TECHNICAL
DOCUMENTATION

Security Policy Guide 23.2

This guide describes the Illumio Core Security Policy including the policy objects. It provides guidance on designing a label schema and lists recommended approaches for Illumio's security policy design including creating rulesets and rules.

Table of Contents

Security Policy

Overview of Security Policy

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

About the Illumio Policy Model

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. By describing workload functionally, policy statements are unambiguous. Illumio users assign four-dimensional labels to their workloads to identify their roles, applications, environments, and locations. Additionally, users specify labels in the scopes for rulesets and in the providers and consumers components of rules, allowing their organization's workloads to communicate with each other.

Labeling workloads and creating the corresponding rulesets and rules define the security policies for workloads. The PCE converts these label-based security policies into the appropriate rules for the OS-level firewalls of the workloads.

The Illumio Policy Model

Illumio gives you the option to manage your security policies by using either adaptive or static policy. Choosing how to implement security policy is possible because of the Illumio policy model.

About the Illumio Policy Model

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. By describing workload functionally, policy statements are clear and unambiguous. Illumio users assign four-dimensional labels to their workloads to identify their roles, applications, environments, and locations. Additionally, users specify labels in the scopes for rulesets and in the providers and consumers components of rules, which allows the workloads in their organization to communicate with each other.

Together, labeling workloads and creating the corresponding rulesets and rules define the security policies for workloads. The PCE converts these label-based security policies into the appropriate rules for the OS-level firewalls of the workloads.

See the following related topics:

- Labels and Label Groups [14] for a description of each label type
- Workloads in the PCE [41] for information about how workloads use labels and for the steps to assign labels to workloads
- Ruleset Scope and Rules for information about using labels in ruleset scopes and rules

Security Policy Guidelines

The following guidelines are recommendations on how to create your security policy in Illumio Core. Creating a security policy is an iterative process, so following these recommendations will provide a broad initial policy, which can then be incrementally improved until a sufficiently robust policy has been established.

When creating your security policy

1. Refine your initial policy to strengthen it by narrowing overly broad access.
2. Use the Visibility Only enforcement to verify and enact your policy.

Enforcement States

After creating a ruleset, you can preview the effects in Illumination using the Draft View. This view shows you the changes that will be enacted by your policy when it is enforced.

- **Visibility Only**: After refining your initial policy, most of the traffic lines in Illumination should be green. No traffic will be blocked and you can check your policy's accuracy. Any new traffic will be displayed as a red line.
- **Selective Enforcement**: Enables you to protect applications or processes on workloads while other services and ports function as if the workloads are in the Visibility Only enforcement state. By using selective enforcement, you can gradually expand the enforcement of policy on your workloads. Using the selective enforcement state is useful for temporarily enforcing security for specific ports in case a vulnerability is detected and action must be taken quickly. Using the selective enforcement state enables security enforcement before you are able to create complete allowlists of what traffic is allowed to reach your workloads.
- **Full Enforcement**: It is useful to move workloads to the Full Enforcement state in stages. This action can be done by workload, by application, by environment, or by datacenter. Start with less critical applications or workloads, stabilize them, then move on to more sensitive systems. This approach minimizes issues to a smaller number of affected workloads.

Understanding Rulesets and Rules

NOTE

In previous releases, this feature was referred to as “Segmentation Rulesets.” In Illumio Core 21.5.0 and later releases, this feature is now referred to as “Rulesets.”

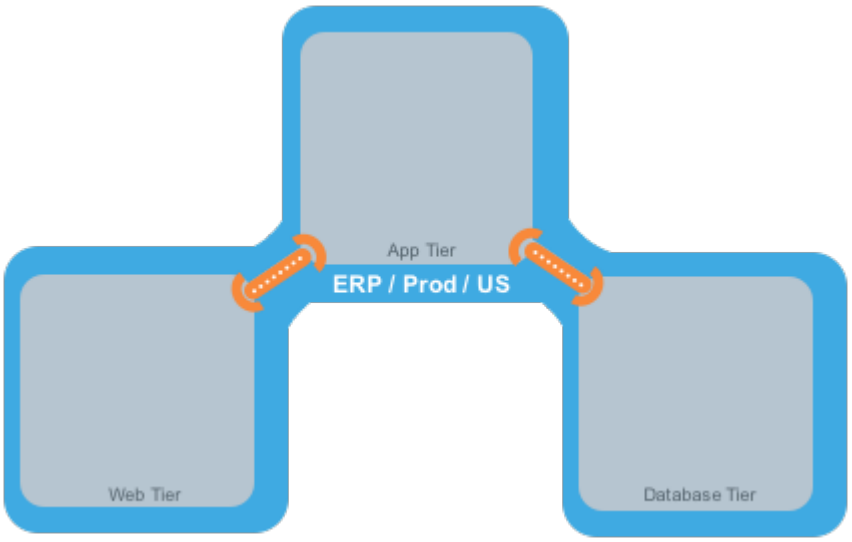
Rules are an integral component of the Illumio security policy. A set of rules is known as a “ruleset” and it specifies the allowed traffic in your network. Create the rules using labels that identify your workloads. See Labels [14] for more information.

Illumio's Illumio Core allowlist model for security policy uses rules to define the allowed communication for two or more workloads. For example, if you have two workloads that comprise a simple application — a web server and a database server — to allow these two workloads to communicate, you must write a rule that describes this relationship.

NOTE

The order in which the rules are written or any possible overlap between rules does not affect the allowlist model, since each rule permits some traffic between workloads.

For example, in the following diagram:



The relationships between the tiers (or workloads, as they are known in Illumio Core) in this example are:

- The Web workload can initiate communications with the App workload (Web → App).
- The App workload can initiate communications with the Database workload (App → Database).

In Illumio Core, the relationship in the diagram above is expressed as two separate rules:

- The Web workload can initiate communications with the App workload.
- The App workload can initiate communications with the Database workload.

To build your network security policy, create a ruleset for each of your workloads. Use labels to identify your workloads and use scopes to apply the rulesets to multiple workloads at once. For more information, see Labels [14] and Rulesets. [84]

NOTE

Illumio recommends creating no more than 500 rules per ruleset, or the PCE web console will not be able to display all of the rules.

If you want to create a ruleset with more than 500 rules, Illumio recommends splitting the rules across multiple rulesets or using the Illumio Core REST API, where there is no limit on the number of rules you can create per ruleset.

Overview of Policy Objects

The PCE contains the following policy objects that help you write your security policy:

- Segmentation Templates [60]: Prepackaged, tested security policies that provide all the rules needed for common enterprise applications.
- Labels and Label Groups [14]: Group similar labels together and use the label groups in rule writing.
- Services [20] Allow you to define or discover existing services on your workloads. When a workload is paired with the PCE (has a VEN installed), it is scanned for any running processes, which are then displayed in the Services list.
- Virtual Services [26]: Allow you to label processes or services on workloads. Virtual services can either be used directly in rules or the labels applied to virtual services can be used to write rules.
- IP Lists [32]: Create IP lists (allowlists) so you can define IP addresses, IP ranges, and CIDR blocks that should be allowed access to your applications.
- Load Balancers and Virtual Servers [34]: Add F5 Load Balancer configurations to the PCE so you can write policy for workloads whose traffic is managed by load balancers.
- **Pairing Profiles**: Configurations that allows you to apply certain properties to workloads as they pair with the PCE, such as applying labels and setting workload enforcement.
- **User Groups**: You can import Active Directory User Groups to write user-based rules for Adaptive User Segmentation [38].

Types of Illumio Policy

This section explains the differences between adaptive and static policy in the Illumio Core.

Adaptive Policy

Without adaptive security, enterprises face an overwhelming number of firewall rules, manual changes required to policies, and the possibility of errors leading to outages or serious vulnerabilities and breaches. Adaptive security automatically accounts for moves, scale, and changes to the applications and infrastructure that are typical of modern datacenters.

Because Illumio bases workload security on a policy model, it enables adaptive security that continuously adjusts to changes in the environment and to changed workload relationships. When a change occurs, the PCE responds dynamically by re-computing the OS-level firewall rules for the impacted workloads. The PCE alerts the VENs of the new OS-level firewall rules. The VENs request the new rules and apply them immediately.

The Illumio Core dynamically adapts and updates security policy when events, such as the following ones, occur in the managed environment.

- Workloads are added to or removed from your environment.
- Workloads change their IP addresses.
- Managed workloads come online and go offline.
- The labels on workloads change.

The PCE does not require Illumio users or automated processes to provision these changes for the PCE to re-compute the OS-level firewall rules for the impacted workloads and transmit them to the VENs.

See the following related topics:

- Pairing in VEN Installation and Upgrade Guide for information about adding workloads to your environment
- IP Lists [32] for information about using them in security policies
- Provisioning [116] for information about provisioning, which is a manual process
- Staged Policy [11] for information about how provisioning differs from adaptive policy

Static Policy

For the large majority of your workloads, adaptive security is the best method for protecting them from the lateral spread of threats. By default, the Illumio Core implements adaptive security for your workloads in all roles, all applications, all environments, and all locations. See Adaptive Policy [7] to learn how Illumio provides adaptive security.

However, in certain scenarios, you might want to control when the VENs apply new or changed OS-level firewall rules to workloads. Using labels, you designate which workloads are impacted by static policy. See Apply Static Policy [11] for the steps to configure static policy using labels.

When you configure the Policy Update Mode for workloads to use static policy, you control when the Illumio VENs running on the workloads apply new OS-level firewall rules that they received from the PCE. The Illumio Core blocks the immediate application of new firewall rules that result from users provisioning policy changes in the PCE and from dynamic updates to firewall rules (adaptive policy) when your environment changes. For example, you add a new rule to a ruleset in the PCE and provision the change, or a change occurs in your environment, such as a workload changes its IP address. In both cases, the VENs for your impacted workloads receive the new OS-level firewall rules from the PCE but they do not apply them until you explicitly select the workloads and click **Apply Policy** in the PCE web console.

See Staged Policy [11] for information about how the Illumio Core uses static policy and stages OS-level firewall updates rather than apply them immediately.

You should view static policy as a Security Setting rather than a type of security policy because configuring workloads to use static policy is a mechanism to control when VENs apply new or updated OS-level firewall rules to affected workloads. You can use the static policy setting to establish an audit trail of which Illumio users apply new OS-level firewall rules to workloads and when they apply them.

Use Cases for Static Policy

By default, the PCE is set to apply security policy updates dynamically through adaptive policy. However, scenarios occur where you want to control when updates to the OS-level firewall rules are applied to workloads.

For example, you might want to control when these updates occur in the following scenarios:

- Corporate policy for business-critical applications requires oversight on when updates to the OS-level firewall rules are applied to workloads.

  For example, a financial institution requires that security updates to its transaction processing application must be explicitly controlled by its security team. The security team authorizes the date and time of the update and applies it in the Illumio PCE.
- The corporate IT team has established policies for applying security updates during disparate maintenance windows.

  The IT team utilizes distributed maintenance windows to lessen the up-time impact on applications; for example, half the application is upgraded during the first maintenance window and the second part during the second maintenance window to keep the application up and running and minimize risk.
- The central security team sets the security policy to static for certain environments and adaptive for others.

  For example, the security policy is adaptive for workloads running in the development environment (using the labels All Applications, Development Environment, and All Locations). However, workloads in the production environment (All Applications, Production Environment, and All Locations) require static policy.

See **Caveats** for guidance on choosing when to configure workloads with static policy.

Example: Static Policy Workflow

The security team for an internet retail application has strict requirements for updating their production environment. They require that all updates to the OS-level firewall rules for their Database tier running in production must be applied during maintenance windows. For their Illumio-managed workloads, they configure a static policy that has the following labels: Role: Database, Applications: All, Environment: Production, Locations: All.

A spike in customer demand occurs and their production environment automatically scales by adding servers to the Web tier. The Illumio PCE detects the web servers connecting to the Database tier workloads and re-computes their security policy to include rules for the web servers. The PCE re-compute the OS-level firewall rules for those workloads and sends them to the VENs running on the Database workloads. The VENs stage the updates locally but they do **not** apply them to OS-level firewalls.

A maintenance window opens and a security team member filters the Database workloads in the PCE to determine which ones have staged security policy. She selects these workloads and applies the staged changes.

The VENs request the latest OS-level firewall rules from the PCE to ensure that all changes are included. The PCE sends the latest OS-level firewall rules to the VENs and they apply them.

Static Policy Prerequisites, Limitations, and Caveats

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

Prerequisites

- You must be a member of the Global Organization Owner role or Global Administrator role to manage Security Settings and add static policy.
- The VENs on affected workloads must be running version 17.2 or later. Earlier versions of VENs cannot stage static policy. They will apply security policy updates immediately to workloads even though you configured them to use static policy.

Limitations

- You should provision label gGroups before adding them to static policy.
- In the following situations, a VEN will apply a security update immediately and will not stage it even though the workload on which the VEN is running is configured to use static policy:
  - When you pair a new workload, the VEN applies the policy it receives from the PCE immediately.
  - When a VEN detects tampering, it requests security updates from the PCE and applies them immediately.
  - A VEN is offline when a user applies changes to their workloads. The VEN comes back online, connects to the PCE, and receives updated OS-level firewall rules. The VEN applies the updated rules to the workload even though it is configured to use static policy.

    NOTE

    When a VEN goes offline and online, its OS-level firewall rules can become out-of-sync from the rules of other VENs that remained online.

    See Staged Policy [11] for an explanation of how the VENs stage policy.

    Because of the possibility for a VEN to apply security updates immediately, Illumio recommends that you do not provision security policy updates until the updates are final. Keep the updates in Draft state until you complete them.
- To maximize performance, the PCE transmits 5,000 updated OS-level firewalls to the VENs at a time until all updates are sent.

Caveats

Illumio recommends implementing static policy for special cases and advanced users should oversee the process.

The Illumio Core is designed to ensure that your workloads are protected by the latest versions of your security policy across your environment. Users provision policy changes or the PCE responds dynamically to changes in the environment. In both cases, the PCE re-computes new OS-level firewall rules incorporating the changes, and sends them to the VENs to be applied immediately.

However, when you configure workloads to use static policy, you override this design by controlling when the VENs apply the security update to the workloads. As a result, you can have

inconsistent security policy across your managed environment and cause communication disruptions between workloads.

Troubleshooting communication issues is difficult when the workloads within a scope are using different versions of a security policy.

Illumio recommends that you keep the number of workloads in your environment that utilize static policy as low as your business processes allow.

Apply Static Policy

By default, the Illumio Core implements adaptive security for your workloads in all roles, all applications, all environments, and all locations. See Adaptive Policy [7] to learn how Illumio provides adaptive security.

However, you might want to control when updates to OS-level firewall rules are applied to your workloads by adding static policy.

You designate which workloads use static policy by configuring the Policy Update Mode in the Security Settings. To configure the Policy Update Mode, you specify labels for the role, application, environment, and location. Any workloads within the scope of the specified labels will use static policy. You can add multiple scopes. Overlap between the scopes does not affect how workloads use static policy.

Label groups are not supported with static policy currently. To create scopes using multiple labels from the same type, add them as separate scopes. For example, you have four Role labels added to the PCE: Web, Database, API, and Mail. You want to add static policy for the Web and Database roles only so you add two scopes.

See Static Policy Prerequisites, Limitations, and Caveats [10] for information before you complete this task.

To add static policy:

1. From the PCE web console menu, choose **Settings** > **Security**.
2. Choose **Edit** > **Manage Policy Update**.
   The page refreshes with the settings to configure Static as the Policy Update Mode.
3. Click **Add**.
   A dialog box appears in which you set the scope of the static policy.
4. Select labels to select workloads for static policy.
5. Click **OK**.
   The static policy appears in the list.
6. Click **Provision** from the PCE web console toolbar.

Staged Policy

Understanding the distinction between using static policy to stage updates to OS-level firewall rules and provisioning security policy is important because the actions differ in crucial ways.

When you configure workloads to use static policy, the PCE sends the new OS-level firewall rules for Linux iptables or the Windows Filtering Platform (WFP) to the VENs and they stage

them locally. The VENs do not apply the new firewall rules immediately. You must select the workloads and explicitly click **Apply Policy** in the Workloads page to activate the staged OS-level firewall rules.

Configuring a set of workloads to use static policy does not eliminate the requirement to provision policy updates for those workloads. Through provisioning, you update the PCE's version of your security policy.

When you provision security policy changes, you trigger the PCE to apply these changes to the workloads. When the workloads are set to use static policy, the VENs on the workloads will stage the changes until you explicitly click **Apply Policy**. However, under certain circumstances, the VENs could apply the latest changes before you explicitly click **Apply Policy**. See Static Policy Prerequisites, Limitations, and Caveats [10] for information.

TIP

The orange badge on the Provision button (top toolbar) indicates the number of changes you need to provision.

In addition to rulesets and rules, you must provision changes to the Illumio policy objects, such as services, IP lists, and label groups. To make security policies easier to maintain and update, Illumio supports including re-usable policy objects in intra- and extra-scope rules. When you update a policy object, all the rules using the object are updated without you needing to change each rule where the object is included.

When you provision changes to rulesets and policy objects, the PCE saves your security policy as a new version. It recomputes the OS-level firewall rules for all the workloads affected by the change and instructs the VENs on those workloads to download the updated OS-level firewall rules.

See the following topics related to provisioning:

- Overview of Policy Objects [7] for a description of each type of policy item
- Provisioning [116] for the policy items that require provisioning
- Active vs Draft Versions to learn how provisioning establishes the active version of policy

Determine When Workloads Have Staged Policy

Workloads Page

The Workloads page displays each VEN's current state in the Policy Sync column. You can filter your workloads by this column to quickly determine which ones have staged OS-level firewall rules.

- **Active (Syncing):** The PCE is in the process of sending new policy to the VEN. Typically, this process takes only a few seconds.

> **NOTE**
> Workloads configured for adaptive policy and static policy can appear in the active (syncing) state while the PCE is sending new policy.

- **Staged:** The VEN has received the latest OS-level firewall rules but has not applied them.
- **Active:** The VEN has received, applied, and confirmed all policies sent from the PCE. (Active workloads have a green dot icon.)

For more information about the VEN Policy Sync states, see "VEN Policy Sync" in VEN Installation and Upgrade Guide.

Workload Details

The Workload details page provides important information about when and how your workloads received staged policy.

- The General section indicates whether the workload is configured to use static policy (Policy Update Mode field) and displays the date and time that the VEN staged the policy (Last Policy Staged field).
- The VEN section includes the Policy Sync state, which can be active (syncing), staged, active, error, warning, and suspended.

> **NOTE**
> These fields will not appear in the General or VEN sections when all your workloads are configured to use adaptive policy.

Apply Staged Policy

See Static Policy Prerequisites, Limitations, and Caveats [10] for information before you complete this task.

1. From the PCE web console menu, choose **Workloads**.
   The Workloads page appears.
2. (Optional) Use the Workload property filter in the following ways:
   - To find all your workloads that are configured to use static policy, choose **Policy Update Mode** > **Static Workloads**.
   - To find workloads that have staged policy that needs to be applied, choose **Policy Sync** > **Staged Workloads**.
3. To apply staged policy to specific workloads, select the workloads and choose **Apply Policy** > **Update Selected Workloads**.

> **NOTE**
> - Choosing **Update Selected Workloads** only applies staged policy. It does not provision pending policy changes for workloads that are configured to use adaptive policy even when you selected them.
> - If you applied policy to a subset of workloads with staged policy, the remaining workloads will continue to use the older policy.
> - The **Apply Policy** button is enabled only when you have workloads with staged policy waiting to be applied.

4. To apply policy to all workloads with staged policy, choose **Apply Policy** > **Update All Workloads**.

   NOTE

   If you filtered workloads by label and chose **Update All Workloads**, the PCE applies the staged updates to all the workloads matching that label scope and not just the workloads appearing in the PCE web console page.

   The Apply Policy dialog box appears displaying the number of workloads the staged policy will be applied to.
5. Click **OK**.
   The VEN applies the staged policy and displays the status of the update.

Security Policy Objects

This section describes the policy objects that you can use to write security policies.

Labels and Label Groups

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

Label Types

Label	Description
Role 	This label type allows you to describe the "role" (or function) of a workload. In a simple two-tier application consisting of a web server and a database server, there would be two roles: Web and Database. You can use the same role as many times as you want in other rulesets for different applications. **NOTE** The Role label cannot be used to define the scope.
Application 	This label type allows you to describe the application that a workload supports. When two servers in a two-tier application have a relationship with one another because one provides a service (like a database) to another, they likely constitute an application. If an organization has 100 applications, and each application has a separate web role and separate database role, the application role separates each one of the Web and Database role.
Environment 	This label type allows you to describe a workload based upon its stage in the product development lifecycle, such as QA, staging and production.
Location 	This label type allows you to describe a workload based upon its location. For example, Germany, US, Europe, Asia. Or, Rack #3, Rack #4, Rack #5; or datacenter AWS-east1, AWS-east2, and so on.
Flexible labels	You can define custom label types to reflect additional characteristics of the workloads in your installation. Create any label type that meets your organization's business needs. For example, you might want to label workloads according to their operating systems. The maximum number of labels is 20.

Additional Dimensions

A given workload cannot have more than one label per type. It's possible to allow a workload that used a service or services or across boundaries to communicate; for example, if a server is playing multiple roles, such as a database server used by two different applications, Illumio recommends that you create different role labels for that workload.

System Default "All" for Labels

When you log into the PCE for the first time as the organization owner, the following default labels are provided:

Label	Description
Role	Web, Database, API, Mail, Single Node App, Load Balancer
Environment	Production, Stage, Dev, Test
Applications	None
Location	None

The built-in (default) Environment, Application, and Location labels are defined as “All,” which enables you to create broad policies to cover All Applications, All Environments, and All Locations.

To avoid confusing policy writers, Illumio recommends not creating labels named “All Applications,” “All Environments,” or “All Locations” (exactly as written in quotes).

When you attempt to create labels of these types with the exact name as the system defaults, for example “All Applications,” an “HTTP 406 Not Acceptable” error will be displayed.

NOTE

You can modify or delete these default labels at any time.

Filtering Labels and Label Groups

You can use the property filter at the top of the Policy Objects > Labels or Label Groups pages to find the label or labels groups you are looking for.

You can filter by label type and exact label name on the Labels or Label Groups page. Similarly, you can filter by label name, description, and provision status on the Label Groups page.

To filter Labels, select Name or Type.

Select Name, Description, Provision Status, or Type to filter Label Groups.

Create a Label Type

Illumio Core provides the default label types Role, Application, Environment, and Location. You can define custom label types to reflect additional characteristics of the workloads in your installation. Create any label type that meets your organization's business needs. For example, you might label workloads according to their operating systems. The maximum number of labels is 20.

To create a new label type:

1. From the PCE web console menu, choose **Settings** > **Label Settings**.
2. On the Label Settings page, click **Add**.
3. Enter a unique Key. The PCE will use this key to identify the label internally. For example, OS.
4. Enter singular and plural versions of the Display Name (Operating System and Operating Systems).
5. Choose an icon, and enter a one- or two-character unique initial to be displayed with the icon (such as OS).
6. Choose foreground and background colors to be used when the label is displayed.

7. Click **Save**.

The new label type will appear in the web console UI wherever the default label types appear, such as in the Type dropdown selector when creating a new label.

Create a Label

1. From the PCE web console menu, choose **Policy Objects** > **Labels**.
2. On the Labels page, click **Add**.
3. Name: Enter a label name.
4. Type: Select one of the types such as Environment, Application, Role, Business Unit, or
5. Click **Save**.

You cannot create a label name that already exists, regardless of its alphabetic case. For example, you cannot create a new label named "WINDOWS" if "Windows" already exists.

Label Workloads

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

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

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

Edit Labels for Multiple Workloads

You can add, modify, or remove labels on multiple workloads. This approach saves time when you want to apply or remove the same label or set of labels to more than one workload at a time. In the Illumio Core 20.1.0 release and higher, if you want to delete a Label and it was used by a Virtual Server, you can determine whether it was in use. The "In use by" column on the Labels page includes Virtual Servers. The Labels' summary page also displays the "In Use By Virtual Servers Yes/No" field.

NOTE

Remember that label changes do not require provisioning, so mass label changes can potentially have a major impact on your rulesets, rules, and overall security policy.

1. From the PCE web console menu, choose **Workloads**.
2. Select the checkboxes next to the workloads you want to change labels.

3. Click **Edit Labels**.
4. Add or remove labels assigned to the selected workloads in the Edit Labels dialog box. The top of the dialog indicates how many workloads will be affected by the label change. Depending on the assigned labels, you have three general options:
   - When the selected workloads share the same label of a specific type (for example, Role), you can change the current label by clicking the little **X** on the label to remove it. Then, you can type or select a new label assignment.
   - When the selected workloads have different labels of the same type, faded text in the Label field indicates that the workloads contain multiple labels. You can click in the Label field and add a new label.
   - When you remove a label assignment, that label is removed from all selected workloads.
5. When you are finished, click **OK**.

Label Groups

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

For example, you have workloads residing in data centers in Dallas, New York, and Washington and you want to apply a rule to all those workloads. Instead of using the labels for Dallas, New York, and Washington in three separate rules, you can define a Location label group named US, add those three location labels to the label group, and use the US label group.

You can customize the columns to display labels as follows:

- Container Settings
- Deny Rules
- IP Forwarding
- Label Groups
- Last Modified By
- Last Modified On
- Loopback Interfaces
- Name
- Provision Status
- RBAC
- Reject Connections
- Rulesets
- Statis Policy
- Type
- Type (Role, Application, Environment, Location, or a custom-defined Flexible Label type)

Policy Calculation Using Label Groups

Label groups can be nested, so it is important to understand how label groups can affect policy.

NOTE

You cannot assign a label group to a workload - only individual labels can be applied to workloads. Label groups can only be used in rulesets.

Create a Label Group

Create label groups when you want to combine several labels that share common characteristics into a single label category. You can use the label group in a rule after the labels are added to a Label Group.

1. From the PCE web console menu, choose **Policy Objects** > **Label Groups**.
2. On the Label Groups page, click **Add**.
3. In the Add Label Group page, choose the label type and enter a name for the label. You cannot create a label group name that already exists, regardless of its alphabetic case. For example, you cannot create a new label group named "WINDOWS" if the label group name "Windows" already exists.
4. Click **Save**.
5. In the Members tab, enter a label name to find labels to add to the group, and then click **Add**. You can add as many labels (or label groups) of the same type to the group as desired.

You cannot create a label group name that already exists, regardless of its alphabetic case. For example, you cannot create a new label group named "WINDOWS" if the label group name "Windows" already exists.

Use a Label Group in a Scope

When you use a label group in a scope, the label group is expanded into multiple scopes. Cross-communication is not allowed.

For example, to create a scope that applies to all environments other than production, first create a Non-Prod label group which consists of the labels for the Dev, QA, and Stage environments. The following ruleset (scope + rule):

Scope:

- App: HRM
- Env: Non-prod
- Loc: US

Rule:

- Providers: DB
- Services: MySQL
- Consumers: DB

This means “workloads in all Non-Prod environments (Dev, QA, and Stage) can communicate within their environments with the DB using MySQL” and would allow the following communication:

- HRM | Dev | US | DB ← HRM | Dev | US | DB

The following communication would not be allowed, since the Environment labels are different and cross-communication is not allowed:

- HRM | Dev | US | DB ← HRM | QA | US | DB

and
- HRM | Dev | US | DB ← HRM | Stage | US | DB

Use a Label Group in a Rule

When you use a label group in a rule, the label group is expanded into multiple rules. Cross-communication is allowed.

For example, the Non-Prod label group is used again here, but in the rule and not the scope, which allows cross-communication. The following ruleset (scope + rule):

Scope:

- App: HRM
- Env: All
- Loc: US

Rule:

- Providers: Non-prod DB
- Services: MySQL
- Consumers: Non-prod DB

This means “allow MySQL from Non-Prod DB to Non-Prod DB for the HRM application in All environments located in the US" and would allow the following communication:

- HRM | Dev | US | DB ← HRM | Dev | US | DB
- HRM | Dev | US | DB ← HRM | QA | US | DB
- HRM | Dev | US | DB ← HRM | Stage | US | DB
- HRM | QA | US | DB ← HRM | Dev | US | DB
- HRM | QA | US | DB ← HRM | Stage | US | DB

Services

When workloads are paired with the PCE, the VEN discovers all running processes and services on a workload and makes those services available for use when writing rules. You can see those discovered services when you view the Processes tab on the Workload's details page.

However, you can also create your own to services to specify the service type, as well as the ports and protocols the services use to communicate.

NOTE

Service names can be unrestricted, for example, `sc.exe qsidtypemyservice`. You can write rules with unrestricted service IDs (SIDs). When there is a restricted SID, you should write rules without the SID. Including the service with a restricted SID type causes the traffic to be dropped and might cause traffic between the Reported view and Draft view to be reported inaccurately.

Service Types

When you create a service, you can choose one of two general types:

- **All OS: Port-Based:**: This type of service can be used for writing rules for any workloads and is defined by specifying a port and protocol, a port range, or in some cases, only the protocol. For example: `80 TCP`, `1000-2000 TCP`, `500 UDP`. For GRE or IPIP, you only need to specify the protocol.
- **Windows: Process/Service-Based:** This type of service can be used for writing rules for Windows Workloads only, and is defined by specifying one of the following combinations or scenarios:
  - **Port and/or Protocol, Windows Process, and Windows Service**
    `443 TCP c:\windows\myprocess.exe myservice`
  - **Port and/or Protocol and Windows Process**
    `443 TCP c:\windows\myprocess.exe`
  - **Port and/or Protocol and Windows Service**
    `443 TCP myservice`
  - **Windows Port and/or Protocol**
    `514 UDP`
  - **Windows Process**
    `c:\windows\myprocess.exe`
  - **Windows Service**
    `myservice`

Windows Process-based Rules

Rules to Allow System Created Processes

You can create rules to allow all system-initiated processes in Windows. This approach allows all traffic related to drivers and other operating system modules. You can create a service of type Windows—process or service-based—with word "system" (case-insensitive) in the Port/Protocol text input field. Once you create this service, you can use it in rules.

To create a service that allows all system-initiated processes:

1. From the PCE web console menu, choose **Policy Objects** > **Services**.
2. Click **Add**.
3. Enter a name and description for the service you are adding.
4. ATTRIBUTES:

   Operating System

   To add a service definition, from the Operating System drop-down, select either **All Operating Systems:Port Based** , **Windows Inbound: Process/Service-Based**, or **Windows Outbound: Process/Service-Based**

   If you select **All Operating Systems: Port-Based**, you can only indicate a port, a protocol, or both, separating the port and protocol with a space. For example, port `512 TCP`.

   If you select **Windows Process/Service-Based**, from the Port and/or Protocol drop-down, specify a port/protocol, a process or service, or a port/protocol with a process or service, separating the port and protocol with a space. For example, port `512 TCP`, process `C:\windows\myprocess.exe`, and Windows service,`myprocess`.

   Service Definitions

   To remove a service definition, from the Operating System drop-down, select either **All Operating Systems:Port Based** or **Windows Process/Service-Based**:

Click the check box next to the Port and/or Protocol. You may select a single or multiple entries.

Click **Remove**.

Service Using Windows Environmental Variables

The Windows environmental variable can be used to specify the full path. This can be done by creating a Service of type Windows: Process or Service based with the environment variables in the Port Protocol text input field

NOTE

Currently, only the Windows System variable is supported for use in the process path. For example `%systemroot%\myprocess.exe`

Rules can be created to allow all system-initiated processes in Windows. This will allow all traffic related to drivers and other operating system modules. This can be done by placing the word **system** (case-insensitive) in the text input field.

To create a service that uses Windows environmental variables:

1. From the PCE web console menu, choose **Policy Objects** > **Services**.
2. Click **Add**.
3. In the Name field, enter `system` (case-insensitive).
4. From the Operating System drop-down list, select **Windows: Process/Service-based**.
5. In Ports & Protocols, specify the port/protocol, separating the port and protocol with a space. For example:

   `%systemroot%\myprocess.exe`
6. Click **Save**.

IGMP Services

You can add Internet Group Management Protocol (IGMP) as a service for use in rules to write granular inbound or outbound policy for IGMP, which is typically used for multicast. No range is required for IGMP.

You can export IGMP traffic in JSON, CEF, or LEEF format.

You can also create and update services using the IGMP protocol using the Illumio Core REST API.

See "Services" in REST API Developer Guide for information about using the REST API to create services.

Caveats

- When IGMP service is used in a rule, all IGMP types are allowed; however, granular control and specific multicast addresses are not supported.
- IGMP is not supported in the Illumination map.

ICMP Services

ICMP can be added as a service and used in rules to write granular inbound or outbound policy for ICMP. ICMP is usually used for traceroute and path MTU discovery.

You can export ICMP traffic in JSON, CEF, or LEEF format.

NOTE

When these services are blocked, they do not appear in the Blocked Traffic list and the connection is dropped silently.

ICMP types/codes (such as 0 ICMP or 3/2 ICMP) are supported. The ICMP range is from 0 to 255.

The following table describes the correct format for each type of supported ICMP rule:

Example	Format	Meaning in Rule
ICMP (on a new line)	Protocol name only	Allow all ICMP traffic
3 ICMP	Type = 3 Protocol name = ICMP	All ICMP traffic of type 3 (Destination Unreachable) is allowed regardless of the code used in the rule.
3/6 ICMP	Type = 3 Code = 6 Protocol name = ICMP	Only type 3 and code 6 ICMP traffic is allowed.
3 ICMP, 6 ICMP	Type 3 of ICMP, Type 6 of ICMP	Only type 3 and type 6 ICMP traffic is allowed regardless of the code used in the rule.

TIP

Use this format to add as many types as you need.

ICMP traffic is displayed in Explorer, similar to TCP/UDP traffic. From the 19.1.0 release on, you can see ICMP traffic flows in Illumination and the App Groups Map. You can choose to conceal them by using the filter in Illumination.

You can also create and update services that use the ICMP protocol using the Illumio Core REST API. See Services in REST API Developer Guide for information about using the REST API to create services.

Caveats

- ICMP is not supported for virtual services.
- When an ICMP service is used in a rule, all ICMP types are allowed; however, granular control and specific multicast addresses are not supported.
- When you enable IPv6 on Windows VENs, IPv6 system rules are not propagated to those VENs. You need to write security rules to ensure robust IPv6 functionality. The ICMPv6 types that are required in those rules are as follows:

ICMPv6 Message	ICMPv6 Type
Router Solicitation Message	133
Router Advertisement Message	134
Neighbor Solicitation Message	135
Neighbor Advertisement Message	136

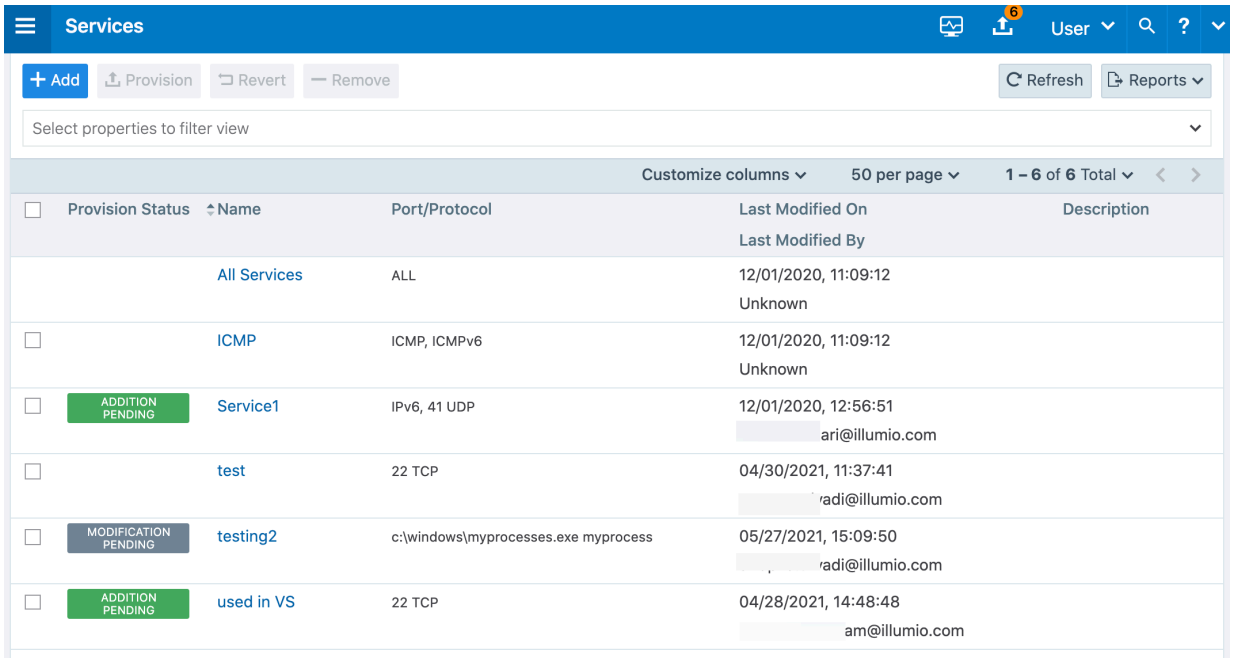
View or Edit a Service

To view or edit an existing service:

1. From the PCE web console menu, choose **Policy Objects** > **Services**.
2. Click the name of the desired service. You can filter the list by various attributes. See Filter the Services List [24] for details.
3. On the details page for the service, you can view information about the service, including its general data, attributes , and, if appropriate, the external data for the service and ransomware protection details.
4. Click **Edit** to change selected portions of the service definition. Some portions might not be editable.
   - To remove a service definition, from the Operating System drop-down, select either **All Operating Systems: Port-Based** or **Windows Process/Service-Based**.
   - To remove a specific service definition, click the check box next to the Port and/or Protocol. You may select a single or multiple entries.
5. Click **Remove**.

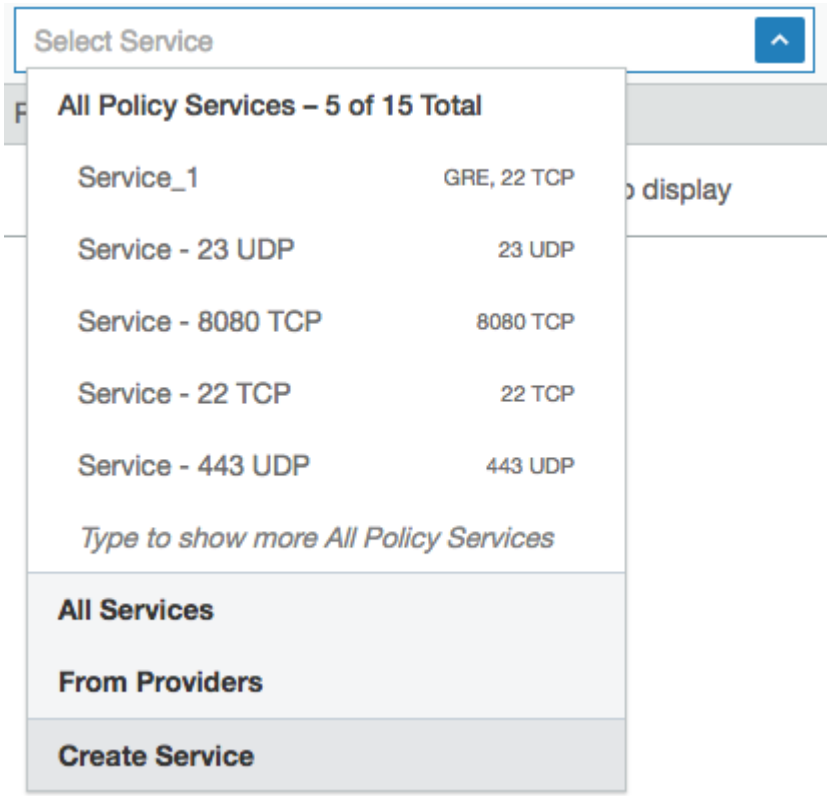
Filter the Services List

The property filter at the top allows you to filter the Services list by entering a service name, description, port, protocol, and provision status (draft or active).



Services in a Rule

When you create a rule, you can select a service to indicate the allowed communication between workloads and other entities.



Create a Service

When you create a rule, you can select a service to indicate the allowed communication between workloads and other entities.

When you create a service, that service becomes available to use in a rule.

For a list of the types of services you can create, see Service Types [20].

To create a service from the Services page:

1. From the PCE web console menu, choose **Policy Objects** > **Services**.
2. On the Services page, click **Add**.
3. Enter the service a name and description (optional).
4. Under Attributes, choose whether you want to create a port-based or Windows service-based service.
5. In the Port and/or Protocol section, click **Add** and enter the ports, using a space to separate them from the protocol. To enter a range, separate the port numbers by a hyphen. You can also copy and paste lists of services from another source here.
6. When the service uses any UDP ports, enter them as well.
7. Click **Save**.

Virtual Services

Virtual services (previously known as bound services) allow you to label processes or services on workloads. Virtual services can either be used directly in rules or the labels applied to virtual services can be used to write rules.

Overview of Virtual Services

A virtual service can be used in the following scenarios:

- **Apply rules to a single service:** Represents a service or process on a workload using a name or label. This approach allows you to write policy to allow other entities to communicate only with that service. The policy does not need to change when the service is moved to a different workload or a new set of workloads. Only the workload bindings on the virtual service need to be changed. The PCE dynamically calculates the required rules on the updated workloads to allow this service.
- **Apply rules to multiple services (on same workload):** Represents each service or process running on a workload with a different set of labels. You can write rules to allow other entities to communicate only with that service. The policy does not need to change when this service is moved to a different workload or a new set of workloads. Only the workload bindings on the virtual service need to be changed. The PCE dynamically calculates the required rules on the updated workloads to allow the service.

From the 18.3.1 release on, Illumination, Policy Generator, and Explorer support virtual services. You have to assign labels to a virtual service in order to write label-based rules. A virtual service does not have an enforcement, so you need to refer to the enforcement of its bound workloads.

Virtual services are provisionable objects, which means they must be created and provisioned before they can be applied to workloads. However, the bindings are not provisionable objects, so the bindings can be changed without having to provision the changes. Additionally, port overrides have been moved from the virtual service to the workload binding. See Provisioning [116] and Bind a Virtual Service to a Workload [31]for more information.

How Virtual Services Work

For example, if a single workload is running both an Apache Tomcat and Apache HTTP server, supporting an HRM and ERP application respectively, you can create a virtual service for each service and then label one service as belonging to an HRM application and one belonging to an ERP application. You can then write a set of label-based rules that apply only to the Apache Tomcat process serving the HRM application, effectively isolating it from the ERP application.

In the following example, two different virtual services are created: one for an HRM database and one for an ERP database. The following configurations would allow the web to communicate with the database for each application (HRM or ERP) in the specified environment (Prod or QA) in the specified location (US or EU):

Virtual Service - HRM

- **Name:** HRM-DB
- **Labels:** DB | HRM | Prod | US
- **Service:** MySQL
- **Bound to:** Workload - Database 1, Port Override: 3308
- **Scope:** HRM | Prod | US
- **Rule:** DB ← From Providers ← Web

Virtual Service - ERP

- **Name:** ERP-DB
- **Labels:** DB | ERP | QA | EU
- **Service:** MySQL
- **Bound to:** Workload - Database 1, Port Override: 3309
- **Scope:** ERP | QA | EU
- **Rule:** DB ← From Providers ← Web

Virtual Services in Rule Writing

When you create rules for virtual services using the Policy Generator or from Illumination, you need to add the “Uses Virtual Services only” option or “Uses Virtual Services and Workloads” option in the Providers or Consumers field of the generated rules. You can configure virtual services using port or port range.

NOTE

Custom iptables rules and SecureConnect are not supported with virtual services.

When you write a rule in a ruleset, you need to specify the following values:

- A service
- Providers of the service
- Consumers of the service

For example:

Web provides Apache Tomcat service to All Workloads

When you write rules using virtual services, you do not need to select a service in the rule, because the virtual service is both the service and the provider of the service.

For example:

Virtual Service Apache Tomcat is provided to All Workloads

When you want to treat the providers as a virtual service, select “Uses Virtual Services” or “Uses Virtual Services and Workloads” from the Providers drop-down list as the service.

When you want to write a rule applicable for all virtual services labeled “Database,” you would write it the same way and select “Uses Virtual Services” or “Uses Virtual Services and Workloads” as the providing service.

NOTE

Workloads labeled “Database" are not be impacted by the above rule. To include them, you need an additional rule listing the specific service applicable.

When you want to use a virtual service as a provider, select “Uses Virtual Services” or “Uses Virtual Services and Workloads” from the Provider drop-down list.

When you select a specific service, then the rule applies only to workloads that have the selected label.

For example, for the following virtual service rule:

- DB | MySQL | Web

The rule is only applied to workloads that use the DB label.

However, when the virtual service rule is the following type of rule:

- DB | Uses virtual services or uses virtual services and workloads | Web

The inbound side of rule is applied to all workloads bound to the virtual service using the DB label.

Advanced Configuration for Virtual Services

You have two advanced configuration options to consider when configuring a virtual service:

- **Apply To: Host Network or Internal Bridge Network:** This optional setting allows you to determine if the rules associated with the virtual service are applied over an internal bridged network or the host network. If you choose Internal Bridge Network, the rules associated with the virtual service are programmed into the FORWARD chain on Linux iptables (rules to internal bridge are ignored by Windows in this current implementation). Or, you can specify that a virtual service's rules are applied over the host network, programmed into the INPUT/OUTPUT chains in Linux iptables. Stateless rules are not supported when associated with FORWARD chain; instead, stateful rules are programmed.
- **Optional Configuration: IP Overrides:** Allows you to specify IP addresses or ranges (CIDR blocks) to be used for programming the rules associated with the virtual service instead of using the IP address of the bound workload. When IP overrides are specified on a virtual service and the virtual service is used in a rule, the IP addresses programmed on other hosts communicating with the virtual service are the IP addresses and subnets specified in the IP overrides rather than the IP addresses of the workloads bound to the virtual service.

A combination of stateless rules and forwarding rules on the same host, port, and consumer is not supported. For example, when a workload has a service running on a port with stateless rules, a forwarding rule to allow traffic to a container running on the same host using the same port does not work when the consumer is the same.

Host-Only Network

Example of a virtual service rule using host network (default):

Providers	Services	Consumers
Virtual Service X	From Providers	Workload B
Virtual Service X is bound to workload A, with service 80 TCP		Workload B has IP address 192.168.0.200
Workload A has IP address 192.168.0.100		

This rule programs the following security policy:

- An inbound rule on workload A for 80 TCP with source address 192.168.0.200
- An outbound rule on workload B for 80 TCP with destination address 192.168.0.100

When you add an IP override, the subnet 172.16.0.0/16 on the BPS, this rule programs the following security policy:

- An inbound rule on workload A for 80 TCP with source address 192.168.0.200
- An outbound rule on workload B for 80 TCP with destination subnet 172.16.0.0/16

The IP override dictates that for device that is allowed to communicate with this virtual service, use the addresses/subnets specified in the IP overrides.

Internal Bridge Network

When you remove the IP override and change to Internal Bridge Network, this rules programs the following security policy:

- An inbound rule on workload A for 80 TCP with source address 192.168.0.200 on the FORWARD chain of the firewall

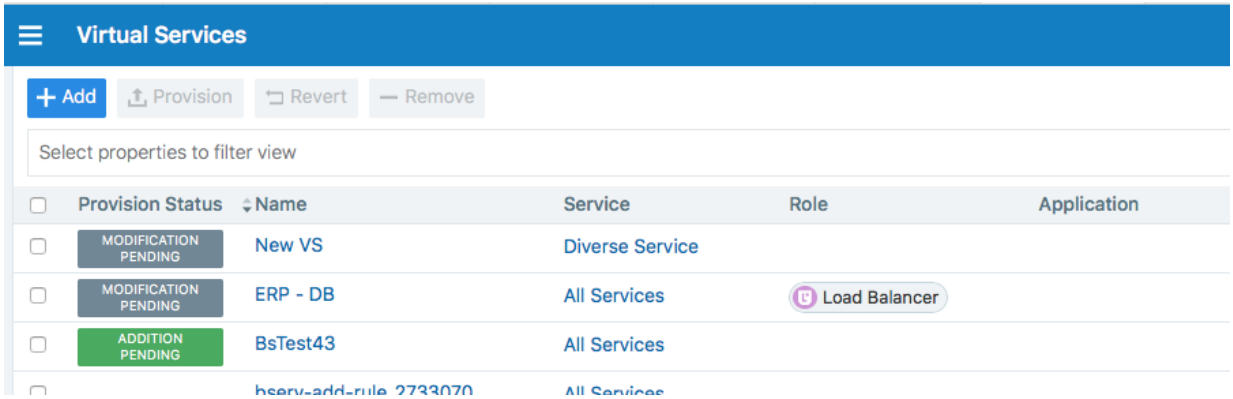
This means that the rule applies to traffic destined for somewhere other than the host network namespace that hits the host firewall.

- An outbound rule on workload B for 80 TCP with destination address 192.168.0.100.

Filter the Virtual Services List

You can filter the Virtual Services list by using the properties filter at the top of the list. For example, you can filter and search by label. In the case of DNS-based rules, you can also filter and search by the following objects:

- Service or port
- IP entry or DNS entry (for example, search for *.google.com)



Add a Virtual Service

When adding a virtual service, you need to give it a name, select the service, and apply labels to it.

Then, you need to bind it to the workload where the service is running. This binding instructs the PCE where to enforce the rules for this virtual service.

When you configure two rules with the same service ports and one of the rules is stateless and the other stateful, the stateless rule takes precedence.

NOTE

A virtual service must be provisioned before binding it to a workload. See Provisioning [116] for more information.

1. From the PCE web console menu, choose **Policy Objects** > **Virtual Services**.
2. Click **Add**.
   The Add Virtual Service page appears.
3. Enter a name for the service.
4. From the Service drop-down list, select the service or enter a service name.
5. Select a Role, Application, Environment, and Location label.
6. (Optional) Choose whether you want the rules associated with the virtual service to be applied over an internal bridged network instead of a host network (default behavior).

- **Internal Bridge Network:** The rules associated with the virtual service are programmed into the FORWARD chain on Linux iptables.
- **Host only network:** The rules associated with the virtual service are applied over the host network, programmed into the INPUT/OUTPUT chains in Linux iptables.

7. (Optional) In the IP addresses field, you can override the IP address of the workload bound to the virtual service and specify different IP addresses or CIDR block that will be used for programming the virtual service rules.
8. Click **Save**.

   The virtual service is created and labeled; next, provision it and bind it to a workload. See Provisioning [116] for more information.

NOTE

SecureConnect is not supported for virtual services.

Bind a Virtual Service to a Workload

When you bind a virtual service to a workload, it enables the PCE to program rules to the VEN on the workload the virtual service is bound to.

If the workload binding ever changes, the rules of your ruleset are dynamically recalculated for the new binding.

NOTE

Before binding a virtual service to a workload, the virtual service must be provisioned. See Provisioning [116] for more information.

1. From the PCE web console menu, choose **Policy Objects**, > **Virtual Services**.
2. Select the virtual service you want to bind to a workload.

   The Virtual Services details page appears.
3. Click the **Workloads** tab.
4. Click **Bind**.
5. In the Workloads drop-down list, select the workload to which you want to bind this virtual service.
6. To allow this virtual service to use a different port than the one specified, select the Override ports checkbox.

NOTE

When you select **All Services** as the service for the virtual service, you cannot enable port overrides on the workload bindings.

7. In the Ports/Protocols section, enter the TCP and UDP ports for this virtual service to use.
8. Click **Save**.

IP Lists

IP lists allow you to define allowlists of trusted IP address, IP address ranges, or CIDR blocks that you want to allow into your datacenter and to be able to access workloads and applications in your network.

Overview of IP Lists

After you define an IP list, you can use it in rulesets to create rules for workload traffic flows. When you provision the rulesets, the workload only allows IP addresses in the IP list to access workload services.

The default IP list "Any" represents all IPv6 addresses as well as all IPv4 addresses. Rules that use IP lists are programmed on one side of the connection only. IP lists can be used as a provider or a consumer.

NOTE

To allow outbound access to IP lists, Illumio recommends using an intra-scope rule to prevent application of the rule to a broader set of workloads than intended.

Example of IP List Usage

For example, the following ruleset (scope + rules):

	App	Env	Loc
Scope	**HRM**	**Prod**	**US**
	Providers	**Services**	**Consumers**
Rule	DB	SSH	Corp-HQ

Means "allow SSH from Corp-HQ to the database."

This ruleset:

	App	Env	Loc
Scope	**All**	**Prod**	**All**
	Providers	**Services**	**Consumers**
Rule	Corp-HQ	SSH	DB

Means "allow SSH from the database to Corp-HQ."

This ruleset:

	App	Env	Loc
Scope	All	Prod	All
	Providers	Services	Consumers
Rule	Any	Any	Any

Means “do not apply Any IP list to anything.”

Create an IP List

1. From the PCE web console menu, choose **Policy Objects** > **IP Lists**.
2. Click **Add**.
3. Enter a name for the IP list.
4. Add IP addresses, IP address ranges, or CIDR blocks to define the list.

TIP

You can copy and paste lists of IP addresses from other sources.

5. Click **Save**.

IP List Exclusions

In IP lists, you can exclude certain IP addresses or subnets from a broader IP subnet.

For example, you might want to exclude a list of IP addresses within an IP range that should not access certain workloads. Or, you might want to open up a set of workloads to any IP address (0.0.0.0/0 and ::/0), but exclude a set of IP addresses that keep attempting unauthorized access to your workloads.

NOTE

Any (0.0.0.0/0) refers to IP addresses not associated with workloads while “All workloads” refers to workloads within a scope.

When you use an IP list with exclusions in a rule, any IP addresses that are marked as exclusions are not allowed, while all the others in the IP list are allowed.

To create IP list exclusions:

- To add an IP address or subnet exclusion, use an exclamation point followed by the IP address, CIDR block or IP range. The excluded IP addresses must be within the included IP range.

For example, you added 192.16.0.0/12 as an allowed IP address and you want to exclude an IP address from this CIDR block, enter the following value:

`!192.31.43.0-192.31.43.100`

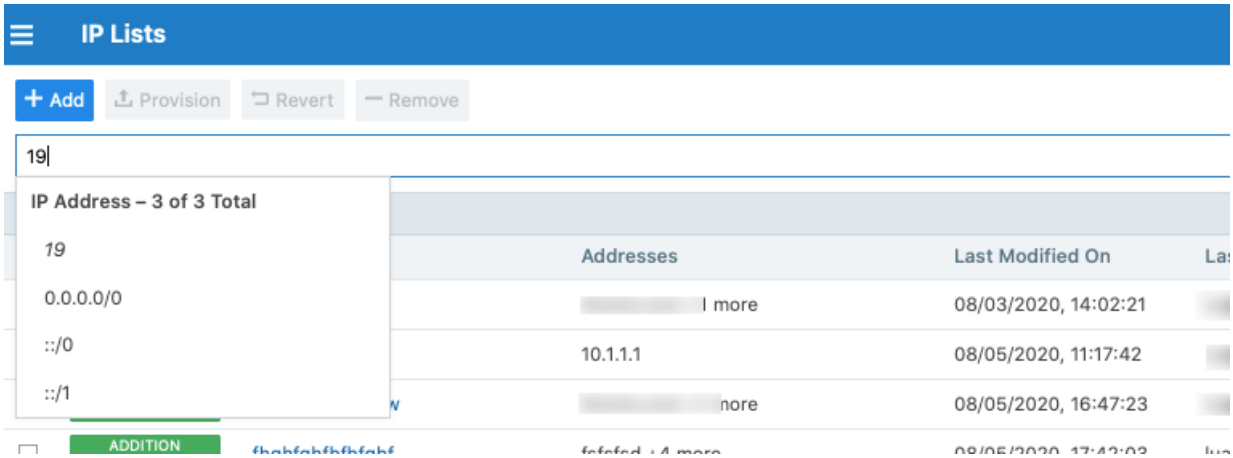
- To add a CIDR block but exclude a portion of the CIDR block, enter the following values:

  `10.0.0.0/8 !10.1.0.0/24`

  In this example, the first block would be included and the second block would be excluded.

Filter IP Lists

You can filter the IP list page using the property filter at the top of the list. You can filter list by entering an IP list name, description, IP address, FQDN, and provision status (draft or active).



Load Balancers and Virtual Servers

Load Balancers

Illumio Core supports activation of enforcement on F5 BIG-IP Local Traffic Manager (LTM), BIG-IP Advanced Firewall Manager (AFM), and AVI Vantage systems.

IMPORTANT

From the Illumio Core 19.3.0 release onwards, the Network Function Controller (NFC) is no longer supported. The F5 interface has been moved from the PCE in to the Network Enforcement Node (NEN).

Since the NFC has been discontinued, you need the NEN to interface with Load Balancers. The NEN has both switch and load balancer capabilities.

By applying labels to your load balancer's virtual servers, you can write rules that allow client workloads in front of the load balancer to communicate with the virtual IP address of the load balancer's virtual servers. By adding labels to the pool members behind a virtual sever, you can allow communication from the load balancer to the members of the pool. The source for this communication is determined by the load balancer. The Illumio Core programs policies on the load balancer to enforce security policy. The PCE uses the load balancer's REST APIs to read and write security policies to configure security rules.

The PCE supports configuration of two load balancer units if they are configured in Active/Standby or Active/Active modes. The PCE needs to be configured with the user name and password of an administrative user who has read-write access to all configurations on the load balancer.

The PCE configures new objects on the load balancer and does not alter any existing configurations. When an Illumio-created object in the load balancer configuration is modified, the PCE detects it as tampering and modifies the configuration back to the intended state so that the correct security policy is enforced.

The Illumio Core dynamically adjusts policies on the load balancer based on application and topology changes in the datacenter so that the Illumio Core can enforce consistent security policy on load balancers across the datacenter and cloud environments, as well as show the application traffic in Illumination. The Illumio Core keeps track of the policy it programmed and reconfigures policy if it was altered on the load balancer manually or by other means.

The Illumio Core makes use of the following constructs on load balancers:

- **LTM:** iRules on LTM provide capability to restrict application access. When LTM is used as enforcement mechanism, the Illumio Core uses virtual-server based iRules and Datagroup Lists.
- **F5 AFM:** AFM provides stateful firewalling on BIG-IP. When AFM is used as an enforcement mechanism, the Illumio Core uses Network Firewall policies in the virtual server section and address-lists in the network firewall. Illumio supports the F5 BIG-IP Application Services 3 Extension (referred to as BIG-IP AS3). AS3 is a flexible, low-overhead mechanism for managing application-specific configurations on a BIG-IP system.
- **AVI:** The Illumio Core uses the Network Security Policy rules to program AVI Vantage.

NOTE

Configuring two F5 units in Active/Standby mode is supported. However, clustering is not supported.

F5 BIG-IP Requirements

The Illumio Core uses its REST API to program F5 load balancers, which means that F5 needs to be running a software version that supports REST-API. The requirements include:

- BIG-IP 11.5.x or higher
- Utilize SNAT or Auto-map mode

AVI Vantage Requirements

- AVI Vantage 18.2.3 or higher

Configure Load Balancers

You can add a load balancer using the PCE web console. However, before you add a load balancer, you need to pair the NEN with the load balancer functionality enabled with the PCE.

NOTE

A load balancer does not need to be provisioned to work. However, the virtual servers you associate with this load balancer do need to be provisioned.

1. From the PCE web console menu, choose **Infrastructure** > **Load Balancers**.
2. Click **Add**.
3. Specify a name for the load balancer and provide a description.
4. From NEN hostname, select the NEN that you want to manage policy programming for this particular SLB.
5. From Device Type, select appropriate load balancer device type.
6. From number of devices, select **(1) Standard** or **(2) HA Pair**.

   The load balancer details are displayed.
7. Specify the following settings to enable the PCE to connect to the load balancer:
   - Management IP address or FQDN of the load balancer
   - Port on which to connect
   - Username
   - Password
8. Select **Verify TLS** to verify the trust of the TLS certificate provided by the load balancer before connecting to it.
9. Click **Save**.

About Virtual Servers

Virtual servers in the Illumio Core contain two parts:

- A virtual IP address (VIP) and port through which the service is exposed
- Local IP address(es) used to communicate with backend servers (pool members).

A virtual server is similar to a workload. It can be assigned labels and has IP addresses, but does not report traffic to the Illumio Core. Each virtual server has only one VIP. The local IP addresses are used as a source IP address for connections to the pool members (backend servers) when the virtual server is operating in SNAT mode or Auto mode. These IP addresses are likely to be shared by multiple virtual servers on the server load balancer.

A virtual server is identified by a set of labels. The consumers and providers for a virtual server can be assigned different labels, which could place them in the same group or a different group in Illumination. See "Groups in Illumination" in Visualization Guide.

Providers are allowed to have an incomplete label set (for example, only a Location label), so the providers can be in all groups within the specified location. As a result, a single virtual server can have providers in any group or in any number of groups in Illumination.

Virtual Server Members and Labels

The Illumio Core allows you to write rules to allow communication with workloads managed by a load balancer using labels.

Virtual Server Members

When you configure load balancers in the PCE, it connects to the load balancer using the Illumio Core REST API. The PCE reads all the load balancer virtual servers configurations and

populates the Discovered Virtual Servers tab of a load balancer's details page. Any virtual servers associated with the load balancer can be converted to a managed virtual server for use with the PCE. When you configure the virtual server in the PCE web console, you can apply labels to the virtual servers. After configuring a virtual server, you can write a rule that allows other clients to communicate with it.

The members behind a virtual server are specified by configuring a set of labels in the virtual server configuration. A set of four Illumio labels can be applied on the Virtual Server Members tab, which is used to match the same set of labels on workloads in the virtual server's pool. If any of the workloads in the virtual server pool share the same set of four labels specified under the Virtual Server Members tab, then any rule you write with the virtual server also applies to the workload members.

Configure Virtual Servers

After adding a load balancer to the PCE, you can manage its virtual servers. To each virtual server, you can apply labels through the Virtual Server details page. Applying labels to a virtual server allows you to add the virtual server to a rule.

When the policy is enforced on the virtual server by the NEN, access from any IPs/Workloads to the Virtual Server is controlled according to the rules defined by the policy. The NEN removes the rules from the virtual server when the policy is no longer enforced.

Configuring a load balancer's virtual servers consists of these three settings:

- **Enforced or Not Enforced:** When you select Enforced, any rules you write using the labels associated with the virtual servers and any of its members are enacted. Selecting Not Enforced disables the labels and any policy written that affects the virtual server or its members is disabled.
- **Service:** Select the service to use for the rules that allow access to the virtual server. For example, HTTPD 80 TCP.
- **Labels:** You must apply one each of the four Illumio labels to the virtual server: Role, Application, Environment, and Location. Assigning labels enables the virtual server to be used in rules.

NOTE

Virtual servers are considered a security policy item, so any changes to a virtual server configuration must be provisioned before any of those changes take effect and become active.

Virtual Server Limitations

- Illumination does not support location-level and application-level maps.
- If a single SNAT pool is shared between multiple virtual servers, the Illumination map does not render correctly.
- SNAT and Auto-map modes of F5 virtual servers are supported. Transparent mode is not supported.

NOTE
Before any virtual server configuration can go into effect, you need to provision your changes.

Filter the Virtual Server List

You can filter the Virtual Servers list by using the properties filter at the top of the list. For example, you can filter and search by label. You can also filter and search by the following objects:

- Virtual server mode
- Virtual IP address, the VIP port number, or VIP Protocol
- Server Load Balancer

Configure a Load Balancer's Virtual Servers

1. From the PCE web console menu, choose **Infrastructure** > **Load Balancers**.
2. Select the load balancer for which you want to configure virtual servers.
3. Select the **Virtual Servers** tab.
4. Select one of the load balancer's virtual servers and click **Manage**.
5. Select one of the virtual servers and click **Edit**.
6. Enter a name and description for the virtual server.
7. To enable the virtual server's policy, select **Enforced**.
8. Select a service to associate with the virtual server. The service selected enables that service to be used in rules you write for this virtual server.
9. Select one each of the four labels to assign to the virtual server.
10. Click **Save**.
11. Before any virtual servers can go into effect, they must be provisioned.

Adaptive User Segmentation

Illumio's Adaptive User Segmentation (AUS) allows you to leverage Microsoft Active Directory User Groups to control access to computing resources in your organization. With this feature, you can create user groups in the PCE that map directly to your Active Directory Groups.

Overview of Adaptive User Segmentation

You can then write rules with these groups so that you can control outbound access on specific workloads—such as a VDI desktop—based on the group membership of the user logged in to that workload.

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.

If you have a Windows workload that controls access to other resources in your network, such as a VDI desktop that has the VEN installed on it, you can add both the VDI desktop

workload and Active Directory User Groups to the rule. Writing this type of rule allows user access only to the resources that are explicitly allowed by the rules.

This type of rule is represented by an icon, where the VDI desktop and AD User Group are added as the consumers of a ruleset, and entities that these user groups are allowed to access are added as providers.

Add Active Directory User Groups

1. From the PCE web console menu, choose **Policy Objects** > **User Groups**.
2. In the User Groups page, click **Add**.
3. In the Add User Group page, enter a name, system identifier (SID), and description for the Active Directory Group.
4. Click **Save**.

   The new Active Directory Group appears in the User Groups list. You can now use the user group in a ruleset to control access to specific workloads.

NOTE

A maximum of 100 User Groups can be displayed.

User Group-Based Rules for AUS

1. From the PCE web console menu, choose **Rulesets and Rules > Rulesets**.
2. In the Rulesets list, click **Add**.
3. Enter a name for the ruleset.
4. Select an Application, Environment, and Location label to define the ruleset scope.
5. Click **Save**.

   In the Rules section, you can start writing identity-based rules.
6. If necessary, expand the *Intra-Scope Rule* section.
7. In the Consumers drop-down list, select the user group that you want to provide access to the other workload.
8. From the Providers drop-down list, select the workloads or labels that you want to provide access to by a user group.
9. In the Services drop-down list, select the service that you want the user groups to be able to access on the providing workloads.
10. Click the **Save** icon at the end of the row.
11. To add additional rules to the ruleset, Click the **Add** (+) icon.

To enact these changes on the workloads this ruleset affects, provision your changes.

Export Reports

Using the Export Reports feature, you can download PCE objects in JSON and CSV formats. These reports are very useful when you want to share the data with application owners, managers, executives, or auditors who do not have access to the PCE.

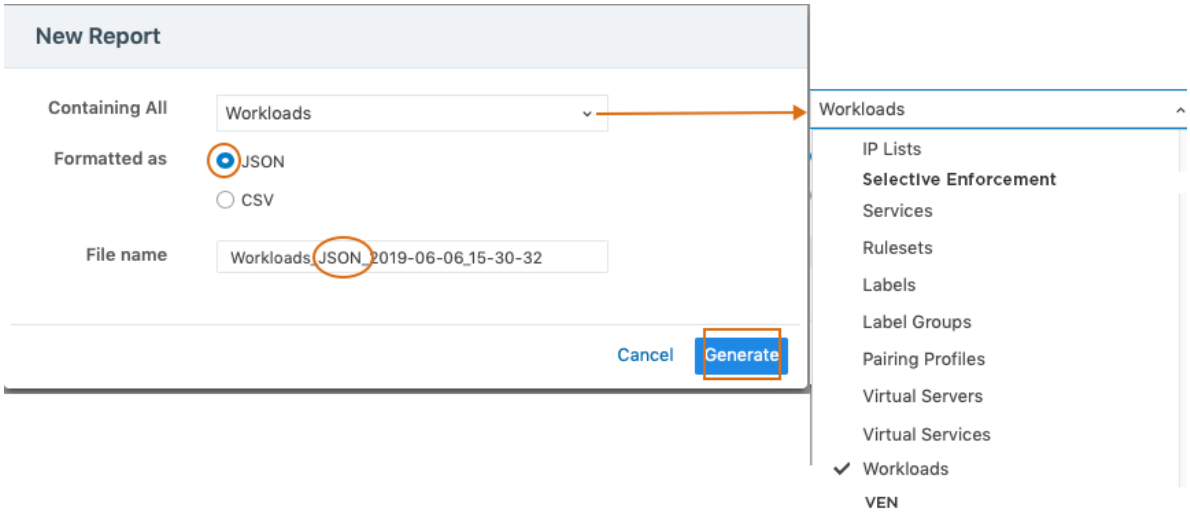
Overview of Export Reports

CSV is the most common and popular format because you can import it into other tools like CMDBs. You can export the following objects into an export report:

- Workloads
- Rulesets
- IP lists
- Pairing profiles
- Services
- Labels
- Label groups
- Virtual services
- Virtual servers

Generate an Export Report

1. From the PCE web console menu, choose **Troubleshooting** > **Export Reports**.
2. Click **New Report**.
3. From the Containing All drop-down list, select the object for which you want to generate the report.
4. Select the format, JSON or CSV.



5. Click **Generate**.

Workloads

This section describes workload attributes, it's enforcements, and how to create managed and unmanaged workloads.

Workloads have the following attributes:

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

Workloads in the PCE

This section describes how to manage workload by using the Workload pages in the PCE web console.

Overview of Workload Attributes

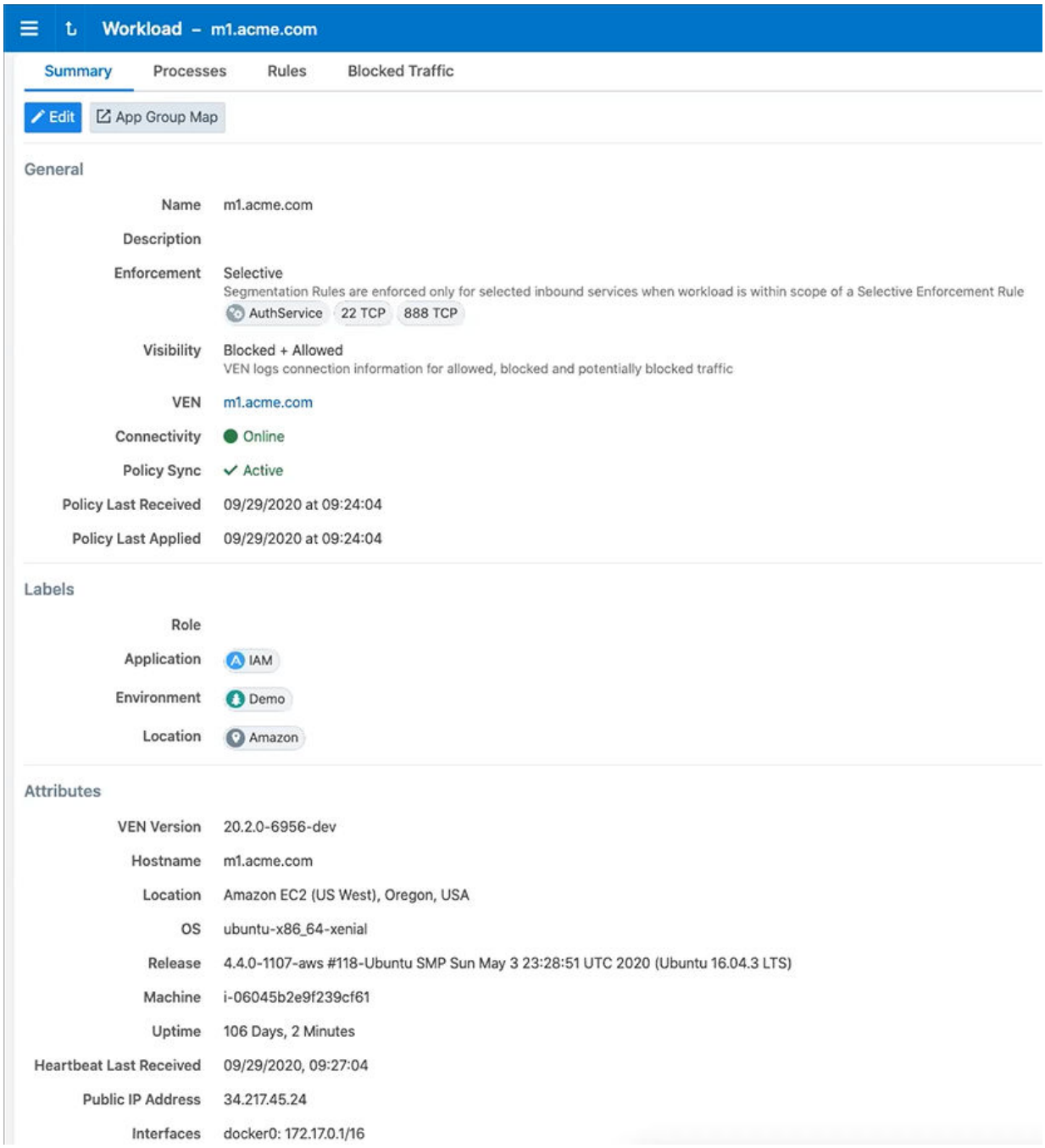
Workloads have the following attributes:

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

Workload Summary

The workload summary displays information about the workload, including the user-specified attributes at the time of pairing and information that the Illumio Core has automatically detected about the workload, specifically:

- The name of the workload
- A description (if provided)
- The Workload Enforcement States [125]
- The visibility the VEN uses
- The dates when the policy was revised and last applied
- The workload's VEN connectivity status; see "VEN-to-PCE Communication" in VEN Administration Guide.
- The workload's VEN policy sync status; see "VEN Policy Sync" in VEN Administration Guide.
- Any labels applied to the workload
- Workload system attributes (such as VEN version number, hostname, and uptime)



Workload Enforcement States

Policy state determines how the rules affect a workload's network communication. The Illumio Core includes four policy states for workloads. If a workload is unmanaged, the Policy State column is not displayed on the workload list page.

Idle

The Idle state is used to install and activate VENs on workloads without changing the workload's firewalls. In the Idle state, the VEN on the workload does not take control of the workload's host firewall but uses workload network analysis to provide the PCE relevant details about the workload, such as the workload's network interface, operating system, and traffic flows. This information is captured in the following ways and intervals:

- Traffic flows: a snapshot is taken every 10 minutes.
- Operating system: included in the Compatibility Report every four hours.
- Workload network interface: reported to the PCE anytime it changes.

A pairing profile can be used to pair workloads in the idle state.

NOTE

SecureConnect (IPv6 compatibility) is not supported on workloads in the Idle state. When you activate SecureConnect for a rule that applies to workloads that are in both Idle and Non-idle policy states, it can impact the traffic between these workloads.

Visibility Only

In the Visibility Only state, the VEN takes control of the host firewall, attempts to load kernel modules if required, and reports traffic flows to the PCE. The VEN will never block traffic in Visibility Mode (see note below). In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the datacenter and the applications running in it. Visibility Only is useful when firewall policies are not yet known, allowing you to discover the application traffic flows in the organization and then generate a security policy that governs required communication.

NOTE

Depending on the workload's operating system, it may be possible for existing configurations or third-party tooling to be already interacting with the host firewall prior to VEN deployment. Therefore, Illumio recommends that you activate the VEN in Idle mode and then run the Compatibility Report to help you determine if Firewall Coexistence mode is required.

Selective Enforcement

Segmentation rules are enforced only for selected inbound services when a workload is within the scope of a Selective Enforcement Rule.

Full Enforcement

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

Visibility Level

You can choose from three levels of visibility for workloads. These modes allow you to specify how much data the VEN collects from a workload when in the Full Enforcement state:

- **Off:** The VEN does not collect any information about traffic connections. This option provides no Illumination detail and demands the least amount of system resources from a workload.

This property is only available for workloads that are in the Full Enforcement state.

- **Blocked:** The VEN only collects the blocked connection details (source IP, destination IP, protocol and source port and destination port), including all packets that were dropped. This option provides less Illumination detail but also demands fewer system resources from a workload than high detail.
- **Blocked + Allowed:** The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections. This option provides rich Illumination detail but requires some system resources from a workload.

Workload Processes

In the Workload Processes tab of the Workload detail page, you can view the processes currently running on the workload.

For each process running on the workload, the following information is listed:

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

To organize the listed items, you can select the column headings to sort the processes by that attribute. For example, when you click the Protocol column heading, the processes are grouped by protocol so that all processes using UDP are listed together and all processes using TCP are listed together.

NOTE

On the Workload Processes tab, when you delete the binary for that process while the process is running, the PCE appends the process name with "(deleted)."

The UDP - PCE UI processes tab shows both server and client UDP processes and ports.

On the Services tab for a workload, both UDP client and server processes show up along with their port numbers. For TCP, only listening ports/processes are presented.

For UDP, only listening ports/processes should be presented. The information is coming from service-reports sent by VEN once every 24 hours.

Customers depend on this information to understand the provider-processes in their datacenter and write policies to allow traffic from needed workloads.

Workload Rules

The Illumio Core has two types of rules:

- **Inbound Rules:** Show all the services on the workload and the interface endpoints that are allowed to communicate with these services.

- **Outbound Rules:** Show all the interface endpoints that the services on that workload are allowed to communicate with.

To apply rules to a workload, create a ruleset and then make sure that the ruleset and workloads share the same labels.

NOTE

The workload rules are listed against individual IP addresses in an ipset. The PCE places a limit on the size of the returned data. The PCE web console displays an error message whenever the PCE exceeds a certain number of rules and that count is the number of peer-to-peer rules calculated for that workload.

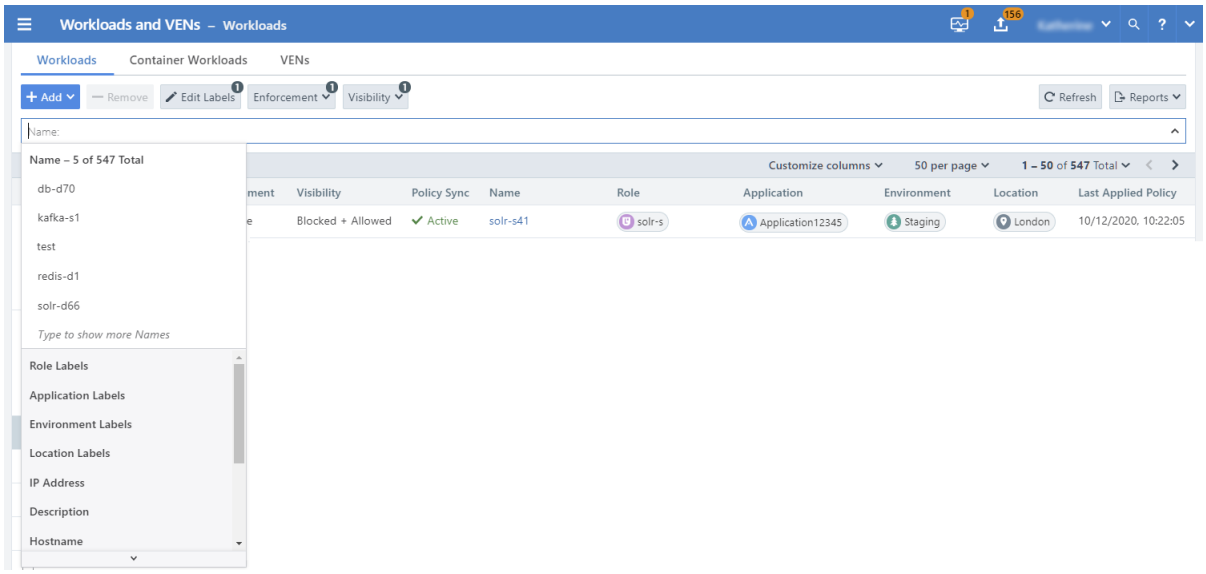
Workloads Blocked Traffic

The Blocked Traffic tab shows you all traffic that attempted to communicate with your workload but was blocked due to policy. For information, see Blocked Traffic [54].

Filter the Workloads List

You can filter by one or any combination of workload labels and properties. For example, you can use the Workload filters to see only workloads that have the Role label named Web, that are running Linux Ubuntu, that are in the Build policy state, with a VEN policy sync status of Active, that have a specific IP address, and that have “asset” in the hostname.

- Use the filter at the top of the Workloads and VENs page to do a label-based search. For example, you can filter the list to view all workloads that have the Application label “Application12345.”



- You can filter workloads based on their properties, such as workload name, IP address, description, hostname, OS family, VEN connectivity, and when a policy was last applied to or received by the workload, and when was the last heartbeat received.

Click the **Refresh** button to refresh the content of the page with the latest information without clearing the filters or the results.

Use a Wildcard to Filter Workloads

To help sort and organize large numbers of workloads, the Workloads filter supports a wildcard character for the Name and Hostname properties.

To filter the list of workloads on the Workloads page, select either the Name or Hostname property from the drop-down list and enter the search terms using the asterisk (*) character as a wildcard. The asterisk can represent any number of characters.

For example, you can enter “db-*auto” using the Name property to find workloads with names that include “db,” “-auto,” and any number of characters in between (for example, “db-prod-auto,” “db-dev-auto,” or “db-12-auto”).

At least one non-wildcard character must be included before or after the wildcard character. An error message is displayed when you include only the wildcard character in the search field.

NOTE

The auto-complete feature is disabled when the wildcard character is used.

Use Clone Alerts to Filter Workloads

Workloads can be filtered according to whether a clone has been detected. If the are are any workloads that are in the clone detected state, a red banner (similar to workloads in suspension) is displayed at the top of the workload list page.

The VEN communicates with the PCE using HTTPS over Transport Layer Security (TLS). Additionally, a clone token is generated. When an agent token is mistakenly or maliciously reused on another workload, the clone token is used to detect the condition and disambiguate the hosts. The clone token is periodically rotated. The agent token is never rotated.

To filter by clone alerts:

1. In the PCE web console, display the Workloads List page.
2. Look for an alert banner indicating some workloads are in "clone detected" state. This banner will appear only if, for example, you pair one or more VENs and then clone the VEN(s).
3. Click the filter link on the banner. The list now shows only the "clone detected" workloads.
4. Click on one of the "clone detected" workloads. An alert is displayed on the detail page for that workload.
5. If you stop, unpair, or repair the cloned VEN, you can come back and see that the messages and alerts are removed from the Workloads List page.

Enforce a Workload Policy State

1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.
2. Select the workload that you want to change the Enforcement state..
3. From the Enforcement drop-down list, select **Idle**, **Visibility Only**, **Selective**, or **Full** depending on how you want to allow or block traffic connections.

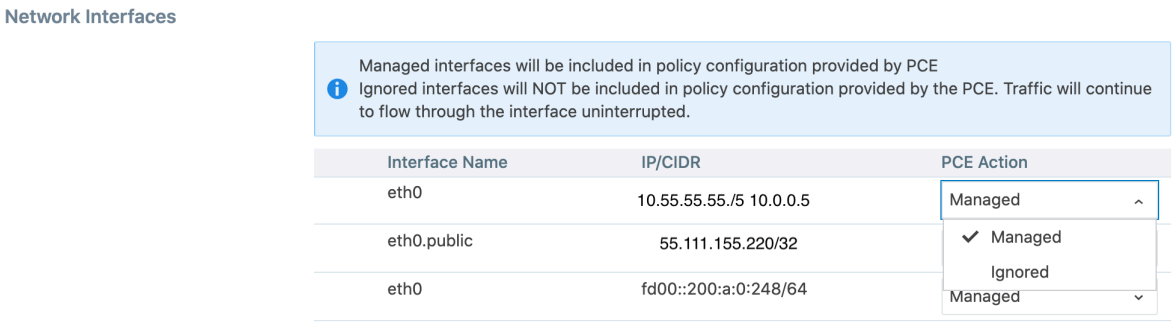
A dialog box appears directing you to confirm your change.

4. Click **OK**.

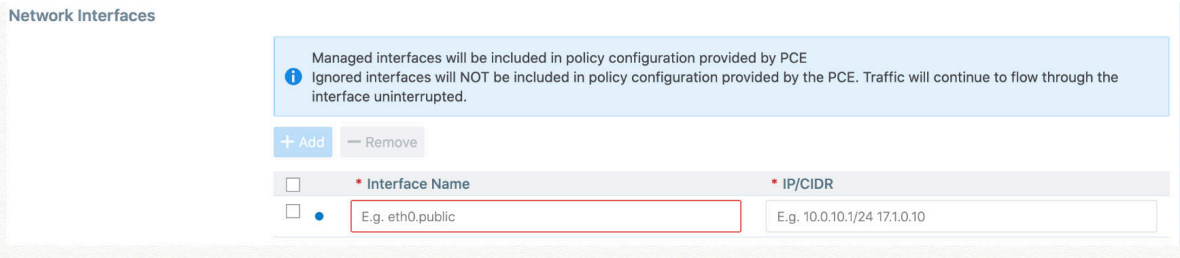
Set Workload Interfaces to Ignored

You can set interfaces from being Managed to Ignored in the PCE web console. You can use this option when you want the workload to ignore visibility and enforcement on the interconnected interfaces of database clusters such as, Oracle RAC. During pairing, you can set one or more interfaces to Ignored, which causes the first downloaded firewall to ignore those interfaces. After you set an interface to Ignored, that interface is not be included in the policy configuration and traffic flows uninterrupted through it without any change in latency. You can see which interfaces are marked as Ignored on the Workloads' Summary page.

1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.
2. Click a workload to open the details.
3. Click **Edit**.
4. In the Network Interfaces section, change interfaces from Managed to Ignored using the PCE Action drop-down list.



In case you are editing an unmanaged workload, you will not have the option to ignore the workload using the PCE Action drop-down. That drop-down menu does not exist for unmanaged workloads. You can still provide information on the Interface Name and the IP/CIDR address.



5. Click **Save**.

Workloads and VENs

The Workloads navigation menu includes Workloads, Container Workloads, and VENs. You can see all your workloads, container workloads, and VENs on separate tabs. You can view their configuration, do workload or VEN-specific actions, and find the related VENs and workloads.

An idle workload does not program a firewall, therefore the Rules page of an idle workload does not show its rules.

The VENs are listed in a new page separate from workloads. The VEN-related actions are not available under the Workloads tab.

Manage Workloads and VENs

NOTE
Users with the Workload Manager role can manage workloads and VENs.

You can select VENs to unpair, refresh, and generate support reports. Container workloads (if any) are displayed under the Container Workloads tab.

Click the **Unpair** button to unpair a VEN.

On the Unpair VEN page, select the appropriate radio button to define the Final Firewall Status:

Firewall Status	Description
Remove Illumio Policy	This is the default option. Linux: Removes Illumio policy and retains the coexistent firewall rules AIX/Solaris: Removes Illumio policy and reverts firewall rules to the pre-pairing state Windows: Removes firewall WFP filters and activates Windows firewall
Open all ports	All OS system: leaves all ports open
Close all ports except remote management	Linux/AIX/Solaris: temporarily allows only SSH/22 until the system is rebooted Windows: allows only RDP/3389 and WinRM/5985, 5986

Proceed with unpairing as follows:

Pairing Method	Policy Mode	Unpair Action
Pairing Key	Visibility only/ Enforced	• Uninstalls the selected VEN(s). • Removes policy for the associated workloads. • Policies are configured in to the host firewall based on options selected in "Select final firewall status".
Pairing Key	Idle	• Uninstalls the selected VEN(s). • Removes policy for the associated workloads. • No changes to the host firewall.
PKI Certificate or Kerberos	Visibility only/ Enforced	• Uninstalls the selected VEN(s). • Associated workloads become unmanaged but retain labels and IP addresses. • Policies are configured in to the host firewall based on options selected in "Select final firewall status".
PKI Certificate or Kerberos	Idle	• Uninstalls the selected VEN(s). • Associated workloads become unmanaged but retain labels and IP addresses. • No changes to the host firewall.

Delete a workload from the PCE

You cannot directly delete workloads from the PCE, as the workload represents an entity that the PCE does not control. You can unpair the VEN on that workload from the VENs tab on the Servers & Endpoints/Workloads menu, which will remove the workload from the workloads table.

Enhanced Data Collection

The Enhanced Data Collection optional feature on the PCE is now fully available starting in the 22.5.10 release, after being a preview feature available with the 20.2.0 release. When enabled, the PCE reports the amount of data transferred in to and out of workloads and applications in a data center. The number of bytes sent by and received by the provider of an application are provided separately. You can see these values in traffic flow summaries streamed out of the PCE. You can enable this capability on a per-workload basis in the Workload page. You can also enable it in the pairing profile so that workloads are directly paired into this mode.

To enable Enhanced Data Collection you need a License file. For information about obtaining the license, please contact Illumio Customer Support.

Once licensed, enable Enhanced Data Collection for a workload with the Visibility button.

- On the Workloads an VENs -Workloads page, select **Visibility > Enhanced Data Collection**.

  You can also enable Enhanced Data Collection as a Visibility option in the Pairing Profile page by selecting the radio button "Enhanced Data Collection".

After the VEN's visibility level is set to Enhanced Data Collection, it starts reporting the number of bytes transferred over the connections. The PCE collects this data, adds relevant information, such as labels, and sends the traffic flow summaries out of the PCE.

The direction reported in flow summary is from the viewpoint of the provider of the flow.

- Destination Total Bytes Out (dst_tbo): Number of bytes transferred out of provider (Connection Responder)
- Destination Total Bytes In (dst_tbi): Number of bytes transferred in to provider (Connection Responder)

The number of bytes includes:

- L3 and L4 header sizes of each packet (IP Header and TCP Header)
- Sizes of multiple headers that may be included in communication (when SecureConnect is enabled)
- Retransmitted packets.

  The bytes transferred in the packets of a connection are included in measurement. This is similar to various networking products such as firewalls, span-port measurement tools, and other network traffic measurement tools that measure network traffic.

Term	Description
dst_tbi	**Destination Total Bytes In** In Total bytes received till now by the destination over the flows included in this flow-summary in the latest sampled interval. This is the same as bytes sent by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_tbo	**Destination Total Bytes Out** Out Total bytes sent till now by the destination over the flows included in this flow-summary in the latest sampled interval. This is the same as bytes received by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_dbi	**Destination Delta Bytes In** In Number of bytes received by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes sent by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_dbo	**Destination Delta Bytes Out** Out Number of bytes sent by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes received by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
interval_sec T	**Time Interval in Seconds** Duration of latest sampled interval over which the above metrics are valid.

Connection State	Description
A	**Active:** The connection is still active at the time the record was posted. Typically observed with long-lived flows on source and destination side of communication.
T	**Timed Out:** Flow does not exist any more. It has timed out. Typically observed on destination side of communication.
C	**Closed:** Flow does not exist any more. It has been closed. Typically observed on source side of communication.
S	**Snapshot:** Connection was active at the time VEN sampled the flow. Typically observed when the VEN is in Idle state.

Container Workloads

The Container Workloads page lists the containers that exist on the PCE.

The page contains this information:

Column	Description
Summary	**General** Information about the container's Name, namespace/project, policy state, and so on.
	Labels Information such as Role, Application, Environment, Location
	Attributes Information about Interfaces and Workloads
Containers	Information about a specific container.
Rules	Information about rules.

Workload Setup Using PCE Web Console

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

About Creating Managed Workloads by Installing VENs

When you install a VEN on a workload and pair it to the PCE, it becomes a managed workload because it can be managed using the PCE. For more information, see "VEN Installation Using VEN Library in PCE" in VEN Installation and Upgrade Guide.

Unmanaged Workloads

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

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

Add an Unmanaged Workload

You can add unmanaged workloads from the Workloads list. After assigning labels, write label-based Rules [96] that apply to unmanaged workloads.

TIP

You can also create an unmanaged Workload from a blocked traffic IP address. See Create Unmanaged Workload from Blocked Traffic [58] for information.

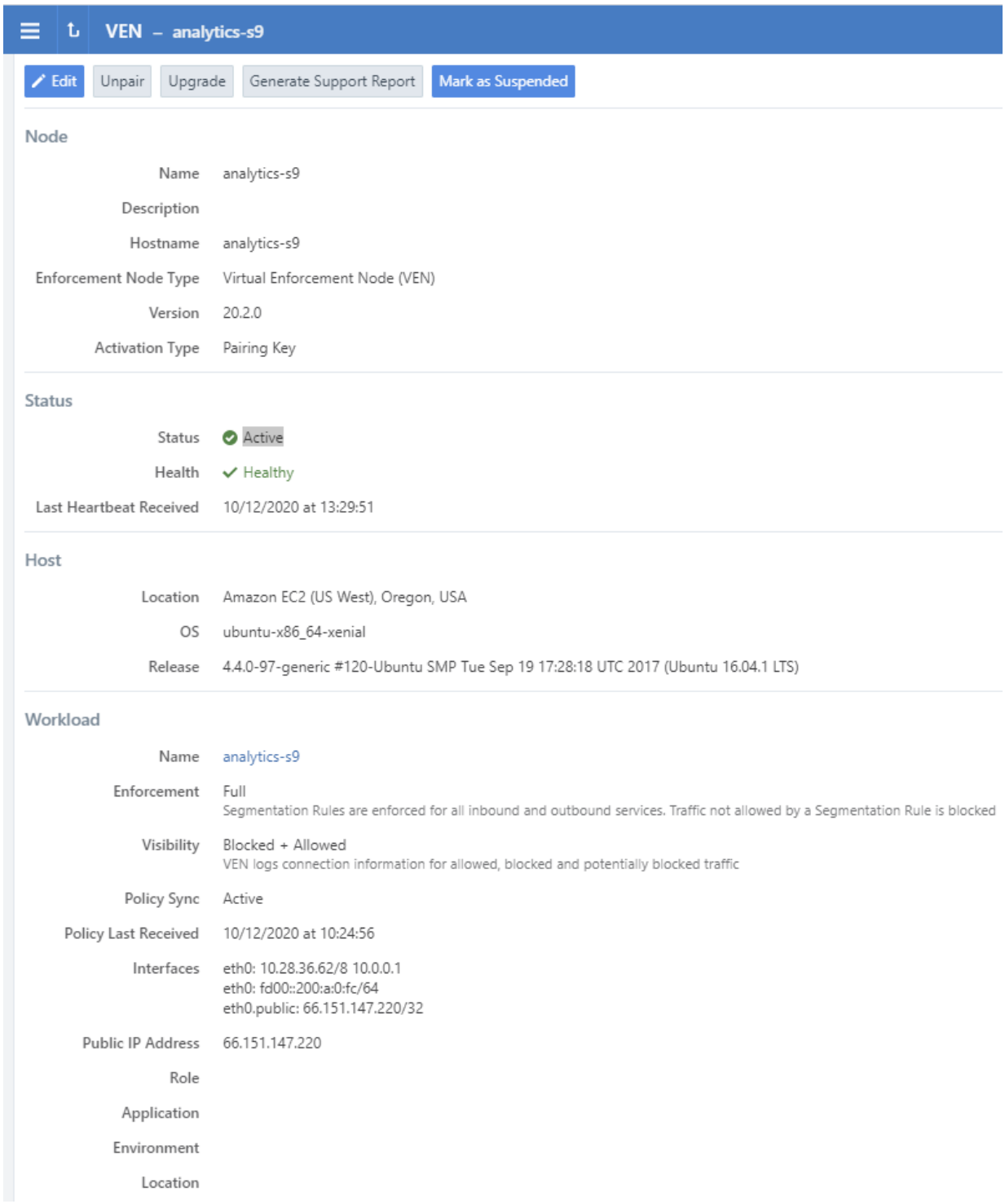
1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.
2. Click **Add** > **Add Unmanaged Workload**.
3. In the Add Unmanaged Workload details page, enter a name and description for the unmanaged workload.
4. In the Label section, select the labels you want to be applied to the unmanaged workload.
5. In the Attributes section, enter all the relevant information about the unmanaged workload, such as its hostname, IP addresses, location, and OS.
6. In the Processes section, enter the name and the port and protocol for the process.
7. (Optional) In the Machine Authentication ID field, enter all or part of the DN string from the Issuer field of the end entity certificate (CA Subject Name). Complete this field when you plan to use this unmanaged workload with the AdminConnect feature because the unmanaged workload is a laptop running Windows or Linux. See "Secure Laptops with AdminConnect" for information.
8. Click **Save**.

VEN Administration on Workloads

You can monitor the connectivity, policy sync, and health status of the VEN from the PCE web console. To view VEN health status, see the VEN list page for your managed environment. From the PCE web console menu, choose Workloads and VENs > VENs. The VEN list page appears.

For more information about managing VENs on workloads, see "About VEN Administration on Workloads in VEN Administration Guide.

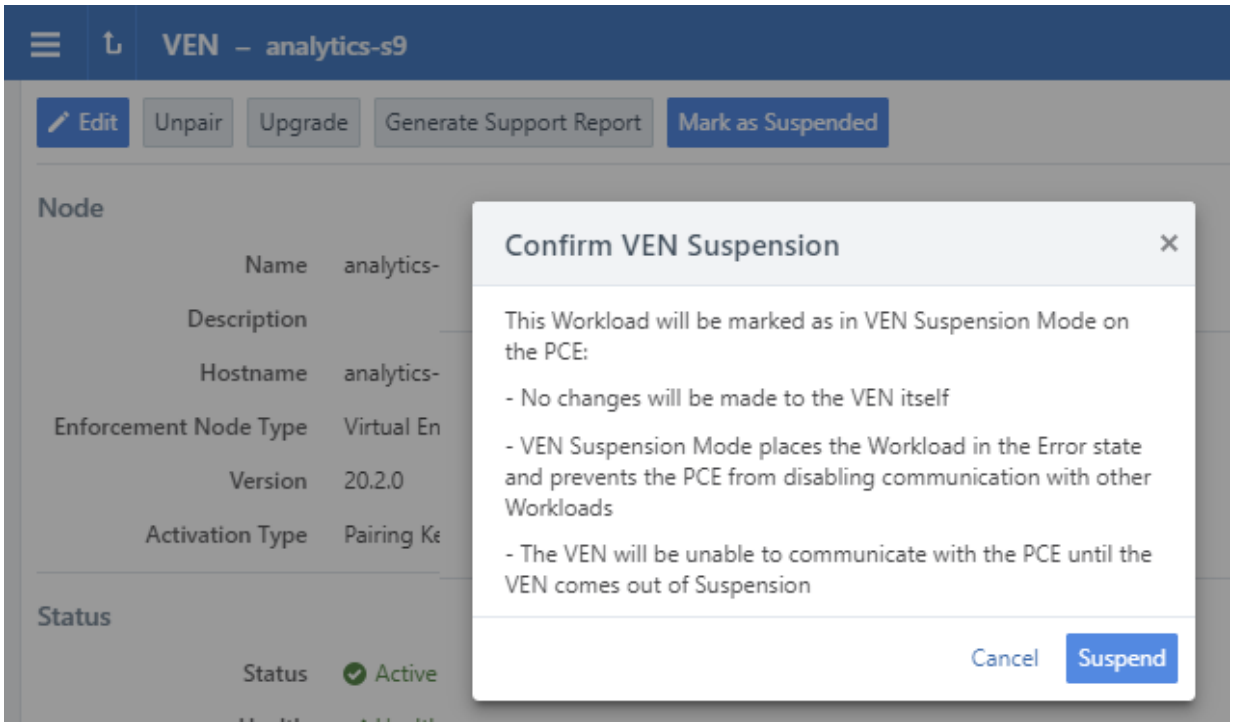
VEN Details for a Workload



VEN Suspension

You can mark a workload as suspended by using the PCE web console. Choose **Workloads and VENs** > **VENs** from the PCE web console menu to suspend a VEN. Select your VEN to open its details page and click **Mark as Suspended**.

For more information about suspending and unsuspending VENs, see "VEN Suspension Using PCE Web Console" in VEN Administration Guide.



Loopback Interfaces

(Works with Linux VENs) VENs can report loopback interfaces and enforce policy on them.

The VEN reports all interfaces, including loopback interfaces. If the VEN detects an interface that is a loopback interface, but is not in the standard defined IP block that is meant for loopback interfaces (127.0.0.0/8), the VEN reports this as a loopback interface to the PCE. If the workload is in the scope where loopback interfaces are to participate in policy enforcement, the workload distributes the IP address to peers and enforces policy on that interface.

The scope where loopback interfaces are to participate in policy enforcement is defined through the PCE web console.

1. Log in to the web console as a Global Ruleset Provisioner or a Global Org Owner.
2. Choose **Settings** > **Security**.
3. Click the Loopback Interfaces tab.
4. Choose labels to define the scope.

Blocked Traffic

Blocked traffic identifies blocked and potentially blocked traffic among workloads and other entities managed by the PCE.

IMPORTANT

In the 19.1.0 release, blocked traffic was marked for deprecation and will be turned off by default in a future release. When a large number of traffic summaries are reported to the PCE, the blocked traffic functionality consumes more memory, which can cause side-effects such as:

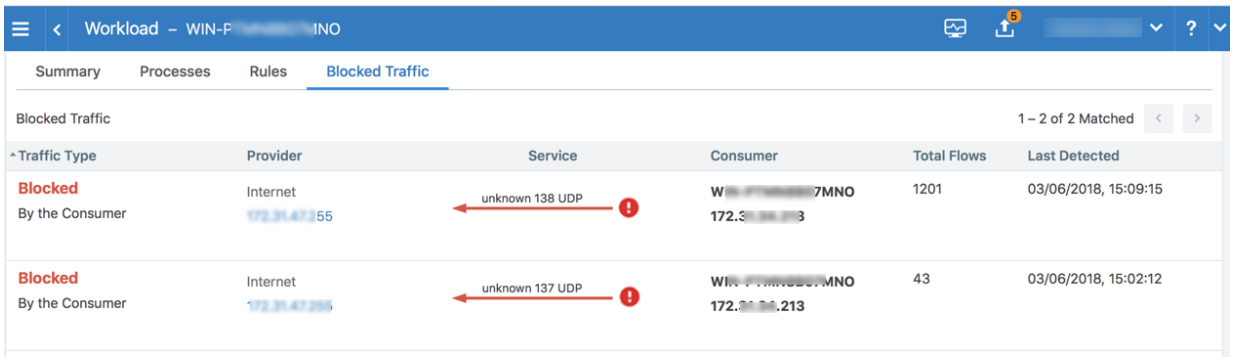
- Illumination dropping some traffic flows
- PCE slowing down due to extra processing

When upgrading to 19.3.0, Illumio recommends that you turn off blocked-traffic by setting the appropriate value in the PCE `runtime_env` file.

The functionality provided by blocked traffic is available in Explorer. In 18.3.1 and later, when the Explorer feature is configured, the Blocked Traffic page was updated using the Explorer data. The Blocked Traffic page will continue to work using the data from Explorer.

Overview of Blocked Traffic

To view the Blocked Traffic page, choose **Troubleshooting** > **Blocked Traffic** from the PCE web console menu. The Blocked Traffic tab 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 port and protocol of the service, as well the IP address of the consumer, the total number of flows, and the time last detected.



Under the following conditions, traffic is marked as potentially blocked or blocked based on the active policy at the PCE when the latest flow was recorded:

- Traffic is blocked when a workload is in the enforced state and the PCE doesn't have rules in the active policy to allow that traffic.
- Traffic is potentially blocked when a workload is in a Visibility Only state and the PCE doesn't have rules in the active policy to allow that traffic.

Traffic that is blocked in the following ways is reported as blocked traffic in the Illumination map, regardless of the workload enforcement:

- Firewalls on the workload not managed by Illumio Core

- WFP policies not managed by Illumio Core

Existing connections are reported as static connections during pairing. These connections display as blocked or potentially blocked until new traffic for the connections is detected.

When you select the blocked connection, the Detail view provides more information on when the connection was last reported (when available).

The Blocked Traffic page allows you to verify that only unauthorized traffic is blocked and permitted communication between workloads is not unintentionally blocked before moving workloads to the enforced state.

You can use the page buttons in the upper left to navigate the listings. You can also use the **Refresh** button to refresh the content of the page with the latest information without clearing the filters or the results.

NOTE

Only the latest 500 blocked traffic entries are displayed.

For each traffic record, the following information is displayed:

- **Traffic Type:** Specifies whether the traffic is blocked or potentially blocked and whether it is blocked by the consumer or by the provider.
- **Provider:** Displays the workload name and IP address of the provider.
- **Provider Labels:** Displays labels assigned to the provider.
- **Service:** Displays the process name, port, and protocol information of the traffic that was reported along with an indication of whether the record was reported by the consumer or the provider.

  NOTE

  For optimal scale and performance, when the PCE has two connections with the same source workload, destination workload, destination port, and protocol but the process or service names are different, the two connections are combined in the Illumination map. The process or service name that was part of the most recently reported connection is displayed.
- **Consumer:** Displays the workload name and IP address of the consumer.
- **Consumer Labels:** Displays labels assigned to the consumer.
- **Total Flows:** Displays the total number of traffic flows for that connection.
- **Last Detected:** Displays a timestamp for the most recent recorded connection.

NOTE

When the provider reports the record, the information in the consumer column is grayed out. When the consumer reports the record, the information in the provider column is grayed out.

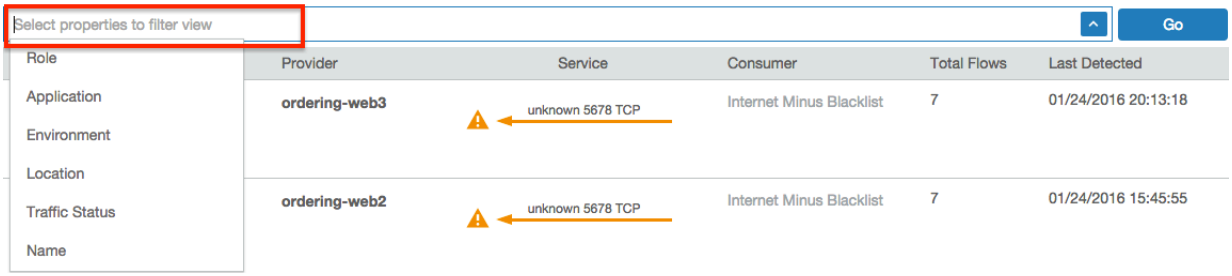
From the 18.3.1 release on, the traffic entries displayed on the blocked traffic page cannot be removed via the PCE web console.

Filter Blocked Traffic

The Blocked Traffic page displays the 500 most recent entries from all workloads managed by the PCE. When you are monitoring or writing rules for a specific set of workloads, use Blocked Traffic filters to display up to 500 of the most relevant entries based on the 10,000 entries in the PCE.

The PCE web console allows you to use filters to display only the blocked traffic entries of interest. You can filter based on workload name, label, traffic type (blocked or potentially blocked), or any combination of these attributes. When you apply the filter by clicking **Go**, the 500 most recent entries that match the search criteria are displayed.

To filter blocked traffic, type the keywords for the filter in the Select properties to filter view field at the top of the Blocked Traffic page.



NOTE

You can filter blocked traffic using multiple properties at the same time. Only entries that match all the entered criteria are displayed.

To specify the type of results, click the arrow at the end of the text entry field and select one or more of the available properties:

- Role
- Application
- Environment
- Location
- Traffic status
- Workload name

After entering your keywords, click **Go** to the right of the text entry field. The results display below the text entry field. The following information is included:

- **Traffic Type:** A link to additional information about that entry
- **Provider:** The provider of the service
- **Service:** The service type

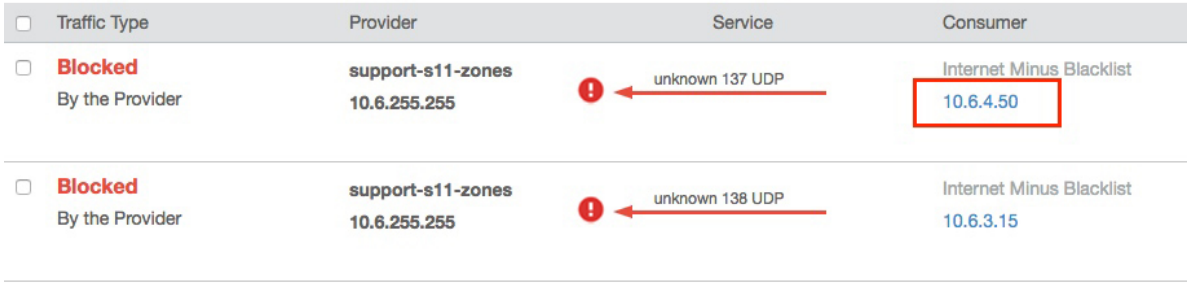
- **Consumer:** The consumer of the service
- **Total Flows:** The total number of times this blocked traffic flow occurred
- **Last Detected:** A timestamp (in hh:mm:ss format) of the last time this flow occurred

Create Unmanaged Workload from Blocked Traffic

In some cases, your policy might be blocked from the IP address of a host that you want to allow to communicate with one of your managed workloads. You can do this by converting the IP address to an unmanaged workload, which enables the PCE to permit it to be used in policy.

Click the IP address in the blocked traffic event and fill out the Unmanaged Workload page. Once you have converted the IP address into an unmanaged workload, you can use it in rulesets to allow other managed workloads to communicate with it, or you can later convert it into a managed workload by pairing it. For more information about unmanaged workloads, see Unmanaged Workloads [51].

1. From the PCE web console menu, choose **Troubleshooting** > **Blocked Traffic**.
2. From the list of blocked traffic events, under the Consumer column, click any of the linked IP addresses.

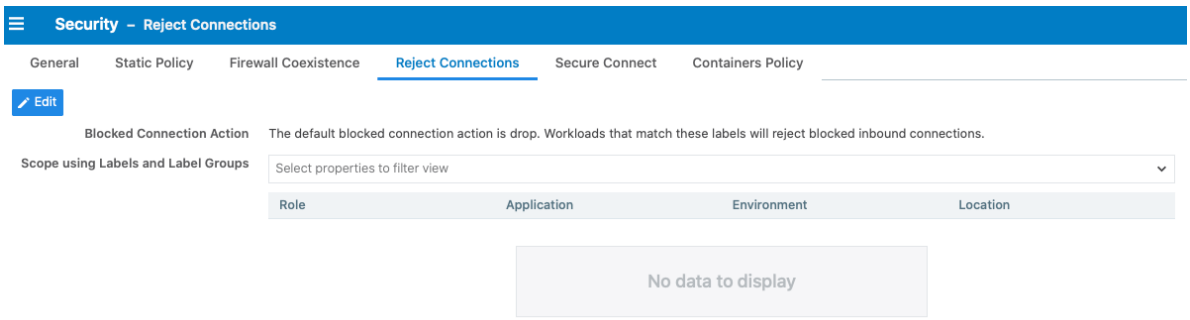


   The Unmanaged Workload page appears.
3. Complete all the fields and click **Save**.

   You can now use the unmanaged workload in your policy. For example, you can configure rules to allow incoming traffic from this unmanaged workload to other managed workloads.

Reject Connections

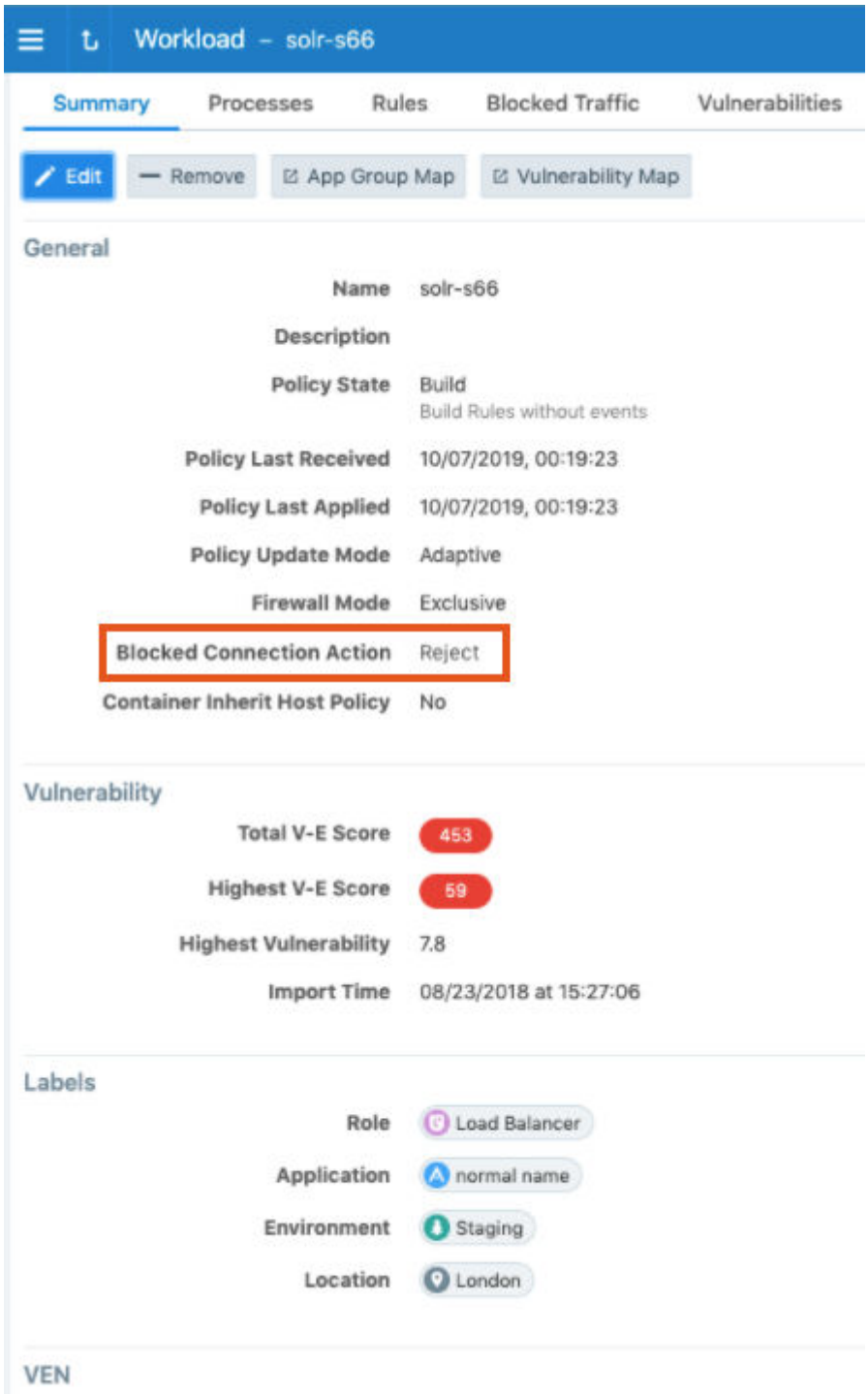
You can configure Workloads to reject traffic that does not meet the required policy, instead of blocking it in the *Enforced* state. You can edit *Reject Connections* from the **Settings > Security** menu option.



A new firewall security setting provides two options:

- Reject blocked inbound traffic: When this setting is applied, the firewall is configured to send:
  - TCP RST for TCP connections

  - ICMP port unreachable for UDP connections
  - ICMP protocol unreachable for other connections
- Drop disallowed traffic (default).
- The setting acts at the VEN level and not at the interface level. It is selected by a Label set.
- It is visible on the Workload detail page.



Create Security Policy

This section describes how to create a security policy in the Illumio Core. Creating a security policy is an iterative process. Illumio recommends creating a broad initial policy, which you can incrementally improve until you establish a sufficiently robust policy.

Segmentation Templates

Applications can be a complex set of services and processes that have different components which communicate with other applications. For example, you might find an application in your Illumination map that has many processes communicating through several ports to connect to and receive connections from Active Directory. Some of these processes, such as Netlogon, can use 10,000 or more dynamic ports as it's communicating with Active Directory. The ports that are used at any given time can be unpredictable. Creating security policy for these types of applications is a complex and time consuming endeavor.

Overview of Segmentation Templates

To deliver Segmentation Templates, Illumio leveraged our knowledge of enterprise applications, such as Active Directory, Exchange, and SharePoint, because we know the services and the different processes that these applications use.

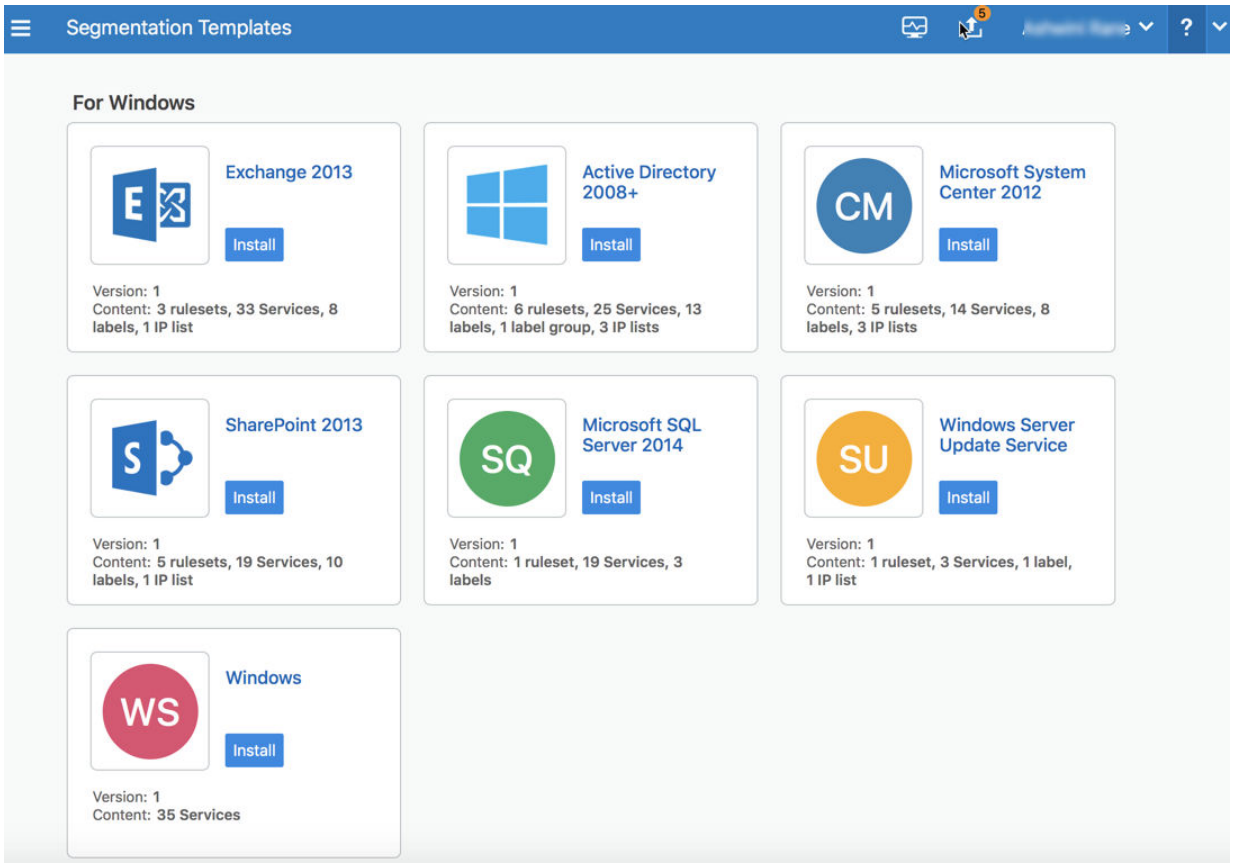
Illumio Segmentation Templates provide prepackaged, tested security policies that provide all the rules needed for common enterprise applications. They can be deployed in minutes; thereby reducing the time it takes to protect key computing assets. They simplify the definition and implementation of security policy while reducing errors and preventing security gaps for widely-used, business critical applications.

Each Segmentation Template serves two purposes. Illumio customers can see an example of how to add the security policies required to protect the application in question. Secondly, customers can use the Segmentation Template as designed to secure the application quickly in their organization.

When you install a Segmentation Template, the PCE web console automatically adds the necessary policy objects (such as services, rulesets, and labels) to allow the communication required for that application.

Catalog Retrieved from Support Portal

When you go to the Segmentation Templates page, the PCE web console automatically retrieves the latest Segmentation Templates catalog from the Illumio Support portal and displays it in the web console.



To manually locate the catalog on the Illumio Support portal:

1. From the PCE web console menu, choose **Troubleshoot** > **Segmentation Templates**.
   A dialog box appears prompting you to log into the Illumio Support portal. (While you are logged into the PCE web console, you only have to log into the Illumio Support portal once.)
2. Click **Log In** and, if prompted, enter your Illumio Support portal username and password. (Illumio Cloud customers are automatically logged into the Illumio Support portal.)

   NOTE

   Internet connectivity is not required to use the Segmentation Templates. When you are connecting to the PCE web console from a device that does not have internet connectivity, you must access the Illumio Support portal from another device that has internet connectivity and download the templates locally to that device before you can use them. See Upload a Segmentation Template [65].

   The Illumio Support portal automatically redirects you back to the Segmentation Templates page and the templates appear in the page. The templates are organized by operating system.
3. To view the contents of a Segmentation Template, click its name or icon.
   The Segmentation Template details page describes the template and lists all the policy objects that belong to the template. Policy objects appear as hyperlinks when they have already been installed by another template. (Templates can share policy objects.)

Features of Segmentation Templates

Segmentation Templates share the following key features.

Template Contents

Each Segmentation Template adds an associated group of unique, non-overlapping, predefined services, and can contain any of the following policy objects:

- Labels
- Label groups
- IP lists
- Rulesets

Some templates contain all the rulesets, services, and labels needed to secure a given application. Other templates contain port-based service definitions only.

Dynamic Processes and Ports

Using Segmentation Templates is especially useful in Microsoft environments, which must accommodate a range of dynamically used ports for RPC. Other Microsoft applications (such as Active Directory) require opening dynamic port ranges. Rather than opening only the ports in use, network-based solutions leave open an entire range of ports, effectively leaving the security environment wide open.

The Illumio PCE is service and process aware. Because of this, installing Segmentation Templates can protect against dynamic processes (like Netlogon) and add the correct policy to open only the ports that are active at a time.

Segmentation Templates are designed to use the specific processes and path used by the server rather than dynamic ports and apply the exact set of fine-grained rules required for protection.

Sharing Policy Objects

Services, labels, label groups, and IP lists can be used by more than one Segmentation Template. A ruleset, however, is never used by multiple templates.

Identifying Policy Objects Added by Templates

You can identify all objects added to the PCE that are part of Segmentation Templates. In the External Data Set field of the object's details page, the PCE identifies these policy objects by labeling them using the following convention:

IST – *type_of_object*

(Where IST stands for Illumio Segmentation Template)

Additionally, the PCE provides full names to increase readability. For example, “IST - [AD] - Client to Domain Controller” appears as “IST - Active Directory Client to Domain Controller.”

Segmentation Template Prerequisites and Limitations

Segmentation Templates are bound by the following prerequisites and limitations.

Internet Connectivity

Internet connectivity is not required to use the Segmentation Templates. For example, you might be connecting to the PCE web console from a device that does not have internet connectivity.

Illumio stores the Segmentation Templates on the Illumio Support portal. When the device from which you are connecting to the PCE web console does not have internet connectivity, you can connect to the Illumio Support portal over the internet using another device and download the Segmentation Templates locally, then upload them to the PCE web console from that device.

When you choose **Troubleshoot** > **Segmentation Templates** from the PCE web console, you are prompted to log into the Illumio Support portal to download the templates. When you do not have internet connectivity from your device and have already downloaded the templates to another device, you can skip this step.

See Catalog Retrieved from the Support Portal [60] for information.

Upgrade Policy Object Installed by Segmentation Templates

The PCE recognizes when policy objects are installed by Segmentation Templates from the values in the External Data Reference field. Therefore, if you installed a Segmentation Template prior to 17.2 or you modified the contents of this field for an object, the PCE cannot recognize that a template installed the object and you cannot update it while updating the template.

Unique Names for Labels, Label Groups, and IP Lists

In the PCE web console, the names of policy objects must be unique. For example, when you have an existing label, label group, or IP list that has the same name as a label, label group, or IP list in a template, the template installation will end and prompt you to change the name of the policy object in your organization.

NOTE

In Segmentation Templates, policy objects are named using the following convention: IST – *type_of_object*

Delete Labels Associated with Segmentation Templates

When you have provisioned a ruleset or label group associated with a template, the labels associated with the template cannot be removed until the rulesets and label groups are removed and the removal is provisioned.

About Editing Segmentation Templates

Installing a Segmentation Template adds a predefined set of services and can add labels, label groups, IP lists, and rulesets.

Editing a policy object associated with a Segmentation Template is no different from editing any other policy object in the PCE web console. Also, the display and designation of a Segmentation Template does not change in the PCE web console after you edit the policy objects associated with it.

However, before you edit the policy objects installed by a Segmentation Template, you should be aware of the following caveats.

Edit the Names or IDs of Policy Objects

The PCE assigns each policy object associated with a template an ID number, which the PCE web console displays in the Description and External Data Reference fields of the object details or Summary pages.

The PCE tracks all objects associated with Segmentation Templates by their names. In Segmentation Templates, these policy objects are named using the following convention:

IST – *type_of_object*

Changing the policy object name does not affect the PCE validation that it is installed; however, using the Illumio API to edit the External Data Reference field does affect the PCE validation that it is installed.

NOTE

Illumio strongly recommends you do not change the IDs in the External Data Reference fields.

Delete Policy Objects or Editing Their Attributes

Deleting policy objects associated with templates or editing their attributes is subject to the following caveats:

- When you remove a policy object associated with a template after the template is installed, the PCE will re-add the object when the template is updated.

  For example, you remove the common LDAP service, which is associated with a Segmentation Template. When Illumio releases an update for the template, installing that update will re-add the common LDAP ports to the PCE.
- When you edit the attributes of policy objects associated with a template (for example, edit the ports or protocols of a service, or the scope or rules of a ruleset), the PCE web

console will prompt you to specify whether to preserve or overwrite your changes when you update the template to the next version.

Install a Segmentation Template

1. Retrieve the Segmentation Template Catalog [60].
   When a template has not been installed, an **Install** button appears on the page.
2. Click **Install**.
   The end user licensing agreement (EULA) appears.
3. Accept the EULA and click **Continue**.
   Before the PCE installs the template, it checks that the policy objects required by the template don't conflict with any existing policy objects in your organization. The time that the check takes depends on the number of policy objects in your organization. When f the PCE finds any conflicts during the check, it cancels the installation and doesn't install any policy objects. You are prompted to rename the conflicting objects.
   When the check is successful, the PCE adds the included policy objects in Draft mode so that you can review or edit them before provisioning them. See Provisioning [116] for more information.
   As the policy objects are added, links to the objects appear in the template details page.

NOTE

Global policy objects—such as All Services and Any (0.0.0.0/0 and ::/0)—don't include links in the Segmentation Template details page to the objects.

Upload a Segmentation Template

Internet connectivity is not required to use the Segmentation Templates. However, Illumio stores them on the Illumio Support portal. When you are connecting to the PCE web console from a device that does not have internet connectivity, you can retrieve the templates using another device (which has internet connectivity), then manually upload then to the PCE web console so that you can install or update them.

When you download a Segmentation Template from the Illumio Support portal, you save the template locally as a JSON file.

1. Log into the Illumio Support portal with your Illumio Support username and password.
2. Click **Tools** > **Illumio Segmentation Templates**.
3. Navigate to the Segmentation Templates and download them locally.
4. Log into the PCE web console and choose **Troubleshoot** > **Segmentation Templates**.
   The Segmentation Templates dialog box appears.
5. Click **Load File**.
   A dialog box appears prompting you to specify the Segmentation Template file to upload.
6. Click **Choose File**.
   A file explorer appears.
7. Navigate to the file and click **Open**.
   The Segmentation Templates dialog box reappears.
8. Click **Load**.
   The page refreshes and a tile for the Segmentation Template appears in the page.

Update a Segmentation Template

Updating a Segmentation Template to a later version can edit or add services, rulesets, labels, label groups, or IP lists. However, updating a template never removes policy objects added by a previous version.

NOTE

Later versions of templates are fully backwards compatible with previous versions.

1. Retrieve the Segmentation Template Catalog [60].
   When a new version of a Segmentation Template is available for a template that you have installed, the template has an **Update** button.
2. Click **Update**.
   If you edited the Segmentation Template after installing it, a dialog box appears prompting you to specify how to install the new version. For example, you added a new port and protocol to a service added by the template. You can revert the template to the Illumio list of ports and protocols for that service or keep your changes.
3. If necessary, choose how to handle template changes:
   - **Overwrite:** The PCE replaces the policy objects that you edited with the version in the new template and removes the word "edited" after the ID number in the External Data Reference field.
   - **Preserve Changes:** Your changes to the policy objects added by the template are kept.

NOTE

If you have edited multiple policy objects associated with a template, you must choose whether to overwrite or preserve all your changes. You cannot overwrite some and preserve some.

The PCE updates the version numbers of all policy objects associated with the template even when the new template changes only a subset of the objects associated with the template.

NOTE

Segmentation Templates can share policy objects; therefore, a policy object can have a later version than a template it's associated with because the object was updated by another template. For example, you can have version 1 of a template installed and it includes version 2 of some policy objects.

Uninstall a Segmentation Template

1. Retrieve the Segmentation Template Catalog [60].

After you install a Segmentation template, an **Uninstall** button appears on the page.

2. Click **Uninstall**.

   When you uninstall a Segmentation Template, the PCE removes all the policy objects that are associated with that template except when an object is in use. Policy objects that are shared with other installed templates are not removed. Policy objects that are added to other policy objects are not removed. For example, you added a service associated with a template to a ruleset.

Policy Generator

The Policy Generator simplifies the Illumio policy creation process by recommending the optimal security policy for your App Groups. You can use it to accelerate security workflows and reduce the risk of human error while creating security policy.

Overview of Policy Generator

The Policy Generator uses network traffic to recommend and generate micro-segmentation policies for every workload and application, regardless of it's location. It can generate rules for applications running on physical devices, virtualized platforms, and behind network devices on-premises or deployed in the cloud.

Policy Generator supports the creation of DNS-based rules under all the wizards (intra-scope, extra-scope, and IP lists). You can edit the proposed virtual services and add wildcards.

Application owners use the Policy Generator to write the following types of rules for the applications they manage:

- Intra-scope rules
- Extra-scope rules
- Rules using IP lists.

For more information about each rule type, see Rulesets [84], Rules [96], and IP Lists [32].

For a selected App Group, the Policy Generator provides:

- A workflow to create a ruleset that controls internal and external traffic.
- A way to assess your current rule coverage, which represents the number of detected connections that are controlled by rules divided by the total number of connections.

  You can increase your rule coverage by creating rules for detected connections that are not controlled by rules. The Policy Generator proposes rules for connections that are not allowed currently by rules and displays the consolidated flow count for each new proposed rule to help ensure the maximum impact on rule coverage.

  NOTE

  The Policy Generator calculates rule coverage automatically every 24 hours or after creating a draft ruleset.

  You can rewrite rules as your datacenter needs change and the Policy Generator will show you the before and after effect of those rules.

- A way to assess your current rule coverage, which represents the number of detected connections that are controlled by rules divided by the total number of connections.
- Visualization of the traffic between roles associated with a specific application, as represented by App Groups.
- Options to select the level of granularity for new rules; see About Granularity Levels for Rules [68] for information.

The first time you use the Policy Generator for an App Group, it creates a new draft ruleset with the title of the selected App Group. When you use Policy Generator again to create additional rules, it adds them to the existing ruleset that was created by the Policy Generator. You review the proposed rules and can customize them before you save them into a draft ruleset. For Windows, the Policy Generator detects and suggests Windows process- and service-based rules accordingly. You can edit the service before saving it.

NOTE

You must provision the rules to apply them to workloads. See Provisioning [116] for more information.

When an App Group has several consumers communicating with a specific provider, the Policy Generator merges all the consumers into one rule for easy readability and better scalability.

On the Summary tab of the Ruleset page, any rulesets created with Policy Generator have the default description “Automatically generated using the Illumio Policy Generator” and the value of `illumio_policy_generator` for the External Data Set field. The value for the External Data Reference is the App Group name.

Policy Generator Prerequisites and Limitations

The Policy Generator is bound by the following prerequisites and limitations:

- You cannot add Role-level rules until Role labels have been added to all workloads in the App Group.

  When some workloads in an App Group do not have Role labels, you can still write an App Group level rule using Policy Generator to allow all the workloads to communicate with each other.
- Rule coverage is updated one App Group at a time.

About Granularity Levels for Rules

The following options allow you to select the restrictiveness of your security policy.

Intra-Scope Rules

Granularity Level	Description
App Group Level	(Also known as micro-segmentation or Ringfencing) All workloads in the App Group can communicate with each other across all services. This option is best for creating a broad initial policy that can be further refined later if needed.
Role Level - All Services	All workloads with a specific Role label can communicate with all workloads with Role labels matching the observed flows across all services. This option is useful for restricting role-to-role traffic between workloads when you have many core services that need to communicate with these workloads. When a workload is missing the Role label, the Policy Generator excludes that connection from the wizard.
Role Level - Specified Services	(Also known as nano-segmentation) All workloads with a specific Role label can communicate with all workloads with Role labels matching the observed flows across specified services, based on the collected traffic flow summaries. When a matching port/protocol cannot be located in an existing service, a new service with the necessary port/protocol is created when the proposed rules are saved. Use this option to create the most restrictive policy.

Extra-Scope and IP List Rules

Granularity Level	Description
All Services	Workloads can communicate over all services. This service policy type provides less restriction for workload communication.
Specified Services	Workloads can communicate over specified services. This service policy type provides more restriction for workload communication.

Ways to Access Policy Generator

You can access Policy Generator from the following locations in the PCE web console:

Entry Point	Description
Policy Generator	Launches the Policy Generator. You must select an App Group to begin.
App Group Map > App Group panel > Start Policy Generator	Launches the Policy Generator for the App Group selected. When you've opened a Consuming App Group and selected the App Group, the Policy Generator creates an extra-scope rule. You can proceed or add more Consuming App Groups.
Illumination > Group panel > Start Policy Generator	Launches the Policy Generator for the App Group selected. **NOTE** App Groups must be configured to use three labels to start the Policy Generator from the Illumination map.
Rulesets and Rules > Start Policy Generator	Launches the Policy Generator. You must select an App Group to begin.
Rulesets and Rules > Ruleset Details > Start Policy Generator	When a ruleset was created using the Policy Generator, the ruleset scopes and Rules tab includes a **Start Policy Generator** button. Clicking the **Start Policy Generator** button, launches the Policy Generator with the App Group selected.
Troubleshooting > Blocked Traffic > Start Policy Generator	Launches the Policy Generator. You must select an App Group to begin.
App Group Map > App Group panel > Mitigate Vulnerabilities	Launches the Policy Generator. You can update your policy to minimize the risks due to the vulnerabilities.

Create Intra-scope Rules with Policy Generator

1. From the PCE web console menu, choose **Policy Generator**.
   The Select App Group page appears. The page displays when the Policy Generator last calculated the coverage for each type of rule. Click the refresh icon to recalculate Rule coverage.
2. Select an App Group.
   See Segment Multiple App Groups with Policy Generator [76] for information about adding App Group level rules for multiple App Groups.
3. Click the **Start with Intra-Scope** button.
   The Intra-Scope Rule Configuration page appears.
4. In the Choose Intra-Scope Rule Configuration section, select a granularity level for the rules.
   See Create Intra-Scope Rules with Policy Generator [70] for a description of these rule granularity levels.
   The detected connections (including details such as provider, port/protocol, and consumer) appear in the Review All Connections section.

Rule Configuration	Connections Displayed
App Group Level	Labels, ports, and protocols in a single row
Role Level - All Services	Number of connections and associated labels
Role Level - Specified Services	Associated labels and ports/protocols

NOTE

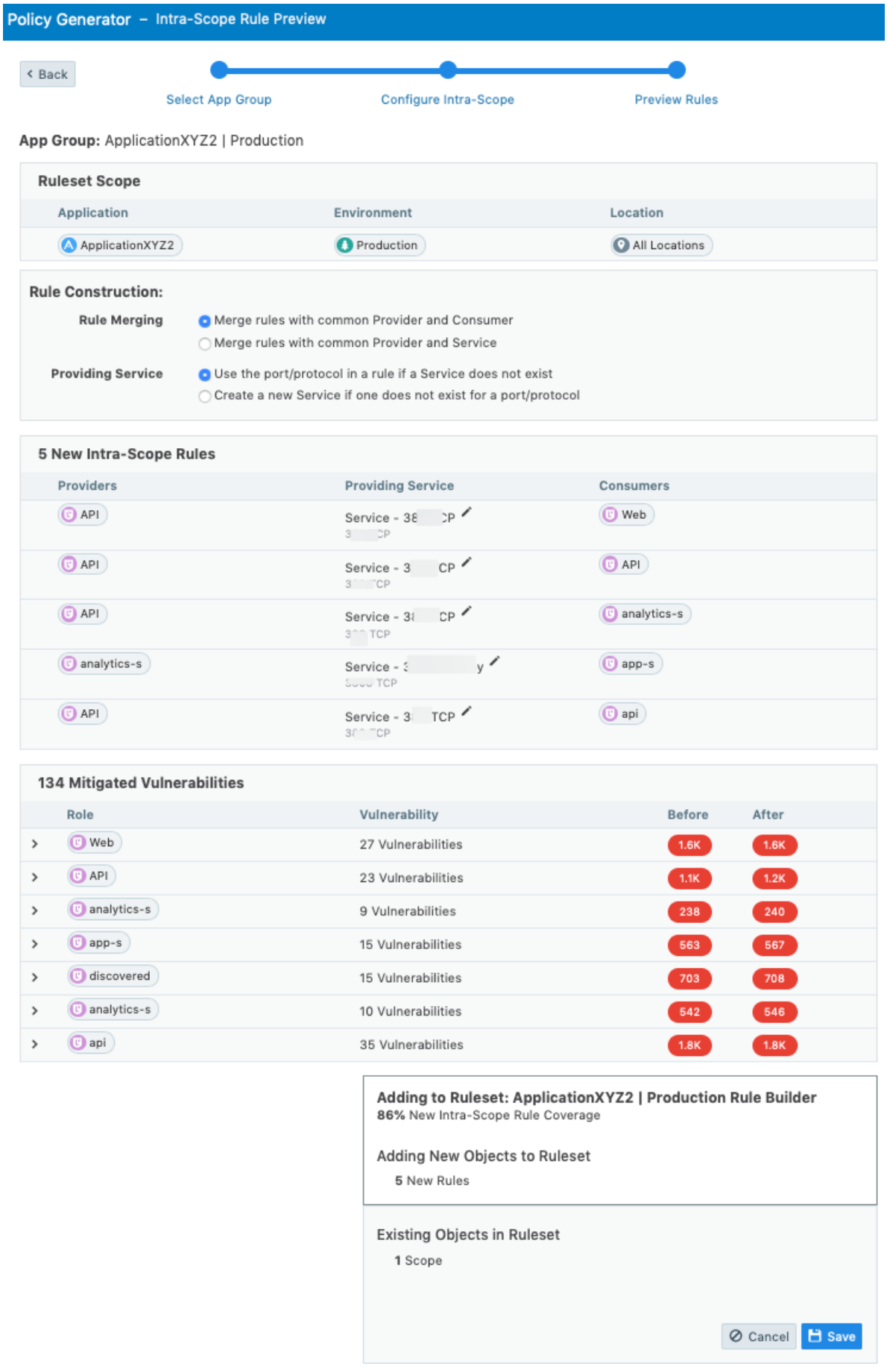
The Policy Generator displays a truncated list of ports and protocols when the App Group has more than four types of ports or protocols. To display the remaining ports or protocols in a modal window, click the **+ More** link.

5. (Optional for Role level) To exclude a connection from the proposed rules, click **Exclude**. The row is grayed out to indicate that no rules will be proposed for this connection and the amount of rule coverage decreases. To include an excluded connection, click **Include**.

NOTE

At least one connection must be included to continue.

6. Click **Next**.
   The proposed rules appear in the Preview page.


Policy Generator – Intra-Scope Rule Preview
Back
Select App Group
Configure Intra-Scope
Preview Rules
App Group: ApplicationXYZ2 | Production
Ruleset Scope
Application
Environment
Location
ApplicationXYZ2
Production
All Locations
Rule Construction:
Rule Merging
Merge rules with common Provider and Consumer
Merge rules with common Provider and Service
Providing Service
Use the port/protocol in a rule if a Service does not exist
Create a new Service if one does not exist for a port/protocol
5 New Intra-Scope Rules
Providers
Providing Service
Consumers
API
Web
API
API
analytics-s
analytics-s
app-s
API
api
134 Mitigated Vulnerabilities
Role
Vulnerability
Before
After
Web
27 Vulnerabilities
1.6K
1.6K
API
23 Vulnerabilities
1.1K
1.2K
analytics-s
9 Vulnerabilities
238
240
app-s
15 Vulnerabilities
563
567
discovered
15 Vulnerabilities
703
708
analytics-s
10 Vulnerabilities
542
546
api
35 Vulnerabilities
1.8K
1.8K
Adding to Ruleset: ApplicationXYZ2 | Production Rule Builder
86% New Intra-Scope Rule Coverage
Adding New Objects to Ruleset
5 New Rules
Existing Objects in Ruleset
1 Scope
Cancel
Save

7. (Optional) To edit the service for a rule, click the pencil icon beside a service. The Edit Service dialog box appears.

   Select a service from the drop-down list or create a new one. You can select services that have broader ranges of ports. The list includes every service that matches that port and protocol. When you've added a service that has multiple ports and protocols or ranges, they all appear in the list.

   Select **Apply Changes to all matching ports** to allow the service to be used in other rules that match that service. You are prompted to allow the Policy Generator to merge rules. To cancel the merge, reload the page and start over.

   When you create a process-based service, the connection appears like it's not covered.

   For information about creating a service, see Create a Service [25].
8. To accept the proposed rules, click **Save** and **OK**.

   The Policy Generator Successful message appears which displays the number of new rules and services. The rules are added to a draft ruleset. Click **Continue with App Group** to add extra-scope rules or rules using IP lists for the same App Group. On the last step of the Policy Generator, you can return to the App Group to add or append to the rules.

> **NOTE**
> You must provision the rules to apply them to workloads. See Provisioning [116] for more information.

Create Extra-scope Rules with Policy Generator

When you create extra-scope rules, the Policy Generator displays all traffic that originates from a different App Group and is targeted at the selected App Groups. The Policy Generator displays all App Groups that the selected App Groups communicate with. You can choose which connects to cover with rules.

1. From the PCE web console menu, choose **Policy Generator**.

   The Select App Group page appears. The page displays when the Policy Generator last calculated the coverage for each type of rule. Click the refresh icon to recalculate rule coverage.
2. Select an App Group.

   See Segment Multiple App Groups with Policy Generator [76] for information about adding App Group level rules for multiple App Groups.
3. Click the **Start with Extra-Scope** button.

   The Extra-Scope App Group Selection page appears.
4. Select one or more Consuming App Groups and click **Next**.

   For each App Group, the Policy Generator displays the current number of connections and connections covered by a rule.

> **NOTE**
> Consuming App Groups with 100% rule coverage are not displayed in the page.

   The Configure Extra-Scope page appears.
5. Select whether to configure rules by App Group or by role:
   - **App Group Level:** All workloads in the specified App Group can communicate with all workloads in the other App Groups
   - **Role Level:** Specified workloads in the App Group can communicate with specified workloads in the other App Groups

6. Select the permitted services for the rules:
   - **All Services:** Workloads can communicate over all services
   - **Specified Services:** Workloads can communicate over specified services

   See Extra-scope Rules [98] and IP Lists [32] for more information.
7. Review the connections selected for the proposed rules.

   App Groups are separated by a thick line and the organization of the connections differs depending on the selected configuration. Connection details are organized based on your selection:

Selected Configuration	Details Organized by:
App Level + Specified Services	App Group and port/protocol
App Level + All Services	App Group
Role Level + All Services	Role and App Group
Role Level + Specified Services	Role and port/protocol

8. (Optional for any configuration except App Level + All Services) To exclude a connection from the proposed rules, click **Exclude**.

   The row is grayed out to indicate that no rules will be proposed for this connection and the amount of rule coverage decreases. To include an excluded connection, click **Include**.
9. To preview the rules proposed by Policy Generator, click **Next**.

   The Extra-Scope Rule Preview page appears.
10. (Optional) To edit the service for a rule, click the pencil icon beside a service. The Edit Service dialog box appears.

    Select a service from the drop-down list or create a new one. You can select services that have broader ranges of ports. The list includes every service that matches that port and protocol. When you've added a service that has multiple ports and protocols or ranges, they all appear in the list.

    Select **Apply Changes to all matching ports** to allow the service to be used in other rules that match that service. You are prompted to allow the Policy Generator to merge rules. To cancel the merge, reload the page and start over.

    When you create a process-based service, the connection appears like it's not covered.

    For information about creating a service, see Create a Service [25].
11. To accept the proposed rules, click **Save** and **OK**.

    The Policy Generator Successful message appears, which displays the number of new rules and services. The rules are added to a draft ruleset. Click **Continue with App Group** to add intra-scope rules or rules using IP lists for the same App Group.

NOTE

You must provision the rules to apply them to workloads. See Provisioning [116] for more information.

Create Rules Using IP Lists with Policy Generator

Policy Generator creates rules that use IP lists as intra-scope rules.

When using IP lists to create rules, the Policy Generator defines a connection as a role on a port and protocol to an IP address. For example, when you have five IP addresses that are included in an IP list, the Policy Generator displays five connections.

1. From the PCE web console menu, choose **Policy Generator**.
   The Select App Group page appears. The page displays when the Policy Generator last calculated the coverage for each type of rule. Click the refresh icon to recalculate rule coverage.
2. Select an App Group.
   See Segment Multiple App Groups with Policy Generator [76] for information about adding App Group level rules for multiple App Groups.
3. Click the **Start with IP Lists** button.
   The IP List Selection page appears.
4. Select the IP lists for which you want to write rules and click **Next**.
   The Configure IP List page appears.

TIP

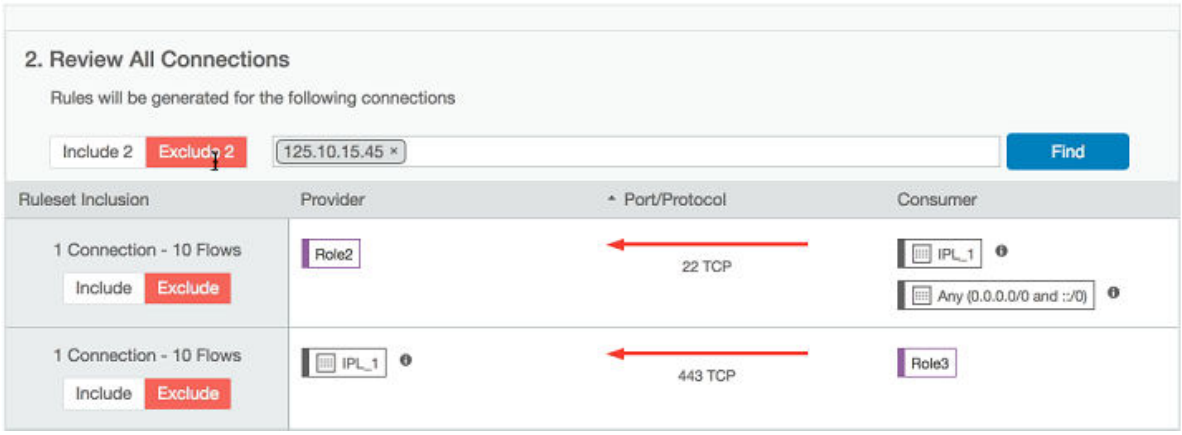
- To view the IP addresses configured in a list (not the IP addresses in the traffic), expand an IP list by clicking the arrow icon in the Name column.
- To write rules covering all connections, select the Any IP list. This list covers all connections because it includes all the IP addresses.
- Each IP address can be part of more than one IP list and you can choose which list to write your rules to.
- When you choose overlapping IP lists, you can write overlapping rules. When an IP address is in more than one IP lists, the rule is going to be in all those IP lists.
- You can write rules for inbound and outbound connections, or both. For example, you can write permissive rules for outbound traffic, and specific rules for inbound traffic.

5. Select whether to configure rules by App Group or by role:
   - **App Group Level:** All workloads in the specified App Group can communicate with all workloads in the other App Groups
   - **Role Level:** Specified workloads in the App Group can communicate with specified workloads in the other App Groups
6. Select the permitted services for the rules:
   - **All Services:** Workloads can communicate over all services
   - **Specified Services:** Workloads can communicate over specified services

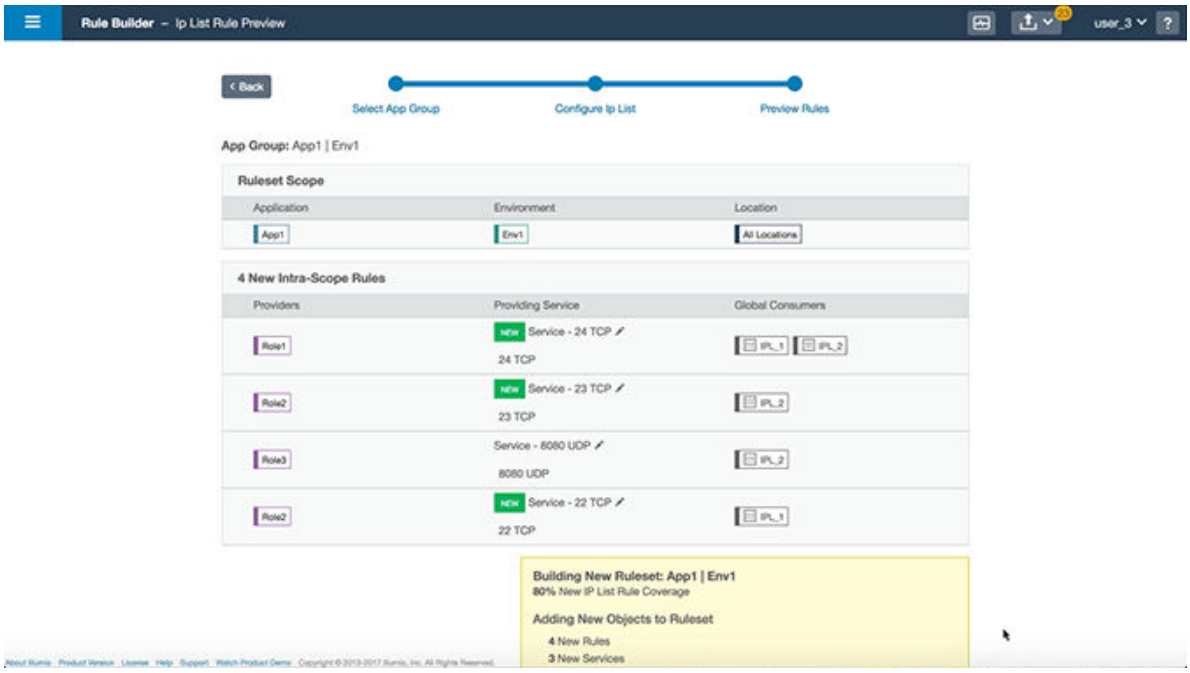
   It writes a rule for anything that those IP lists applied to.

TIP

- To display the IP addresses of the traffic for each port and protocol, hover over the info (i) icon in the Consumer column.
- To filter connections by the IP address of the traffic, port number, protocol, role, and label, use the search field above the list of connections. You can use the search field to find and exclude specific traffic.
- To quickly include or exclude all traffic, use the **Include** and **Exclude** buttons by the search field. You can exclude all traffic, then selectively include specific connections.



7. To preview the rules proposed by Policy Generator, click **Next**.
   The IP List Rule Preview page appears.



8. (Optional) To edit the service for a rule, click the pencil icon beside a service. The Edit Service dialog box appears.
   Select a service from the drop-down list or create a new one. You can select services that have broader ranges of ports. The list includes every service that matches that port and protocol. When you've added a service that has multiple ports and protocols or ranges, they all appear in the list.
   Select **Apply Changes to all matching ports** to allow the service to be used in other rules that match that service. You are prompted to allow the Policy Generator to merge rules. To cancel the merge, reload the page and start over.
   When you create a process-based service, the connection will appear like it's not covered.
   For information about creating a service, see Create a Service [25].
9. To accept the proposed rules, click **Save** and **OK**.
   The Policy Generator Successful message appears, which displays the number of new rules and services. The rules are added to a draft ruleset.

Segment Multiple App Groups with Policy Generator

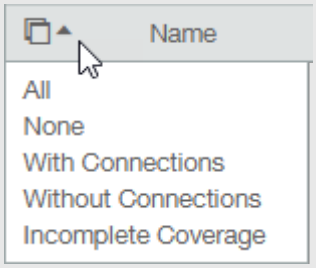
You can apply nano-segmentation (also known as ringfencing) on multiple App Groups using the Policy Generator. Nano-segmenting App Groups allows all workloads to communicate across all services within each App Group.

When segmenting App Groups, the Policy Generator creates one ruleset per App Group. The ruleset includes a rule that covers traffic for all workloads to all workloads on all services.

1. From the PCE web console menu, choose **Policy Generator**.
   The Select App Group page appears. The page displays when the Policy Generator last calculated the coverage for each type of Rule. Click the refresh icon to recalculate rule coverage.
2. In the Select App Group down-down menu, select **Segment Multiple App Groups** from the bottom of the list.
   The Choose App Groups page appears.
3. Select the App Groups to segment and click **Next**.

TIP

- To recalculate rule coverage for an App Group, hover over the Last Calculated column and click the refresh icon. The column displays the time that the rule coverage was calculated.
  The column indicates whether the ruleset for the group has been edited since the last calculation and triggers you to recalculate it.
- To quickly select App Groups using different criteria, click the arrow icon to the right of the Name column:



- The Choose App Groups page displays all your App Groups regardless of their percentage of rule coverage or whether they have connections. For example, the page displays App Groups that have 100% rule coverage and groups with zero connections.

4. To accept the proposed rules, click **Save** and **OK**.
   The Policy Generator Successful message appears, which displays the number of new rules. The rules are added to a draft ruleset.

Core Services Detector

Core services (such as DNS, Domain Controller, NTP, and LDAP) are essential to your computing environment and run on one or multiple workloads. The Core Service Detector feature helps you identify these core services and suggests an appropriate label for them. The Illumio PCE can detect 51 core services. Identifying and labeling these workloads is important because they are centrally connected, and other applications depend on them.

Application owners sometimes don't know enough about the core services or how to identify them. In addition, different teams could be managing core services, and application owners must coordinate with these teams to secure their applications. When you use the Core Services Detector to label and write policies for core services, you can save time on application policies and progress to policy enforcement faster.

NOTE

In a Supercluster, the Core Services Detector is available only on the leader PCE.

For information about using the REST API to manage core services, see the REST API for managing Core Services in REST API Developer Guide.

Enabling Core Services Detection

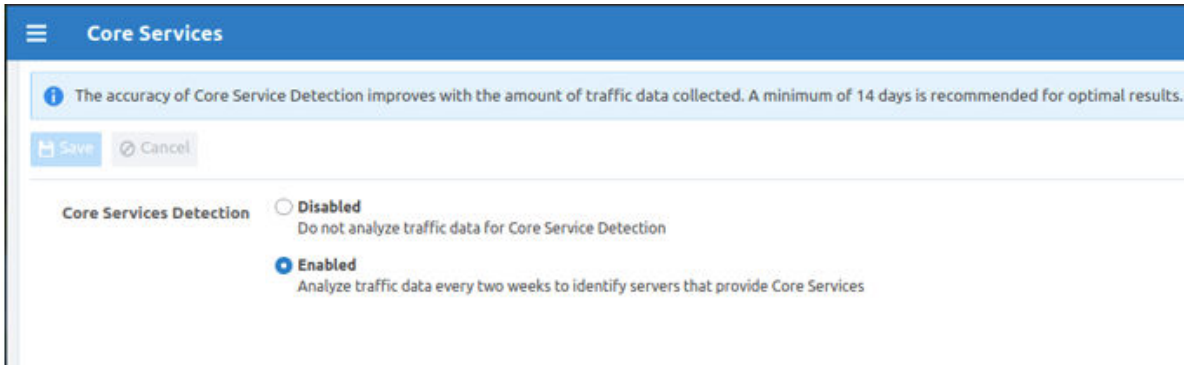
The Core Services Detector is not enabled by default because it is an optional feature. Organizations that have already done extensive work with labeling their core services might not be interested in this feature.

IMPORTANT

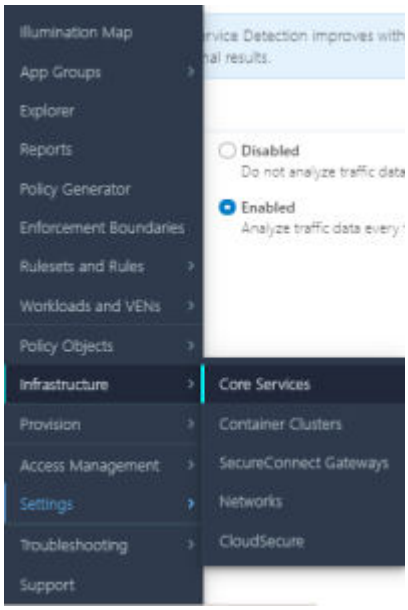
To enable Core Services detection, you must be an Illumio Org Administrator.

To enabled this feature, follow these steps:

1. To obtain access to the Core Services feature in the PCE, update the value for the following parameter in the PCE `runtime_env.yml` file: `core_services_enabled: true`
2. Log into the PCE web console and choose **Settings** > **Core Services**. The setting for the Core Services feature appears.
3. Select **Enabled**.



The **Core Services** menu option will now appear in the PCE web console main menu under **Infrastructure** and you can use the Illumio REST API to manage Core Services.



Workflow for Managing Core Services

Core Services Detector uses a three-step process to identify and manage core services:

1. **Detect:** The detection tool runs in the backend to recommend potential core services (workloads running core services).
2. **Review:** Review recommendations provided by the detection tool and accept or reject them.
3. **Label:** Label accepted recommendations for core services.

Detection Methods

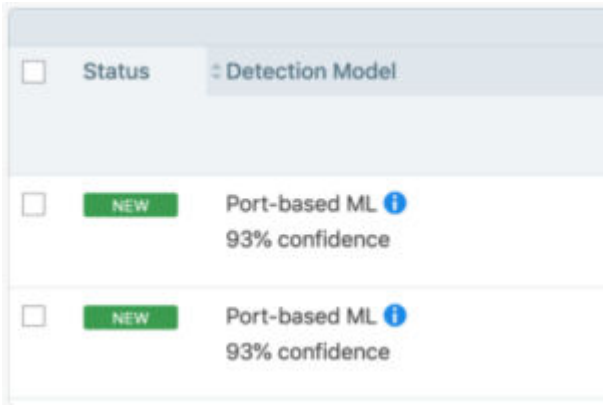
The PCE uses three methods to detect core services:

- **Port Matching:** Rule-based model based on connections to specific ports.
- **Port-based ML:** Machine learning model based on connections to specific ports.
- **Process-based ML:** Machine learning model based on processes running on the server.

NOTE

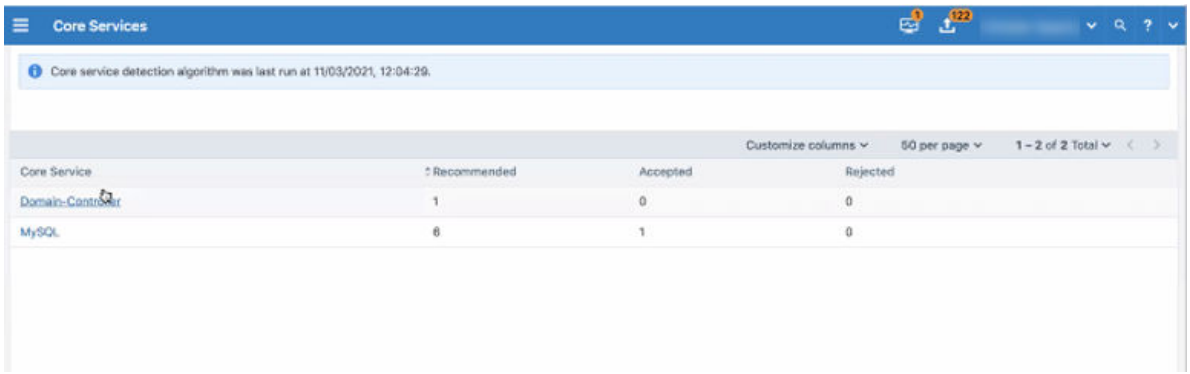
- The method that the PCE uses to detect a core service is not configurable.
- All three algorithms run all the time.
- The core services detection for Microsoft Active Directory uses the machine learning (ML) model.

Example showing how the PCE web console indicates the detection method:

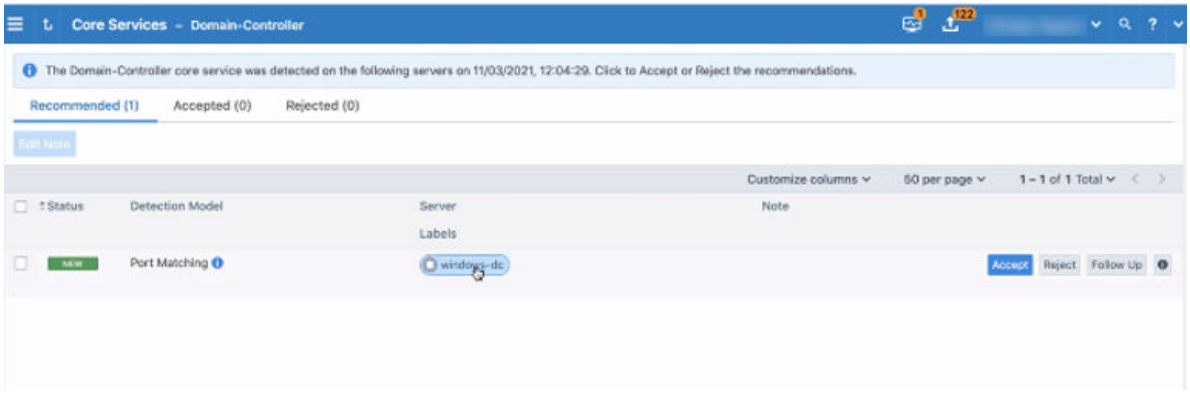


Identify and Review a Core Service

1. From the PCE web console main menu, choose **Infrastructure** > **Core Services**.
   The landing page for core services shows all services detected by the detection tool during the last run.
   It also tabulates the workloads that are recommended as running that particular core service along with the ones previously accepted or rejected for that service.

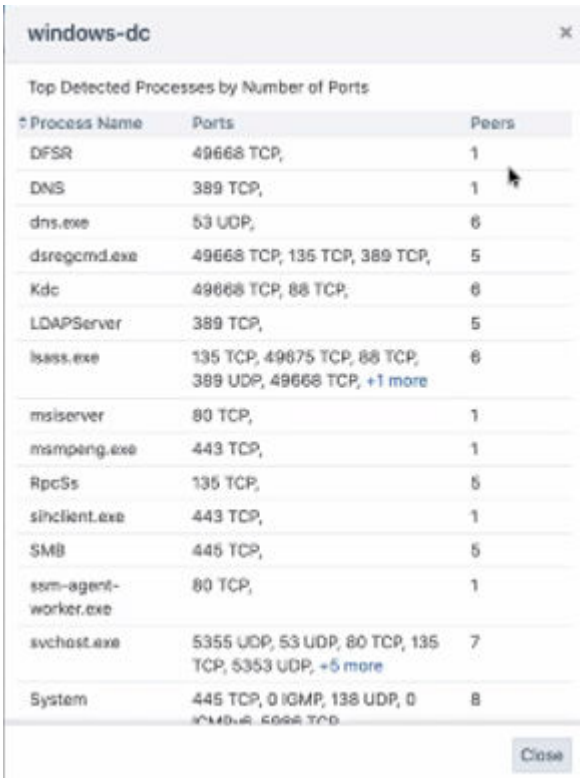


2. Click the link for any of the listed core services. The page refreshes and displays detailed status for that service.

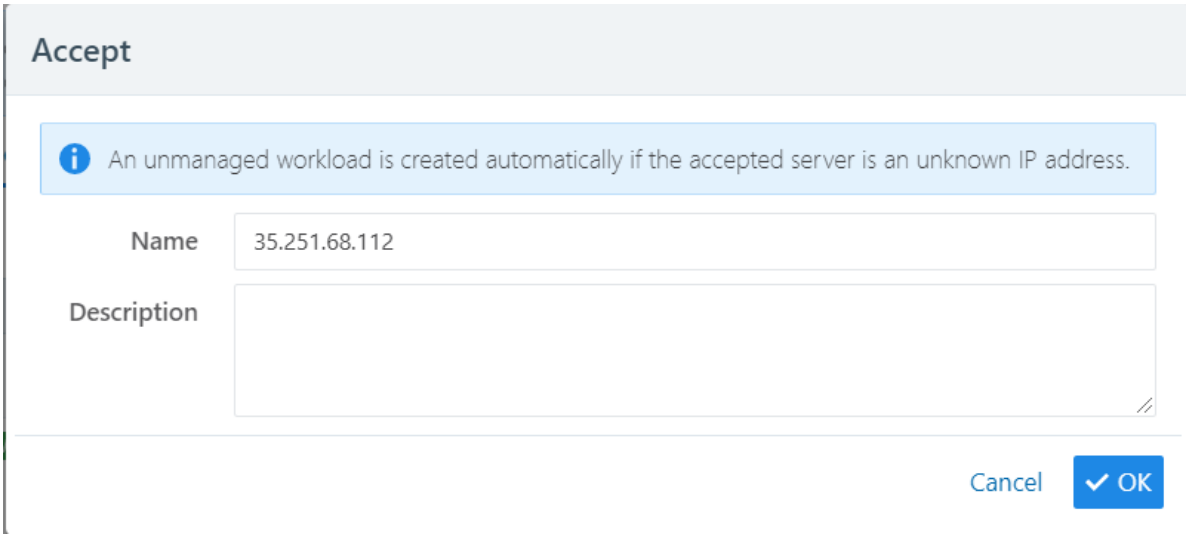


   The details page for a core service provides the following information:
   - **Status:** Shows whether the recommendation is new.
   - **Detection Model:** Indicates with method the PCE used to detect the service.
   - **Server:** Displays the IP addresses and workloads recommended for that particular core service. The column includes either a defined workload or an unknown IP address.
   - **Labels:** For a defined workload, displays the existing labels.

   To see the following details about the service in a pop-up dialog box, click either the detection method or the value in the **Server** column.

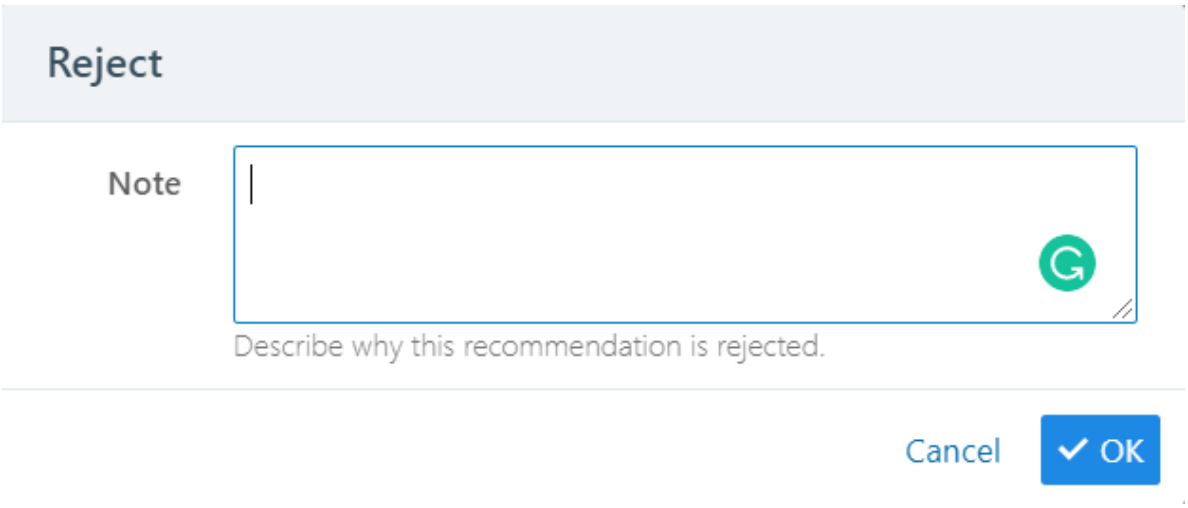


3. Accept or reject the core service by clicking the buttons on the right.
   Accept: If the core service is from an unknown IP address, clicking **Accept** creates an unmanaged workload:



NOTE
Illumio encourages customers to create unmanaged workloads, install VENs on the unmanaged workloads so that they become managed, and then label them to allow enforcement.

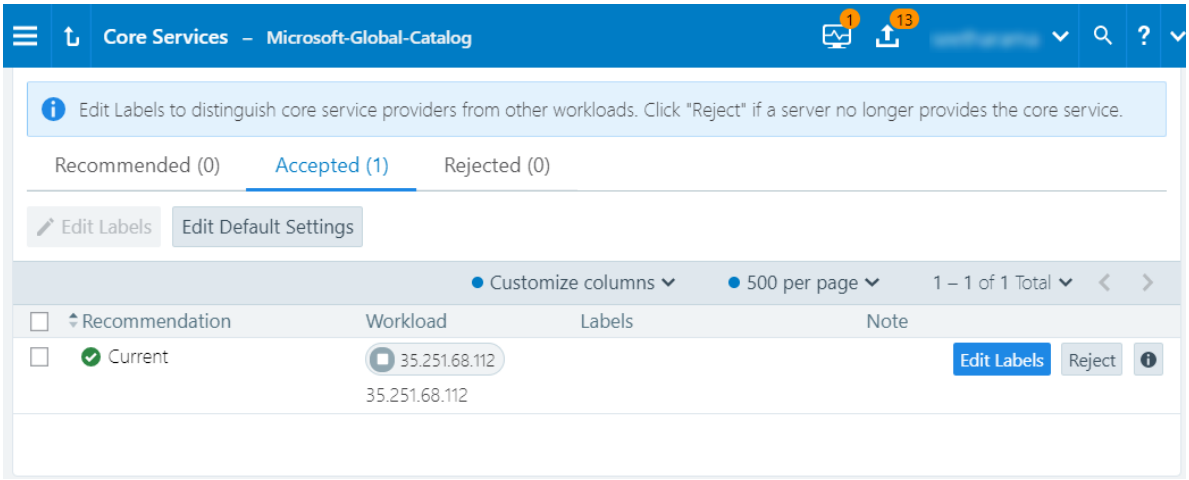
Reject: When you reject the recommendation, that IP address is no longer recommended as a provider of the detected core service.



Follow Up: If you are unsure whether to accept the recommendation, leave a note about your reasons to help in later decision-making.

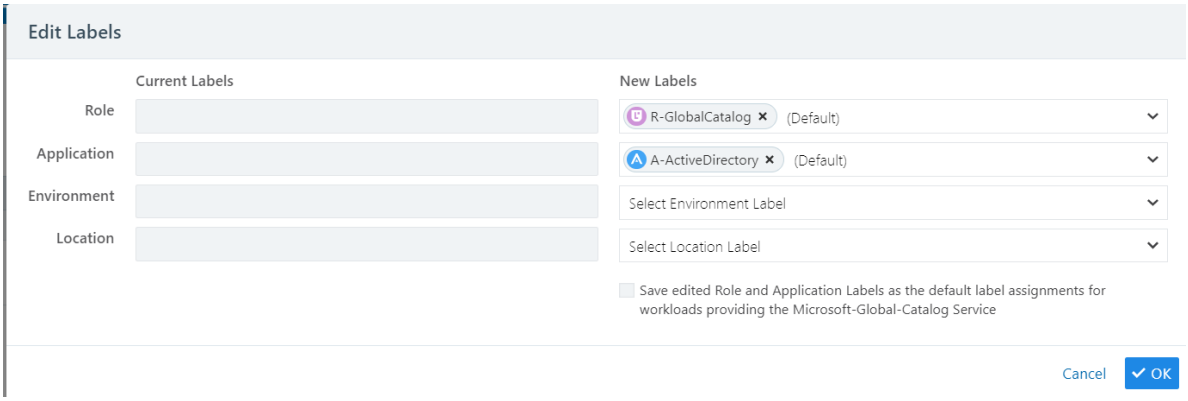
Label the Detected Core Services

1. Once you have accepted a recommendation to label a service, select the **Accepted** tab the Core Services page.



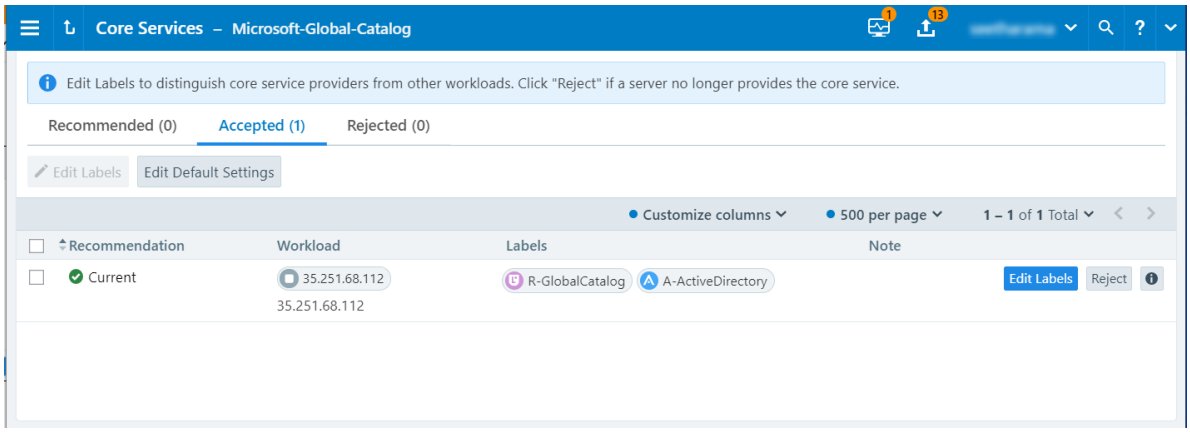
Each service type has its own recommended label.

2. Click **Edit Labels** to see what the current labels are. The **Edit Labels** screen shows the current labels on the left and the recommended label on the right. The types of labels shown include Role, Application, Environment, Location, and any custom label types you have defined using flexible labels.



3. Click **OK** to accept the recommended labeling.

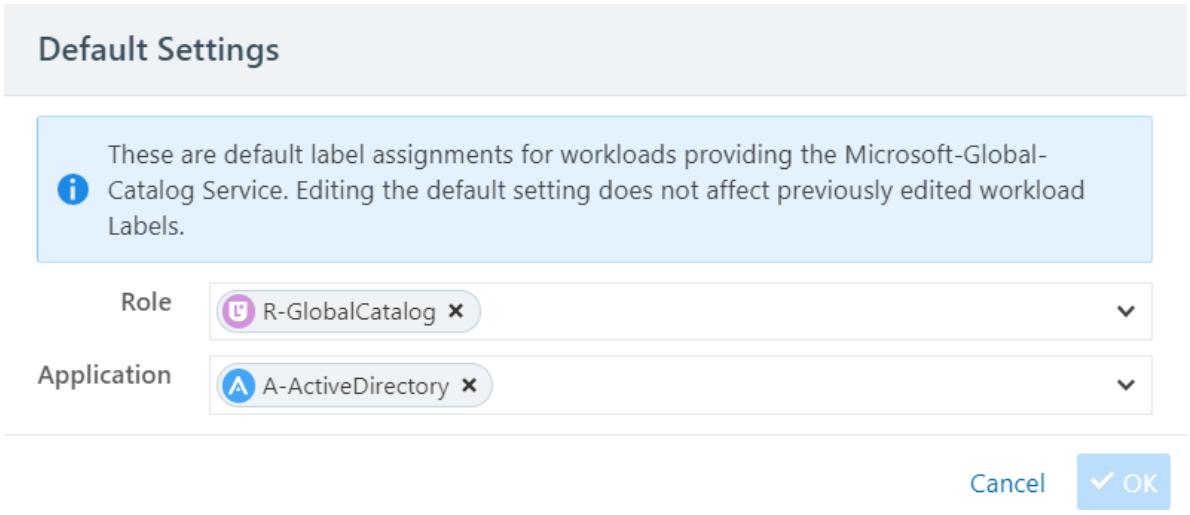
The page refreshes and displays the labels added for the core service.



4. When required for your network environment, change the default labels by selecting the **Edit Default Settings** button and modifying the labels as necessary.

IMPORTANT

To change the default label assignments, you must be an Illumio Org Administrator.



NOTE

Changing the default label assignment does not change any of the previously edited workload labels.

Scanner Detection

Starting in Illumio Core 22.4, scanners running in a network can be automatically detected, much as services are detected.

IMPORTANT

Scanner detection by default is not enabled. You must manually enable scanner detection at the Core Services page. After being enabled, scanner detection runs every 24 hours to detect scanner traffic.

After a scanner is detected, the src_port can be used to create a collector-side traffic filter, so that traffic originating from that src_port will be dropped and not stored in the PCE.

Rulesets

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

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

NOTE

In previous releases, this feature was referred to as "Segmentation Rulesets." In Illumio Core 21.5.0 and later releases, this feature is referred to as "Rulesets." Some images might still display the previous feature name.

Basic versus Scoped Rulesets

You have the option to create basic or scoped rulesets. You can choose whether you want to include scopes when creating new rulesets. The **Scope** field appears in the **Add Ruleset** dialog box only when the PCE is configured to display scopes in rulesets. When the PCE is configured to create scopeless rulesets, you create simple rules that do not apply to specific environments, locations, applications, or other categories you may have defined using flexible label types. These rules are scopeless rules because they do not belong to a ruleset that uses scopes.

You might want to create these basic rules when you are new to using Illumio Core and you are creating your first security policy rules. For example, you might want to create a simple rule to control SSH traffic for all your workloads. As you become more familiar with Illumio Core or you need to create more complicated rules, you can choose to create scoped rules; namely intra-scope, extra-scope, and custom iptables rules. Creating scoped rules allows you to create rulesets and rules that are defined for specific environments, locations, applications (typically larger environments), or other categories you define in flexible label types.

When the PCE is configured to create scopeless rulesets, you can still add a scope to a ruleset after saving the ruleset. From the **Ruleset Actions** menu at the top right corner of the **Ruleset** page, select **Add Scope**.

For more information about rulesets, see also Rule Writing [106] in this guide.

NOTE

The ability to create scoped rules is only enabled when the PCE is configured to display scopes.

Behavior of Scopeless Rulesets in PCE Web Console

The following details apply to scopeless rulesets in the PCE web console:

- A option in the Policy Settings page determines whether new rulesets are created with or without scopes. However, the permission every Illumio Core user has to create rulesets is always based on the scopes they have access to even when the PCE is configured to create scopeless rulesets. Stated another way, disabling scopes in rulesets does not invalidate the Ruleset Manager or Ruleset Provisioner roles used for user authentication (also known as role-based access control). For more information about these roles, see "Role-Based Access Control" in PCE Administration Guide.
- When the PCE is configured to create scopeless rules, the Ruleset details page for a ruleset displays a single **Rules** tab where you add basic rules, including container hosts as consumers.
- When you add a scope to a scopeless ruleset after creating the ruleset, the page refreshes and displays **Intra-scope Rules** and **Extra-scope Rules** tabs. If any rules include container hosts for consumers, those rules are moved to the **Extra-scope Rules** tab.
- Adding custom iptables rules is not available for scopeless rulesets. To create custom iptables rules, you must add a scope to the ruleset.
- When you remove all scopes from a ruleset, the PCE merges the rules in the **Intra-scope Rules** and **Extra-scope Rules** tabs into a single **Rules** tab. However, any custom iptables rules created in the ruleset remain in the **Custom Iptable Rules** tab.

Ruleset Scope

NOTE

The Scope field only appears when the PCE is configured to display it.

The scope of a ruleset determines which workloads receive the ruleset's rules and enables the rules in a ruleset to apply to workloads in a group (one scope).

When workloads share the same set of labels defined in a ruleset's scope, those workloads receive all the rules from the ruleset. When you add a second scope, all the workloads within both scopes receive the rules from the ruleset.

A single scope is defined by using labels that identify the workload:

- **Application:** To what application (for example, ERP or HRM) do these workloads belong?
- **Environment:** Which type of environment (for example, development, production, or testing) describes these workloads?

- **Location:** Where are these workloads located—either physically (for example, rack server or AWS) or geographically (for example, US, EU, or CA)?
- **Flexible labels:** If you have defined custom label types, you can use them to define a scope.

NOTE

The Role label should not be used in the scope.

For example, a scope (or collection of workloads that the rules are applied to) is defined as ERP | Prod | US, which means that the rules apply to any workload that meets the following three requirements:

- Workloads in the ERP application
- Workloads in the Prod (Production) environment
- Workloads in the US location

That example is relatively simple, but combining rules and scopes can be used to create complex security policies.

For example, the following ruleset (scope + rules):

Scope		
App	**Environment**	**Location**
HRM	Prod	US
Rules		
Source	**Destination**	**Service**
Processing	DB	MySQL
Web	Processing	Tomcat
Corp-HQ	Web	Apache

Allows the following communication:

- Processing | HRM | Prod | US → DB | HRM | Prod | US
- Web | HRM | Prod | US → Processing | HRM | Pod | US

• Corp-HQ | HRM | Prod | US → Web | HRM | Prod | US

Single Ruleset Scopes

Using a single scope in a ruleset narrows the list of workloads that the rules apply to and allows workload cross-communication.

When you are defining rules, you have the option of using the “All” label in the scope. The “All” label applies to all instances of that label type (Application, Environment, Location, or a flexible label type that you have defined). For example, creating a rule with a scope of “All | All | All” means that the rule applies to all workloads.

When you create a rule with a scope of “HRM | All | US,” this rule applies only to workloads using the HRM and US labels, regardless of Environment (“All”). For example, the following ruleset:

Scope		
App	**Environment**	**Location**
HRM	(unspecified)	US
Rule		
Source	**Destination**	**Service**
Processing	DB	MySQL

Means “The HRM application in the US can initiate communications between Processing and DB in any environment” and allows the following communication:

NOTE

(1) Assume below that “Dev” and “Prod” are types of Environment labels.

(2) When no label is specified in the scope for a given dimension, any label for that dimension is within the scope.

• Processing | HRM | (Env label unspecified) | US | → DB | HRM | Anything | US

- or -

- Processing | HRM | Dev | US | → DB | HRM | Dev | US
- Processing | HRM | Prod | US | → DB | HRM | Dev | US
- Processing | HRM | Dev | US | → DB | HRM | Prod | US
- Processing | HRM | Prod | US | → DB | HRM | Prod | US

Multiple Ruleset Scopes

NOTE

The Scope field only appears when the PCE is configured to display it.

Using multiple scopes in a ruleset applies the rules to each scope in isolation and does not allow workload cross-communication.

For example, consider the following ruleset:

Scope		
App	**Environment**	**Location**
HRM	Prod	US
HRM	DEV	US
Rule		
Source	**Destination**	**Service**
Processing	DB	MySQL

This rule and scope state:

“Workloads using the HRM application in the Prod environment in the US can initiate communications between Processing and the DB."

And

"Workloads using the HRM application in the Dev environment in the US can initiate communications between the Processing and the DB.”

The rule and scope **do not** state:

"Workloads using the HRM application in the Prod and Dev environments in the US can initiate communications between the Processing and the DB."

This example **does** allow the following communication:

- Processing | HRM | Prod | US → DB | HRM | Prod | US

And

- Processing | HRM | Dev | US → DB |HRM | Dev | US

But **not**

- Processing | HRM | Prod | US → DB |HRM | Dev | US

Combine Labels in Scopes and Rules

NOTE

The Scope field only appears when the PCE is configured to display it.

When the same type of label is used multiple times in a rule, they are expanded as multiple rules with one label for each rule.

The following examples further demonstrate how scopes work with rules.

The following ruleset:

Scope		
App	**Environment**	**Location**
HRM	(unspecified)	US
Rules		
Source	**Destination**	**Service**
Dev	Prod	MySQL
DB	DB	MySQL

IMPORTANT

When no label is specified in the scope for a given dimension, any label for that dimension is within the scope.

Means:

"Allow the database used by the HRM application in the Dev environment to communicate with the database used by the HRM application in the Prod environment"

and allows the following communication:

DB | HRM | Dev | US → DB | HRM | Prod| US

The following ruleset:

Scope		
App	**Environment**	**Location**
(unspecified)	(unspecified)	US
Rules		
Source	**Destination**	**Service**
ERP	HRM	MySQL
Dev	Prod	MySQL
DB	DB	MySQL

IMPORTANT

When no label is specified in the scope for a given dimension, any label for that dimension is within the scope.

Means:

“Allow the database used by the ERP application in the Dev environment located in the US to communicate with the database used by the HRM application in the Dev environment located in the US”

And allows the following communication:

DB | ERP | Dev | US → DB | HRM | Dev | US

The following ruleset:

Scope		
App	**Environment**	**Location**
(unspecified)	Dev	US
(unspecified)	Prod	EU
Rules		
Source	**Destination**	**Service**
ERP	HRM	MySQL
DB	DB	MySQL

IMPORTANT

When no label is specified in the scope for a given dimension, any label for that dimension is within the scope.

Allows the following communication:

- ERP | (App label unspecified) | Dev | US → HRM | All | Dev | US
- ERP | (App label unspecified) | Prod | US → HRM | All | Prod | US
- DB | (App label unspecified) | Dev | US → DB | All | Dev | US
- DB | (App label unspecified) | Prod | US → DB | All | Prod | US

NOTE
When the service in a rule is DNS, the consumer must be an IP List.

Enable or Disable Scopes for Rulesets

In Illumio Core 22.2.0 and later releases, you can control whether rulesets use a scope.

The *Scope* field appears in the **Add Ruleset** dialog box only when the PCE is configured to display scopes in rulesets.

IMPORTANT
You must have Global Administrator access to the PCE to manage PCE settings and configuration.

To globally enable or disable scopes in the PCE:

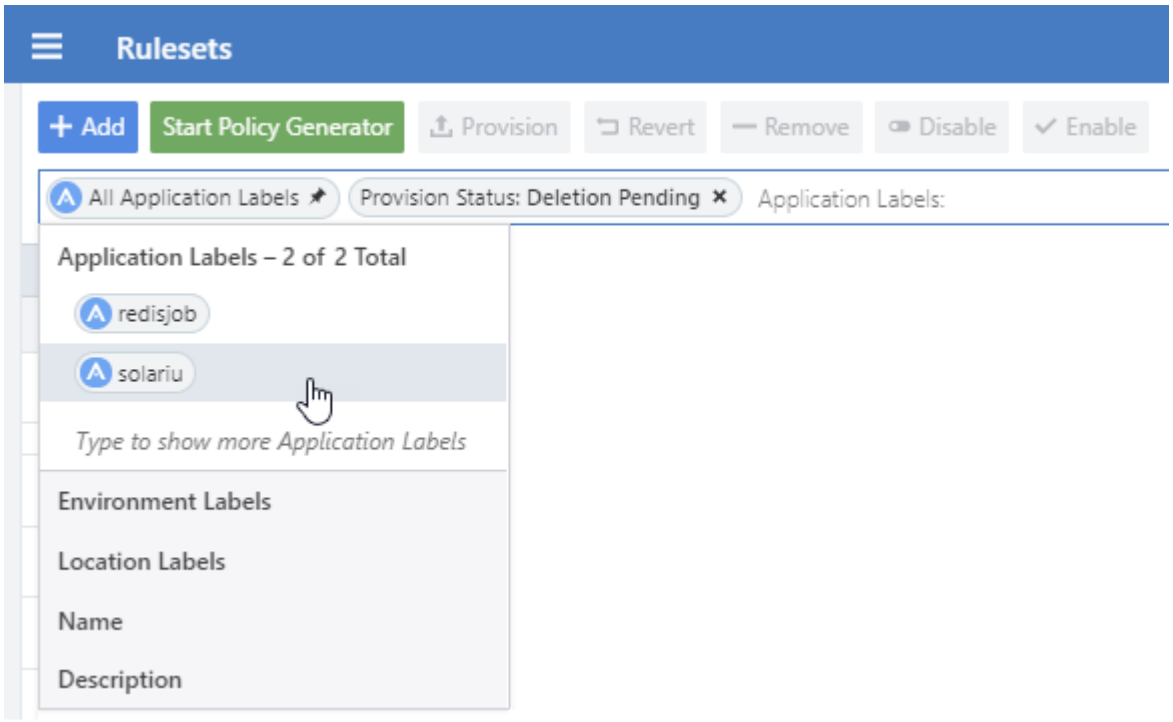
1. From the PCE web console main menu, choose **Settings** > **Policy Settings**.
2. Click **Edit**.
   The page becomes editable.
3. In the *Scopes in Rulesets* section, toggle between **Yes** and **No** for the Display Scopes in Rulesets value depending on whether you want to enable scoped rulesets in the PCE.
4. Click **Save**.

Ruleset Status

You can view the ruleset status on the Ruleset page. The current status of each ruleset (enabled or disabled) is displayed in the Status column. When you change a ruleset but have not yet provisioned the change, the type of change (addition, deletion, or modification) appears in the Provision Status column with the word “Pending” to indicate that these changes must be provisioned to be applied.

Filter the Rulesets List

You can filter the rulesets list using the label and property filter at the top of the list. You can filter the list by entering a label type to show only those rulesets that use the selected labels. You can further filter the list by selecting specific properties of the rulesets. For example, you can filter the list by provision status, such as rulesets that are in draft state and have not yet been provisioned.



Create a Ruleset

NOTE

This procedure provides the steps to create a ruleset when scoped rulesets are enabled for the PCE. If scoped rulesets are disabled for the PCE, you can always add a scope after creating the ruleset.

You can create a ruleset to write rules that define the allowed communication between workloads in a single group or multiple groups. See "Groups in Illumination" in Visualization Guide.

When you write a rule for a Windows workload, you can add a Windows service name without specifying a port or protocol and the rule will allow communication for that service over *any* port and protocol.

The following task creates a single scope, which means the rules in the ruleset apply to a single group. To apply the rules to another group, add a second scope, which is indicated by the group's labels.

To create a ruleset:

1. From the PCE web console menu, choose **Rulesets and Rules > Rulesets**.
   The Rulesets page appears.
2. Click **Add**.

3. Enter a name for the ruleset.
4. Select the labels for the ruleset: Application, Environment, Location, or any custom label types you have defined using Flexible Labels.

   These labels define the scope for your ruleset, which is the range or boundary of your ruleset. The scope defines the workloads affected by this ruleset, which is all workloads that share the same labels in the scope.

   NOTE

   The Scope field only appears when the PCE is configured to display it.

5. Click **Save**.

Now that the ruleset is created, you can add rules to define your security policy. See Rules for information about the types of rules you can add.

NOTE

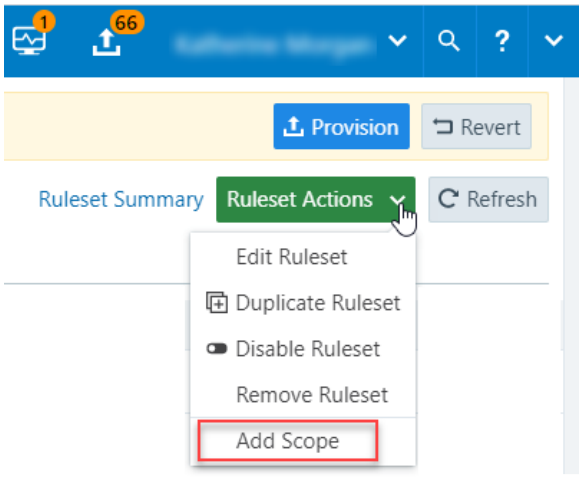
Illumio recommends creating no more than 500 rules per ruleset, or the PCE web console will not be able to display all of the rules.

If you want to create a ruleset with more than 500 rules, Illumio recommends splitting the rules across multiple rulesets or using the Illumio Core REST API, where there is no limit on the number of rules you can create per ruleset.

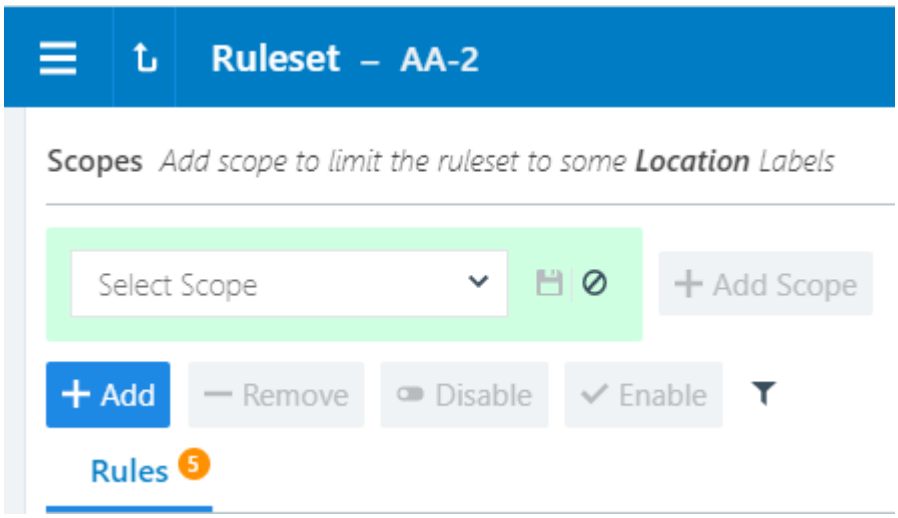
Add a Scope to a Scopeless Ruleset

When the PCE is configured to create scopeless rulesets, you can still add a scope to an existing ruleset.

1. In the Ruleset details page, select **Add Scope** from the **Ruleset Actions** menu at the top right corner of the page.



   The page refreshes and displays a drop-down list to select an existing scope.



2. Open the **Select Scope** list and select the labels you want to include for the ruleset scope.
3. When done selecting labels, click the **Save** icon.
   The page refreshes and the new scope appears at the top of the page.

Create a Ruleset with Multiple Scopes

NOTE
The Scope field only appears when the PCE is configured to display it.

You can create rulesets with multiple scopes to define the allowed communication between workloads in one or more groups. See "Groups in Illumination" in the Visualization Guide for information.

How you define the scope in a ruleset enables you to write rules for workloads in multiple groups (two or more scopes). Each scope corresponds to one group. The scope defines the boundaries of the rules in the ruleset.

To create a multi-scope ruleset:

1. From the PCE web console menu, choose **Rulesets and Rules > Rulesets**.
   The Rulesets list page appears.
2. Click **Add**.
3. Enter a name for the ruleset.
4. In the Scope section, set the labels that define the scope by selecting the them from the drop-down lists. You can use Application, Environment, Location, or any custom label types you have defined using flexible labels.
5. After you select the labels, click **Save**.
   The page refreshes and the Scopes and Rules tab appears.

NOTE
To edit the Scope, click the Edit button .

6. To add another scope, click the Add icon (+).
   A new row appears in the scopes section.
7. Set the labels for the new scope and click the Save icon at the end of the row.

The green Addition Pending icon shows that this addition is pending, so you need to provision the new ruleset in order for the rule to take effect. See Provisioning [116] for more information.

NOTE
This task contains the steps to define multiple-scopes in the ruleset. For information about rules to the ruleset, see Rules [96].

Duplicate a Ruleset

When you have a ruleset that you want to use to create other new rulesets, you can duplicate an existing ruleset.

1. From the PCE web console menu, choose **Rulesets and Rules > Rulesets**.
   The Ruleset list page appears.
2. Click the **Scopes and Rules** tab, and then click **Duplicate Ruleset**.
   The Duplicate Ruleset page appears.
3. Rename the copy of the ruleset.

NOTE
The default name is “Copy of [Ruleset Name]” (where [Ruleset Name] is the name of the original Ruleset).

4. Click **Save**.

After saving the new duplicate ruleset, make any needed scope or rule changes and then provision to apply them. See Provisioning [116] for more information.

Rules

Rules can allow communication between multiple applications or entities in different scopes or the same scope. To write a rule, you need to define three things: A service, a Source of the service, and a Destination for the service. You also need to select the type of rule:

- **Intra-scope rule:** Allow communication within a group. The ruleset scope applies to both Sources and Destinations.
- **Extra-scope rules:** Allow communication between groups.
- **Custom iptables rules:** Allows custom iptables configurations in a ruleset. These rules are managed by the PCE and applied on each managed Linux workload VEN that matches the labels for the scope and receivers.

About Rules

Illumio supports the delegation of rule writing using role-based access control (RBAC). Application administrators can only edit rules where the scope of the ruleset matches the scopes

where they have administrator privileges. They cannot create or manage rulesets if the scope includes “All.”

Rule types allow the application administrator to write rules that allow other applications to communicate with the applications that they manage without requiring global administrator privileges. This feature allows users to group rules required for inter-application and intra-application communication for a specific application into one ruleset.

You can combine multiple types of rules (intra-scope, extra-scope, and custom iptables) in a single ruleset.

You can use multiple services or ports and protocols in a rule. This approach helps reduce the number of rules in your PCEs, which helps improve the PCE performance.

NOTE

You cannot provision drop actions from the PCE in a NAT table for custom IP tables. Doing so results in a firewall generation failure.

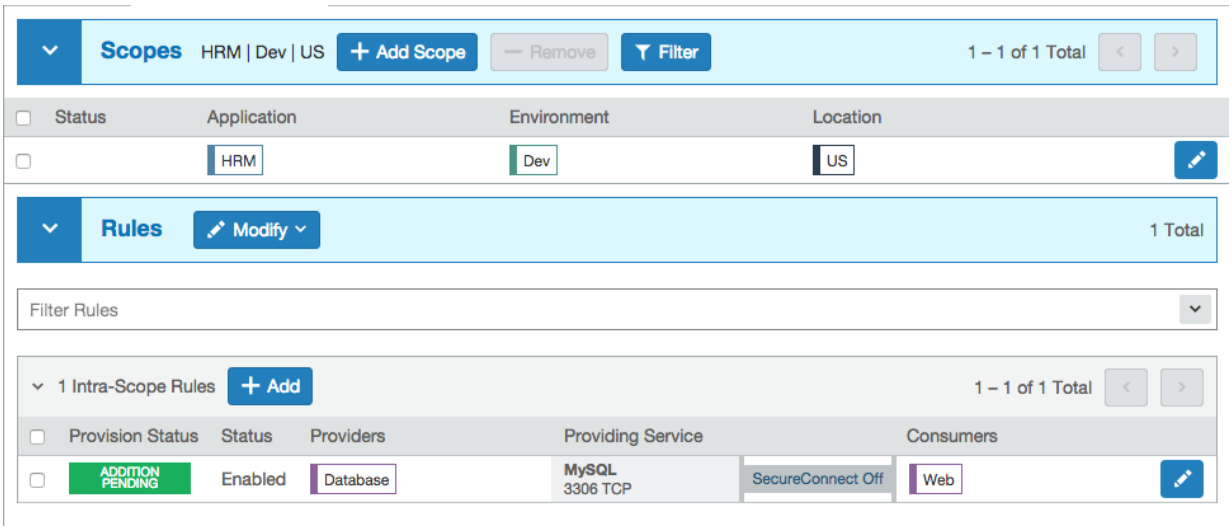
Intra-scope Rules

NOTE

The ability to create intra-scope rules is only enabled when the PCE is configured to display it.

Intra-scope rules allow authorized users to write rules that allow communication between providers and consumers within a specific scope. This rule type is typically used to allow communication between workloads that belong to the same application. For intra-scope rules, the labels used in the scope must match the labels used for both the provider and the consumer. If you don't specify a Label, “All” is used by default.

Example:



In this example, all Database workloads with the labels HRM | US | Dev can accept MySQL connections from all Web workloads with the labels HRM | US | Dev.

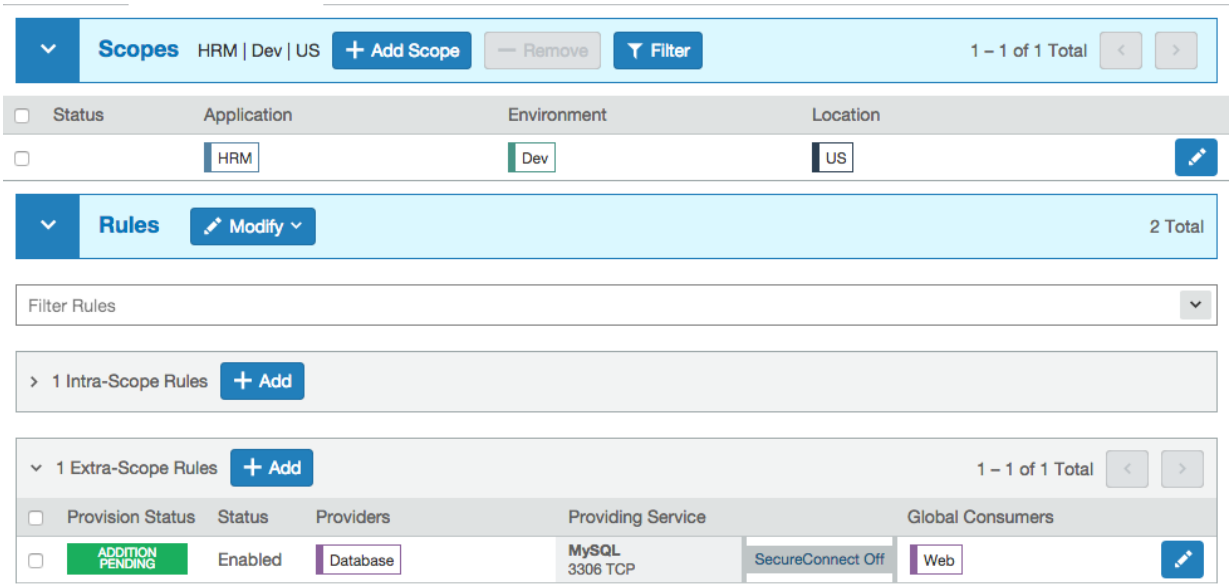
Extra-scope Rules

NOTE

The ability to create extra-scope rules is only enabled when the PCE is configured to display it.

Extra-scope rules allow authorized users to write rules that allow communication between applications. Specifically, you can write rules that allow providers within a scope to be accessed by consumers that can be in or outside the specified scope. For extra-scope rules, the labels used in the scope must match the labels used by the provider. If you don't specify a label, "All" is used by default.

Example:



In this example, all Database workloads with the labels HRM | US | Dev can accept connections on MySQL from all workloads with the label Web, irrespective of other labels.

The MySQL might not belong to the application HRM (for example, the consumers are “Global” and are not restricted by the labels in the scope).

NOTE

If the RBAC user's scope coverage type is “Sources and Destinations,” the user cannot select an IP list as the Source. To select an IP list as a Source in a rule, the scope coverage type must be “Sources Only.” For more information, see "IP Lists" and "Role-based Access Control" in PCE Administration Guide.

Custom iptables Rules

NOTE

The ability to create iptables rules is only enabled when the PCE is configured to display it.

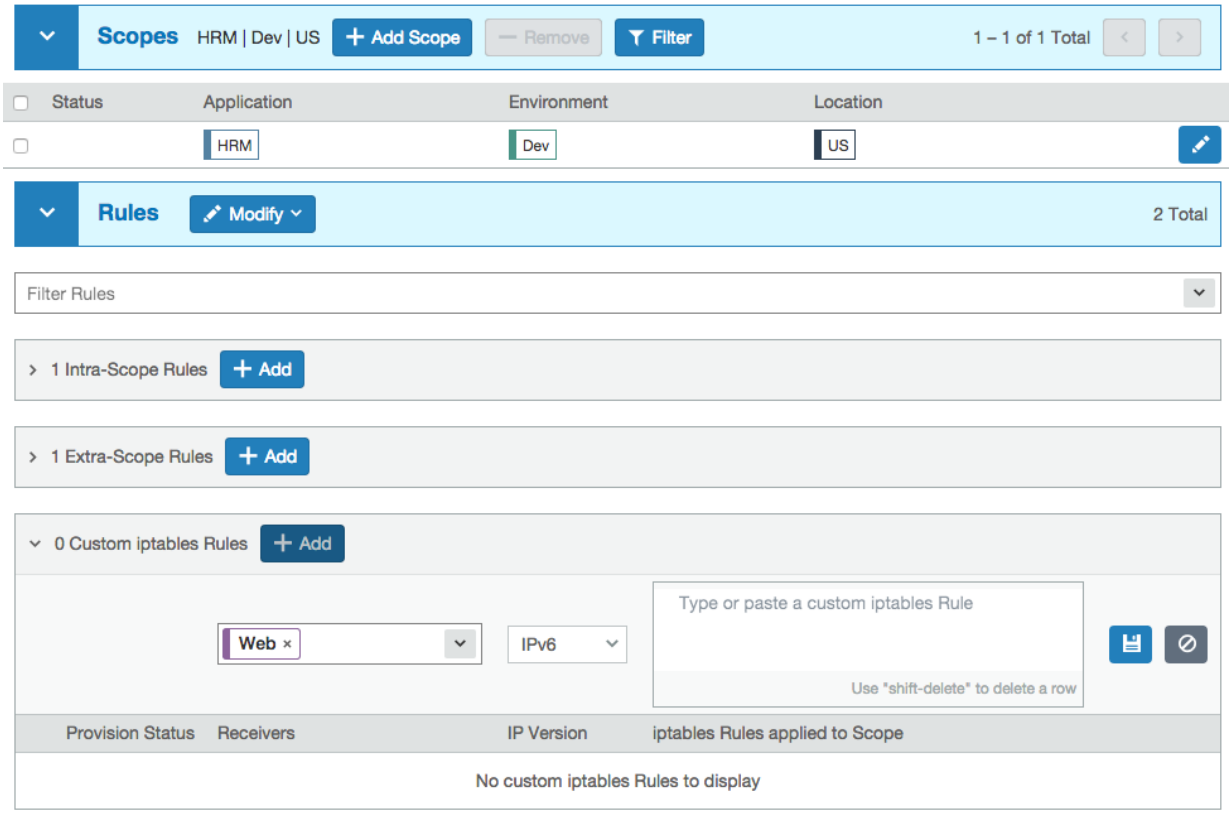
You might have configured iptables directly on your Linux workloads as needed for your application workloads as part of your host configuration. However, when you pair a workload and put a policy into the Visibility Only or Full enforcement mode, the VEN assumes control of the iptables to enact the policy and does not apply any pre-programmed iptables to the policy.

Custom iptables rules in Illumio Core provide the ability for you to program the custom iptables rules needed for your applications as part of the rules managed by the PCE. Custom

iptables rules help preserve any configured iptables from native Linux host configurations by allowing you to include them with the rules for your policy.

To clarify:

- **Iptables** refer to a Linux host configuration before the VEN is installed
- **Rules** refer to statements written by the PCE to determine permitted traffic, typically by assuming control of iptables and programming the new rules
- **Iptables rules** refer to iptables that are inserted as rules onto the VENs and managed by the PCE



Custom rules follow the iptables `-A` (append) command pattern:

`-t`*<table>*`-A`*<chain> <rule>*

Example:

```
-t filter -A INPUT -p tcp -s 10.10.10.10 --sport 8888 -j ACCEPT
```

Custom iptables rules consist of a list of iptables statements and the entities that receive the rules. Each rule can consist of a list of iptables rules, which allows users to group a sequence of rules for a specific function. The custom iptables rules are programmed after the Illumio PCE generates the iptables rules, but prior to the last default rule.

Before they is sent to the VEN, the custom iptables rules are checked for any unsupported tokens (such as names of firewall chains already in use by Illumio, matches against IP sets,

and semicolons). If an unsupported token is included, the rule cannot be saved or provisioned.

If the VEN fails to apply a custom iptables rule because of a missing package or an incorrectly formatted rule:

- The error is reported to the PCE and is logged in the organization events
- The error is displayed in the VEN policy sync status
- The new policy is not used and the last known successful policy is used instead

For policy distribution and enforcement, the VEN creates a custom chain that contains the rules for each table or chain in the iptables. Each custom chain is appended to the end of its corresponding chain in the correct table. When the VEN requests the policy, the iptables command is sent, including the chain where it should be placed.

For security reasons, custom iptables rules only support rules in the `mangle`, `nat`, and `filter` tables.

The following table describes the permitted actions for each iptables type:

Table Name	Chain Names	Custom Rules Support
`raw`	prerouting, output	No
`mangle`	prerouting, input, output, forward, postrouting	Yes
`nat`	prerouting, output, postrouting	Yes
`filter`	input, output, forward	Yes
`security`	input, output, forward	No

Permitted Rule Writing Combinations

The following table explains the valid rule combinations between providers and consumers.

If Provider is	And Service is	Consumer can be
Workload, All workloads, label, label group	Any service	Workload , IP list (including Any (0.0.0.0/0 and ::/0), label, label group, user groups, All workloads
IP list	Any service	Workload, label, label group, user groups, All workloads
Uses virtual services	Not applicable (the service is derived from the virtual service)	Workload, label, label group, IP lists, All workloads, uses virtual service, uses virtual services and workloads
Uses virtual services and workloads	Any service	Workload, label, label group, IP lists, All workloads, uses virtual service, uses virtual services and workloads
Workload, All workloads, label, or label groups	Any service	User groups and one or more of the following: workload, All workloads, label, label groups

Stateless Rules

By default, all rules you write in the PCE are stateful, which means that the host's firewall keeps track of a connection for the entire duration of the session.

For workloads, you can specify stateless packet filtering for a rule ("stateless": true). This means that the VEN instructs the host's firewall to *not* maintain persistent connections for all sessions. You can create this type of a stateless rule for datacenter core services, such as DNS and NTP.

Caveats

In a stateless rule, you can add the following policy objects as consumers:

- An individual workload
- A label (one each of a specific type, up to four total)
- Any IP list plus All workloads

If you attempt to add any other consumers, you receive an error.

The Illumio Core limits the number of stateless rules to 100, to ensure that both stateful and stateless rules coexist on the host in a way that optimizes system and network performance. If you need more than 100 stateless rules in your Illumio policy, contact your Illumio Professional Services Representative for more information.

WARNING

Existing active connections on workloads allowed by a stateless rule (for example, an SSH session) are terminated when workloads receive new rules from the PCE. Those connections need to be reestablished by the clients. For this reason, Illumio recommends that you use stateless rules for services that use high-frequency short-lived connections, such as DNS and SNMP.

Rule Search

When you have a large number of rules organized in rulesets, you can't easily search for rules across rulesets. Segmentation rule search solves this issue by making it simple to search for specific rules.

For example, when you want to know how many rules there are for SNMP (UDP 161) and you have around 200,000 rules organized across 700 rulesets, it is time-consuming to narrow down that search without using this feature.

You can search for and analyze rules that allow communication over a specific port and protocol.

- Segmentation Rule Search allows you to quickly find rules that apply to a set of providers and consumers.

- Providers and consumers can be represented by a workload, an IP address, or a set of labels.
- Using this feature helps you identify rules that are getting applied to your workloads due to unnecessarily broadly applicable rulesets or human errors.

To search for rules:

1. From the PCE web console menu, choose **Rulesets and Rules > Rule Search**.
   The Rule Search page appears.
2. Search for Active or Draft rules.
3. Perform a Basic or Advanced search of your rules:
   - Basic: Searches all attributes
   - Advanced: Searches by provider, consumer, or both.

NOTE

When you perform an advanced search by workload name, the search results do not display the IP list rules when the iplist contains workload IP addresses because the Illumio Core does not resolve CIDRs and ranges within an IP list.

4. From the Results drop-down list, choose to either have the exact match of the selected search filters to be displayed or a match to any of the selected filters (All Results).
5. Click the Column drop-down list to select the attributes you want to be displayed in the search results.
6. Filter options to further narrow your search.
7. Under the Ruleset column, select a ruleset and make changes to the rules.
8. Click **Download** to download the results of your search in JSON format.

Rule Search by Port

The following guidelines and uses cases are provided to clarify how Rule Search works when you search for rules by the port(s) they specify.

General Guidelines

- Single-port searches generally work as expected. See **Row 1** in the Use Case table.
- When searching for a port range, the port ranges in the search and in the rule must match exactly. See **Row 3** in the Use Case table.
- When searching for rules that specify multiple ports, only rules that specify all of the ports are found. See **Row 5** in the Use Case table.

Use Cases: Search for Rules by Port

Row	Use case	Examples (A) Search specifies port(s)	Examples (B) Rule specifies port(s)	Is the rule found?
1	(A) Search for rules that specify only a single port and (B) There's a rule that specifies the same single port	80	80	Yes
2	(A) Search for rules that specify only a single port and (B) There's a rule that specifies a port range that encompasses the searched-for port	80	50-100	No
3	(A) Search for rules that specify a port range and (B) There's a rule that specifies the same port range	50-100	50-100	Yes
4	(A) Search for rules that specify a port range and (B) There's a rule that specifies only a single port within the searched-for range	50-100	80	No
5	(A) Search for rules that specify multiple ports and (B) There's a rule that specifies the same multiple ports	50, 100	50, 100	Yes
6	(A) Search for rules that specify only a single port and (B) There's a rule that specifies multiple ports, including the searched-for port	50	50, 100	Yes
7	(A) Search for rules that specify multiple ports and	50, 80	50, 100	No

Row	Use case	Examples (A) Search specifies port(s)	Examples (B) Rule specifies port(s)	Is the rule found?
	(B) There's a rule that specifies some, but not all, of the searched-for ports			

Policy Check

The Policy Check feature allows you to determine if a rule allowing communication between workloads or between a workload and another IP address already exists. On the Policy Check page, you select two workloads or IP addresses to determine if a rule exists to allow communication between them. Policy check can use a network profile to account for rules affecting outbound traffic to non-corporate interfaces on endpoints. Servers cannot have non-corporate interfaces.

NOTE

You can do a policy check between two workloads, or between a single workload and a single IP address.

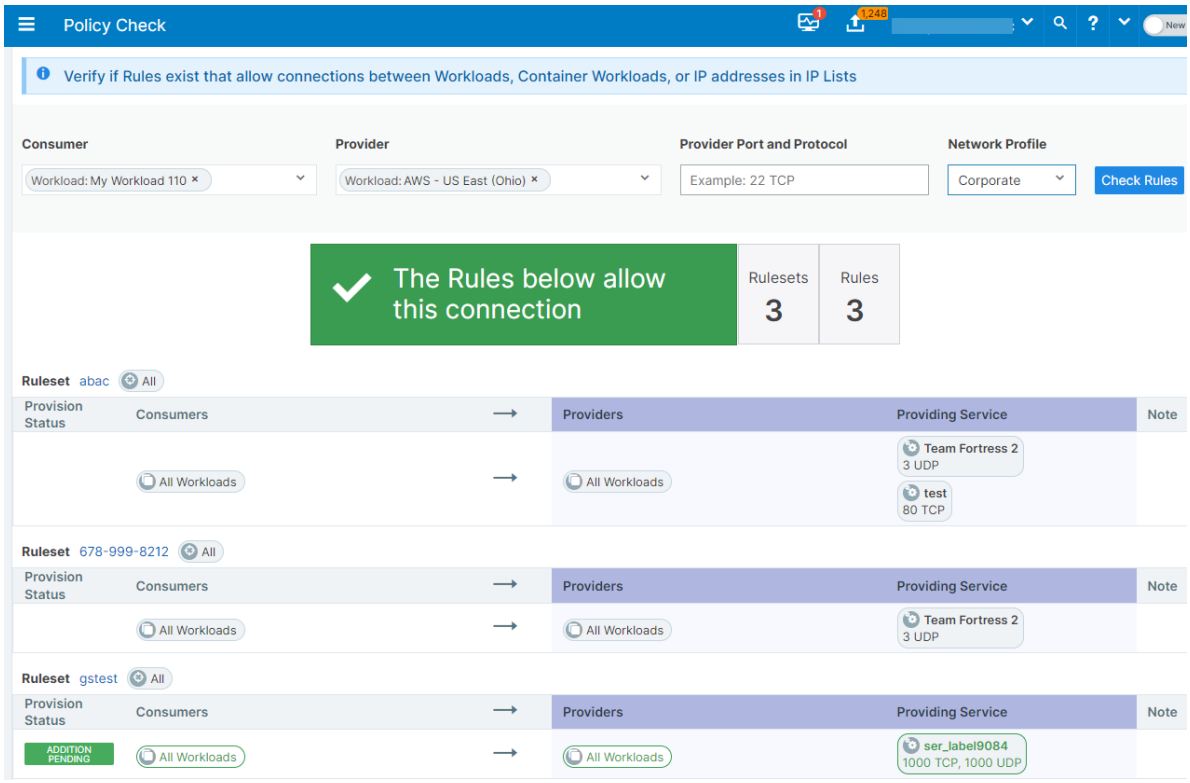
For example, you have created several rulesets for your workloads and applications, and you want to know whether your organization has an existing rule for that traffic before you start writing new rules that duplicate those existing rules.

To perform a policy check:

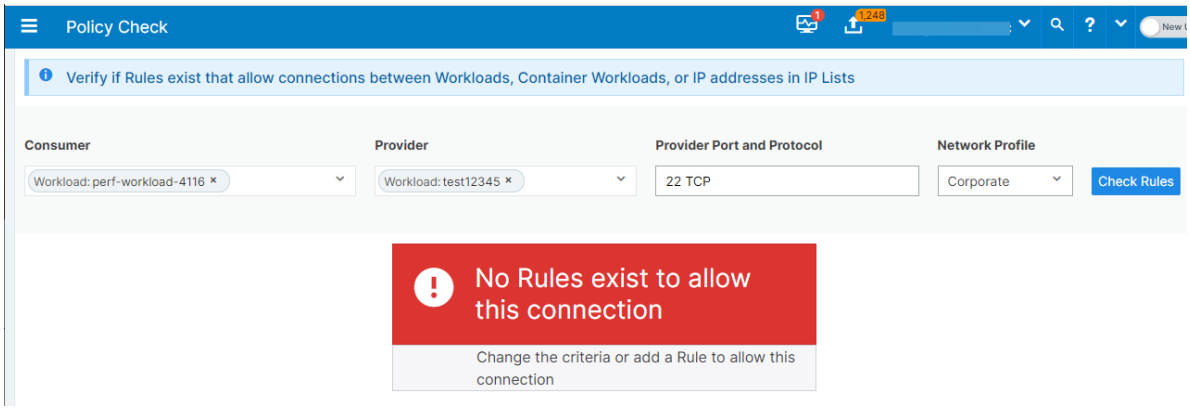
1. From the PCE web console menu, choose **Troubleshooting** > **Policy Check**.
2. In the Consumer field, type or select a workload or IP address.
3. In the Provider field, type or select a workload or IP address.
4. In the Provider Port and Protocol field, enter a port and protocol when the connection is running over TCP or UDP, or just a protocol when the connection is running over GRE or IPIP.
5. In the Network Profile field, choose either Corporate, Non-Corporate Networks (Endpoints Only), or Any.

   If an IP address is specified in both Consumer and Provider fields, the Network Profile value must by Corporate -- that is, searching within the internal corporate network only.
6. Click **Check Rules**.

   If a connection is allowed between the selected two workloads or IP addresses, the page will display at least one rule that allows the connection.



When a rule does not exists, the page displays “No Rules exist to allow that connection.”



Rule Writing

This topic explains how to create the different types of rules in the Illumio Core. For descriptions of the types of rules, see Rules [96].

NOTE

For information about creating rules for traffic flows by using Explorer, see "Add Rules for Traffic Flows Using Illumination Plus" in Visualization Guide.

TIP

You can also use the Illumination map to write rules. For information, see "Write a Group Level Rule In Illumination" in Visualization Guide.

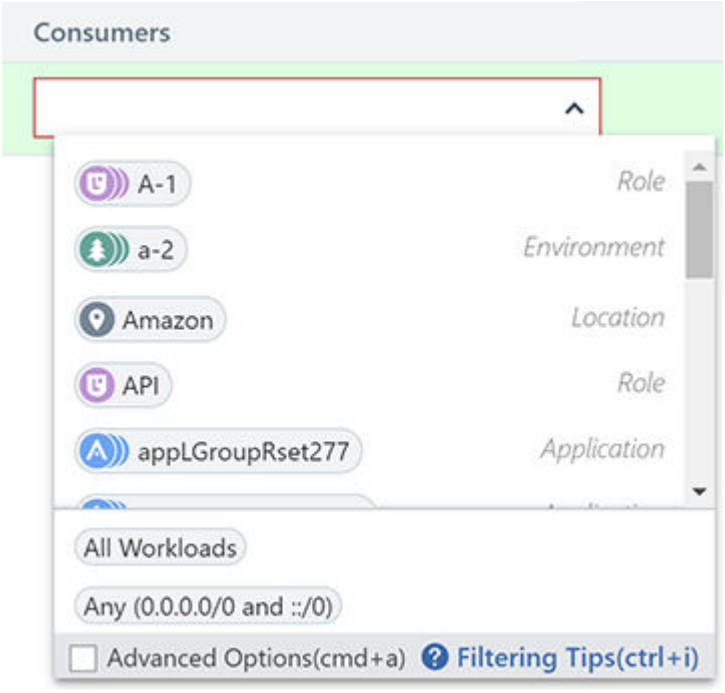
NOTE

In previous releases, this feature was referred to as “Segmentation Rulesets.” In Illumio Core 21.5.0 and later releases, this feature is now referred to as “Rulesets.” Some images might still display the previous feature name.

Basic and Advanced Modes for Rules

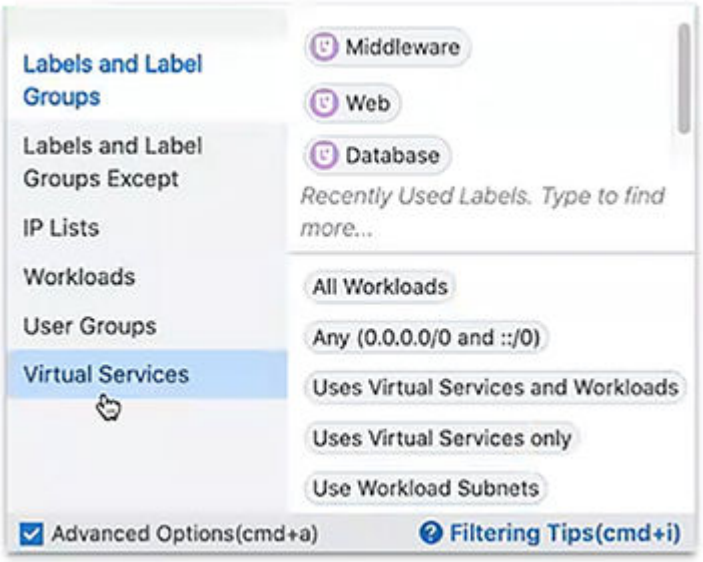
In Illumio Core 22.2.0 and later releases, the dialog boxes in the PCE web console are split into a simple mode and an advanced mode.

In the simple mode, you can select labels and label groups for your rules. Your most recently used labels appear in this screen, then as you type, the UI auto-completes the names to find labels in the PCE.



To access the advanced options for rules, select the **Advanced Options** checkbox:

A panel appears on the left providing the following policy objects that you can add to your rules:



In **Advanced Options**, you can also select *Use Workload Subnets* and *Container Host* options for Consumers and *Use Workload Subnets* and *Virtual Servers* for providers.

Create an Intra-Scope Rule

NOTE
The ability to create intra-scope rules is only enabled when the PCE is configured to display it. To perform this procedure, the PCE must be enabled to create scoped rulesets.

Intra-scope rules allow communication within a group. The ruleset scope applies to both providers and consumers. For more information about intra-scope rules, see Intra-scope Rules [97].

1. If necessary, create a Ruleset or open an existing one. See Rulesets [84] for information.
2. In the Ruleset page, click the **Add** > **Add Intra-Scope Rule**.
   A row appears for the new intra-scope rule.
3. From the Consumers drop-down list, select the labels to define the consumer. To add a policy exception, IP list, individual workload, user group, or virtual service, select the **Advanced Options** check box and select the policy objects for the rule.

NOTE
The consumer must match the Ruleset scope.

4. In the Providers drop-down list, select the labels to define the provider. To add a policy exception, IP list, individual workload, user group, or virtual service, select the **Advanced Options** check box and select the policy objects for the rule.

   For a full list of permitted provider and consumer combinations in a rule, see Permitted Rule Writing Combinations [101].
5. From the Providing Service drop-down list, select a service (for example, PostgreSQL).

   NOTE
   Only one service or all services can be selected.
6. (Optional) To specify additional options for the rules, such as SecureConnect, Machine Authentication (also known as AdminConnect), create a stateless rule, or a rule for non-BRN networks, select the option from the **Rule Options** drop-down list.

   For more information, see SecureConnect, AdminConnect, and Stateless Rules in this guide.
7. After completing your selections, click the **Save** icon ( ) at the end of the row for that rule.

   NOTE
   To edit this rule, click the **Edit** icon at the end of the row.

   After adding a rule, the Status column displays a green Addition Pending icon. To enforce this rule, you must provision the change. For more information about provisioning, see Provisioning [116].

Create an Extra-Scope Rule

NOTE
The ability to create extra-scope rules is only enabled when the PCE is configured to display it. To perform this procedure, the PCE must be enabled to create scoped rulesets.

Intra-scope rules allow communication within a group. The ruleset scope applies to both providers and consumers. For more information, see Extra-scope Rules [98].

1. If necessary, create a Ruleset or open an existing one. See Rulesets [84] for information.
2. In the Ruleset page, click **Add** > **Add Extra-Scope Rule**.

   A row appears for the new intra-scope rule.
3. From the Consumers drop-down list, select the labels to define the consumer. To add a policy exception, IP list, individual workload, user group, or virtual service, select the **Advanced Options** check box and select the policy objects for the rule.

   NOTE
   The consumer does not need to match the Ruleset scope.

4. In the Providers drop-down list, select the labels to define the provider. To add a policy exception, IP list, individual workload, user group, or virtual service, select the **Advanced Options** check box and select the policy objects for the rule.

   For a full list of permitted provider and consumer combinations in a rule, see Permitted Rule Writing Combinations [101].
5. From the Providing Service drop-down list, select a service (for example, PostgreSQL).

   NOTE
   Only one service or all services can be selected.
6. (Optional) To specify additional options for the rules, such as SecureConnect, Machine Authentication (also known as AdminConnect), create a stateless rule, or a rule for non-BRN networks, select the option from the **Rule Options** drop-down list.
7. After completing your selections, click the **Save** icon ( ) at the end of the row for that rule.

   NOTE
   To edit this rule, click the **Edit** icon at the end of the row.

   After adding a rule, the Status column displays a green Addition Pending icon. To enforce this rule, you must provision the change. For more information about provisioning, see Provisioning [116].

Create a Custom iptables Rule

NOTE
The ability to create iptables rules is only enabled when the PCE is configured to display it. To perform this procedure, the PCE must be enabled to create scoped rulesets.

Custom iptables rules allow you to integrate existing iptables into a ruleset. For more information about custom iptables rules, see Custom iptables Rules [99].

NOTE
Creating custom chains is not supported.

About Custom iptables Rules

- **Receivers column:** Shows the labels representing the resource that receives the custom iptables rule.
- **IP Version column:** Specifies the IP version used for this traffic.

- **Iptables Rules applied to Scope column:** Contains the entire iptables.

To add a custom iptables rule:

1. If necessary, create a Ruleset or open an existing one. See Rulesets [84] for information.
2. In the Ruleset page, click the **Add** > **Add Custom Iptables Rule**.
3. A row appears for the new iptables rule.
4. In the Receivers drop-down list, select the entity or entities that will receive the iptables rules by selecting or typing a label name.

   NOTE
   More than one label can be selected. When you select labels as receivers, the custom iptables rules are sent only to workloads matching those labels and not virtual services or virtual servers.

5. From the drop-down IP Version drop-down list, select the IP version (IPv4 or IPv6).
6. Type or paste the iptables commands into the Type or paste a custom iptables rule field. Supported iptables display in green. Unsupported iptables or iptables with errors display in red.

   NOTE
   The iptables commands must begin with `-t`. To delete a row, use **Shift+Delete**.

7. After completing your selections, click the **Save** icon ( ) at the end of the row for that rule.

   NOTE
   To edit this rule, click the **Edit** icon at the end of the row.

   After adding a rule, the Status column displays a green Addition Pending icon. To enforce this rule, you must provision the change. For more information about provisioning, see Provisioning [116].

When you provision a new custom iptables rule, the VEN performs basic validation before applying on the Linux workload host firewall. If this validation test fails, the VEN will log an event and switch to an Error State. If the validation is successful, the VEN installs the custom iptables rules before the last default rule.

NOTE
Ordering is not guaranteed across custom iptables rules. Any iptables rule that is closely tied to or depends on other iptables rules must to be written as part of the same rule. For example, when you have three iptables rules to allow ICMP Types 3, 8, 13 and another rule to drop other types of ICMP traffic, all four of these iptables rules must be a part of the same ruleset.

Write Multicast Rules

You can write rules to allow multicast traffic between workloads by writing two rules that follow a very specific workflow.

Multicast Use Case 1

For example, you want some database workloads labeled DB to have multicast for data replication and you want to allow the multicast traffic.

To do this:

1. Create an unmanaged workload or an IP list to represent the multicast group IP address (for example, mDNS Group: 239.0.0.251).
2. Create a service with port (for example, mDNS: UDP 5353).
3. In the ruleset, create these two rules:

Rule	Provider	Service	Consumer
1	mDNS Group	mDNS Group	DB
2	DB	mDNS Group	DB

In Rule 1, the consuming entity DB allows outbound packets from DB *to* 239.0.0.251.
In Rule 2, the mDNS group allows inbound packets *from* DB.

Multicast Use Case 2

For example, you want to ensure that the DB workloads receive a multicast feed on 224.5.5.5:5800 (multicast source).

To do this:

1. Create an unmanaged workload or an IP list to represent the multicast source (for example, Stock-Feed-Group: 224.5.5.5).
2. Create a service with the correct port (for example, Stock-Feed-Service: UDP 5800).
3. In the ruleset, you create these two rules:

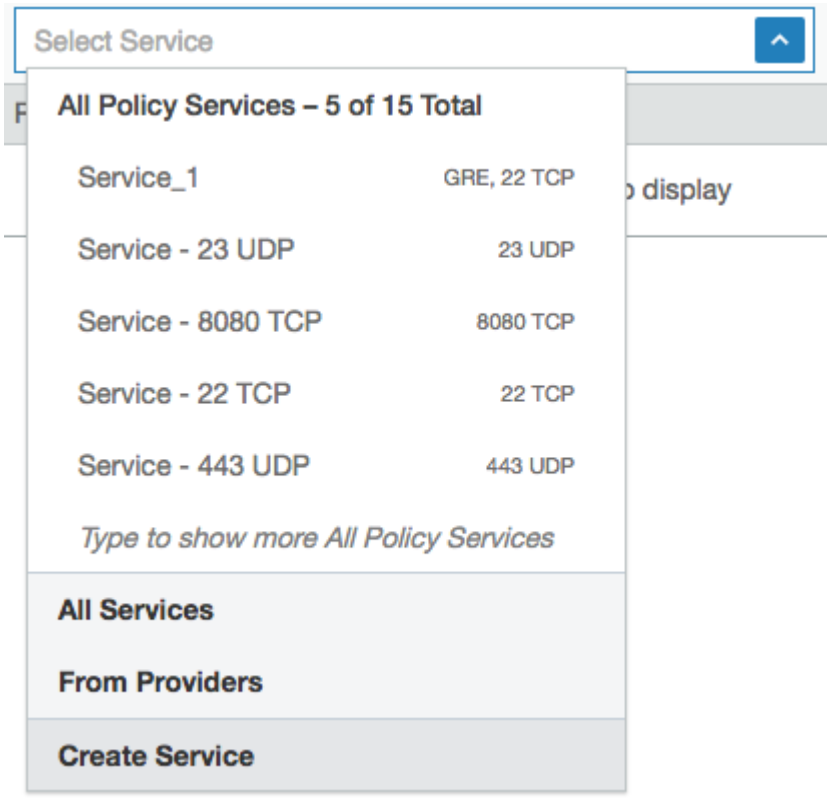
Rule	Provider	Service	Consumer
1	Stock-Feed-Group	Stock-Feed-Service	Multicast-Source
2	DB	Stock-Feed-Service	Multicast-Source

In Rule 1, the Stock-Feed-Service allows outbound packets from Multicast-Source *to* 224.5.5.5.
In Rule 2, the provider DB allows inbound packets *from* Multicast-Source.

Create Service While Creating Rule

To make rule writing easier, you can create a new service in a ruleset as you are writing rules.

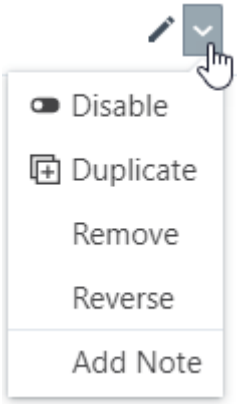
1. Create an Extra-Scope [98] or an Intra-Scope Rule [97] if scopes are enabled for the PCE; otherwise, add a basic rule.
2. In the Providing Service drop-down list, select **Create Service** at the end of the list.



3. In the Create Service pop-up that appears, enter a name for the service in the Name field and optionally a description in the Description field.
4. In the Attributes section, choose whether you want to create a Port-Based [21] or Windows Service-Based service [21].
5. In the Ports section, enter the ports (including any UDP ports) used by the service. To enter a range, separate the port numbers by a hyphen (-). You can also copy and paste lists of services. To delete a row, use **Shift+Delete**.
6. Click **OK**.

Tips for Managing Rules

- To modify an existing rule, click the edit icon ( ) at the end of the rule row.
- To modify or remove an existing rule, open the Edit menu for that rule at the end of the row.



- To remove multiple rules, select their checkboxes and click the **Remove** (−) button in the **Rules** header row at the top of the page.
- To enable or disable multiple rules, select their checkboxes and click the **Enable** or **Disable** button in the **Rules** header row at the top of the page.
- To filter your existing rules, click the Filter icon ( ) in the **Rules** header row at the top of the page. The filter drop-down menu appears. Click the drop-down list and select an option to filter rules by label, IP lists, label groups, virtual services, virtual servers, workloads, user groups, services, All workloads, or Any (0.0.0.0/0 and ::/0). If there are no rules that match the selected criteria, a message appears indicating that no rules match your filter criteria.
- After creating or modifying a rule, the **Provision** button appears at the top of the page and the status of the rule appears at the beginning of the rule row indicating the current provisioning status of the rule (for example, "• Pending" or "– Pending").

Add a Note to a Rule

You can add a note to a rule to document more information about that rule for context. The note is visible to all users in the organization, but can only by edited by users with Ruleset Manager privileges for the ruleset.

NOTE

You must provision the changes after adding a note to a rule.

1. Select a rule on the Rulesets page.
2. Open the drop-down list after the **Edit** icon and select **Add Note**. Enter the note in the drop-down entry field that appears. You can enter up to 255 characters.
3. Click **Save**. You must provision the changes to confirm the note.

Details:

- To indicate the rule contains a note, the following icon is displayed in the Note column: .
- To edit an existing note, select the note icon. The entry field displays the existing text. Make any needed changes, then click the Save icon in the lower-right to save the changes to the note.

Duplicate a Rule

1. Select the ruleset on the Rulesets page.
2. Select the drop-down list next to the **Edit** button of the rule to be duplicated.
3. Select **Duplicate**. The rule is duplicated in Edit mode, allowing you to make any needed changes.
4. Click **Save**.

After saving the duplicate rule, you must provision the ruleset changes to apply them.

Reverse a Rule

To expedite the rule writing process, you can duplicate and reverse existing rules. The entity selected as the provider in the original rule will be the consumer in the reversed rule and the entity selected as the consumer in the original rule will be the provider.

Caveats:

- Only intra-scope rules are supported. Extra-scope and custom iptables rules cannot be reversed.
- Only rules that use the following resources are supported: Labels, label groups, workloads, IP lists, All workloads, and Any.
- When you do not have sufficient privileges due to RBAC, an error message displays.
- Only one rule can be reversed at a time.
- When the original rule is disabled, the reversed rule is disabled as well.

To reverse (swap Providers and Consumers) in a rule:

1. Select the ruleset on the Rulesets page.
2. Select the drop-down list next to the **Edit** button of the rule to be reversed.
3. Select **Reverse**. The rule is reversed in Edit mode allowing you to make any needed changes.
4. Click **Save**.

After saving the reversed rule, you must provision the ruleset changes to apply them.

Reorder Rules

Ruleset owners have the ability to rearrange rules in a specific order to improve readability on the Rulesets details page. Different rule types can be reordered independently.

After reordering the rules, you must provision the changes for them to take effect. Rearranging rules does not affect the order in which they are enforced in the policy.

NOTE

You can only reorder rules in rulesets that you own. For more information, see "Role-Based Access Control" in PCE Administration Guide.

To customize the arrangement of the rules, click the handle icon at the beginning of a rule row and drag the rule up or down to change its order. The other rules are rearranged to accommodate the move. When you place the rule in its new location, the numbers of the rules are reassigned to reflect the new order. If you delete a rule, it remains in place but is appended with “– Pending.”

NOTE

If more than one user is reordering the rules at the same time, the most recent changes are saved.

FQDN-Based Rules

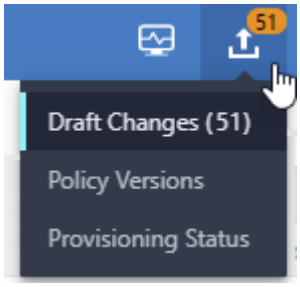
Applications across datacenters and cloud environments are responsible for a vast amount of east-west traffic. This traffic is the result of communication between workloads, including

bare-metal, virtual machines, and containers. However, many applications might need to communicate with services, such as SaaS, PaaS or external registries. These services are coupled with an IP address but that address might be unknown or the services might only be reachable by a URL because their IP addresses are frequently changing. This situation introduces a challenge to security teams because security policies are based on IP addresses or subnets. Administrators can allow outbound communication to any workload or to a broad range of IP addresses to overcome this challenge; however, this approach opens a security gap. To resolve this challenge, Illumio has added FQDN-based visibility and enforcement to its Illumio Core.

Provisioning

When you provision updates, the PCE recalculates any changes made to rulesets, IP lists, services, label groups, and security settings, and then transmits those changes to all VENs installed on your workloads.

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.



Items that Require Provisioning

The following security policy items must be provisioned before they can take effect:

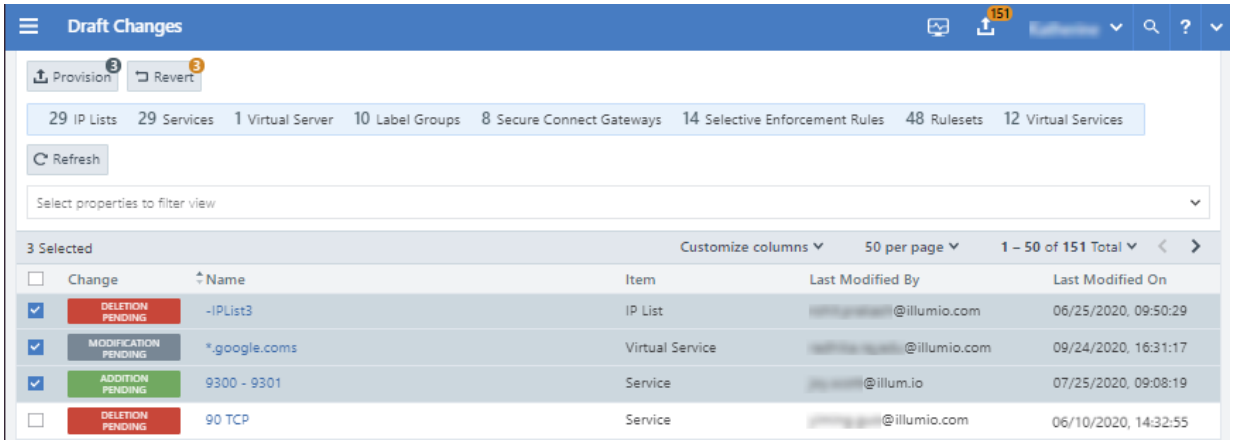
- Rulesets
- Rule notes
- IP lists
- Services
- Label groups
- Security settings
- Virtual services
- Virtual servers

Provision All or Selected Items

When you create or change security policy items (such as rulesets, IP lists, services, label groups, and security settings), you can provision the item immediately from the item page after you save the change.

You can click **Provision** button on the top PCE web console toolbar, which allows you to see all of the security policy changes that require provisioning. The list shows any items that have been modified (gray) or deleted (red), or added (green).

In the list of changes requiring provisioning, you can select all items, or select items individually to provision.



Dependencies for Partial Provisioning

When you select only some items to provision (rather than provisioning all policy item changes), some of those items might have dependencies that are also provisioned. Before you commit to the provision, the PCE shows you the items that are dependent and will also be provisioned.

NOTE

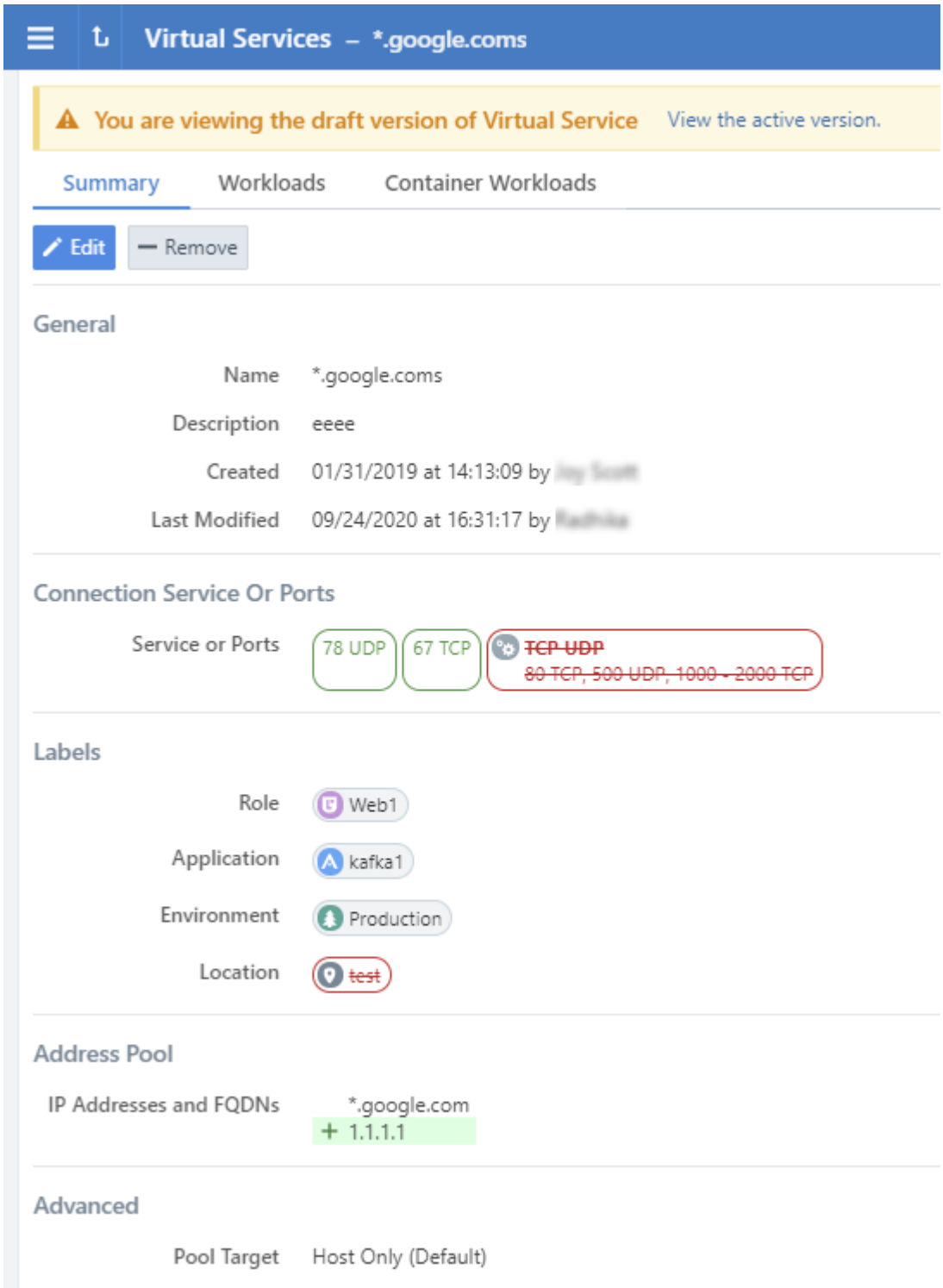
You cannot partially provision resources with more than 500 dependencies. All changes must be provisioned at the same time.

Active vs Draft Versions

Any changes you make to security items, such as rulesets, services, IP lists, label groups, and security settings, need to be provisioned. All the changes you make to those items are considered to be in a “draft” state (non-versioned) until you provision them. After you provision your changes, those changes become the “active” version.

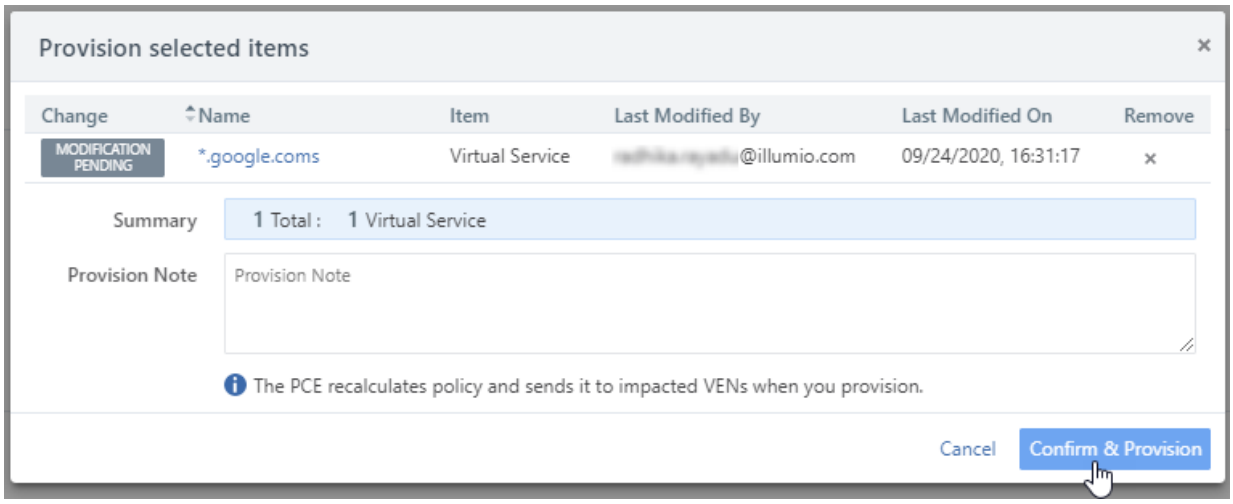
When you edit a security item that has been published at least once, and new changes have occurred since the last provisioning, you see a note at the top of the page that indicates the item is currently in draft state.

If you want to view the active version, click the **View the active version** link.



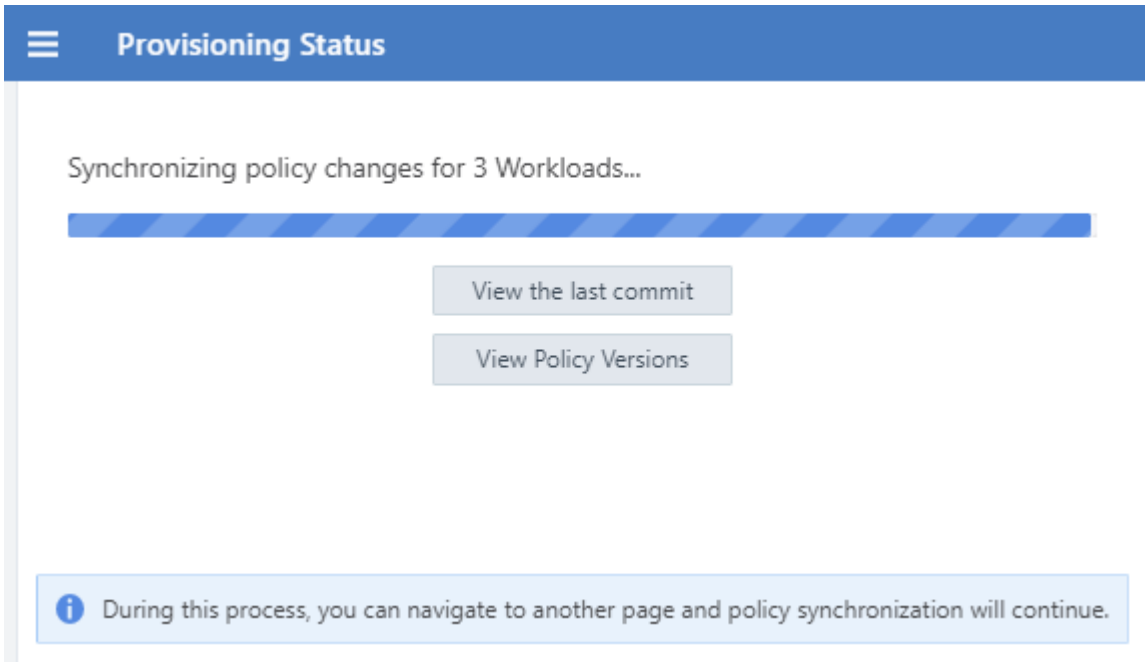
Provisioning Progress Indicator

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.



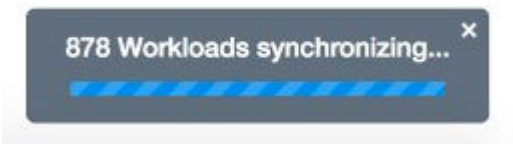
On the Provisioning page, you can:

- View the previous policy change by clicking **View the last commit**
- View a list of provisioned changes by clicking **View Provision History**



NOTE
If multiple subsequent policy changes have been provisioned, the number is the total number of workloads that have not yet received all provisioned policy changes, not just the most recently provisioned changes.

During this process, if you navigate to another page, the policy synchronization will continue and a window in the lower-right displays the number of workloads pending synchronization with the latest policy.



To return to the Provisioning page, click the window in the lower right corner or select **Provisioning** from the drop-down Provisioning list.

When the provisioning completes successfully, a confirmation message displays.

NOTE

If multiple users simultaneously provision changes, the Provisioning progress indicator is updated to show the new changes, so all users will see the same Provisioning progress indicator.

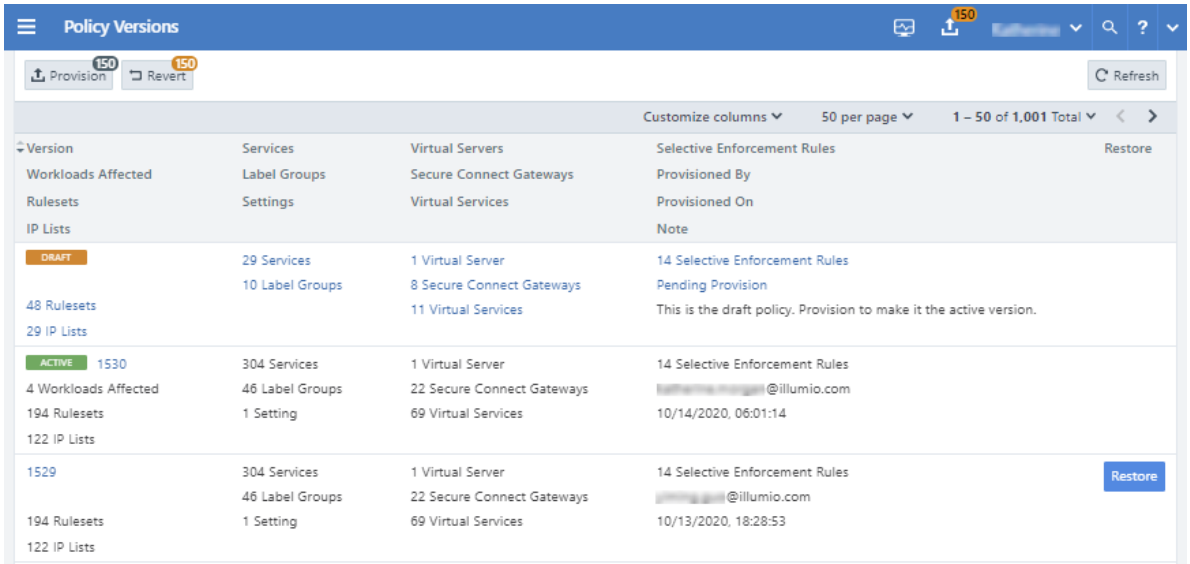
Policy Versions

Each time you provision changes to policy items (such as rulesets, services, IP lists, label groups, and security settings), the entire set of changes you provisioned receives a version number. You can view the history of your policies and view their differences.

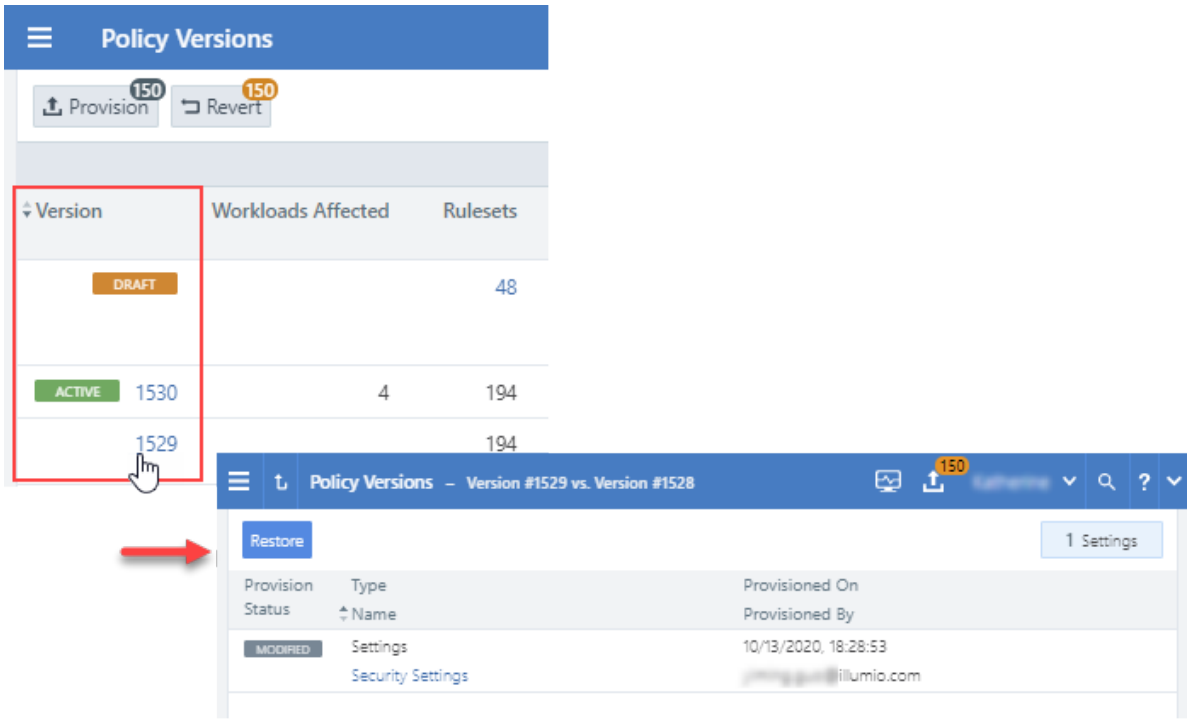
You can select a previous version to see information about that specific version. By default, the PCE retains only the last 1000 versions of the policy and automatically removes the older versions for improved performance. When a new change is provisioned, the oldest version of the policy is removed.

1. From the PCE web console toolbar, click the **Provision** button and choose **Policy Versions**.

   The Provision History page appears, which displays the history of the last provisions in your organization.



2. To view details about the changes, click one of the items. For the selected item, you can see the changes that were provisioned in this version.



Provision Changes

If you have made any changes to provisionable objects, such as rulesets, IP lists, services, label groups, and security settings, you need to provision those changes before they can take effect.

1. From the PCE web console toolbar, click the **Provision** button > **Draft Changes**.
   The Draft Changes page appears, which displays a list of 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 one, several, or all the items you want to provision.
3. Click **Provision** to see a preview of the changes that will occur when you provision them.

> **NOTE**
> When you selectively choose items to provision, some of those items might have dependencies that are also published. Any object dependencies are also be provisioned.

4. You can add a note to the provision. If a note is mandatory, the **Confirm & Provision** button is grayed out until you enter text in the field. After you enter appropriate text in the field the button is enabled.
5. Click **Confirm & Provision** to push all the policy changes to workloads.

Revert Provisionable Changes

Any changes you make to policy configuration items (rulesets, IP lists, label groups, services, or security settings) appear as pending provisioning. You can revert those changes before you provision them.

1. From the PCE web console toolbar, click the **Provision** button > **Draft Changes**.
   The Draft Changes page appears, which lists all security policy items have been added, modified, or removed. You also see a summary of changes based on item type.
2. Select individual items to revert or you can revert all changes.
3. Click **Revert**.

Restore Policy

With the policy restore feature, you can revert to an older version of the policy when the newly provisioned policy did not work as expected.

NOTE

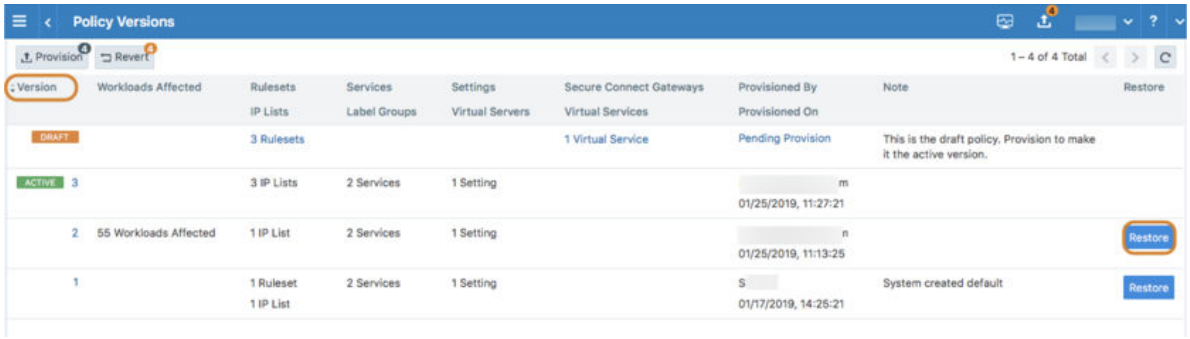
You need to be a Global Administrator or Global Organization Owner to use this feature.

The older version of the policy is copied to the current working draft version. You can immediately provision it to replace the version that is not working.

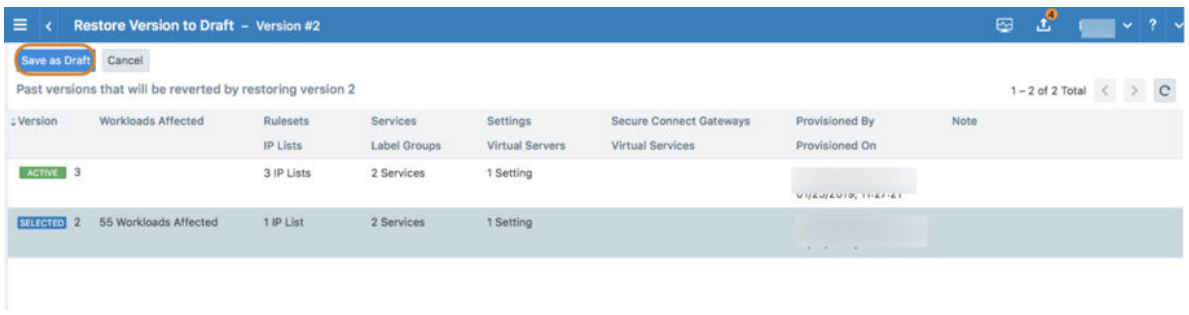
When there are pending changes, you cannot restore to a previous version. If you try to restore to this version, it will result in references to deleted non-versioned objects such as labels and workloads, the restore will fail, and an error message will be displayed.

To revert to an older policy version:

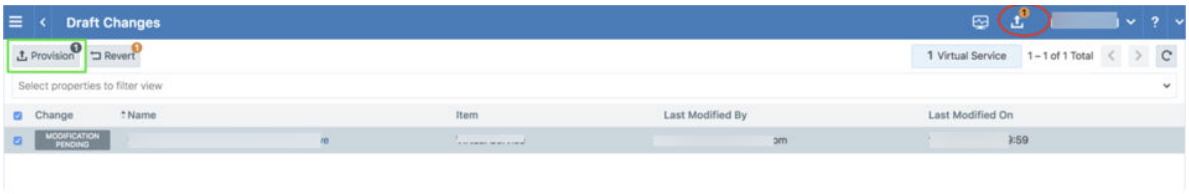
1. Choose **Provision** > **Policy Versions** from the PCE web console menu or from the top-right provision menu.
   The policy versions are displayed under the **Version** column.
2. Click **Restore** for the policy version that you want to revert to.



3. Click **Save as Draft** to restore the policy to the selected version.



4. Review the draft changes and click **Provision** to restore the policy to the selected version or click **Revert** to return to the Policy page.



Provisioning Note Setting

You can 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 enabled, you must 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 Core does not validate the content entered in the Provision Note field.

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

NOTE

You must have the correct role and permissions to access this feature. If necessary, contact your Illumio administrator for assistance.

To make the provision note mandatory:

1. From the PCE web console menu, choose **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**.

Policy Enforcement

This section describes the ways that you can enforce security policy for your managed workloads. This section assumes that you have already created the policy objects necessary for your security policy approach, created rulesets and rules, and installed VENs on your workloads.

See the following topics and sections for information about those tasks:

- Security Policy Objects [14]
- Create Security Policy [60]
- About Creating Managed Workloads by Installing VENs [51].

Ways to Enforce Policy

Illumio provides several ways to enforce policy on your managed workloads. For information about creating a managed workload, see Workload Setup Using PCE Web Console [51]. For information about creating security policy by defining rulesets and rules, see Rulesets [84] and Rules [96].

Enforcement States for Rules

The Illumio policy model follows an allowlist model whereby all communication between workloads is denied unless explicitly allowed by Illumio security policy. Users create rules to allow traffic between their workloads. For information about the allowlist model, see Understanding Rulesets and Rules [5].

This method of controlling traffic ensures secure communication between your workloads. However, as you work toward applying the allowlist model for security policy, you might choose a more targeted approach to applying security policy. In addition to creating rules for your workloads, you can control the enforcement state for your workloads.

A workload's enforcement state operates alongside the rules that govern it. By choosing an enforcement mode, you can separate policy enforcement and visibility states per workload. Applying selective enforcement to a workload is based on one or more labels or label groups.

Using selective enforcement mode, you can protect a subset of your services and ports on your managed workloads. The other ports on the workload remain in visibility-only state and function as if the entire workload is in visibility-only mode. In addition to gradually expanding your policy enforcement envelope, selective enforcement is useful for temporarily enforcing policy on specific ports in case a vulnerability is detected and you need to take action quickly.

Another way to think of selective enforcement of security policy is as an intermediate enforcement state on the workload:

In this intermediate enforcement mode, label-based rules designate the workloads and the services/ports that need to be enforced; while other services and ports are in visibility-only mode. Policy enforcement is applied only on the provider side (ingress traffic) of the rules.

For more information about visibility modes, see "Set Group Enforcement" in Visualization Guide.

Limitations for Applying Selective Enforcement State

- Selective enforcement state is directional. If you want to manage traffic between both ends of a connection, create both provider-centric and consumer-centric policy to apply to inbound and outbound connections.
- Selective enforcement state only applies to managed workloads; it is not supported for NEN-controlled or other unmanaged workloads.
- Virtual Services are enforced at the workload level. As a result, selective enforcement state does not affect virtual services directly; instead, selective enforcement state affects the workloads they are comprised of.

Workload Enforcement States

Policy mode determines how the rules affect a workload's network communication. Illumio Core includes four policy modes for workloads. If a workload is unmanaged, the Enforcement column is not displayed on the workload list page.

Idle

The Idle state is used to install and activate VENs on workloads without changing the workload's firewalls. In the Idle state, the VEN on the workload does not take control of the workload's host firewall but uses workload network analysis to provide the PCE relevant details about the workload, such as the workload's network interface, operating system, and traffic flows. This information is captured in the following ways and intervals:

- Traffic flows: a snapshot is taken every 10 minutes.
- Operating system: included in the Compatibility Report every four hours.
- Workload network interface: reported to the PCE anytime it changes.

A pairing profile can be used to pair workloads in the idle state.

NOTE

SecureConnect rules are only applied to workloads where the VEN is in a non-idle enforcement state.

However, unlike other rules, SecureConnect requires matching rules to be applied to workloads on BOTH sides of any connection. Therefore, SecureConnect traffic is not supported between two workloads where a VEN on either side is in idle state.

Visibility Only

In the Visibility Only state, the VEN inspects all open ports on a workload and reports the flow of traffic between it and other workloads to the PCE. In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the datacenter and the applications running in it. 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.

WARNING

Visibility can disrupt Docker and other applications that rely on NATing and ip-forwarding.

Selective Enforcement

Rules are enforced directionally for selected services when a workload is within the scope of an Enforcement Boundary.

Full Enforcement

Rules are enforced for all inbound and outbound services. Traffic that is not allowed by a rule is blocked.

Visibility Level

You can choose from three levels of visibility for workloads. These modes allow you to specify how much data the VEN collects from a workload when in the Full Enforcement state:

- **Off:** The VEN does not collect any information about traffic connections. This option provides no Illumination detail and demands the least amount of system resources from a workload.

  This property is only available for workloads that are in the Full Enforcement state.
- **Blocked:** The VEN only collects the blocked connection details (source IP, destination IP, protocol and source port and destination port), including all packets that were dropped. This option provides less Illumination detail but also demands fewer system resources from a workload than high detail.
- **Blocked + Allowed:** The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections. This option provides rich Illumination detail but requires some system resources from a workload.

NOTE

SecureConnect rules are only applied to workloads where the VEN is in a non-idle enforcement state.

However, unlike other rules, SecureCionnect requires matching rules to be applied to workloads on both sides of any connection. Therefore, SecureConnect traffic is **not** supported between two workloads where a VEN on either side is in idle state.

Policy Exclusions

In Illumio Core 22.2.0 and later releases, the PCE supports including policy exclusions in ruleset scopes and rules. This topic explains what they are, how they are supported in Illumio Core, and how to add them to your security policy.

Policy Exclusions Described

Using policy exclusions in your Illumio Core policy can greatly simplify the rule writing process. Specifically, using a policy exclusion in a ruleset scope or in rules allows you to replace the inclusion of a large number of required labels with the exclusion of a small number of unwanted labels. Security policy written with policy exclusions can be easier to read and definitely easier to maintain.

Using a policy exclusions gives you a way to state in your security policy that you want a ruleset or rule to apply to "all except *X*," where *X* can be both labels and label groups. To state this another way, "all except *X*" means "All labeled workloads except X" or "All label group objects of a dimension except X."

You can include policy exclusions in ruleset scopes and in rules actors, namely consumers and providers.

Use Cases

The following examples demonstrate a few common use cases for using policy exclusions:

- All environments except Production should be able to pull updates directly from RedHat
- The standard jump boxes should be able to connect to all environments except PCI
- All applications except Quarantine should be able to connect to Core Services

Support for Policy Exclusions

Policy exclusions are supported by Illumio Core features and in the PCE web console in the following ways:

Illumio Core Feature	Details
Ruleset scopes and rules	In rulesets and rules, excluding a label creates an "all-but" rule or boundary that applies to all workloads that don't have that excluded label but do have another label of the same label type as the excluded label. For example, your data center supports three environments: Production, QA, and Development. Adding an exclusion for "All environments except Production" means that the rules apply to all workloads with Environment labels minus the Production label. It does not translate to "All workloads except those with the Production label," which would include workloads that don't have an Environment label. When you create a rule that applies to "All environments but Production," this rule achieves the same affect as creating a rule that applies to the QA and Development environments only.
Labels	Fully supports except for the restrictions below. See Requirements and Restrictions [129].
Label Groups	Label groups are supported for policy exclusions in the same way as labels. For example, you want to create a boundary between Finance applications and all other applications. You create a label group named "Finance Apps" and use it as a policy exclusion. Using label group exclusions is not supported with individual workloads, virtual services, virtual servers, "All Workloads," the "Uses virtual service only" option, the "Uses virtual service and workloads" option, and container hosts. Additionally, you cannot specify exclusions out of label groups. For example, you have created a label group for the environment "Non-production." You want to use the label group except you don't want it to apply to the "Development" environment. You want to create a policy exclusion for the "Development" environment label from the "Non-production" label group. This action is not supported. Selecting to exclude a label group excludes all labels within that group.
Rule Search and filters	You cannot search by policy exclusions; however, any rules that contain policy exclusions appear in the results of your rule search. In label filters and rule search, entering a label name displays both included and excluded labels with that name.
App Groups	**App Groups** > **App Groups List** > select a group > **Rules** tab Rules with policy exclusions appear in the **Rules** tab.
Policy Check	Rules with policy exclusions appear in the **Policy Check** page.
Policy Generator	The PCE does not propose policy exclusions when using Policy Generator to create policy. When using Policy Generator to calculate V-E scores for vulnerabilities (you have the Vulnerability maps feature enabled), Policy Generator won't work for rules that contain policy exclusions because they aren't supported in Policy Generator.
Access Management	Access management (also know as Role-based Access Control or RBAC) detects policy exclusions when determining user access in the PCE. However, you cannot add a policy exclusion to an RBAC role. Policy exclusions are only supported in rulesets and rules. If a ruleset scope includes a policy exclusion based on labels outside the scopes you have permission for, you cannot view or manage those rulesets and rules. For example, a ruleset includes a policy exclusion of "All environments except Production" and you have permission for the Production environment but do not have permission for the Staging environment, you could not view or manage that ruleset.

Illumio Core Feature	Details
Explorer	When writing rules using Explorer, you can choose rulesets containing policy exclusions. You can edit the rules in the ruleset that have exclusions. You can add new proposed rules taking the exclusion scopes into account. However, you cannot add a new policy exclusion to an existing proposed rule or add an exclusion to a new proposed rule.
PCE web console maps	Policy exclusions are applicable to rules; they are not properties of the traffic links (the lines between the workloads) in the Illumio maps (Illumination Map, App Group Map, and Vulnerability Map). When you click **View Rule** for any traffic link, you can view the policy exclusions in the **View Rule** panel.
Enforcement Boundaries	Policy exclusions are not supported in Enforcement Boundaries. However, you can view policy exclusion rules in the **Rules** tab of an **Enforcement Boundary** details page.

Requirements and Restrictions

Requirements

When specifying a policy exclusion, it must be the same label type as the group it's being excluded from; the following examples are allowed:

- All Locations except the New Jersey location
- All Applications except Billing

However, this example is not allowed because it specifies different label types – Location vs Environment:

- All Locations except those with Development systems

Restrictions

- For each label dimension, you can specify an included or excluded label, but not both. The following examples show valid combinations:
  App: Swift
  App: All but Swift
  Env: Prod, App: All but Swift
  Loc: EU, Env: All but Prod
- You cannot specify both included and excluded labels within the same label type. The following examples are invalid combinations:
  Env: Prod, Env: Dev, Env: All but UAT
  Env: Prod, App: HRM, App: CRM, App: All but Swift
  App: HRM + App: CRM - App:Swift
  Loc: EU - Loc: Switzerland
- You cannot use policy exclusions with the following objects in the PCE:
  - Individual (named) workloads

- Virtual servers
- Virtual services
- Container hosts

Create a Policy Exclusion

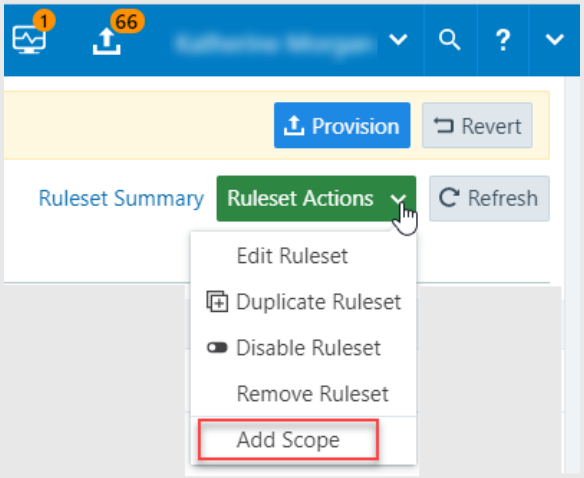
You can add policy exclusions to the scope of a new ruleset and new rules, or edit existing ruleset scopes and rules. This procedure provides the steps to add policy exclusions to the scope of a new ruleset and in new rules. For detailed information about working with rulesets and rules, see Rulesets [84] and Rules [96] in this guide.

1. From the PCE web console main menu, choose **Rulesets and Rules** > **Rulesets**.
   The Rulesets page appears.
2. Click **Add**.
   The Add Ruleset dialog box appears.

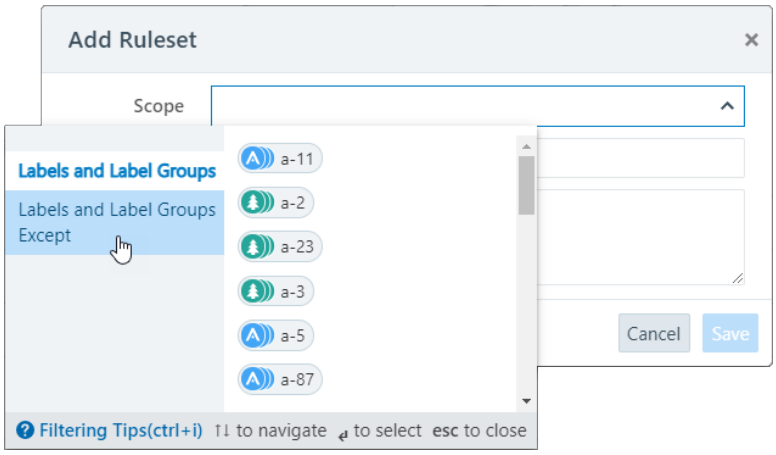
NOTE

The *Scope* field appears in the **Add Ruleset** dialog box only when the PCE is configured to display scopes in rulesets.

If the PCE is configured not to display scopes in rulesets, you can still add a scope with an exclusion after saving the ruleset. From the **Ruleset Actions** menu at the top right corner of the page, select **Add Scope**.



3. To add a policy exclusion to the scope of ruleset, open the Scope drop-down list and select **Labels and Label Groups Except**; then, select labels from the list. When done, click **Save**.



The page refreshes and displays the new ruleset and displays Intra-Scope Rules and Extra-Scope Rules tabs below the scope.

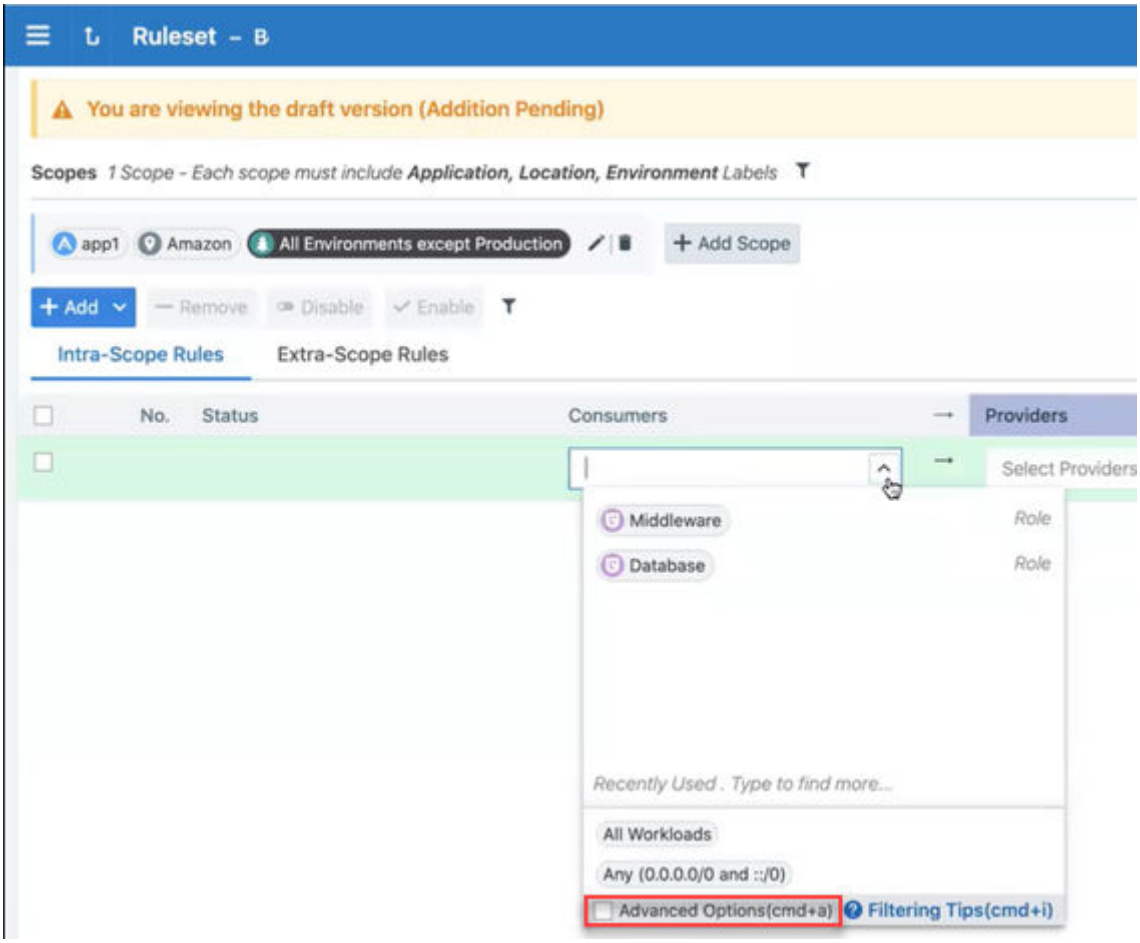
4. Select **Add** > **Add Intra-Scope Rule** or **Add** > **Extra-Scope Rule** depending on the type of rule needed. See Rules [96] in this guide for information about these rule types.

   An empty row for the new rule appears in the page.

5. Configure the values for the row. See Rule Writing [106] in this guide for more information.

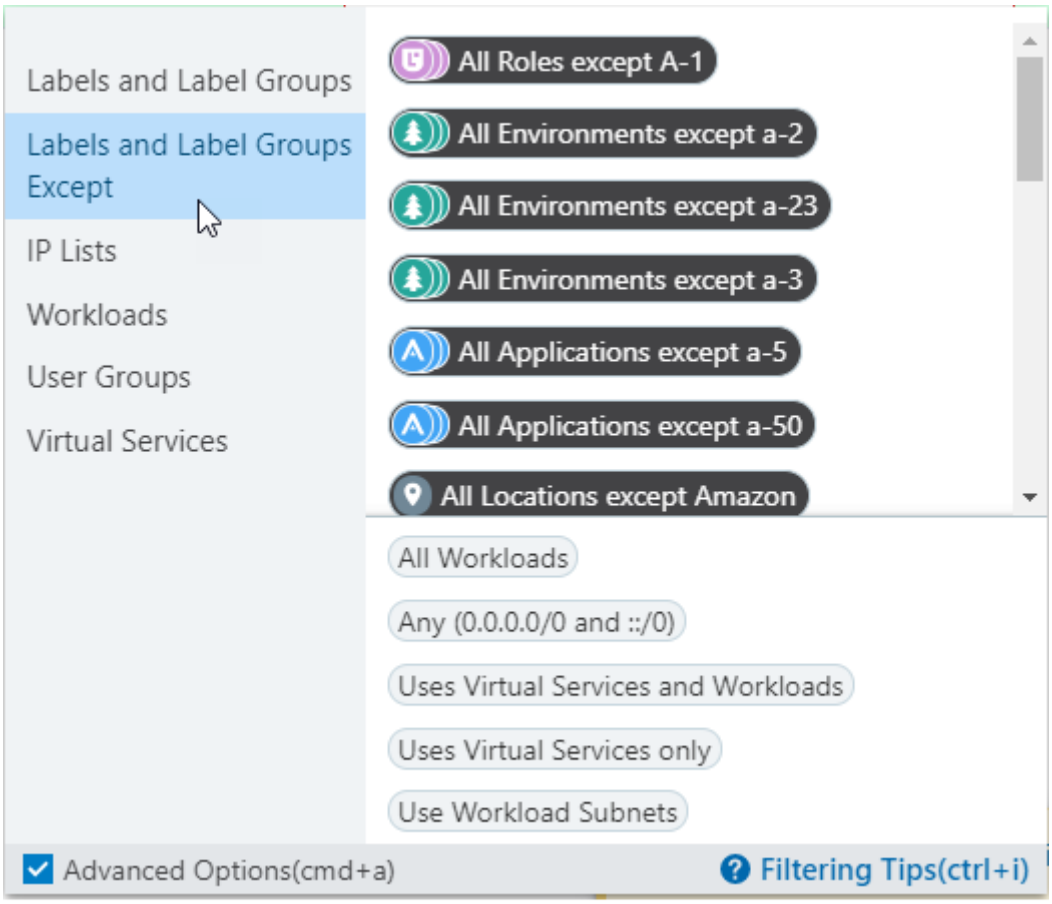
   To add a policy exclusion for either the Consumer or Provider, or both:

   a. From the *Select...* drop-down list, select the **Advanced Options** checkbox.



   A second panel opens displaying your options for adding exclusions.

   b. Select Labels and Label Groups Except and then select labels to exclude from the right-hand list.



c. When done configuring the rule, click the **Save** icon at the end of the rule row. See Rule Writing [106] in this guide for more information about the requirements and steps to fully configure a rule.

IMPORTANT

If you unintentionally create a rule that has conflicting elements between added labels or label groups and excluded labels or label groups, the PCE web console will display a warning that the security policy as configured might not apply. Specifically, the rule won't have an actual effect on workloads because the rule conflicts with the ruleset scope or the union of the two is will not have an impactful effect on workloads.

For example, you create a ruleset that has the scope “all but the Production environment” and then you create a rule in the ruleset that specifies the Production environment. This rule ends up having no effect because the rule conflicts with the ruleset scope and the union of the two is nothing.

Enforcement Boundaries

In the Illumio Core 21.2.0 release, Illumio introduces Enforcement Boundaries, a new feature to speed your journey toward Zero Trust.

The Journey Toward Zero Trust

The Illumio security policy model is based on the principle of Zero Trust. What is Zero Trust? Zero Trust security segments internal networks and prevents the lateral spread of ransom ware and cyber breaches. When implemented, it eliminates automatic access for any source – internal or external – and assumes that internal network traffic cannot be trusted without prior authorization.

Achieving Zero Trust security is possible with the Illumio Core because it bases security policy on an allowlist model. The allowlist model means that you must specifically define what traffic is allowed to communicate with your managed workloads; otherwise, it is blocked by default. It follows a trust-centric model that denies everything and only permits what you explicitly allow—a better choice in today's data centers. The list of what you do want to connect in your data center is much smaller than what you do not want to connect.

From a security perspective, creating policy based on allowlists is the preferred method and has the advantage of specifying what you trust explicitly; however, creating security policy exclusively on the allowlist model has some disadvantages. To start enforcing policy using the allowlist model, you must have a clear and complete understanding of all network communication within your data center. Accounting for all the connections that must be allowed between your hosts and applications is important or you risk business-critical applications breaking. Without this perfect knowledge, you either leave holes in your security, or you block necessary connections that break application functionality.

Approaches toward Reaching Zero Trust

Implementing allowlist security in a greenfield environment is much easier because your knowledge of application connection requirements is current and your application developers can define allowlist policy (rules) as part of the application deployment.

In a brownfield environment, applications are already deployed and running. A data center can have thousands of applications. How do you go about deploying an allowlist model into a brownfield environment? Often, Illumio Core customers implement allowlist security in a brownfield environment by creating security policy one application at a time. By default, the PCE sets the enforcement state to "visibility only" when you install a VEN on a host, thereby allowing you to assess what traffic is reaching the host. You can observe application behavior in reaction to potential security policy, and gradually move applications into full enforcement.

This approach can be very successful in achieving Zero Trust for your environment. However, it can lack the ability to accommodate unplanned security mandates, such as blocking a new security threat, or limiting traffic between corporate headquarters and a new business location.

So, how do you compensate between these two competing goals? Requiring a complete understanding of your data center versus being agile enough to tackle sudden security mandates? The solution is to introduce a new set of rules that determine where rules apply. These rules are referred to as Enforcement Boundaries in Illumio Core. Enforcement Boundaries can block traffic from communicating with workloads you specify, while still allowing you to progress toward a Zero Trust environment.

Enforcement Boundaries: How They Work

Enforcement Boundaries provide the following advantages:

- Unlike firewall policies, boundaries provide a simple policy model that does not depend on rule order.
- Boundaries facilitate a secure path to block traffic to achieve a Zero Trust model.

Enforcement boundaries are separate from allowlist rules. You can use multiple labels in a boundary or specify a label group. They are not limited by label types. Enforcement boundaries can be applied across a set of workloads, ports, and IP addresses.

You can create an Enforcement Boundary between workloads running different operating systems. When you use the existing Illumio Core RAEL labels to designate workloads by OS, creating an Enforcement Boundary by OS is possible.

You can combine Enforcement Boundaries with allowlist rules in your overall security policy. Allowlist rules always supersede Enforcement Boundaries. For example, you might have a server running a legacy NetBIOS file. This server is deployed in your development environment and must communicate with an application running in your production environment. You have already created an Enforcement Boundary blocking traffic between workloads in the development and production environments. You workaround this requirement by creating a specific rule allowing NetBOIS traffic to connect through the ports on the production server.

Summing It All Up

Enforcement Boundaries are...

- Part of the Illumio declarative policy model.

  You define the end state and Illumio Core creates the appropriate native firewall rules. You don't have to worry about rule order. In the traditional firewall, you do.
- Overridden by allowlist policy.
- Directional; you can create Enforcement Boundaries that are provider-centric or consumer-centric.

  For example, you want to block traffic from one location but only in one direction.
- Flexible; they are available for label groups and IP lists.
- Most often used for brownfield deployments.
- Intended to serve as a stepping stone towards a full traditional allowlist policy model.

  Implementing Enforcement Boundaries allow you to start the path toward full enforcement without having full knowledge of your data center environment.

Use Cases for Enforcement Boundaries

Potential use cases for Enforcement Boundaries include:

- Environmental or location separation and individual service enforcement.

  For example, you want to reduce risk in your environment by blocking traffic between your development and production environments.

  You want to control which locations or entities in your environment that can communicate. For example, you organization just acquired another entity and you want to block network traffic between the two locations.
- Blocking traffic from specific services from traversing your network; such as:
  - Unencrypted protocols like unencrypted HTTP traffic unless explicitly allowed to a host.
  - Ubiquitous services in your network; for example, you don't want to allow Telnet access anywhere in your network.

Examples: Ways to Deploy

The following examples illustrate some common ways to utilize Enforcement Boundaries.

Block Traffic Between Environments

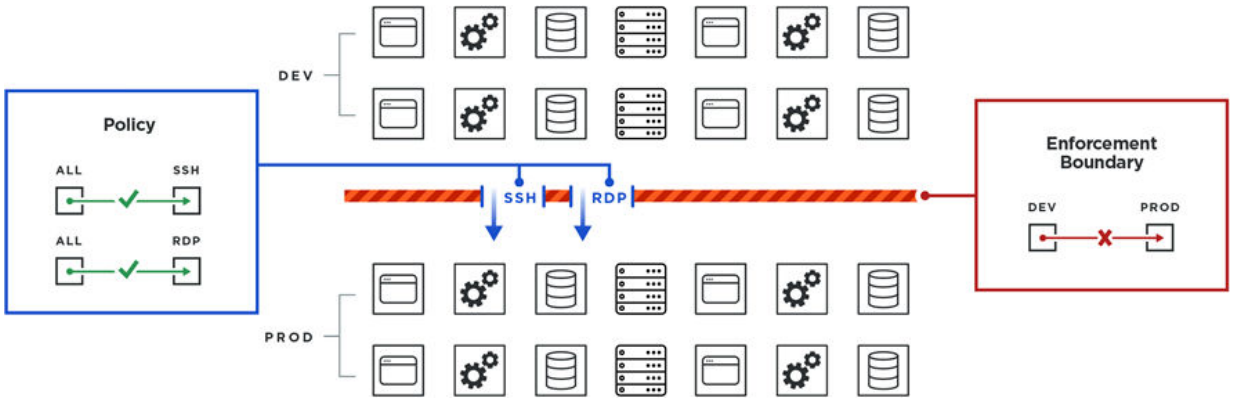
In the following example, an IT organization receives a mandate to implement security policy between the workloads in the development and production environments on a fixed project time line. Approaching this with a Zero Trust model could push implementation past the deadline. Achieving this security goal by using an Enforcement Boundary is achievable. It requires primarily two tasks: deploy VENs on all the workloads and set the Environment label correctly.

In this example, the IT organization can effectively block traffic between these two environments without requiring a complete picture of all port and protocol requirements for all applications or hosts in the production environment. No applications are at risk of breaking in production because required traffic was inadvertently blocked between applications or hosts in production.

Allowed Traffic Supersedes Enforcement Boundary

In this example, you can still allow instances of services to communicate with the production environment. Any policy that you create (the allowlist model) that allows a service to reach applications or hosts running in production still works and the rule will override the Enforcement Boundary. You explicitly create a rule that allows the SSH and RDP services to reach the necessary workloads.

SSH and RDP traffic can reach workloads in production without breaking the boundary blocking traffic from development workloads to production.



Manage Enforcement Boundaries

The topics in this section explain how to set up and manage Enforcement Boundaries in your data center.

Prerequisites and Limitations

Prerequisites

- VENs must be installed on the workloads (must be “managed”); Enforcement Boundaries are not supported for NEN-controlled or other unmanaged workloads.
- The VEN must be at release 21.2.0 or later.
- Workloads must be in the Selective Enforcement state for Enforcement Boundaries to apply to them.

Limitation for Virtual Services

Enforcement Boundaries do not apply to virtual services directly. Virtual services are enforced at the workload level. As a result, Enforcement Boundaries do not affect virtual services directly; instead, they affect the workloads that virtual services are comprised of.

FQDN-based Rules and Enforcement Boundaries

In Illumio Core, the PCE doesn't prevent you from creating IP lists containing FQDNs. In the PCE, you can create a rule for a consumer and an IP list. For example, you create the following IP list and rule in the PCE:

> **IP list 1:** `10.2.1.0/24`
>
> **Rule 1:** `*.dev.illumio.com`
>
> **Rule scope:** IP list 1 ¬ 80 TCP ¬ Environment: Production
>
> **Result:** Workloads in the Production environment will allow `80/tcp` traffic outbound to both `10.2.1.0/24` and `*.dev.illumio.com` (whatever are the IP addresses that FQDNs matching the pattern resolve to).

FQDN-based rules are not fully supported in Enforcement Boundaries. The PCE doesn't prevent you from adding FQDNs to an IP list impacted by an Enforcement Boundary. You can

use the IP list in an Enforcement Boundary. However, the PCE drops the FQDN component when an Enforcement Boundary results in an outbound deny rule to an IP list with FQDNs and the PCE writes a policy error to its log file.

Based on the example above, the Enforcement Boundary only denies traffic not previously allowed by the rule to `10.2.1.0/24` and not to FQDNs matching the `*.dev.illumio.com` pattern. Instead, the PCE generates the error message “partial policy delivered.”

Workflow for Deploying an Enforcement Boundary

To implement an Enforcement Boundary in your data center, complete the following tasks:

1. Install VENs on the workloads you want to protect with an Enforcement Boundary.
   An Enforcement Boundary will only block traffic for managed workloads in the PCE. For information about installing a VEN on a host, see "Workload Setup Using PCE Web Console". See also VEN Installation and Upgrade Guide for detailed information about installing VENs on hosts.
2. Assign the correct labels to each workload.
   For example, to block traffic from your development environment to your production environment, you must correctly assign the Environment label to all necessary workloads. See Labels and Label Groups [14] for information.

   TIP

   Using an Enforcement Boundary to accomplish the security mandate for traffic between development and production is more efficient than deploying a full allowlist model because you need to roll out only the Environment label rather than defining all four label types for your workloads and in your ruleset scopes.

3. Create rulesets and rules for the workloads you want to protect with an Enforcement Boundary.
   See Rulesets [84] and Rules [96] for information.

   WARNING

   Before creating an enforcement boundary, you must create the necessary rulesets and rules because traffic crosses the boundary and when you create it before putting rules in place, the PCE will drop the workload traffic until the rules are in place.

4. For the workloads you want to block traffic, move them into the Selective Enforcement state.
   See Place a Workload in Selective Enforcement State [138] for information.
5. Create an Enforcement Boundary that specifies the labels or IP lists (any IP range or subnet) to identify which workloads will be impacted by the boundary. Additionally, the boundary specifies specific services (or all services) to block traffic for.
   See Add an Enforcement Boundary [138] for information.

IMPORTANT

If you have not created any rules when you add an Enforcement Boundary, the PCE web console displays a message that the boundary has 0 rules. You need to correct this issue as soon as possible.

After you save a new Enforcement Boundary, the PCE calculates the impact of the new boundary and the PCE web console page refreshes to display the **Blocked Connections** tab for that boundary.

The **Blocked Connections** tab lists all the traffic that crosses the new boundary.

6. Review the list of traffic that currently crosses the new boundary and determine which connections need exceptions to the boundary. You can add rules for those exceptions at this point; then, remove them later as you refine you managed environment as you progress to a Zero Trust Security model.

   See Review Traffic Blocked by a Boundary and Add Rules [139] for information.
7. Provision the new Enforcement Boundary and any rules you added for traffic crossing the boundary.

   See Provisioning [116] for information.

Place a Workload in Selective Enforcement State

1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.

   The Workloads page appears.
2. From the Enforcement state drop-down list, choose **Selective**.

   A confirmation dialog box appears listing the impacted workloads.
3. Click **OK**.
4. To apply the enforcement state change to these workloads, provision the state change. See Provisioning [116] for information.

Add an Enforcement Boundary

1. From the PCE web console menu, choose **Enforcement Boundaries**.
2. Click **Add**.

   The Create Enforcement Boundaries page appears.
3. Enter a name for the Enforcement Boundary. Names can contain up to 255 characters.
4. Specify the consumers and providers of the connection. For a definition of “providers” and “consumers,” see Rules [96].
5. In the Providing Services field, select services to block or select **Port** or **Port Range** and enter the port numbers.

   The drop-down list contains a list of all services you have created in the PCE. See Services [20] for the steps to add services to the PCE.

TIP

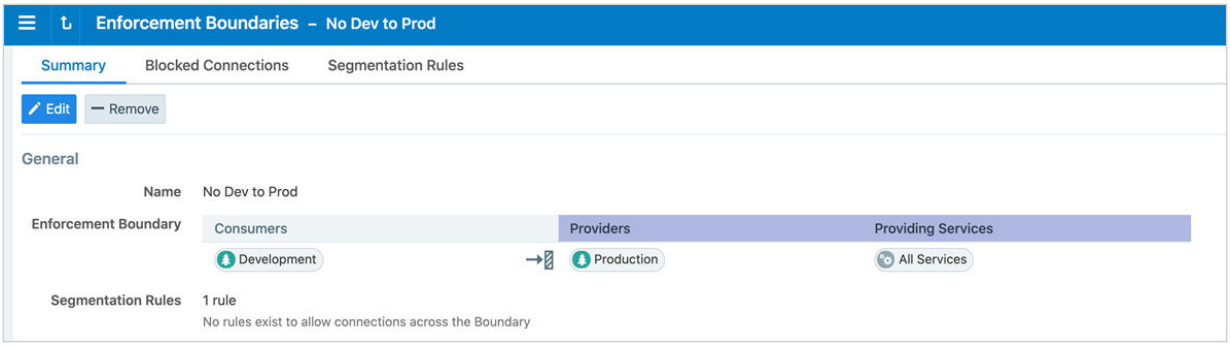
When selecting a providing service, you can select a specific service (or set of services) from the drop-down list. Alternatively, you can select “All Services” from the drop-down list; effectively blocking all traffic from the traffic provider. For example, you might want to block all traffic from your development environments reaching production and you'd select “All Services” for that Enforcement Boundary. See the example below.

6. Click **Save**. A progress bar appears while the PCE saves the boundary.

After you save a new Enforcement Boundary, the PCE calculates the impact of the new boundary and the PCE web console page refreshes to display the **Blocked Connections** tab for that boundary.

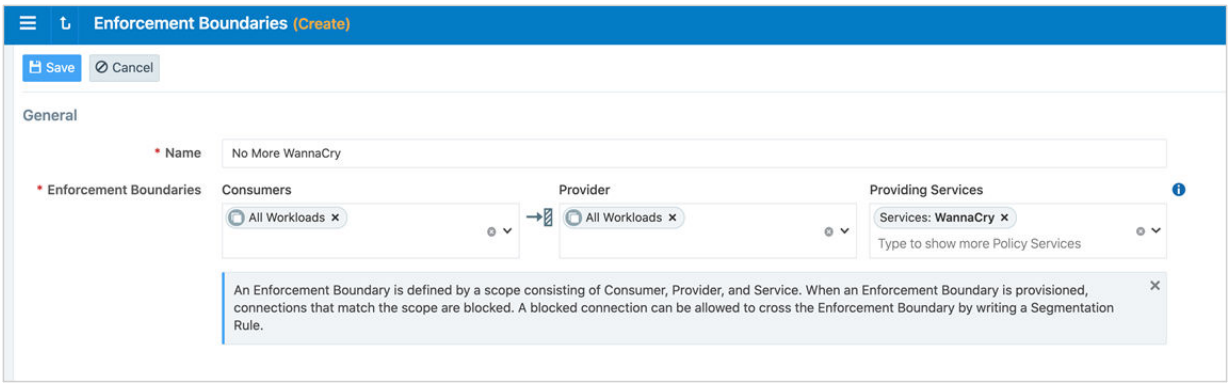
The **Blocked Connections** tab lists all the traffic that crosses the new boundary. See Review Traffic Blocked by a Boundary and Add Rules [139] for the steps to complete the Enforcement Boundary creation workflow.

Example: Summary page for an Enforcement Boundary that blocks traffic between development and production



Example: Enforcement Boundary that blocks traffic originating from the WannaCry service

The following boundary blocks communication for the four ports that are part of the WannaCry service for all workloads from all the workloads.



Review Traffic Blocked by a Boundary and Add Rules

When you add an Enforcement Boundary in the PCE for your managed environment, that boundary can affect large amounts of workloads (assuming all those workloads are in Selective Enforcement state.) Therefore, Illumio recommends you use care to not break any applications that have traffic that currently traverses the new boundary.

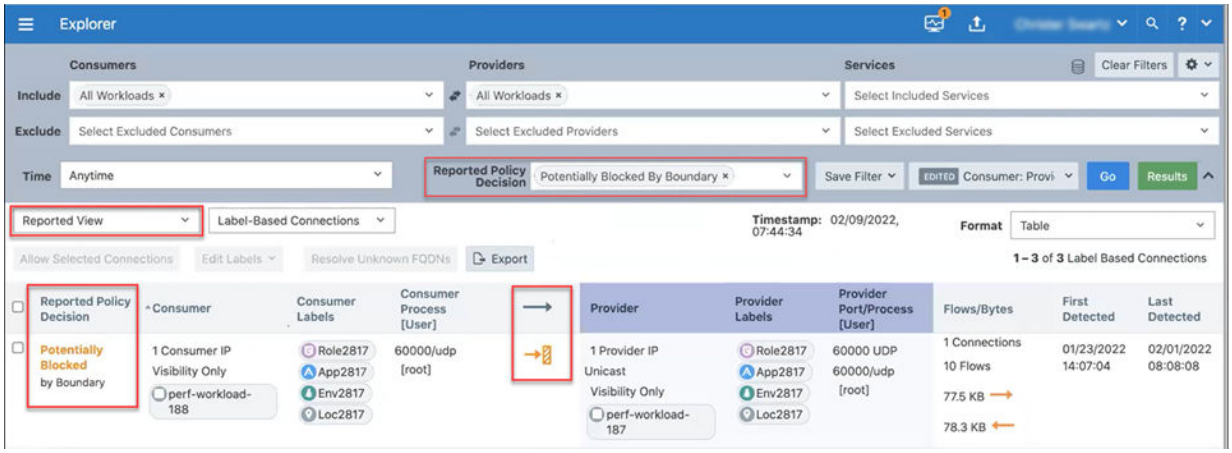
View Traffic Blocked by Boundary in Explorer

The Reported and Draft views of Explorer display traffic blocked by Enforcement Boundaries. You can distinguish when Enforcement Boundaries are blocking traffic from Explorer and use it for troubleshooting.

In particular, you can view information in Explorer about Enforcement Boundaries and where allowed traffic passes through a boundary:

- In selective enforcement, you can see whether traffic flows are blocked by Enforcement Boundaries.
- In full enforcement, you can see whether traffic flows are blocked by Enforcement Boundaries.
- In visibility only mode, you can see whether traffic flows are potentially blocked by Enforcement Boundaries.

Additionally, you can filter traffic flows that are blocked by Enforcement Boundaries in both Draft and Reported views.



NOTE

The ability to pinpoint the exact allow rule that is blocked by an Enforcement Boundary is not supported in the Explorer Reported view. To view this information, switch to the Draft view of Explorer. In Draft view, you can locate the allow rule blocked by an Enforcement Boundary.

View Blocked Connections in Enforcement Boundary Page

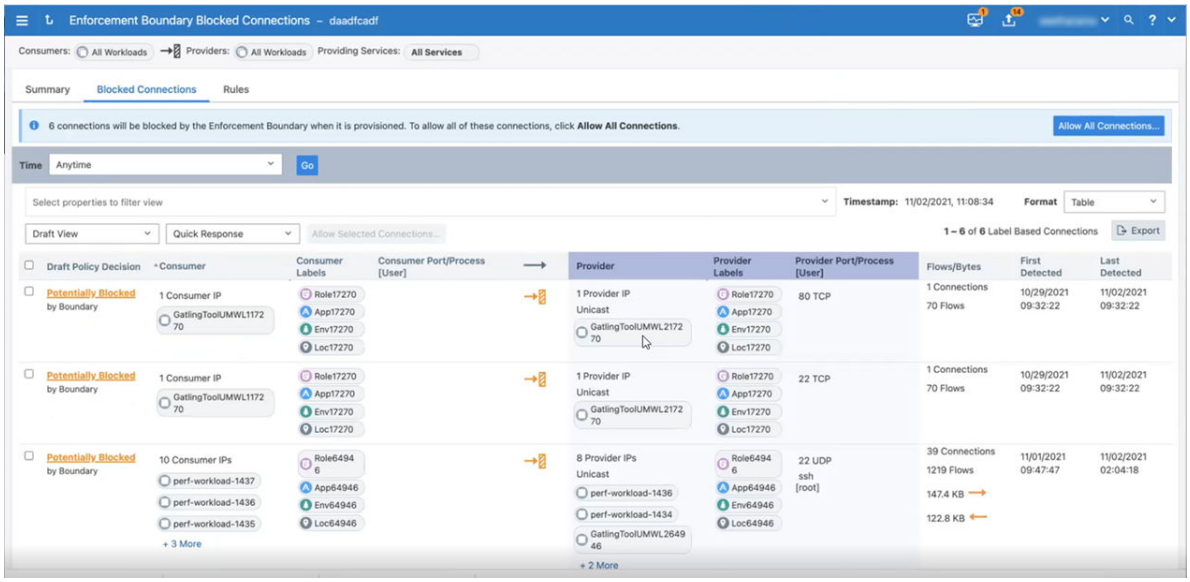
To help evaluate traffic that traverses the boundary, the PCE web console includes a tab for blocked traffic on the Boundary page. This tab essentially runs an Explorer query that returns all the traffic that would be blocked once you provision the new Enforcement Boundary.

IMPORTANT

After you save a new Enforcement Boundary, the PCE calculates the impact of the new boundary and the PCE web console page refreshes to display the **Blocked Connections** tab for that boundary. At this point in the boundary creation workflow, you should review the list of traffic that currently crosses the new boundary and determine which connections need exceptions to the boundary. You can also perform this task for existing Enforcement Boundaries at anytime.

To review traffic blocked by a new boundary and add rules for exceptions:

1. From the Enforcement Boundary Blocked Connections page, review the list of traffic that traverses the boundary and requires an exception to the boundary.



   The PCE creates default rules for this traffic that currently traverses the Enforcement Boundary.
2. To accept the default rules created by the PCE, click the **Allow All Connections** button after reviewing the list of traffic flows traversing the boundary.

   NOTE

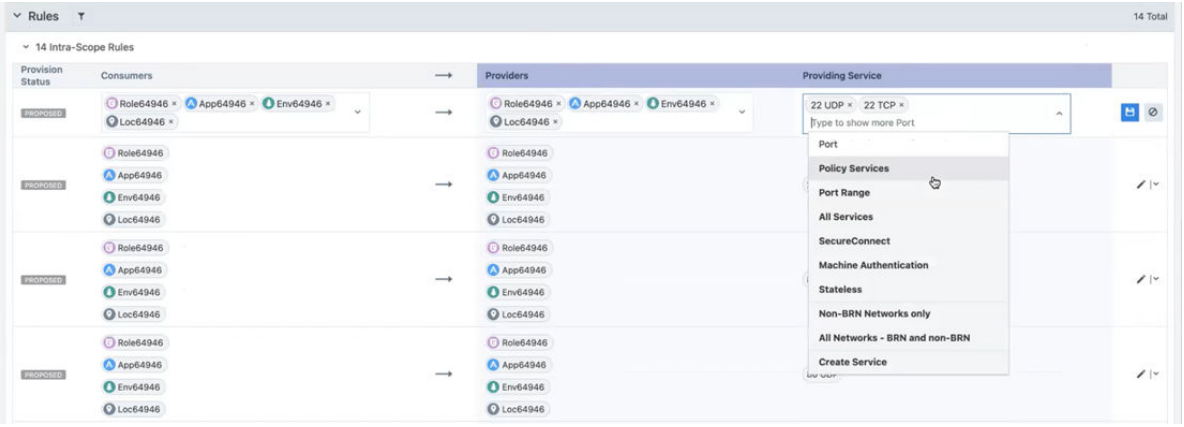
   If you have more than 50 traffic flows blocked by the boundary so that the list of connections spans multiple pages in the PCE web console, clicking Allow All Connections accepts the rules in all pages.

   —OR—

   To review and accept rules for only specified traffic flows, select their check boxes and click the **Allow Selected Connections** button.

   The page refreshes and displays the proposed rules to create exceptions to the Enforcement Boundary. All new rules display the status “Addition Pending” in the **Provision Status** column.
3. To modify and optimize the proposed rules for traffic traversing the boundary, click the **Pencil** icon at the end of the row for the rule you want to optimize. The values for that row become editable. Make changes to the rule as needed and click the **Save** icon.

   For example, you might want to collapse rules for similar protocols into one rule. When you collapse two rules into one, the PCE automatically removes the original duplicate rule.



4. When you are done reviewing and optimizing the proposed rules, click the **Save** button at the top of the page.

   The page refreshes and the Rules tab for the Enforcement Boundary appears. All rules that will traverse the boundary are listed.
5. To provision all pending policy changes, click the **Provision** button at the top of the page. The provisioning process begins.

   See Provisioning [116] for information.

Disable an Enforcement Boundary

You can temporarily disable an enforcement bounday, such as for troubleshooting. You can enable it again when needed.

1. From the PCE web console menu, choose **Enforcement Boundaries**.
2. Select one or more enforcement boundaries you want to disable.
3. Click **Disable**.

   The status of the enforcement boundary changes to Disabled.

When you are ready to enable the enforcement boundary again, select it and click **Enable**.

Remove an Enforcement Boundary

1. From the PCE web console menu, choose **Enforcement Boundaries**.
2. Select the enforcement boundary you want to remove.
3. Click **Remove.**

   A confirmation dialog box appears.
4. Click **Remove** again to permanently delete the enforcement boundary from the PCE.

   The Enforcement Boundaries page reappears. An icon appears beside the enforcement boundary indicating that the deletion is pending.
5. Provision the change. See Provisioning [116] for information.

Secure Workload Connections

This section describes SecureConnect and AdminConnect, which are Illumio provided encryption options.

SecureConnect was developed for host-to-host traffic encryption between paired workloads. AdminConnect was developed to get control access to network resources based on Public Key Infrastructure (PKI) certificates.

SecureConnect

Enterprises have requirements to encrypt in-transit data in many environments, particularly in PCI and other regulated environments. Encrypting in-transit data is straightforward for an enterprise when the data is moving between data centers. An enterprise can deploy dedicated security appliances (such as VPN concentrators) to implement IPsec-based communication across open untrusted networks.

However, what if an enterprise needs to encrypt in-transit data within a VLAN, data center, or PCI environment or from a cloud location to an enterprise data center? Deploying a dedicated security appliance to protect every workload is no longer feasible, especially in public cloud environments. Additionally, configuring and managing IPsec connections becomes more difficult as the number of hosts increases.

SecureConnect Overview

SecureConnect leverages the built-in IPsec subsystem of host operating systems. On Windows hosts, SecureConnect utilizes the Windows IPsec subsystem. On Linux hosts, SecureConnect utilizes StrongSwan and Linux kernel IPsec for traffic encryption.

With SecureConnect, Illumio delivers a feature configuring the Security Policy (SP) necessary to enable traffic encryption between workloads. Once authenticated, encryption and cryptography suites provide confidentiality and data integrity to network traffic between workloads.

The PCE centrally manages all Security Policy (SP) for workloads so that it can be policy-driven. For example, a customer can require that all traffic between their web servers and database servers be encrypted. Selecting the SecureConnect option for these workloads allows the PCE to apply the requisite security policy to your organization to make that happen. SecureConnect reduces the complexity of configuring IPsec encryption and auto-scales per your policy definitions.

SecureConnect Use Cases

Employing SecureConnect is especially beneficial in these common scenarios:

- Facilitate PCI compliance by ensuring that confidential data is encrypted over the network.
- Secure off-site backup and recovery of data across geographically distributed data centers.
- Secure communications across applications and application tiers for regulatory compliance and tighter security.
- Enable secure data migration across different public cloud providers.

SecureConnect Features and Enforcement

SecureConnect works for connections between Linux workloads, Windows workloads, and Linux and Windows workloads.

NOTE

SecureConnect rules are only applied to workloads where the VEN is in a non-idle enforcement state.

However, unlike other rules, SecureConnect requires matching rules to be applied to workloads on BOTH sides of any connection. Therefore, SecureConnect traffic is not supported between two workloads where a VEN on either side is in the idle state.

AdminConnect

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

When you enforce policy on servers for clients that change their IP addresses frequently, the policy enforcement points (PEPs) continuously need to update security rules for IP address changes. These frequent changes can cause performance and scale challenges, and the ipsets of protected workloads to churn.

Additionally, using IP addresses for authentication is vulnerable to IP address spoofing. For example, server A can connect to server B because the PEP uses IP addresses in packets to determine when connections originate from server A. However, in some environments, bad actors can spoof IP addresses and impact the PEP at server B, so it mistakes a connection from server A.

Illumio designed its AdminConnect (Machine Authentication) feature with these environments in mind. Using AdminConnect, you can control access to network resources based on Public Key Infrastructure (PKI) certificates. Because the feature is based on the cryptographic identity associated with the certificates and not IP addresses, mapping users to IP addresses (common for firewall configuration) is not required.

With AdminConnect, a workload can use the certificates-based identity of a client to verify its authenticity before allowing it to connect.

Features of AdminConnect

Cross Platform

Microsoft Windows provides strong support for access control based on PKI certificates assigned to Windows machines. Modern data centers, however, must support heterogeneous environments. Consequently, Illumio designed AdminConnect to support Windows and Linux servers and Windows laptop clients.

AdminConnect and Data Encryption

When only AdminConnect is enabled, data traffic does not use ESP encryption. This ensures that data is in clear text even though it is encapsulated in an ESP packet.

The ESP packets are encrypted when AdminConnect and SecureConnect are enabled for a rule.

Ease of Deployment

Enabling AdminConnect for identity-based authentication is easy because it is a software solution that does not require deploying network choke points like firewalls. It also does not require you to deploy expensive solutions such as Virtual Desktop Infrastructure (VDI) or bastion hosts to control access to critical systems in your data centers.

AdminConnect Prerequisites and Limitations

Prerequisites

You must meet the following prerequisites to use AdminConnect:

Limitations

You cannot enable AdminConnect for the following types of rules:

- Rules that use All services
- Rules with virtual services in sources or destinations
- Rules with IP lists as sources or destinations
- Stateless rules

AdminConnect is not supported in these situations:

- AdminConnect does not support “TCP -1” (TCP all ports) and “UDP -1” (UDP all ports) services.
- You cannot use Windows Server 2008 R2 or earlier versions as an AdminConnect server.
- Windows Server does not support more than four IKE/IPsec security associations (SAs) concurrently from the same Linux peer (IP addresses).

Legal Notice

Resources

- Legal information
- Trademarks statements
- Patent statements
- License statements

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation