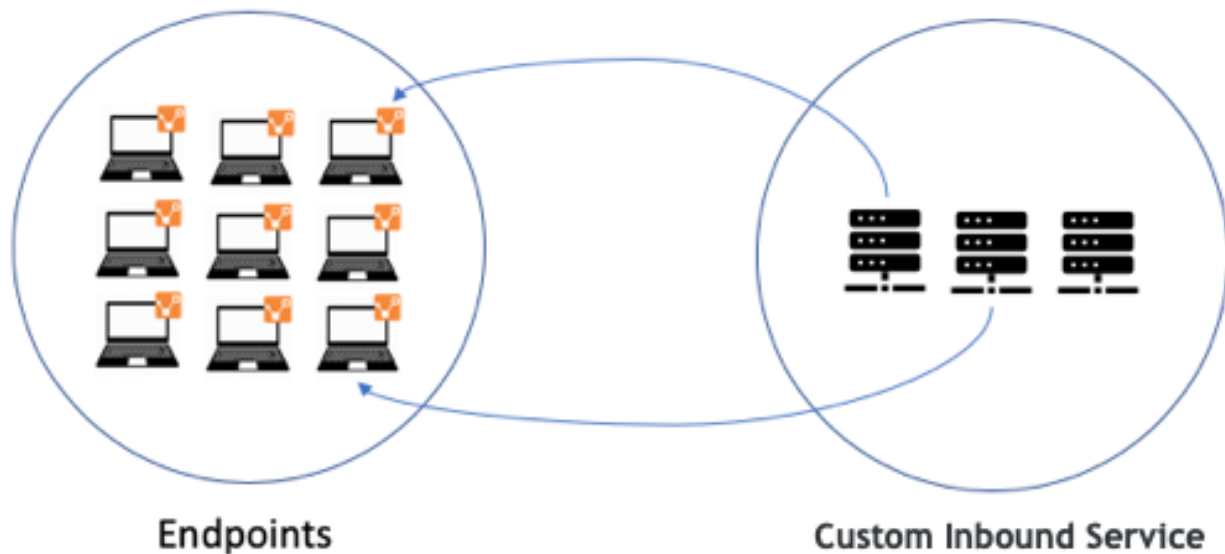
Policy Writing

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.

Inbound Allow-List 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



Outbound Policy

By default, all outbound traffic from a host is allowed.

Services with Dynamic Ports

If case of services with dynamic ports, consider creating a policy that is tied to the process or Windows service and allow all ports. In this way the host firewall will control access only on those ports on which that application is listening.

Deployment

This section describes how to deploy Illumio Edge and get set up with the Illumio Edge-CrowdStrike integration.

Get Started

Account Setup

When you sign-up with Illumio Edge, you will receive an email invitation to create your account and access Illumio Edge. The invitation link is valid for 7 days after which it expires. After creating your account, you can log in to the Illumio Edge web console.

When you log in for the first time, the “Welcome to Illumio Edge” page is displayed. The wizard opens on clicking **Get Started**, which walks you through the Illumio Edge setup steps that are described in the following sections. When you log in the next time, the Illumio Edge dashboard (Groups) is displayed with traffic alerts you have configured.

First time Illumio Edge login: Welcome page

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

Go to Home Page

You have 100 new workloads discovered by CrowdStrike



The following sections describe how to select the incoming services and configure IP Ranges to define security rules for a set of workloads in a Group.

Steps for Illumio Edge-CrowdStrike Integration

To get started with the Illumio Edge-CrowdStrike integration:

1. Click the **Try it now** button in the [CrowdStrike Store](#) to enable the Illumio Edge trial.

After Illumio validates and activates your request, you will receive an invitation email to create your Illumio Edge account.

2. Log into your CrowdStrike User Interface (UI).
 - a. Move your test endpoints in to “Illumio Managed Hosts” hostgroup.

GROUP NAME	HOSTS	GROUP TYPE	CREATED BY
Illumio Managed Hosts	9	Static	api-client-id:acb64e...
Illumio-Finance-179-illuminated-0c7...	2	Static	api-client-id:acb64e...
Illumio-grp1-enforced-a7e914de14...	0	Static	api-client-id:acb64e...
Illumio-grp2-11-enforced-98fc28d4e...	4	Static	api-client-id:acb64e...

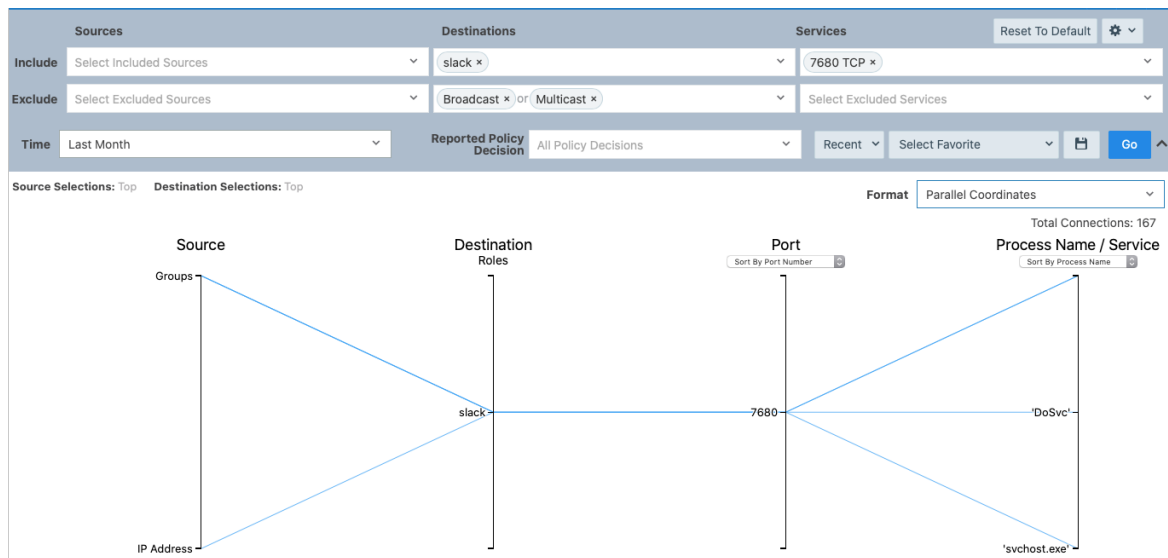
- b. Move hosts in to a specific hostgroup.

Hostname	L	First Seen	OS Version	OU	Prevention Pol...	Firewall Policy	Response Policy	Sensor Update...	USB Device Po...	Status	Sensor Ver...
ILLUMIO-179-ILLUMINATED-0C7...		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IP6-12		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IP6-2		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IP6-3		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IP6-5		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IP6-7		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IPV6-1		Jul...	Windows 10		Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IPV6-4		Jul...	Windows 10		Default (Wind...	Illumio-Financ...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0
ILLUMIO-IPV6-6		Jul...	Windows 10		Default (Wind...	Illumio-grp2-11...	Default (Wind...	Default (Wind...	Default (Wind...	Normal	5.32.114.06.0

3. Log in to your Illumio Edge PCE UI.

You see your workloads in the “Discovered Workloads” section.

- a. Move the workloads in to a Group.
 - b. Write policy to secure your workloads.

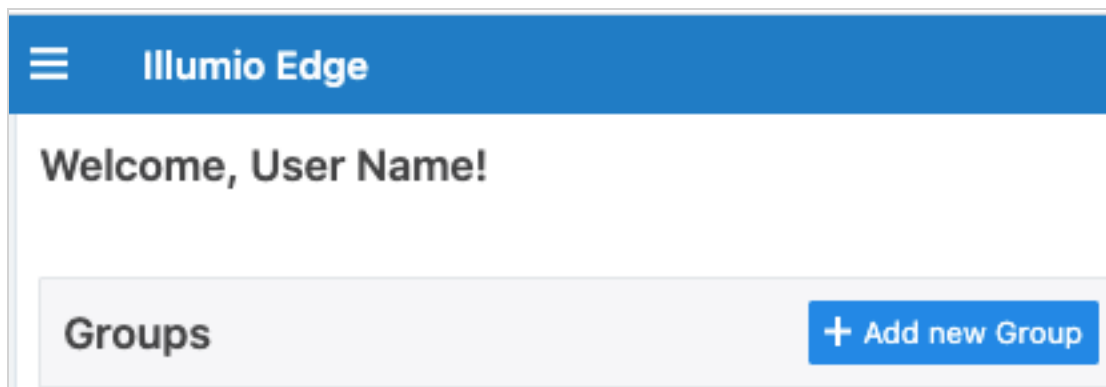


Select Incoming Services

This topic describes how to select the Incoming Services to allow for peer-to-peer communication.

To select incoming services:

1. You define a group and select your desired incoming services. Illumio Edge provides a list of common applications and you can select which items you want.
2. You can add a new Group by clicking **Add new Group** on the Groups page.



3. Enter a name for the new group in the **Name of Group** field, for example "HR."

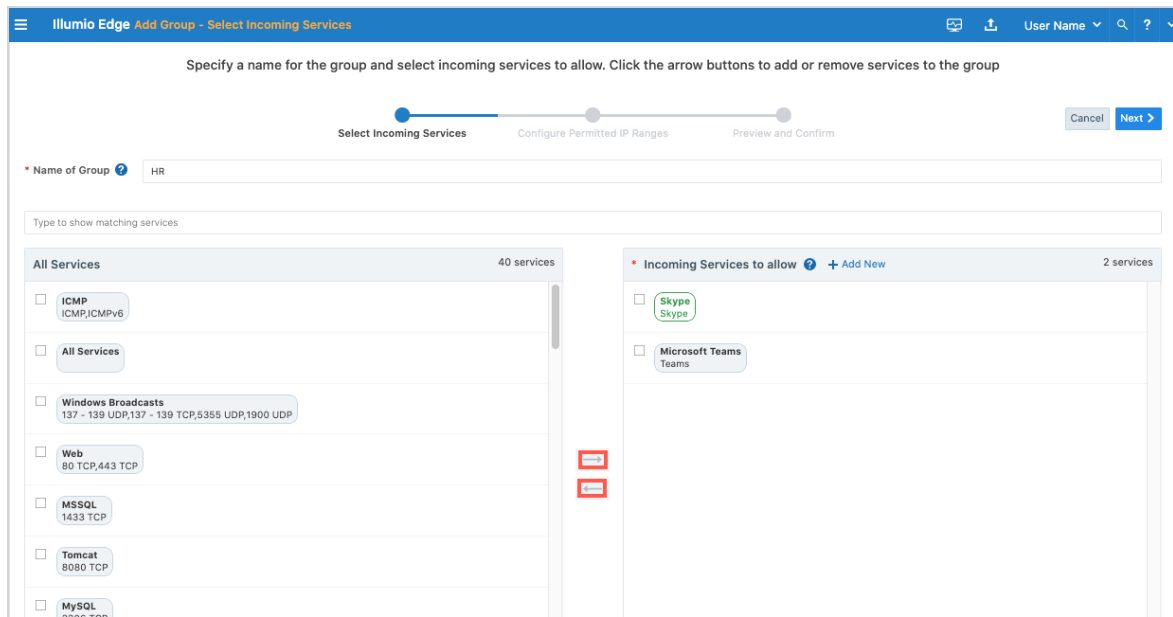
The group you have selected is the group of endpoints that the policy will be applied to.

4. Select your 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.
- You can select the service you want and use right and 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.



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

- If you are using a custom peer-to-peer application that is not in the provided 'All Services' list, click **+Add New** to define that service.

- Enter a **Name**, **Description**, and **Service Definitions** (Port and/or Protocol, Process, and Windows Service) and click **Save**.

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.

- Click **Next** to continue.

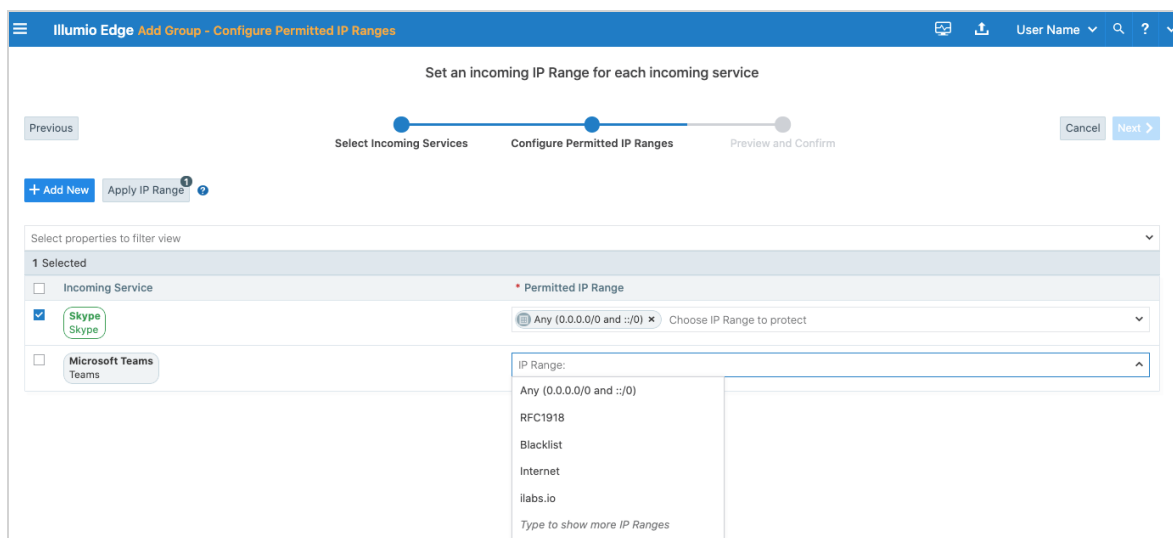
Configure IP Ranges

You configure the authorized **IP Ranges** that are allowed to communicate on the services you have defined in the Select Incoming Services section. For example,

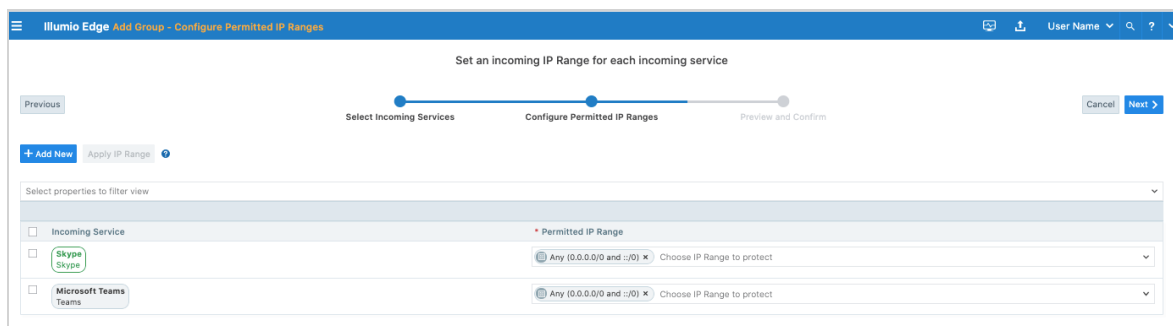
in the case of Skype the IP range can be **Any** because you want all the laptops of employees that belong to the HR group to communicate via Skype with each other. By default, Illumio Edge provides a few IP range options, such as **Any** and **RFC 1918**, which you cannot edit.

To configure IP ranges:

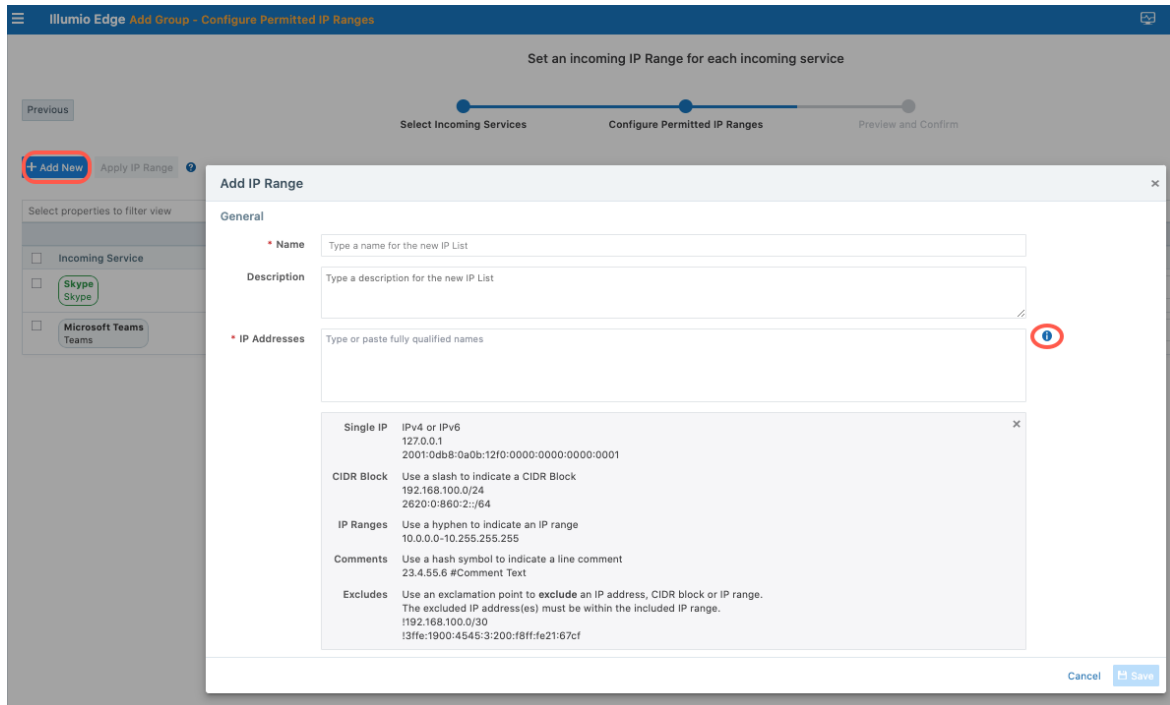
1. Select **Permitted IP Range** from the drop-down menu to select an incoming IP Range that is permitted to communicate for any given incoming service.



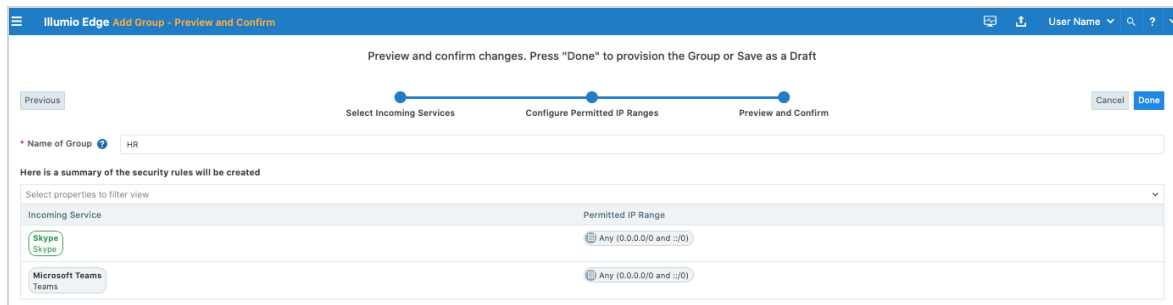
2. You can also click **Apply IP Range** to apply an IP range to one or more of the services.



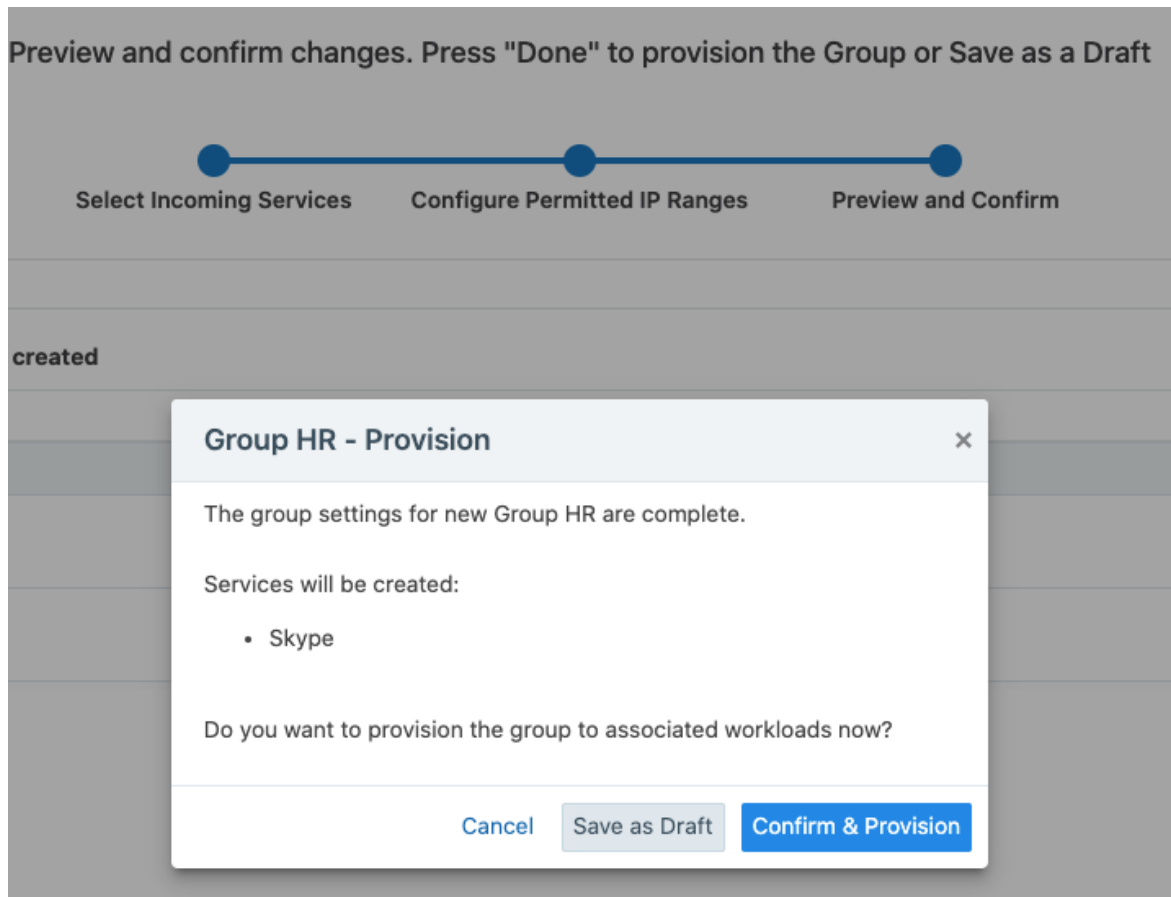
3. Click **+Add New**, if you want to create a new custom IP range. Click the 'i' icon to see the examples.



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.



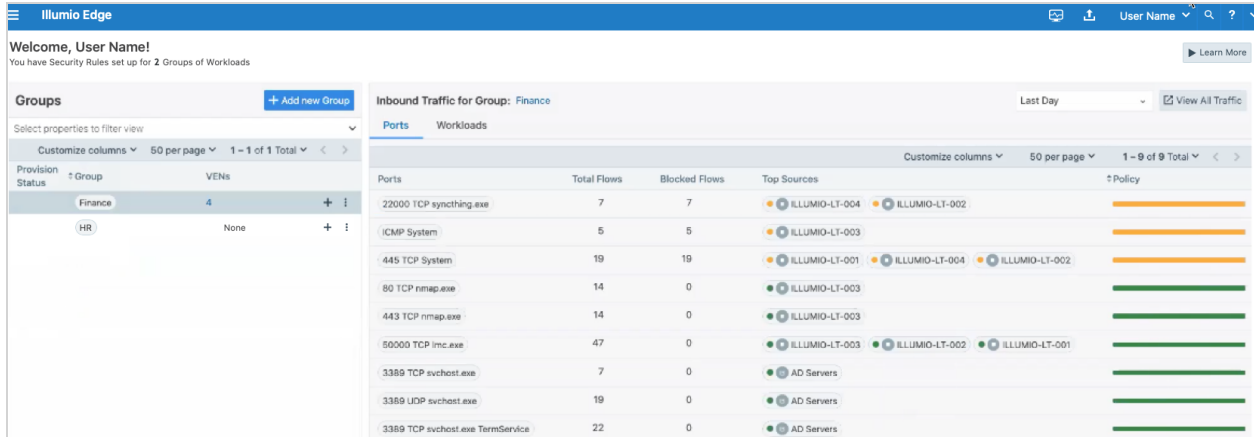
5. Click **Done** to Provision the Rules or Save as a Draft.
6. Verify the information in the pop-up and click **Provision and Confirm** to provision the rule to the associated workloads.

**NOTE:**

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

After successful provisioning, the **Illumio Edge Groups** page is displayed, with the groups and their provision status, and the number of workloads that are associated with that group.

The inbound traffic configured for that group is displayed in the right panel.



For information, see the [Explorer](#) section.

Edge Groups

This chapter contains the following topics:

Illumio Edge Groups and Explorer	22
Workloads	27
Policy Objects for Edge-CrowdStrike Integration	30

This section describes the Illumio Edge Groups page (or it's main dashboard), the Explorer feature, and Workloads that are part of the Illumio Edge-CrowdStrike Integration.

Illumio Edge Groups and Explorer

Groups for Edge-CrowdStrike Integration

The Illumio Edge Groups page offers a 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 and red traffic lines. You can also sort the data based on incoming service, port, or workload. Clicking on any of the lines under the Policy column, opens the Explorer page.

- **Green:** Allowed
- **Red:** Blocked

Traffic is blocked when a workload is in Enforced policy state.

Groups + Add new Group
 Select properties to filter view
 Provision Status: 25 / 1 - 25 of 30 Total

Provision Status	Group	Workloads
	secgroup2	1
	slack	1
	saddasd	None
ADDITION PENDING	xaCSAC	None

Group: saddasd
 Traffic Policy Workloads
Edit Group Refresh
 Type to show matching services
 Customize columns 50 per page 1 - 1 of 1 Total
 Incoming Service Allowed IP Ranges
 All Services Any (0.0.0.0/0 and ::/0)



NOTE:

Only Draft View is available. CrowdStrike does not indicate the type of traffic flow.

Groups + Add new Group
 Select properties to filter view
 Provision Status: 25 / 1 - 25 of 30 Total

Provision Status	Group	Workloads
	secgroup2	1
	slack	1
	saddasd	None
ADDITION PENDING	xaCSAC	None

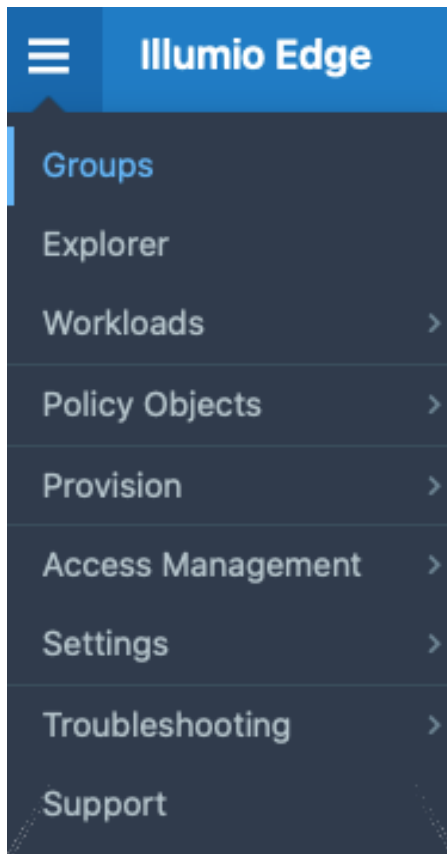
Group: slack
 Traffic Policy Workloads 1
 Top Ports Last Day View All Traffic
 Customize columns 50 per page 1 - 2 of 2 Total

Ports	Total Flows	Blocked Flows	Top Sources	Policy
7680 TCP	77	77	Private, DESK, Private 2	
135 ICMPv6	2	2	Internet	

Explorer for Edge-CrowdStrike Integration

Explorer allows you to analyze traffic flows for auditing, reporting, and troubleshooting purposes. You can access Explorer from:

- Top-left main menu > Explorer
- Clicking on the traffic flow under the Policy column located on the Groups page
- Clicking View **All Traffic** button located on the Groups page



The Explorer displays the traffic flow of workloads in the Group along with the port and protocol, process name, and Windows service name.

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

You can filter either Global (all groups) or per Group, Time, Service, IP Range, and Transmission mode (Unicast, Multicast, or Broadcast). 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.

Explorer

Sources Destinations Services Reset To Default

Include Select Included Sources slack x 7680 TCP x

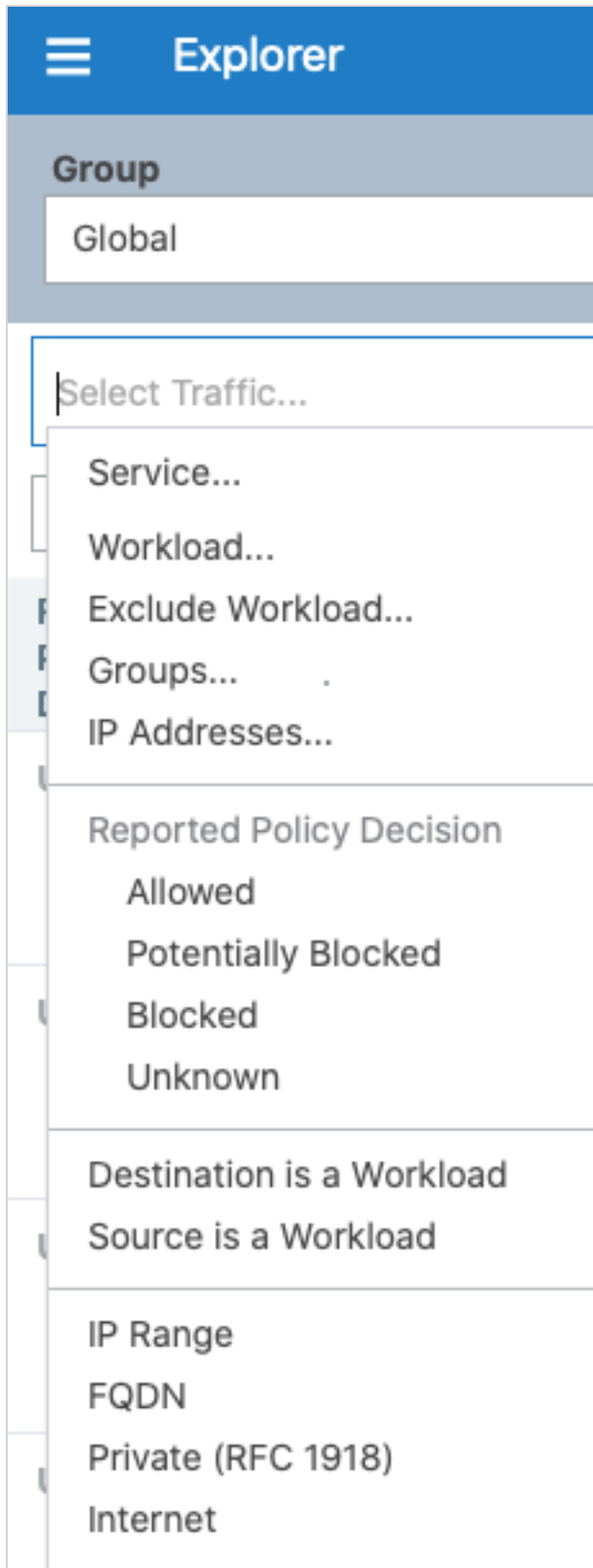
Exclude Select Excluded Sources Broadcast x or Multicast x Select Excluded Services

Time Last Month Reported Policy Decision All Policy Decisions Recent Select Favorite Go

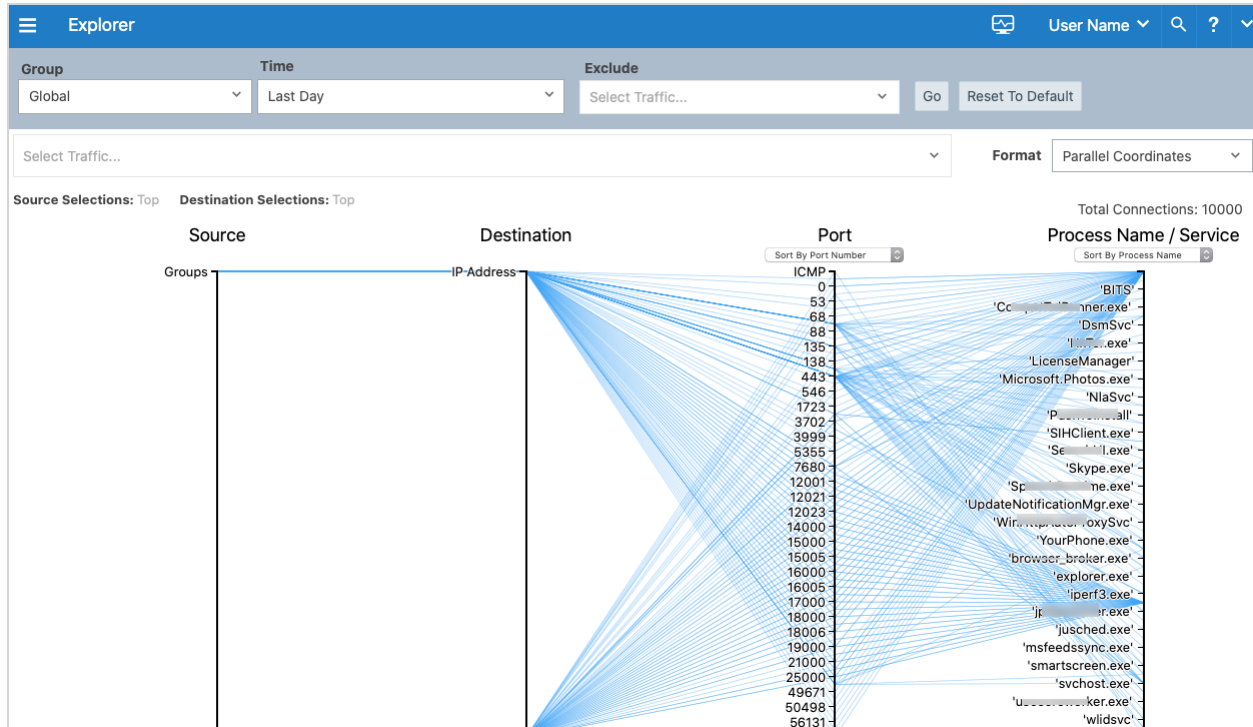
Reported View Export 1 - 50 of 167 Matched Format Table

Reported Policy Decision	Source	Source Groups	Destination	Destination Port/Process [User]	Destination Groups	Flows/Bytes	First Detected	Last Detected
Unknown	172.24.88.105 Private		W10-500AT4P 10.2.18.5 Unicast	7680 TCP	slack	7 flows	11/06/2020 15:49:13	11/24/2020 22:53:28
Unknown	172.24.88.104 Private		W10-500AT4P 10.2.18.5 Unicast	7680 TCP	slack	6 flows	11/10/2020 13:44:29	11/21/2020 14:29:40
Unknown	172.24.88.102 Private		W10-500AT4P 10.2.18.5	7680 TCP	slack	28 flows	11/06/2020 13:26:22	12/02/2020 15:36:01

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.

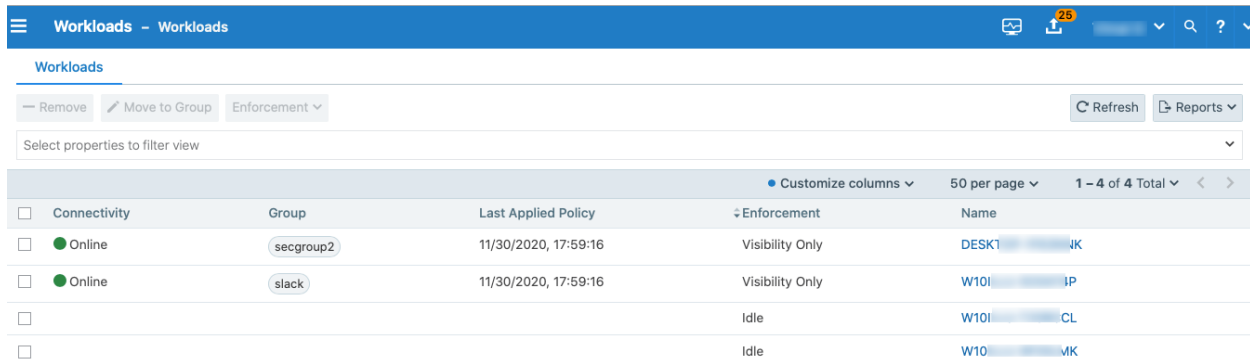


Workloads

The Workloads page displays all your workloads. After you pair workloads, you can view details by clicking a single workload. Only groups that the workload is in are displayed. Each workload, last received, group. You can Edit the Workload description, policy state and managed interfaces.

Workloads Page

You can select one or multiple workloads and move them in to a different Group. On the Workloads page, click on a workload to view and edit it attributes and to view and export the applied rules.



The screenshot shows the 'Workloads' page in the Illumio interface. At the top, there is a blue header with the title 'Workloads - Workloads' and navigation icons. Below the header, there are controls for 'Remove', 'Move to Group', and 'Enforcement'. A search bar is present with the text 'Select properties to filter view'. The main content is a table with the following columns: 'Connectivity', 'Group', 'Last Applied Policy', 'Enforcement', and 'Name'. The table contains four rows of workload data.

Connectivity	Group	Last Applied Policy	Enforcement	Name
<input type="checkbox"/> Online	secgroup2	11/30/2020, 17:59:16	Visibility Only	DESK1...JK
<input type="checkbox"/> Online	slack	11/30/2020, 17:59:16	Visibility Only	W10I...IP
<input type="checkbox"/>			Idle	W10I...CL
<input type="checkbox"/>			Idle	W10I...VK

Workload Policy States

Policy state determines how the rules affect a workload's network communication. After installing an agent on a workload, you can place the workload in one of the three policy states:

- **Idle**

Used for installing and activating the agent without changing the workload's firewall. The agent uses the workload's network analysis to provide relevant details to the PCE.

- **Visibility Only**

In the Visibility Only state, the agent inspects all open ports on a workload and reports the flow of traffic between it and other workloads 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.

The recommended flow of policy state cycle is to start with the Idle mode, next move to the Visibility mode to provision your policies. After confirming that the policies suit your organization needs, move to the Enforced mode.

Workload Summary

On the Workloads page, click on a workload to view its Summary and Rules. Workload attributes provide detailed information such as the hostname, the CrowdStrike agent ID (AID), and other attributes. If a workload belongs to a

particular group, it will receive the rules defined for that group after the ruleset is provisioned.

☰ 🏠 Workload - DESI NK

Summary
Rules

✎ Edit

General

Name	DESI-██████████-NK
Description	CrowdStrike aid: 5aacd9██████████-657dd39cce8
Enforcement	Visibility Only illumio Edge does not block any traffic
Connectivity	● Online
Policy Last Applied	11/30/2020 at 17:59:16

Group

Group	segroup2
-------	----------

Attributes

Hostname	DESKTOP-1F63NNK
OS	Windows
Release	10.0 ServicePack: 0.0.1198
Interfaces	Ethernet0: 10.2.10.39 link-local: fe80::c96f██████████-303:f7b8
Crowdstrike AID	5aacd9c██████████-657dd39cce8

Rules

Inbound rules are those that you define to allow services in to your workloads. The outbound rules are built by default to allow all traffic outbound.

Active version This list shows only active rules for domain interfaces. For non-domain interfaces, all outbound traffic is allowed and all inbound traffic is blocked

[Export to JSON](#)

Inbound Rules

Service	Addresses
Zoom Service	10.0.0.0/24
33434, 5004 UDP	
33434, 5004 TCP	
C:\Program Files (x86)\Microsoft\Skype\...e	10.0.0.1
Skype	
Teams	

Outbound Rules

Service	Addresses
All Services	0.0.0.0/0 0000:0000:0000:0000:0000:0000:0000:0000/0

Policy Objects for Edge-CrowdStrike Integration

The policy objects supported in this release of Illumio Edge are **Services** and **IP Ranges**, which have been described in the Concepts section. Your policy has only two criteria: inbound services and IP ranges.

Inbound Services

From the main menu, navigate to **Policy Objects > Services** to view all the inbound services you have previously defined. You can also create a custom service from the Services page by clicking the **+Add** button.

Services

[+ Add](#) [Provision](#) [Revert](#) [Remove](#)

Select properties to filter view

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 config

☰
Services (Create)

Save
Cancel

General

Name

Description

Service Definitions + Add - Remove

<input type="checkbox"/> Port and/or Protocol	<input type="checkbox"/> Process	<input type="checkbox"/> 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"/>

IP Ranges

Similarly for IP ranges, you can navigate to **Policy Objects > IP Ranges** to view all the IP ranges you have previously defined. You can also add custom IP range from the IP Ranges page by clicking the **+Add** button.

☰
IP Ranges

+ Add
Provision
Revert
- Remove

<input type="checkbox"/>	Provision Status	Name	Addresses	Last Modified On	Last Modified By
<input type="checkbox"/>		AD Servers	10.10.10.7	06/09/2020, 08:20:20	r...@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	10.2.0.0/16	06/09/2020, 08:31:09	r...@illumio.com

IP Range (Create)

Save Cancel

General

Name Type a name for the new IP List

Description Type a description for the new IP List

IP Addresses Type or paste fully qualified names

Single IP IPv4 or IPv6
127.0.0.1
2001:0db8:0a0b:12f0:0000:0000:0000:0001

CIDR Block Use a slash to indicate a CIDR Block
192.168.100.0/24
2620:0:860:2::/64

IP Ranges Use a hyphen to indicate an IP range
10.0.0.0-10.255.255.255

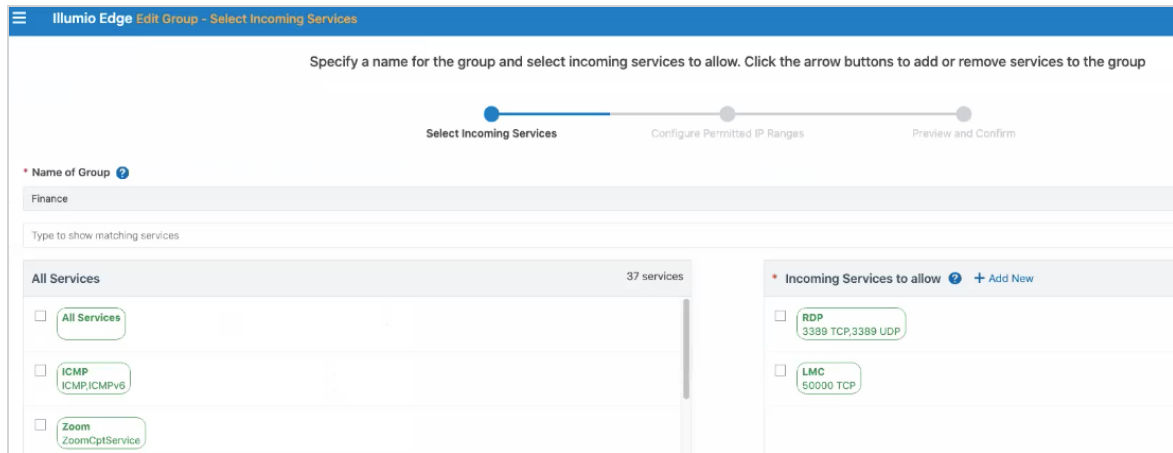
Comments Use a hash symbol to indicate a line comment
23.4.55.6 #Comment Text

Excludes Use an exclamation point to **exclude** an IP address, CIDR block or IP range.
The excluded IP address(es) must be within the included IP range.
!192.168.100.0/30
!3ffe:1900:4545:3:200:f8ff:fe21:67cf

Edit the Policy of a Group

If you want to edit the policy of a group, for example, you want to add a service to the Finance group:

1. From the Edge Groups page, click the name of the group, for example Finance.
The Group page opens, which displays the current policy for that group.
2. On the Group page, click **Edit** to open the Getting Started Wizard.



3. Edit the Group to modify the Incoming Services and IP Ranges as described in the initial section of this guide.

Management

This chapter contains the following topics:

Access Management	34
Provision	41
Settings	42
Troubleshooting	46

This section describes how to manage the various roles provided with Illumio Edge and how to manage policies and settings as well as troubleshooting steps.

Access Management

Illumio Edge includes four built-in Global Roles that grant users access to perform operations as required within your organization. You can assign multiple roles to one user and by mixing and matching the different roles, you can achieve different levels of granularity of permissions.

View Global Roles

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

Role-Based Access – Global Roles				
Global Roles	External Groups	External Users	Local Users	User Activity
Roles				
Global Organization Owner				
Global Administrator				
Global Viewer				
Global Policy Object Provisioner				

The following tables describes the access permissions for each role:

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: cannot 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 ^ Hide</p> <ul style="list-style-type: 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 	<p>Role Global Viewer</p> <p>Granted Access ^ Hide</p> <ul style="list-style-type: none"> 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 ^ Hide</p> <ul style="list-style-type: 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 	<p>Role Global Policy Object Provisioner</p> <p>Granted Access ^ Hide</p> <ul style="list-style-type: 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

Add a Local User

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



TIP:

You can delete a user by selecting their name and clicking **Remove**.

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:
- None (Users without a role have Read Only access when this access is enabled.)
 - Global Organization Owner
 - Global Administrator
 - Global Read Only

External Groups and External Users

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 the user belongs to.

When you use an external corporate Identity Provider (IdP) to authenticate users but your IdP usernames do not use email addresses, email invitations cannot be sent to those users. When you add this type of user, send them a login URL that they can use to set up their Edge accounts and log into the web console. Removing an external user removes the user from the External Users tab and all the user's role memberships. The user's authentication is still managed by your corporate IdP.

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.

Authentication Settings

Choose your **Authentication Method** to authenticate users for accessing the PCE

LOCAL (IN USE)
User will sign into the PCE only with a local credential provided by the user's organization password policy. [Configure](#)

SAML
SAML users can also authenticate to the PCE using local credentials. [Configure](#)

i Sign in to the PCE using either SAML or LDAP along with local credentials.

Learn about supported SSO and LDAP providers
You can use one of the following identity providers for authenticating users with the PCE

[OneLogin](#) [Active Directory Federation Services](#) [Azure AD](#) [Okta](#) [Ping Identity](#)

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.

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.

In Illumio Edge, you can apply access restrictions to user sessions. The list of access restrictions has a column that indicates whether access restriction is applied to a particular user session or not.

**NOTE:**

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

To configure access restrictions:

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**.
3. The **Access Restriction** page is displayed that shows which IP addresses are allowed and where the restrictions have been applied.

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

4. To add a new restriction, click **Add**.
5. Enter the required attributes:
 - Name
 - IP Addresses (you can list up to eight IPv4 addresses or CIDR blocks)
6. Click **Save**.

Save

General

* Name

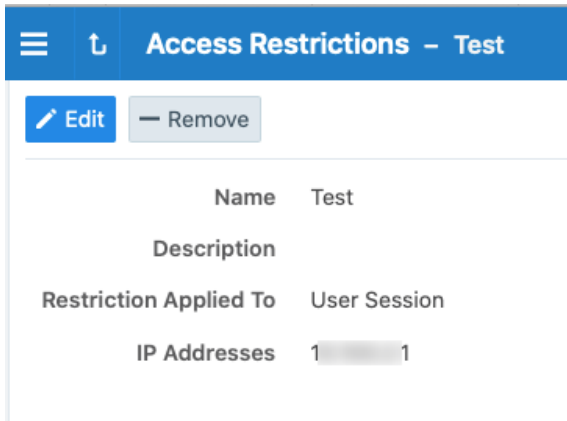
Description

* IP Addresses

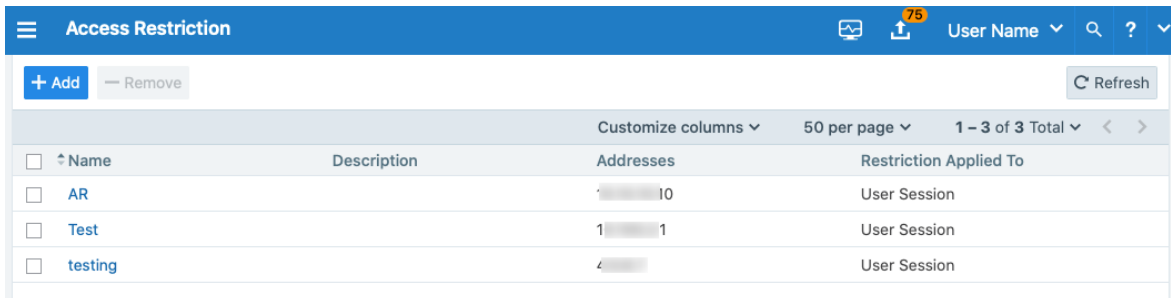
1	10.0.0.1
---	----------

1 Total
Maximum 8 IPv4 Addresses or CIDR Blocks

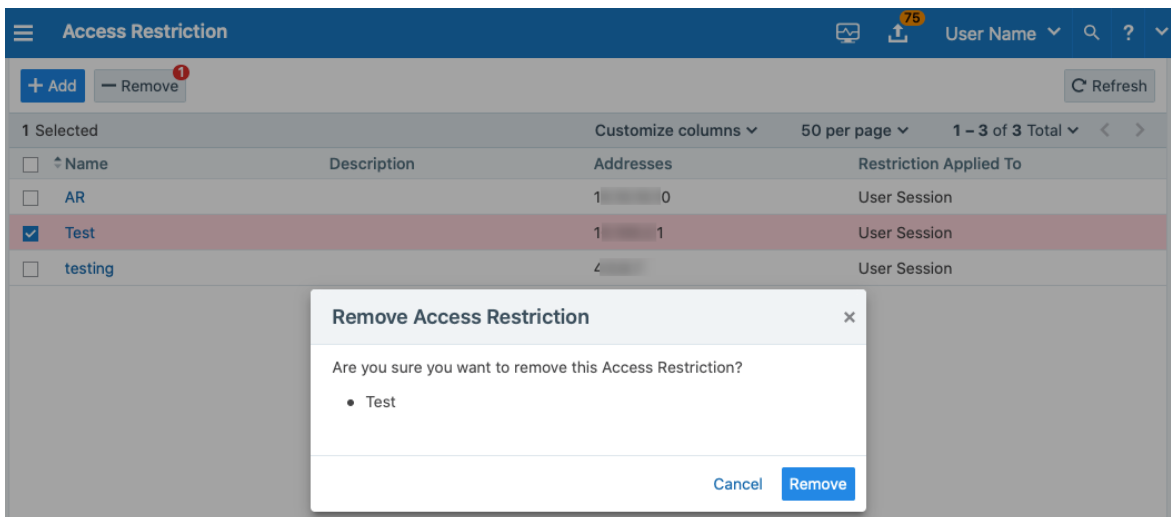
- Click **Edit** to edit the restriction or **Remove** to delete it.



- The newly added restriction is displayed on the Access Restriction page.




- To remove a restriction, select the check-box next to it's name and click **Remove**.
- Click **Remove** to confirm removal of the restriction or click **Cancel** to retain it.

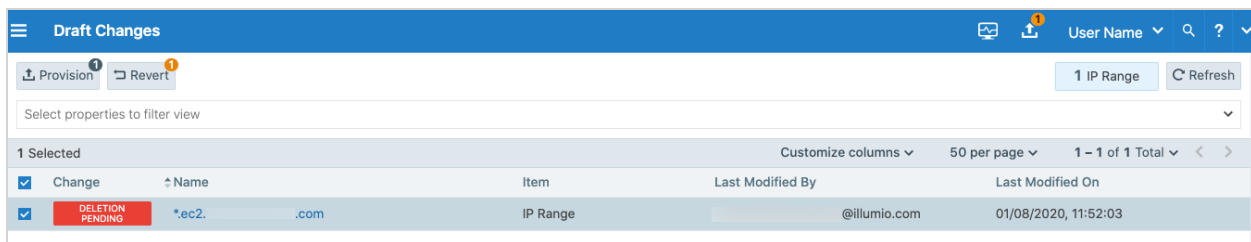


Provision

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

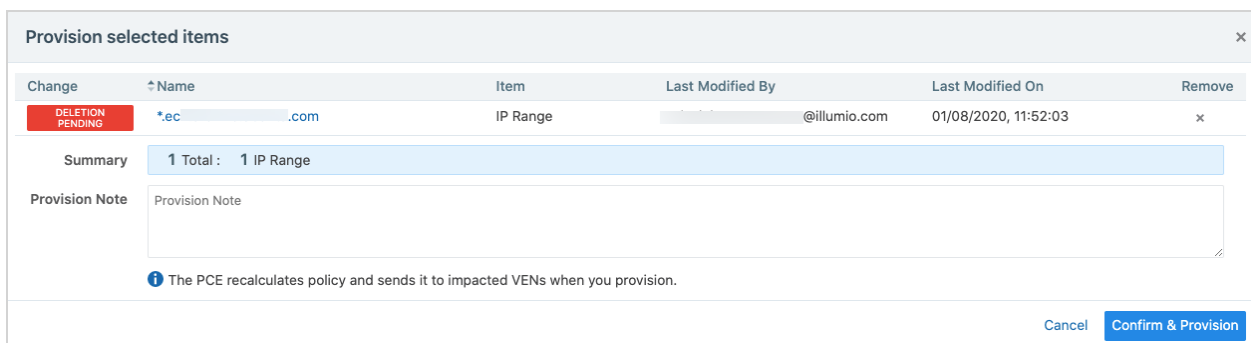
Draft Changes

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 agents installed on your workloads. 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.



Change	Name	Item	Last Modified By	Last Modified On
<input checked="" type="checkbox"/>	*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 workloads that need to be synchronized with the latest provisioned policy changes and the progress for applying the policy changes to those workloads.



Change	Name	Item	Last Modified By	Last Modified On	Remove
DELETION PENDING	*ec2. .com	IP Range	@illumio.com	01/08/2020, 11:52:03	x

Summary 1 Total : 1 IP Range

Provision Note Provision Note



i The PCE recalculates policy and sends it to impacted VENS when you provision.

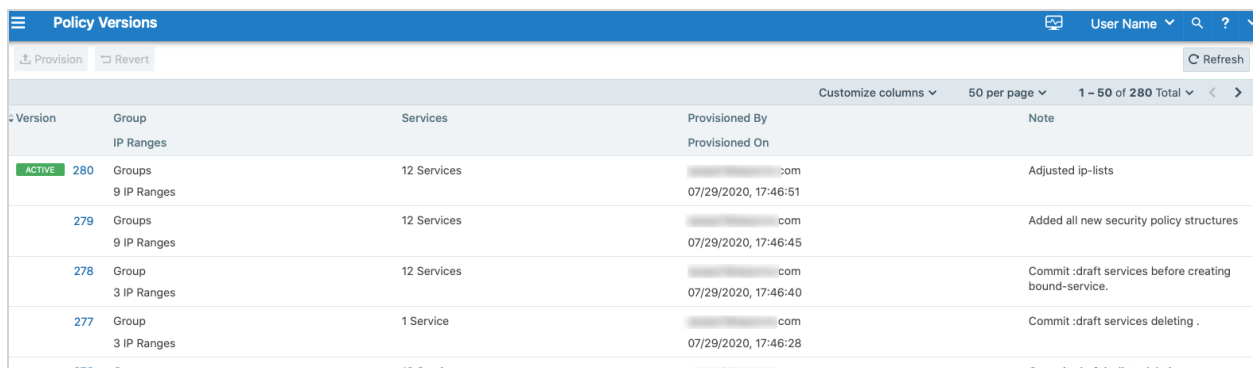
Cancel **Confirm & Provision**

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.



Version	Group	Services	Provisioned By	Note
ACTIVE 280	Groups 9 IP Ranges	12 Services	com 07/29/2020, 17:46:51	Adjusted ip-lists
279	Groups 9 IP Ranges	12 Services	com 07/29/2020, 17:46:45	Added all new security policy structures
278	Group 3 IP Ranges	12 Services	com 07/29/2020, 17:46:40	Commit :draft services before creating bound-service.
277	Group 3 IP Ranges	1 Service	com 07/29/2020, 17:46:28	Commit :draft services deleting .
276	Group	12 Services	com	Commit :draft ip-lists deleting .

Settings

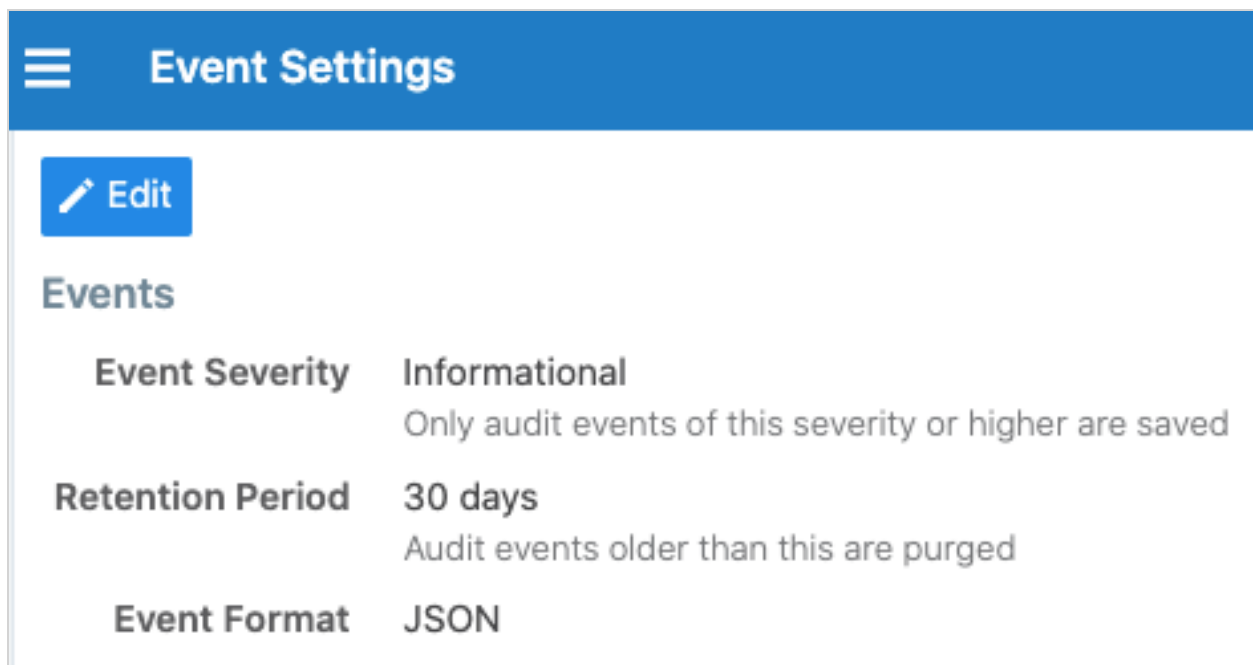
Event Settings

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).



The screenshot shows the 'Event Settings' page. At the top is a blue header with a hamburger menu icon and the text 'Event Settings'. Below the header is a white content area. On the left side of the content area is a blue button with a pencil icon and the text 'Edit'. Below the button is the section title 'Events'. There are three rows of settings:

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

Policy Settings

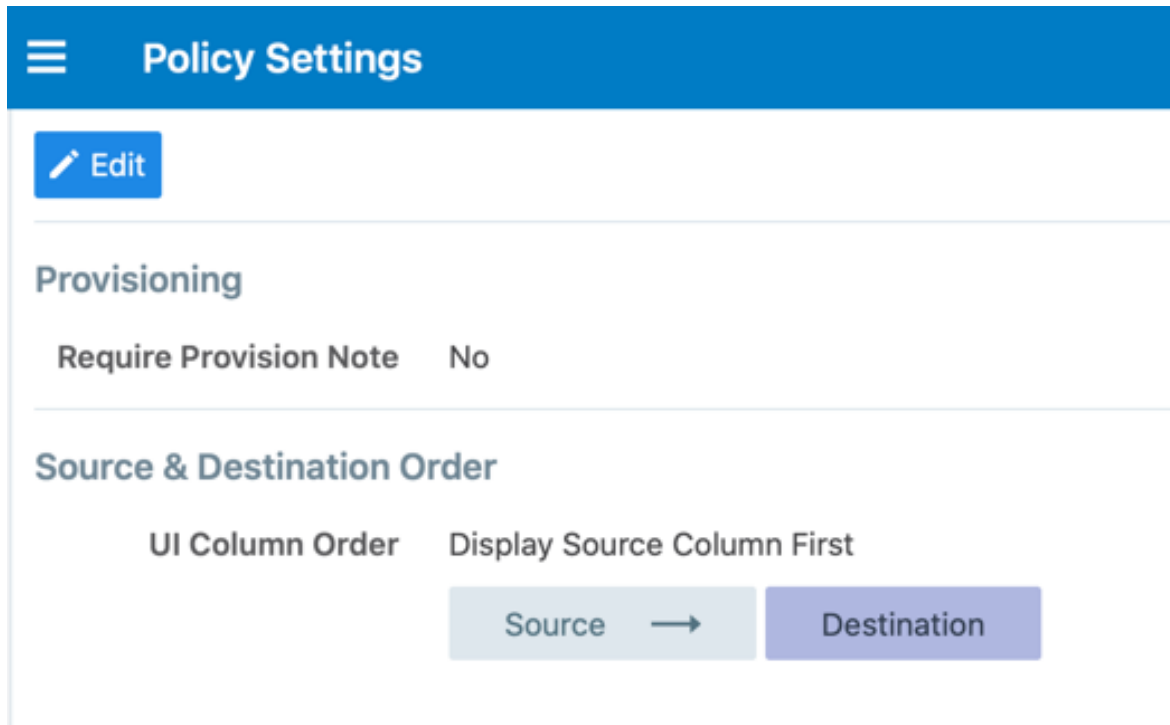
You have the option to make a **Provision Note** mandatory before you provision rules. It is disabled by default, but you can enable it to make it mandatory. This feature supports the need to describe context before provisioning and can support your organization's internal workflow. When it is enabled, you have to populate the note field before provisioning changes.

You might want your users to populate the Provision Note field with a link to your internal bug tracking system or project number for tracking and the error message they see when they leave the field empty will remind them to do so. Illumio Edge does not validate the content entered in the Provision Note field.

When enabled, you cannot provision updates until you enter text in the Provision Note field. The **Confirm & Provision** button is grayed out. After you enter appropriate text in the field the **Confirm & Provision** button is enabled and you can provision the update.

To make the provision note mandatory:

1. Navigate to **Settings > Policy Settings**. The Policy Settings page appears. By default, this option is set to No.



The screenshot shows the 'Policy Settings' page. At the top, there is a blue header with a hamburger menu icon and the text 'Policy Settings'. Below the header is a blue 'Edit' button with a pencil icon. The page is divided into two sections: 'Provisioning' and 'Source & Destination Order'. In the 'Provisioning' section, there is a label 'Require Provision Note' followed by the value 'No'. In the 'Source & Destination Order' section, there is a label 'UI Column Order' followed by the text 'Display Source Column First'. Below this text are two buttons: 'Source' with a right-pointing arrow, and 'Destination'.

2. Click **Edit**.
3. Change the *Require Provision Note* option to Yes.
4. Click **Confirm**.
5. Click **Save**.

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**.

3. Choose the **UI Column Order**.
4. Click **Save**.
5. 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 Internet	Deleted Workload ff02::1 Multicast	ICMPv6 System [NT AUTHORITY\SYSTEM]		4 flows	11/03/2020 02:49:44	11/03/2020 03:06:51
Allowed by Destination	fe80::fd46:f63b:c94d:2a3b Internet	Deleted Workload ff02::1 Multicast	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		4 flows	11/18/2020 06:20:41	11/18/2020 06:34:28

Troubleshooting

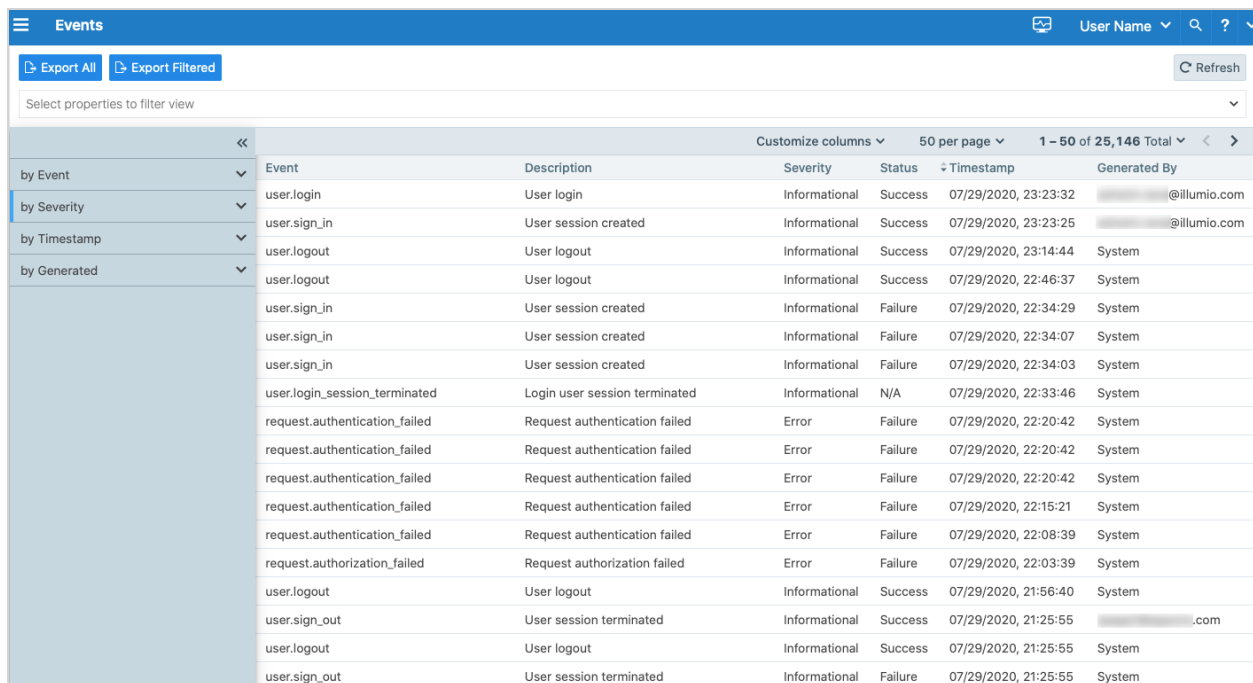
This topic describes how to troubleshoot common issues while using Illumio Edge.

Blocked Traffic

The Blocked Traffic page shows you all traffic that attempted to communicate with your workload 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. You can narrow down the view by filtering based on Group name, Traffic Status, name of the Workload, 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.

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						
by Event		Event	Description	Severity	Status	Timestamp
by Event	▼	user.login	User login	Informational	Success	07/29/2020, 23:23:32
by Severity	▼	user.sign_in	User session created	Informational	Success	07/29/2020, 23:23:25
by Timestamp	▼	user.logout	User logout	Informational	Success	07/29/2020, 23:14:44
by Generated	▼	user.logout	User logout	Informational	Success	07/29/2020, 22:46:37
		user.sign_in	User session created	Informational	Failure	07/29/2020, 22:34:29
		user.sign_in	User session created	Informational	Failure	07/29/2020, 22:34:07
		user.sign_in	User session created	Informational	Failure	07/29/2020, 22:34:03
		user.login_session_terminated	Login user session terminated	Informational	N/A	07/29/2020, 22:33:46
		request.authentication_failed	Request authentication failed	Error	Failure	07/29/2020, 22:20:42
		request.authentication_failed	Request authentication failed	Error	Failure	07/29/2020, 22:20:42
		request.authentication_failed	Request authentication failed	Error	Failure	07/29/2020, 22:20:42
		request.authentication_failed	Request authentication failed	Error	Failure	07/29/2020, 22:15:21
		request.authentication_failed	Request authentication failed	Error	Failure	07/29/2020, 22:08:39
		request.authorization_failed	Request authorization failed	Error	Failure	07/29/2020, 22:03:39
		user.logout	User logout	Informational	Success	07/29/2020, 21:56:40
		user.sign_out	User session terminated	Informational	Success	07/29/2020, 21:25:55
		user.logout	User logout	Informational	Success	07/29/2020, 21:25:55
		user.sign_out	User session terminated	Informational	Failure	07/29/2020, 21:25:55

Export Reports

You can generate reports for Workloads, Services, and IP Ranges in JSON or CSV formats from the **Reports** drop-down menu on the corresponding page and then download the report from the **Troubleshooting > Export Reports** page.

The screenshot shows two screenshots from the illumio interface. The top screenshot is the 'Services' page, and the bottom screenshot is the 'Export Reports' page.

Services Page:

- Header: Services, User Name, Search, Help.
- Buttons: + Add, Provision, Revert, Remove, Refresh, Reports (dropdown).
- Filter: Select properties to filter view.
- Table Columns: Provision Status, Name, Port/Protocol, Last Modified On, Last Modified By, Description.
- Table Data:

Provision Status	Name	Port/Protocol	Last Modified On	Last Modified By	Description
	grp2_win_service_iplist_range	...ava.exe	07/29/2020, 17:46:38	...com	grp2_service_iplist_range
	grp2_win_service_port_CIDR_range	14000 TCP ... 14000exe	07/29/2020, 17:46:38	...com	grp2_win_service_port_CIDR_range
	grp3_win_service_port_CIDR_exclude_ipexe, 16000exe	07/29/2020, 17:46:39	...com	grp3_win_service_port_CIDR_exclude_ip
	grp4_process_name_env_var_si	...nja	07/29/2020, 17:46:39	...com	grp4_process_name_env_var
- Dropdown Menu (Reports): Generate as JSON, Generate as CSV, All Export Reports.

Export Reports Page:

- Header: Export Reports, User Name, Search, Help.
- Buttons: + New Report, Remove, Download, Refresh.
- Table Columns: File name, Containing All, Generated By, Generated At, Status, Retry, Download.
- Table Data:

File name	Containing All	Generated By	Generated At	Status	Retry	Download
Services_CSV_2020-07-30,01-18-52	Services	... illumio.com	07/30/2020, 01:18:52	Done	Regenerate	Download