Illumio Core®

Version 22.1.3

Application Ringfencing Tutorial

June 2022

18000-200-22.1.3

Legal Notices

Product Versions

PCE Version: 22.1.1 (Standard release) | Illumio Core Cloud customers only

For the complete list of Illumio Core components compatible with Core 22.1.1-PCE, see the Illumio Support portal (login required).

Standard versus LTS Releases

22.1.1-PCE is a Standard release. For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Resources

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

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

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

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

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

Contact Information

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

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

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

Contents

Chapter 1

Learn About Application Ringfencing

This chapter contains the following topics:

Before beginning this tutorial, take a moment to verify you have met the tutorial prerequisites and understand the key concepts that will be leveraged in the tutorial lessons.

About this Tutorial

This tutorial includes a series of lessons designed to teach you how to ringfence applications by using two valuable features – Illumination and Policy Generator.

In this tutorial, we describe how to get started with Illumio Core by creating managed workloads and applying application segmentation, also called application ringfencing, which separates individual applications, preventing cross-application communications.

Before You Begin

This tutorial walks you through installing Illumio agents on hosts in your environment. The Illumio platform operates in a secure environment with secure communication between Illumio agents installed in your environment and the Illumio platform. The Illumio agents are lightweight and designed for low resource utilization.

Additionally, you will be creating and testing security policy for your workloads using Illumio's Build and Test policy states. These policy states do not block network traffic to your workloads. They allow you to visualize the impact of the security policy that you create before you enforce it on your workloads.

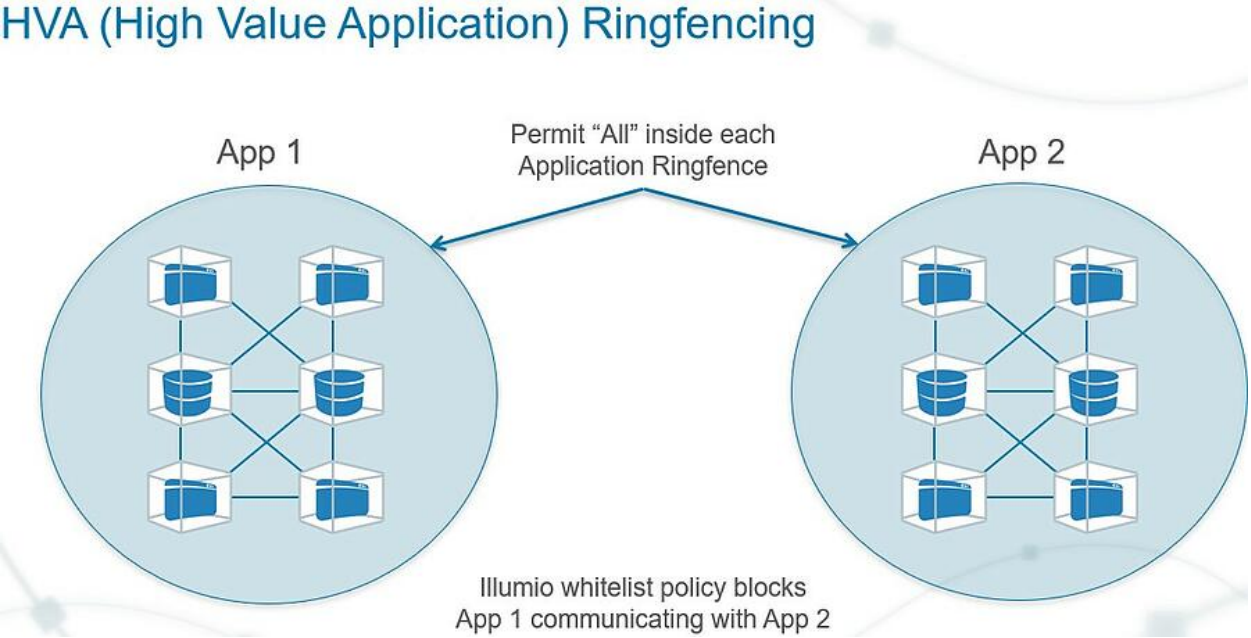
Finally, Illumio recommends you work through this tutorial using hosts running in your testing or staging environments.

About Application Ringfencing

With Illumio Core, you have the power to model and test segmentation policies at different levels: from course-grained to extremely fine-grained segmentation. Most Illumio customers start by applying application ringfencing to their high-value applications.

Unless the initial deployment must satisfy stated compliance or regulatory guidance, the best initial policies start with ringfencing. Ringfencing shrinks the security perimeter from a subnet or VLAN to a single application. It provides the largest impact with the least amount of work, requiring only one line of security policy per application to close off 90 percent of the potential attack surface for east-west traffic movement.

Additionally, application ringfencing provides the greatest flexibility to application owners and developers. Because there is a “permit-any” rule active within the ringfence, changes to the application’s internal communication will always work. An application ringfence allows all workloads within an application group to communicate over any port.



Essential Concepts

Understanding these concepts will help you complete the solutions in this tutorial and give you a deeper understanding of the Illumio technology.

Illumio Core components

The relationship and basic architecture of the platform's components—the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN). Understanding the interaction between the PCE and VEN is essential to learning about Illumio technology.

Policy Compute Engine (PCE)

The brain of the Illumio Core. The Illumio Core stores its program logic and the information it collects in the PCE. The PCE generates and distributes segmentation policies for each VEN connected to it.

Virtual Enforcement Node (VEN)

The local control point of the Illumio Core installed on each workload. It provides information about the workload and enforces policy rules by controlling the Linux iptables or Windows Filtering Platform (WFP) tables on a workload.

Workload

The Illumio generic term for anything with an operating system, such as a bare-metal server, VM, or container (e.g., Docker container).

Workload Policy States

The VEN supports multiple policy states to help with the policy creation process. Illumination shows these states and uses them to visualize traffic.

Pairing

The process of installing the Illumio VEN software on a workload by using a unique secure pairing key.

Rulesets and Rules

The allowlist policies that use labels to generate customized port connections for each workload. Rules are collected into rulesets for versioning. Policies are pushed out to workloads with the matching labels by a process called provisioning.

Providers and Consumers

The Illumio model is provider centric. You declare what ports on providers can be accessed by consumers.

Role Labels

The function of a workload; e.g., for a simple two-tier application consisting of a web server and a database server: Web and Database. Assigning Role labels to workloads allows you to create advanced segmentation policies.

Applications Groups

Are collections of workloads with the same Location, Environment, and Application labels. Applications are a control point for policy. Policy Generator uses application groups as the essential unit.

Micro-segmentation

A security technique that enables fine-grained security policies to be assigned to applications, down to the workload level. It is built around two key principles: granularity and dynamic adaptation. The application of these principles makes micro-segmentation fundamentally different from conventional network segmentation.

Allowlist model

An allowlist policy follows a trust-centric model that denies everything and only permits what you explicitly allow—a better choice in today's datacenters. The list of what you do want to connect in your datacenter is much smaller than what you do not want to connect. This immediately cuts back, if not eliminates, false positives.

Tutorial Prerequisites

This tutorial requires you to have the following data, access, and systems.

- **5 to 20 hosts:** Bare-metal servers or virtual machines (VMs) in your datacenter or a public cloud. They can be running Windows or Linux.
- **Installed packages:** The hosts must have the required packages installed.
- **Development or test applications:** The hosts need to have running applications that are generating traffic data. A distributed application is recommended.
- **Internet HTTPS access over TCP port 443:** Illumio Core needs an outward communication connection for HTTPS using TCP port 443.

Chapter 2

Application Ringfencing Lessons

This chapter contains the following topics:

This tutorial is divided into a series of lessons. The lessons correspond to the major phases of creating an application ringfence in your environment. The lessons are organized to correspond to the workflow for creating an application ringfence.

Pairing Workloads Lesson

In this lesson, you will learn about installing the Illumio agent on compute assets in your datacenter or private or public cloud so that you can apply micro-segmentation policies.

Lesson Prerequisites

This lesson requires you to have the following data, access, and systems.

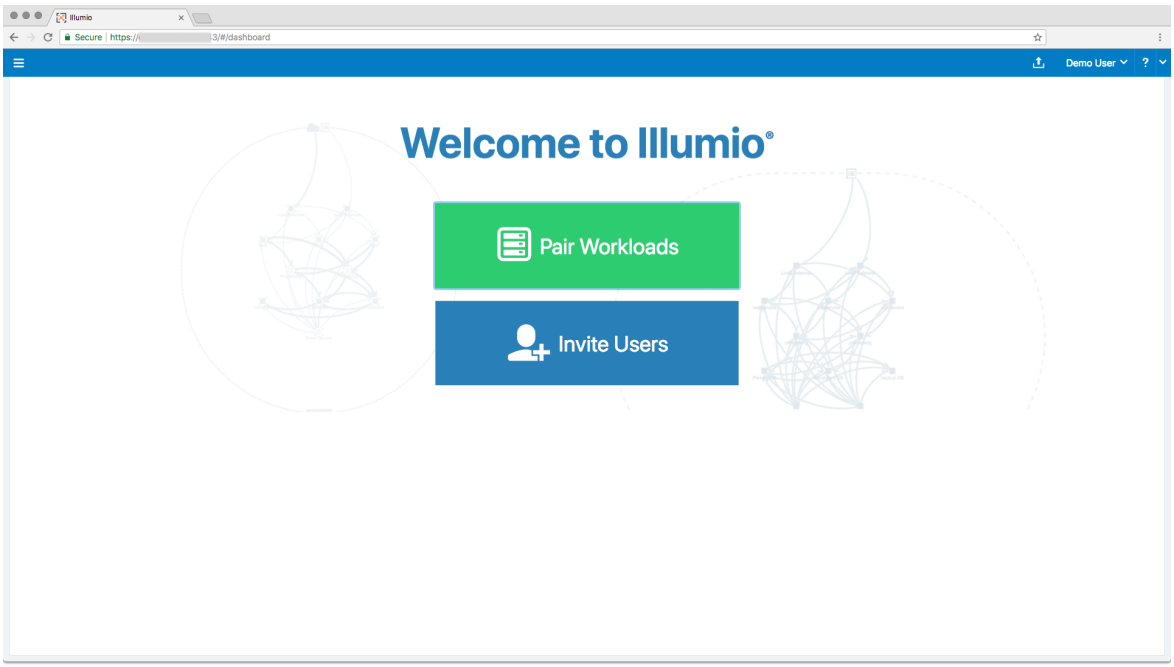
- **Understand essential concepts:** To complete this lesson, you must understand what the Illumio VEN is and how the process of pairing workloads works.
- **5 to 20 hosts:** Bare-metal servers or VMs in your datacenter or a public cloud. They can be running Windows or Linux.
- **Installed packages:** The hosts must have the required packages installed.

- **Supported operating systems and required packages** For information, see OS Support and Package Dependencies on the Illumio Support portal.
- **Development or test applications:** The hosts need to have running applications that are generating traffic data. A distributed application is recommended.
- **Root or Admin access:** You must have Root or Admin access on the hosts to install the VEN. Windows hosts must have PowerShell installed.
- **Internet HTTPS access over TCP port 443:** The hosts must be able to connect outbound over TCP port 443.

Instructions

1. **Log into your Illumio Core.**

   When you log into the Illumio web console the first time, you see the Welcome page, which directs you to pair workloads or add Illumio users.



   The next time you log into the web console, the Illumination map appears.

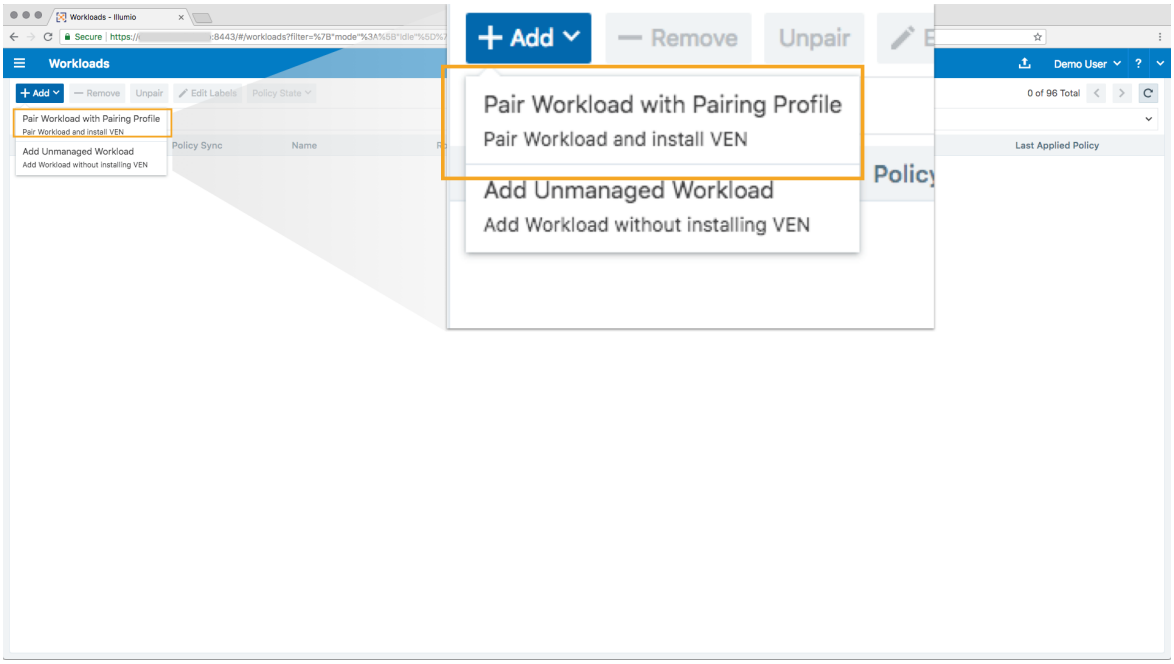
2. **Generate a pairing key and script.**

   The PCE web console provides a default pairing profile containing a pairing key and pairing script so that you can begin pairing workloads. You have the option to create a new pairing profile if you want to configure your own workload pairing settings. This lesson directs you to use the default pairing profile.

You can configure a pairing profile so that it assigns labels to the workloads you pair. The default pairing profile does not contain any labels. You will learn how to apply labels to workloads in a later lesson during this tutorial. The policy state is set to Build mode in the default pairing profile. You will learn about policy states in a later lesson.

The default pairing profile provides unlimited pairing for an unlimited time. You can change this behavior by editing the pairing limit and time. In this lesson, you will use the default settings.

a. If this is your first time logging in, click Pair Workloads in the Welcome page. Otherwise, from the left navigation menu, select Workloads. The Workloads page appears.
b. Select Add → Pair Workload with Pairing Profile.



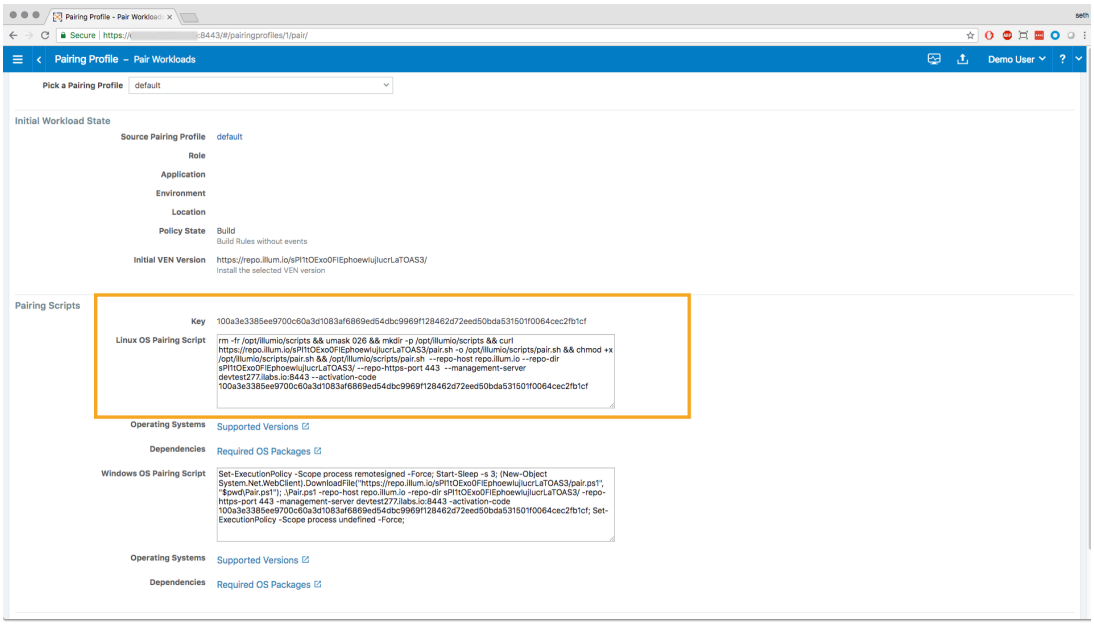
The Pairing Profile page appears with a generated pairing key and scripts for Windows and Linux workloads.

3. **Pair a Linux workload.**

On the Pairing Profile page, you see only one pairing profile named “default” if this is your first time pairing.

a. In the Pairing Script section, copy the Linux pairing script.

b. SSH into the Linux workload you want to pair. Root access on the workload is required for installation of the Linux VEN.



c. In the shell window on the Linux workload, paste the script you copied from the pairing profile and run it.

The workload starts the pairing process. As the pairing script runs, you will see success messages appear.

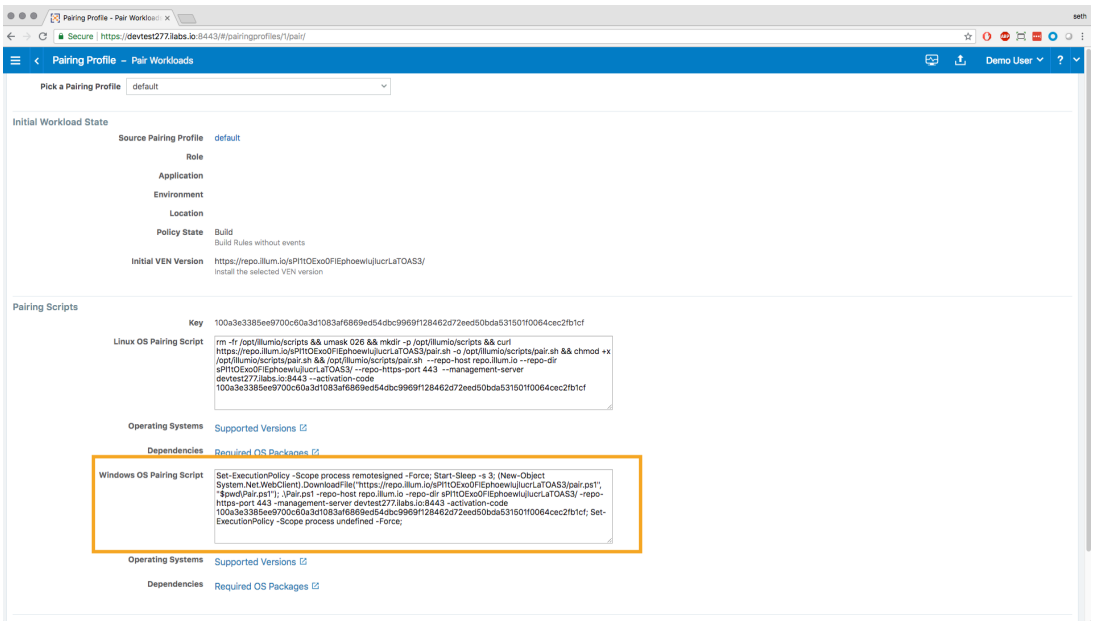
Wait until you see the message “Workload has been SUCCESSFULLY paired with Illumio,” which means your VEN pairing is complete.

4. **Pair a Windows workload.**

On the Pairing Profile page, you see only one pairing profile named “default” if this is your first time pairing.

a. In the Pairing Script section, copy the Windows pairing script.

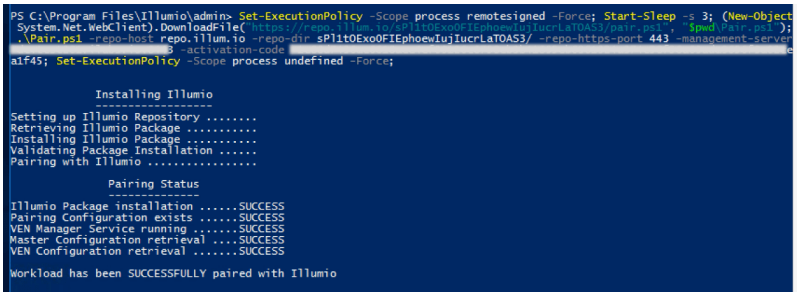
b. On the Windows workload you want to pair, open the Windows PowerShell as an Administrator user.

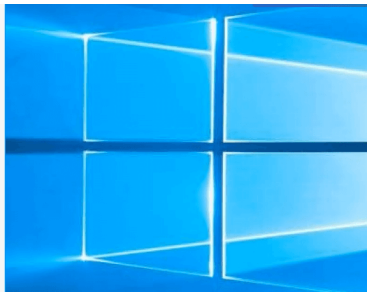


c. Paste the pairing script you copied into the PowerShell command prompt and run it.

The workload starts the pairing process. As the pairing script runs, you will see success messages appear.

Wait until you see the message "Workload has been SUCCESSFULLY paired with Illumio," which means your VEN pairing is complete.





NOTE:
When the Illumio VEN is being installed on a Windows workload, all internet group management protocol IGMP traffic will be blocked. Windows servers typically use IGMP for things like Windows internet naming service (WINS), Windows Deployment Services (WDS), IGMP Router Proxy Mode, or network load balancing (NLB) in multicast mode.

5. **Repeat pairing procedure.**

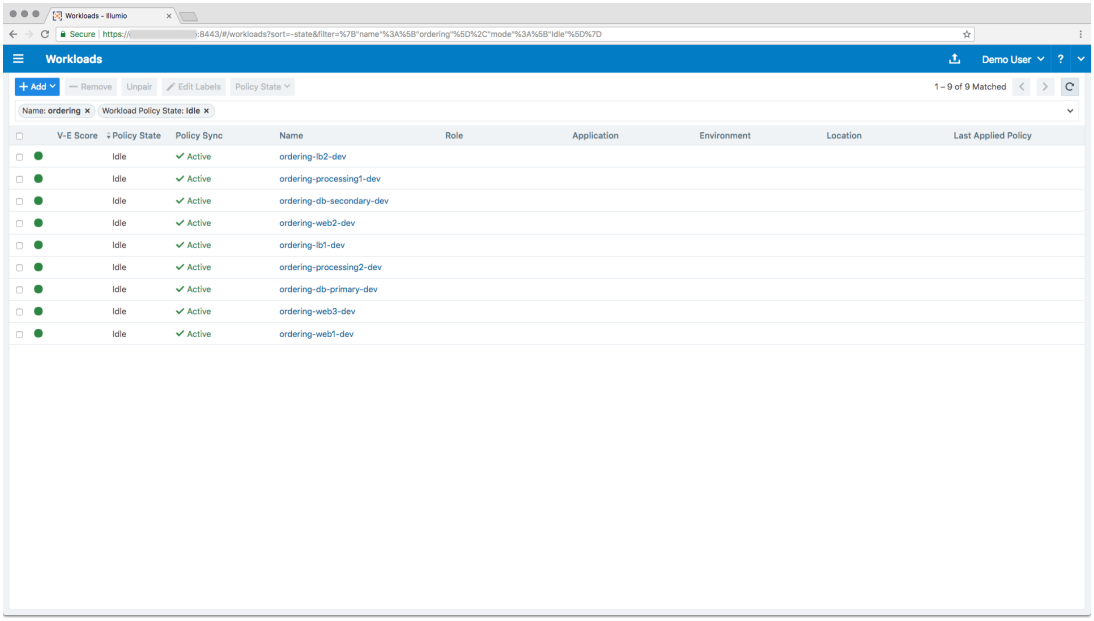
   You can pair as many workloads as you have in your application. The default pairing profile provides unlimited pairing for an unlimited time. You can change this behavior by editing the pairing limit and time.

6. **Validate workload pairing.**

   After the workload is paired, you can validate that the workload is managed by Illumio.

   a. From the left navigation menu, select Workloads.

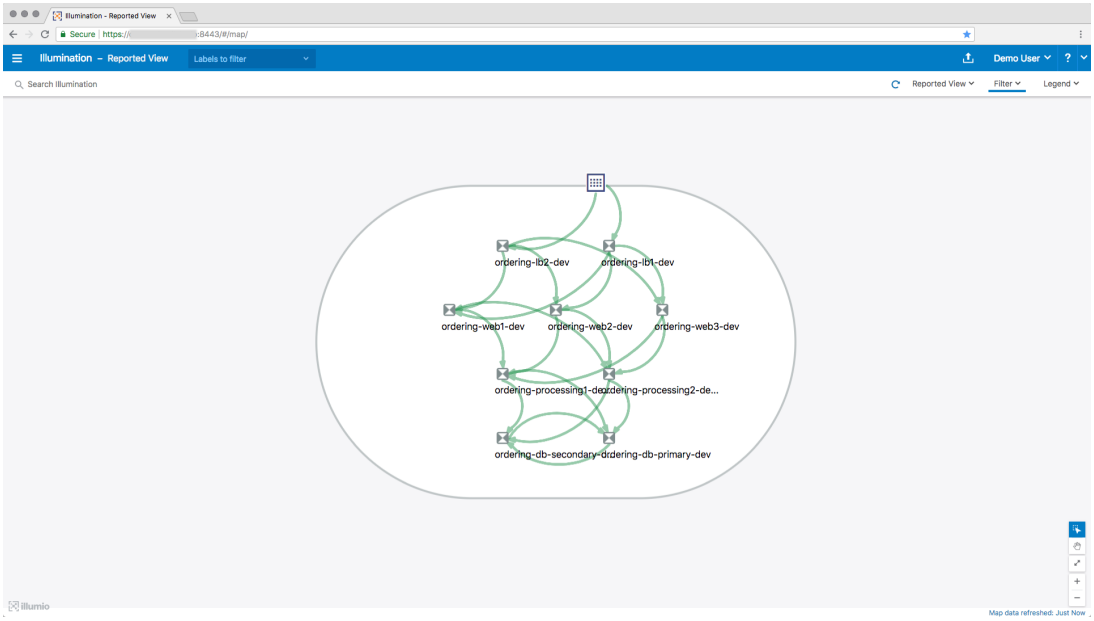
   b. If necessary, click the refresh icon to load the workload you just paired.



NOTE:
When using the default pairing profile in the pairing process, the Label columns are blank as shown above.

   c. Additionally, you can view the workloads in the Illumination map. Select Illu-

mination from the left navigation menu.



That's it! Pair as many workloads as you like.

You will learn all about working with the Illumination map in one of the next lessons.

Labeling Workloads Lesson

In this lesson, you will learn how labels describe the function of your workloads by creating and applying a natural language, metadata system.

Lesson Prerequisites

This lesson requires you to have the following data, access, and systems.

- **Development or Test Applications:** The hosts need to have a running application that is generating traffic data. A distributed application is recommended.
- **Managed workloads:** Completion of the pairing lesson where you installed the VENs on workloads by pairing them with the PCE.

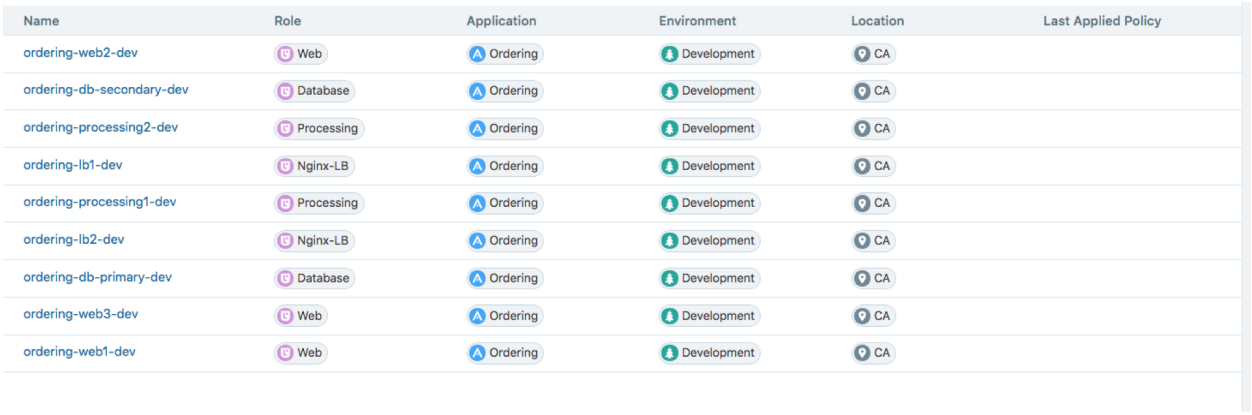
Instructions

Overview of Labels

The Illumio security policy for securing workloads differs from traditional network security policies. Traditional security policies use network constructs, such as VLANs, zones, and IP addresses to tie security to the underlying network infrastructure.

In contrast, the Illumio security policy uses a multidimensional label system to sort and describe the function of workloads. In a general sense, labels abstract the IP addresses, ports, and processes of workloads and infrastructure into a set of easily understood “plain language” labels. In the Illumio Core, labeling is a method of attaching metadata to workloads.

By describing workload functionally through labeling, policy statements are clear and unambiguous. Labeling workloads enables application-centric visibility, and a simplified, understandable, and adaptable model for creating policy. With labels, the application environment can be organized and visualized with more context, showing a view of applications and their components.



Name	Role	Application	Environment	Location	Last Applied Policy
ordering-web2-dev	Web	Ordering	Development	CA	
ordering-db-secondary-dev	Database	Ordering	Development	CA	
ordering-processing2-dev	Processing	Ordering	Development	CA	
ordering-lb1-dev	Nginx-LB	Ordering	Development	CA	
ordering-processing1-dev	Processing	Ordering	Development	CA	
ordering-lb2-dev	Nginx-LB	Ordering	Development	CA	
ordering-db-primary-dev	Database	Ordering	Development	CA	
ordering-web3-dev	Web	Ordering	Development	CA	
ordering-web1-dev	Web	Ordering	Development	CA	

- **Role:** The function of a workload; for example, for a simple two-tier application consisting of a web server and a database server: Web and Database.
- **Application:** The application that a workload supports; for example, a multi-tier, distributed application that you want to manage; for example, Application1234.
- **Environment:** A workload's stage in the product development lifecycle; for example, QA, staging, or production.
- **Location:** A workload's physical location; for example, Germany or Asia, Rack #3, or HQ.

Together, labeling workloads and creating the corresponding rulesets and rules define the security policies for the workloads in the organization. The PCE converts these label-based security policies into the appropriate rules for the OS-level firewalls of the workloads and calculates which of the workloads require the rules so that policy is only delivered where it is needed.

Develop a Labeling Schema

Getting your label design right is one of the most important things you can do for your Illumio deployment. In the Illumio Core, labels are important for the visual

representation of your environment and when writing and managing security policy.

Icon	Description
	The Role label is often the hardest label type to define, but it is the least crucial if the segmentation type used is micro-segmentation, also known as ringfencing.
	The Application label is an important label and usually refers to the business service.
	The Environment label is also important to ensure environmental separation.
	The Location label importance depends on your business application structure.

When creating and applying labels to workloads, we recommend you follow these guidelines.

Common roles

Think of workloads in your environments that play the same common role regardless of the application location or environment they belong to; for example, web, application, database, or load balancer. Create Role labels for all these common workload types.

Important applications

List your most important applications and create Application labels for each. Organize workloads that are part of the application into logical tiers; for example, web, application, and database tier for an ERP or HRM application. Apply common Role labels to each workload in the tier; for example, “web” for web-tier workloads.

Data center core services

Make a list of infrastructure services, such as domain controllers, DHCP, authentication, Microsoft Active Directory, FTP, and monitoring services such as Zabbix or SIEM. Create labels for each core service.

Key environments

Create labels for common environments first; for example, production, development, staging, and testing. Create labels for other environments second; for example, PCI, data replication, and disaster recovery.

Location or virtual designators

Create Location labels that are simple to understand by mimicking your infrastructure location names; for example, physical location (Rack-5-slot2 and New-York) or virtual location (AWS, Azure, and Rackspace).

Use a combination of Location and Environment labels to avoid confusion; for example, instead of Location labels “Domain-A-East” and “Domain-A-West,” use the Environment label “Domain-A” and the Location labels “East” and “West.”

Identify Your Workloads

Answering these basic questions will help you label your workloads.

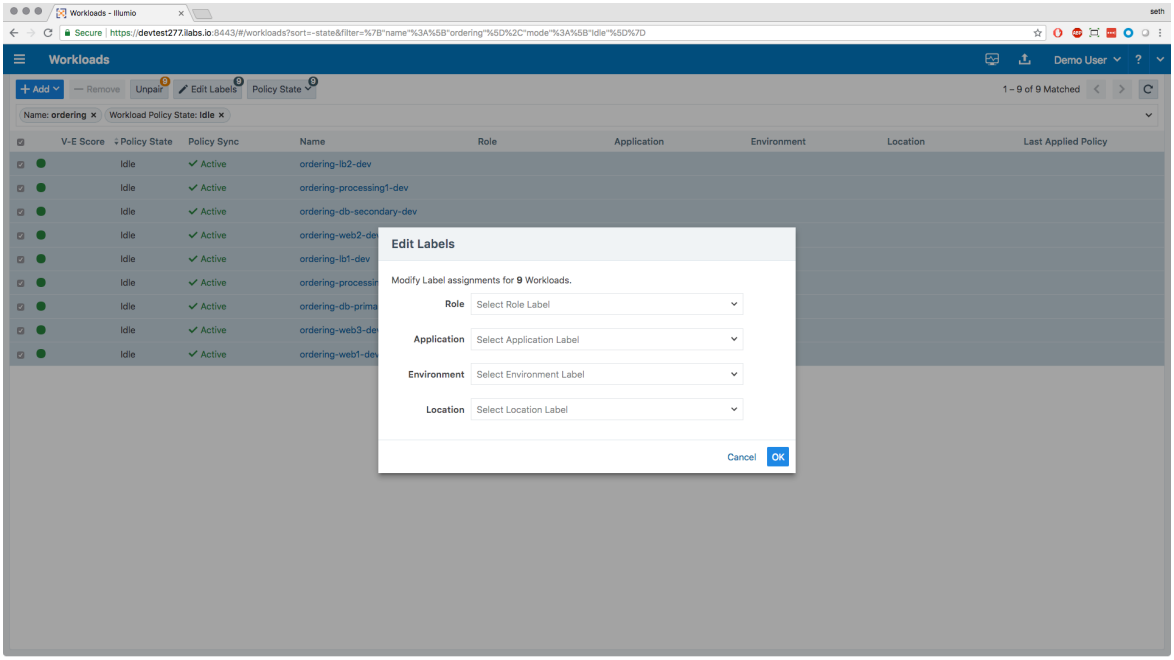
Question		Answer
Location	Where is this workload?	It is at HQ.
Environment	Is it a production, development, or other workload?	It is in the Dev environment.
Application	What is the business this workload provides to the company?	It stores orders for the Ordering system.
Role	What specific part of the business does this workload do? What is its tier? Does its name contain its role?	It stores orders. It is a DB.

Create and Apply Labels to Workloads

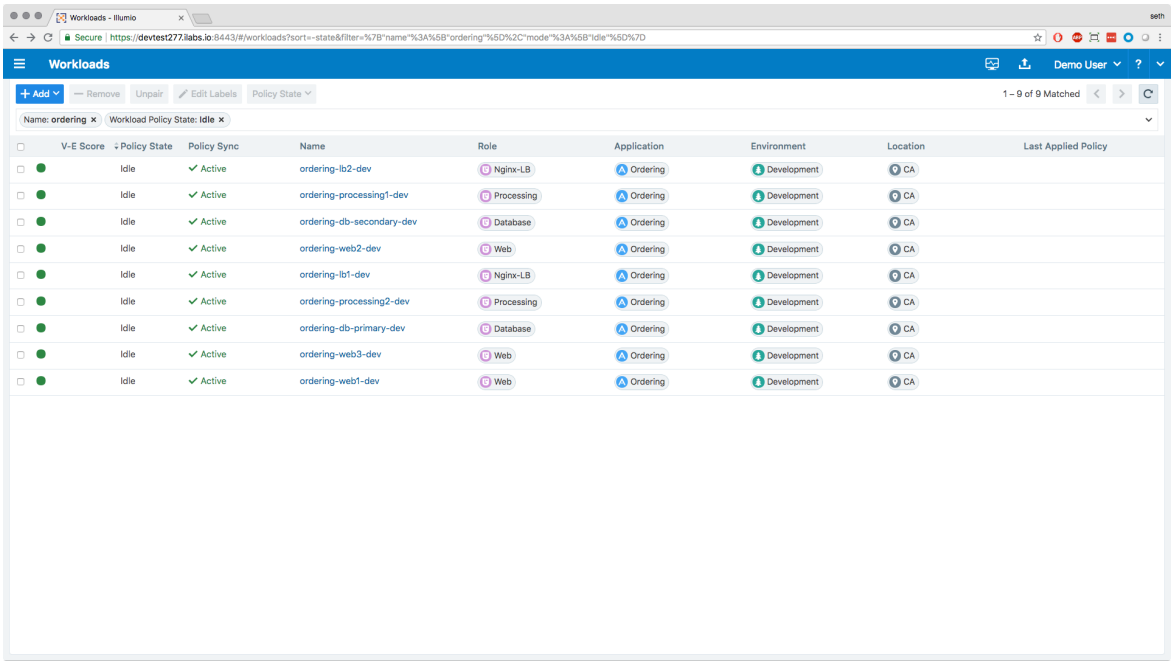
1. From the PCE web console menu, choose **Workloads**.
2. Use the checkboxes to select the workloads to label or re-label them.
3. Click **Edit Labels** on the page tool bar.

4. Pick a label type to assign.

5. Type to select an existing label or to create a new one.



6. Click **OK**. Labels will appear in the workload table.



7. Repeat for all workloads.

TIP:
Multiselect workloads to change the labels for multiple workloads at once.

Once your workloads are labeled, you can write rules using the labels you have applied to them. You will learn all about applying security policy to workloads in one of the next lessons.

Illumination Lesson

In this lesson, you will learn how to visualize your application environment and how inbound and outbound network traffic impacts your workloads.

Lesson Prerequisites

This lesson requires you to have the following data, access, and systems.

- **5 to 20 workloads:** That are running and that you've paired with the PCE.
- **Labeled workloads:** Applied a basic labeling scheme to the workloads (though you can refine it using Illumination).

TIP:
You won't get the full benefit of mapping traffic unless your environment is generating network traffic between the workloads you pair.

- **Development or test applications:** The workloads need to have running applications that are generating traffic data. A distributed application is recommended.

Instructions

About Illumination

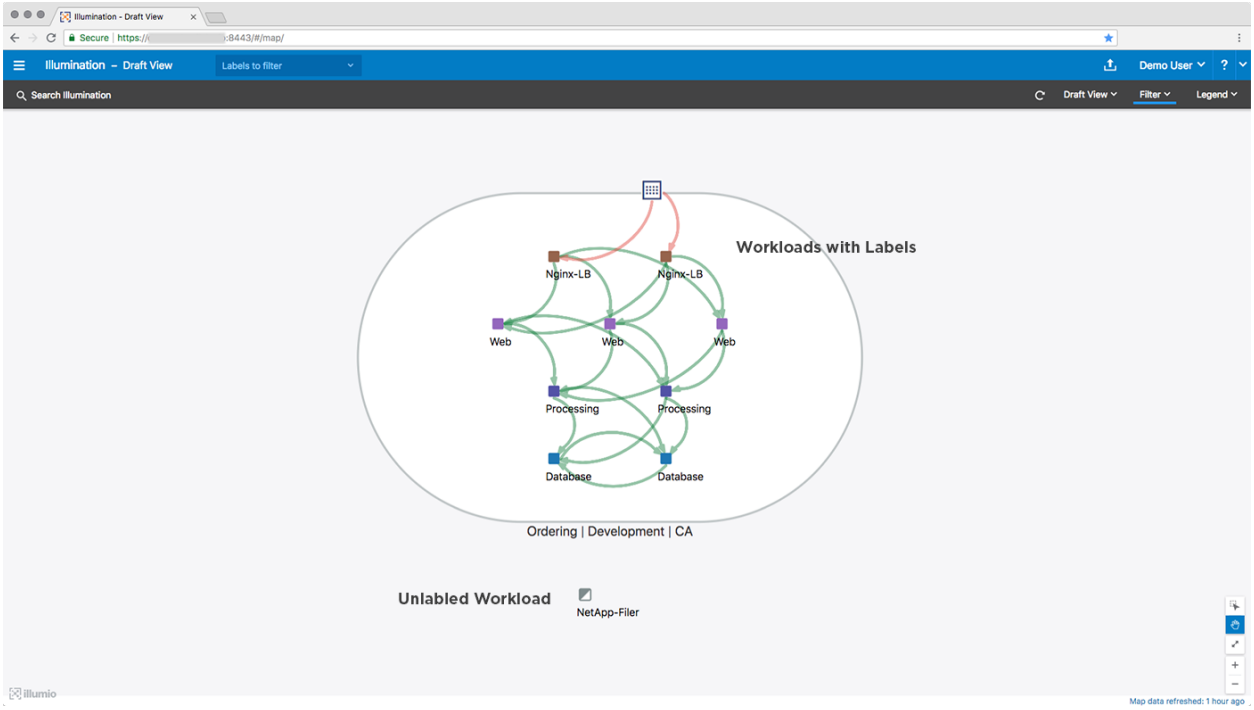
Visibility into your application environment is an important step toward implementing micro-segmentation. It's important to understand what it is that you want a segment. And, understanding the applications inside your environment—not just the applications, but also the workloads that comprise them—is critical.

The Illumio web console includes a visualization tool—the Illumination map—that you can use to reveal the granular details of application traffic flows between specific workloads, allowing you to discover interactions across applications and between the tiers within your applications.

Group Discovery in Illumination

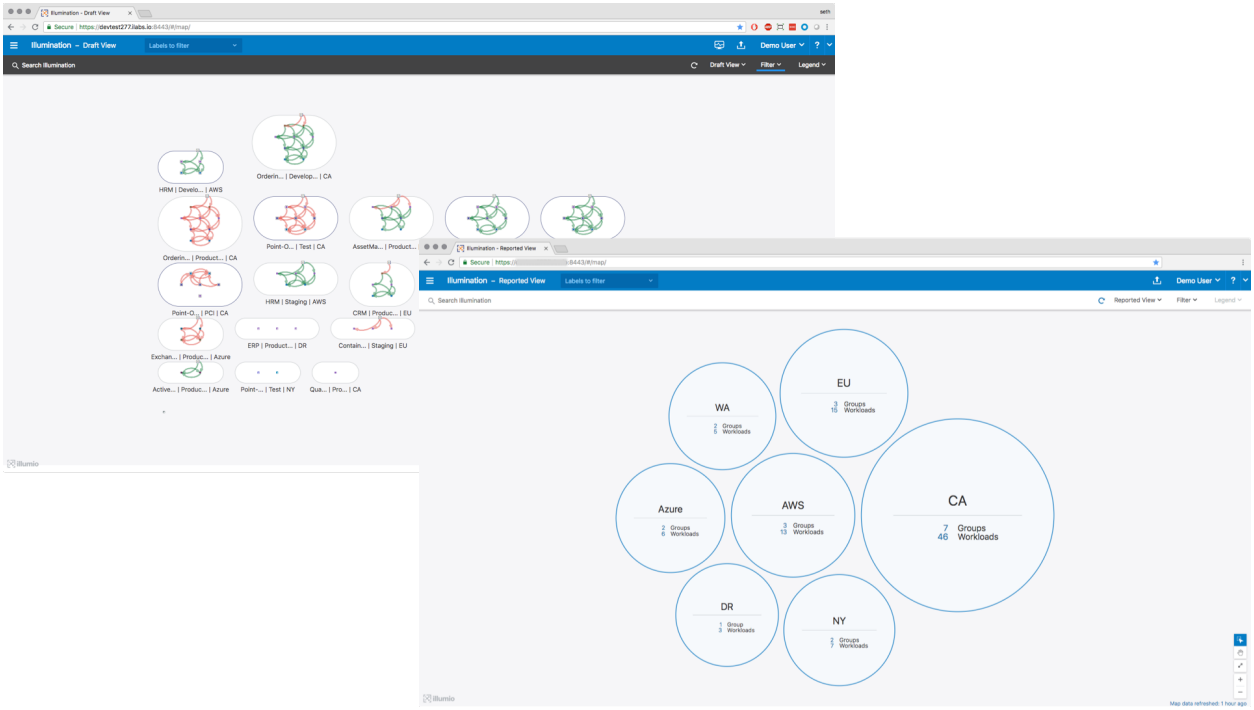
After you pair workloads, they appear in the Illumination map. It displays the inbound and outbound network traffic for your workloads. When you have less than 50 workloads paired with the PCE, you see them all in the Illumination map.

Based on how you label your workloads, the Illumination map forms logical groups.



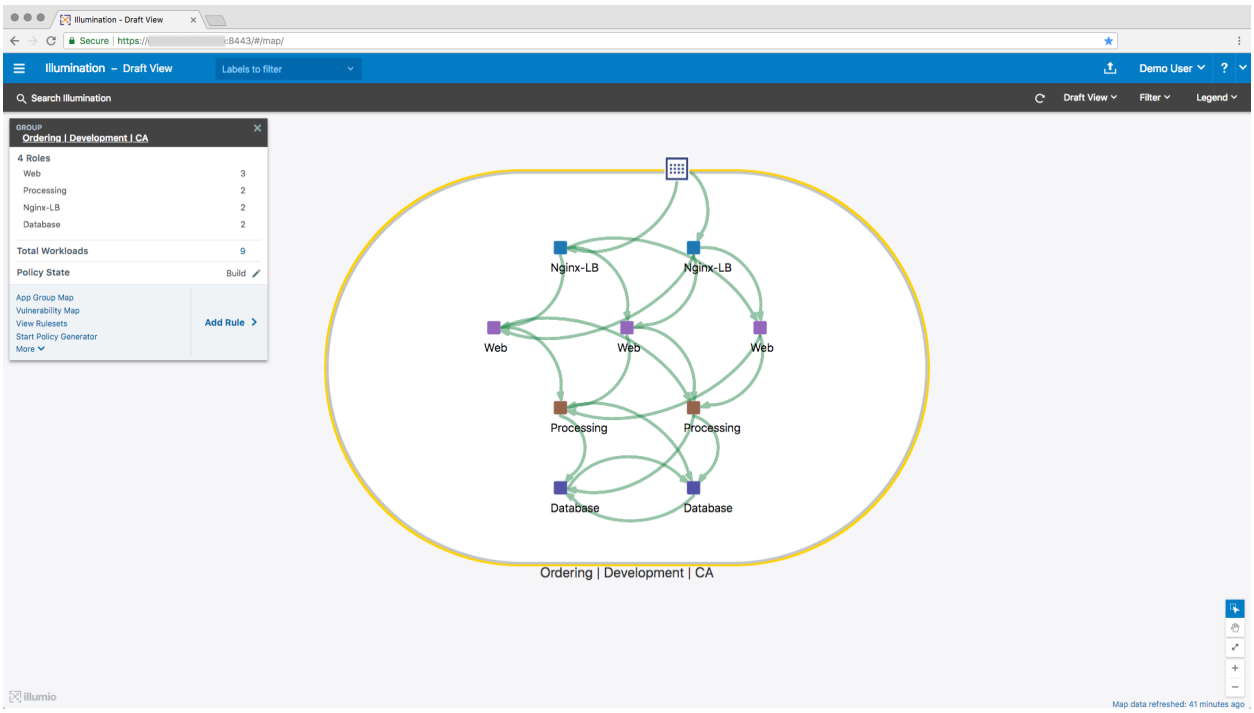
Workloads with the same Application, Environment, and Location labels appear in the same group. Illumination organizes your groups by their Application label. Changing any of a workload's labels moves the workload in the Illumination map and displays inter-group traffic flows.

Auto-scaling Illumination Map



NOTE:
If you have paired more than 50 workloads, the Illumination map switches to displaying your workloads grouped by their Location labels. See the *Visualization Guide* for more information.

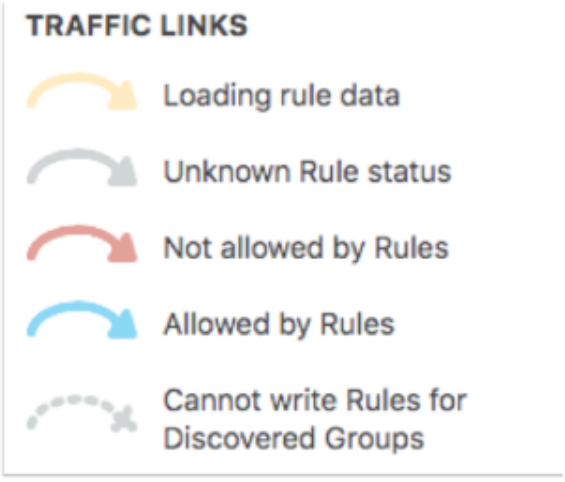
To see details about a group, click the group to zoom in. A command panel appears that displays valuable information about the group.



Traffic Flows

The Illumination map uses a color-coded system to display whether traffic will be allowed or blocked between your workloads.

Normal view mode



Color deficiency mode

The traffic link colors are impacted by two key features in Illumio Core: Workload policy states and the Draft and Reported views of the Illumination map.

Workload Policy States

When you pair a workload with the PCE, you assign a policy state to the workload. The policy state determines how Illumio rules affect a workload's network communication.

NOTE:
The default pairing profile adds workloads with the Build policy state.

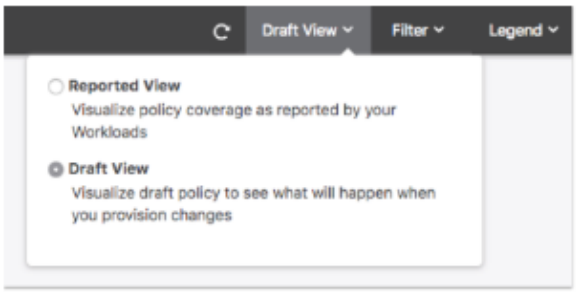
Icon	Name	Description
	Idle	The VEN does not take control of the workload's native OS firewall and no traffic is blocked in this state. When a workload is in the Idle policy state, it reports its traffic flows with green lines (allowed).
	Build	The VEN does not take control of the workload's native OS firewall and no traffic is blocked in this state. When a workload is in the Build policy state, it reports its traffic flows with green lines (allowed). The Idle and Build policy states are similar in the way they display traffic in the Illumination map. They differ in the way they collect traffic data from the VENs.
	Test	The VEN does not take control of the workload's native OS firewall and no traffic is blocked in this state. However, when you view your Illumination map using the Draft view, workloads in the Test policy state display red lines for traffic that would be blocked if the workload was in the Enforced policy state. IMPORTANT: Traffic is reported as blocked traffic unless you've written an Illumio rule allowing the connection.
	Enforced	The VEN takes control of the workload's native OS firewall and blocks traffic unless you've written an Illumio rule allowing the connection.
	Unmanaged	You have created the workload in the PCE by specifying its attributes, such as IP address, hostname, and OS. Unmanaged workloads aren't paired with the PCE and don't have the VEN installed on them. You can apply labels to unmanaged workloads so that managed workloads (with VENs installed) can communicate with unmanaged workloads.

Illumination Map Views

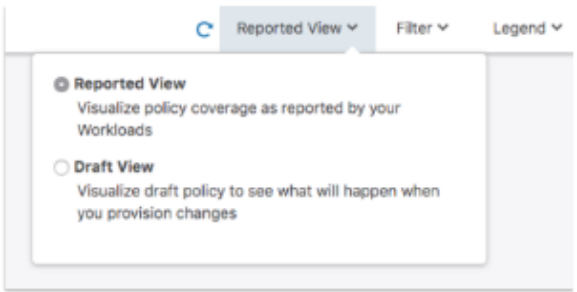
The Illumination map provides two views of the policy data. These views show you what is happening and what will happen after provisioning pending changes from the PCE to the VENs.

Reported	Provides an accurate representation of what is allowed or blocked by the VENs. Use this view to verify your security changes; e.g., you added an Illumio rule allowing traffic or you changed a workload state to Enforced.
Draft	Provides a "what-if" analysis conducted by the PCE. This view is a modeling tool that depicts whether traffic flows known to the PCE will be allowed or blocked, based on the configured policy.

TIP:
To switch between the two views, select the view from the top-right corner of the web console.



Draft View



Reported View

Policy Generator Lesson

In this lesson, you will learn about creating rules to ringfence an application by using the security policy automatically created by Policy Generator.

Lesson prerequisites

This lesson requires you to have the following data, access, and systems.

- **5 to 20 workloads:** That are running and that you've paired with the PCE.
- **Fully-labeled workloads:** The workloads have all four labels assigned to them.
- **Active connections on the workloads:** The hosts need to have running applications that are generating traffic data.

Instructions

About Policy Generator

The PCE web console provides several ways to create security policies for your applications. In this lesson, you will use Policy Generator to create your security policy.

Policy Generator simplifies the Illumio policy creation process by recommending the optimal security policy for your application groups. Policy Generator uses discovered traffic flows to build segmentation policies, thereby saving security teams critical time, accelerating the security workflow, and reducing the risk of human errors. Moreover, it's the simplest way to micro-segment your applications and does not require that you be a security expert or know the IP addresses of all your workloads.

In this lesson, you will secure and segment an application by creating an application ringfencing; ringfencing separates individual applications, preventing cross-application communications. All the workloads in the application group can communicate with each other across all services.

Ways to Access Policy Generator

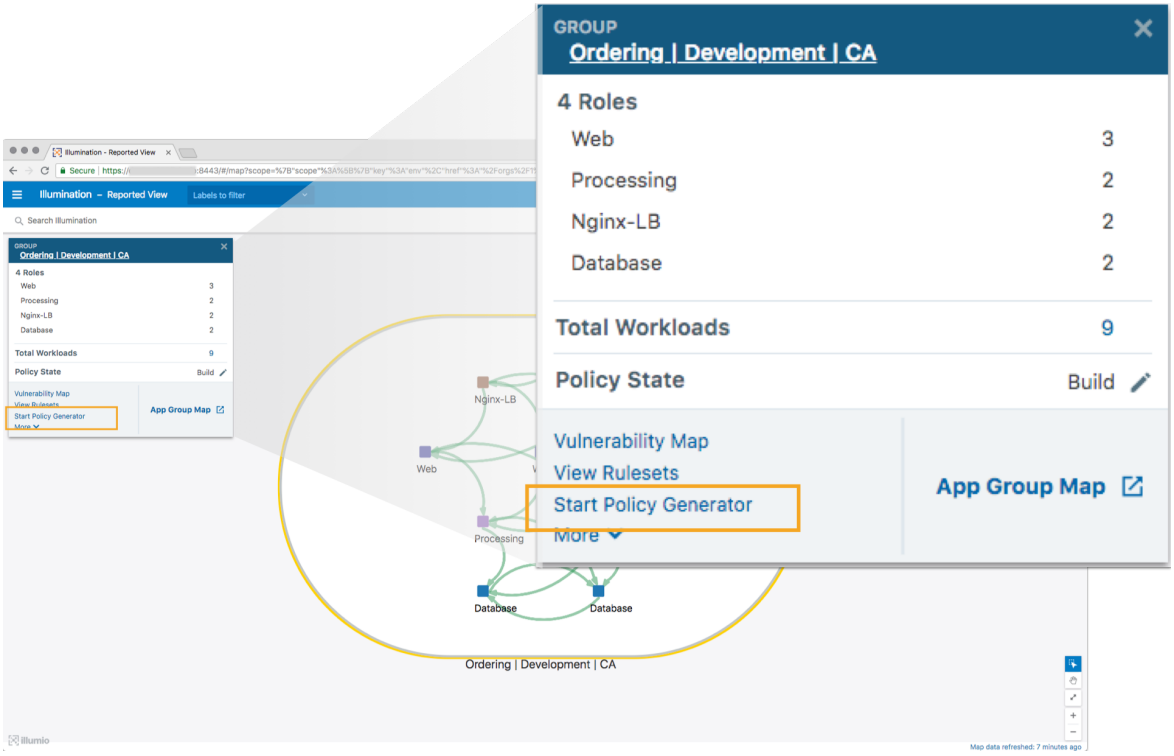
There are multiple ways to access Policy Generator. In this lesson, you access Policy Generator from Illumination.

1. From the Illumination map, select an App Group's oval border.

   IMPORTANT:
   Make sure the Illumination map is in Draft view before continuing.

2. In the command panel, click **Start Policy Generator**. The first page of Policy Gen-

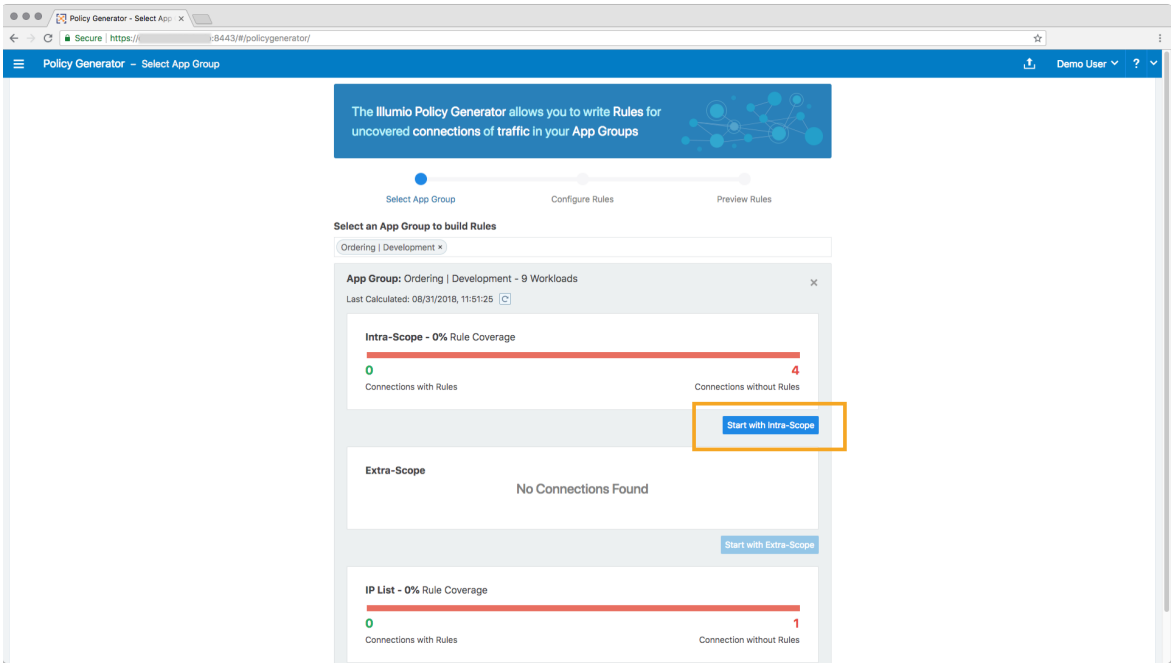
erator appears with the application group selected.



Create Intra-scope Rules

The first time you use Policy Generator for an application group, it creates a new draft ruleset with the title of the selected group. You review the proposed rules before you save them into a draft ruleset. For Windows, Policy Generator detects Windows processes and services and creates the rules accordingly.

1. Click **Start with Intra-Scope**.



   The Intra-Scope Rule Configuration page appears. By default, the option to create policy for application ringfencing (the *App Group Level* option) is selected.

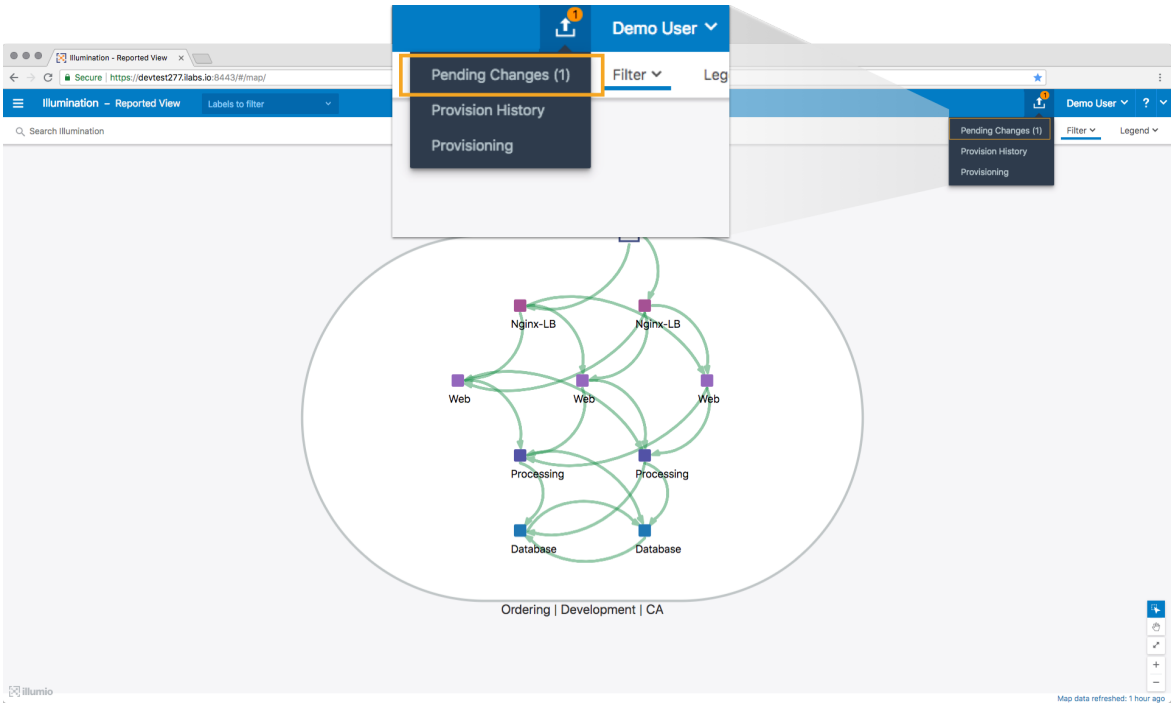
   The page displays all detected connections for the application group, including details about the labels, ports, and protocols, in the Review All Connections section. You cannot exclude any connections from the ruleset because a ringfence policy allows all workloads in the group to talk across all services.

2. Click **Next**. The preview page appears.
3. To accept the proposed rules, click **Save** and **OK**.

Provision Policies

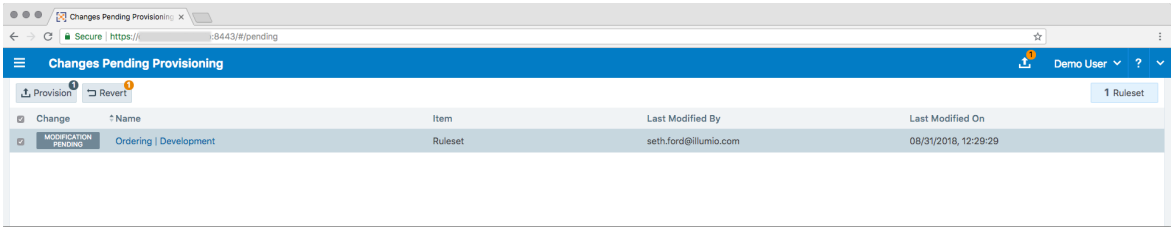
Now that the security policy exists, apply it to the affected workloads so that the VENs add the rules to their native OS firewalls. The process of applying a draft policy is called Provisioning.

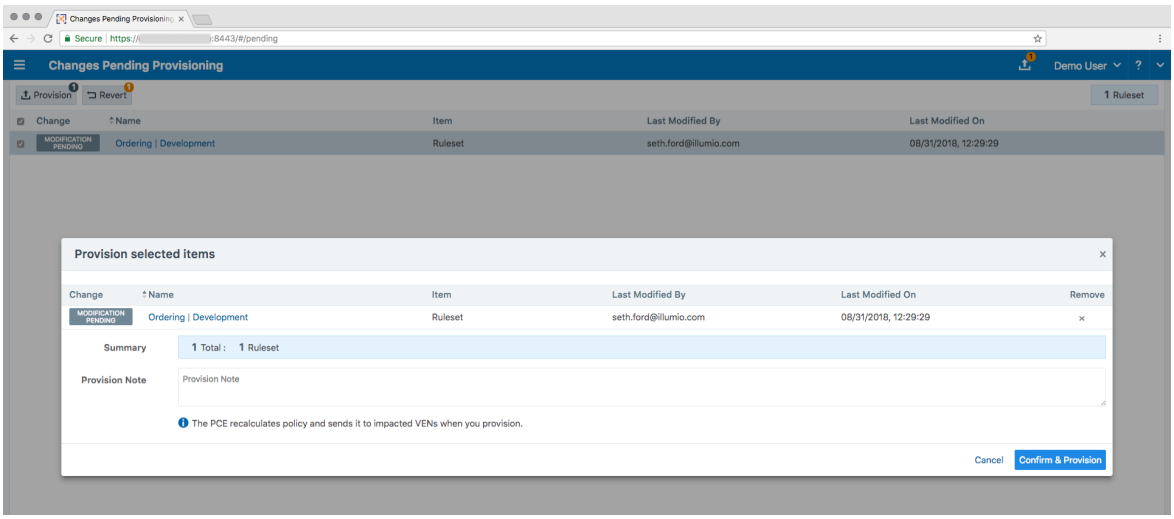
1. To apply the policy to the workloads, provision the new policy. Click the Provision icon on the web console top toolbar and select **Pending Changes**.



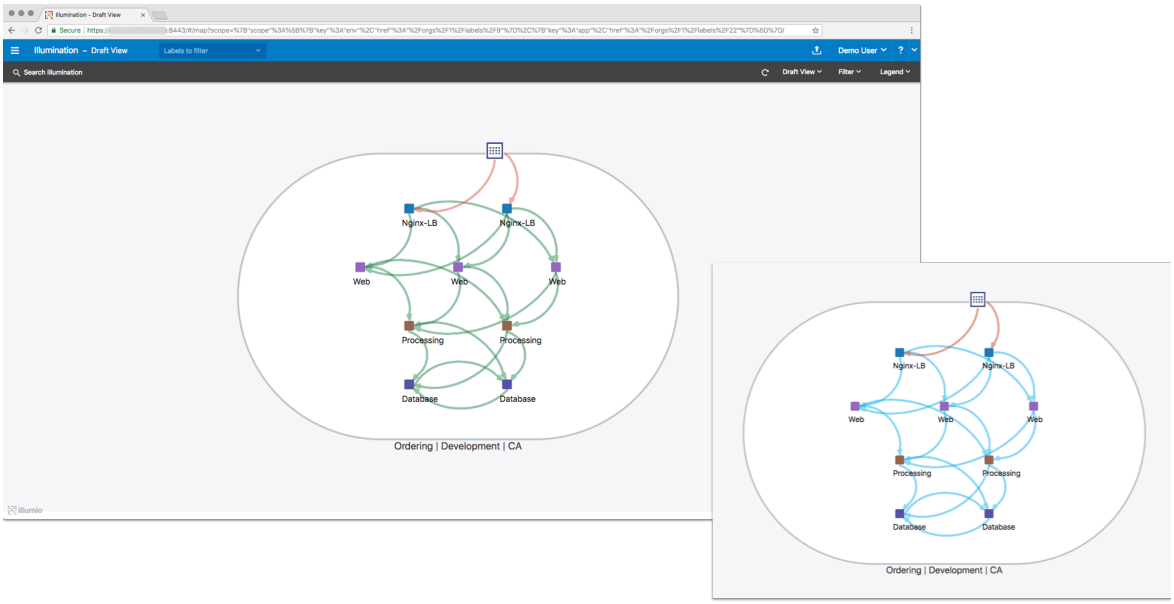
The list displays all policy items that have been added, modified, or removed. The top of the page shows a summary of changes based on item type.

2. Select all the new rulesets, rules, and services created for your application ringfence and click **Provision**.



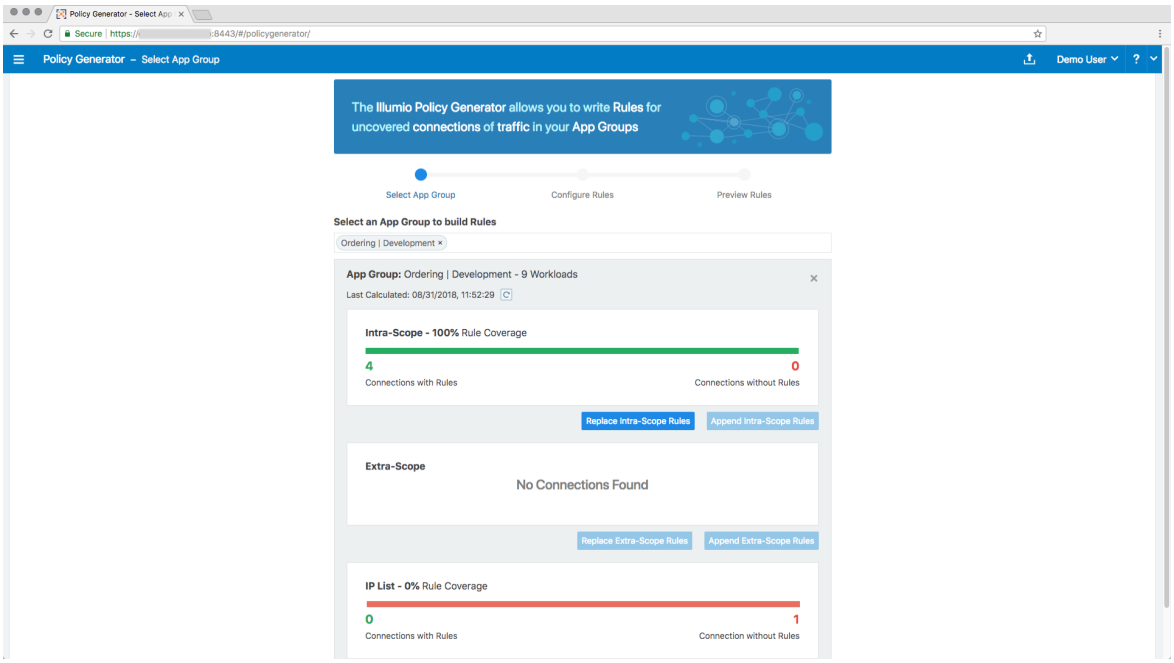


When a policy is provisioned, the policy is made Active. Viewing the Reported view in the Illumination map confirms that the traffic is now allowed.



Color deficiency mode

You can run Policy Generator as many times as you like to get the right policy model.



Congratulations! You have successfully completed this tutorial to apply an application ringfence to your first set of workloads.