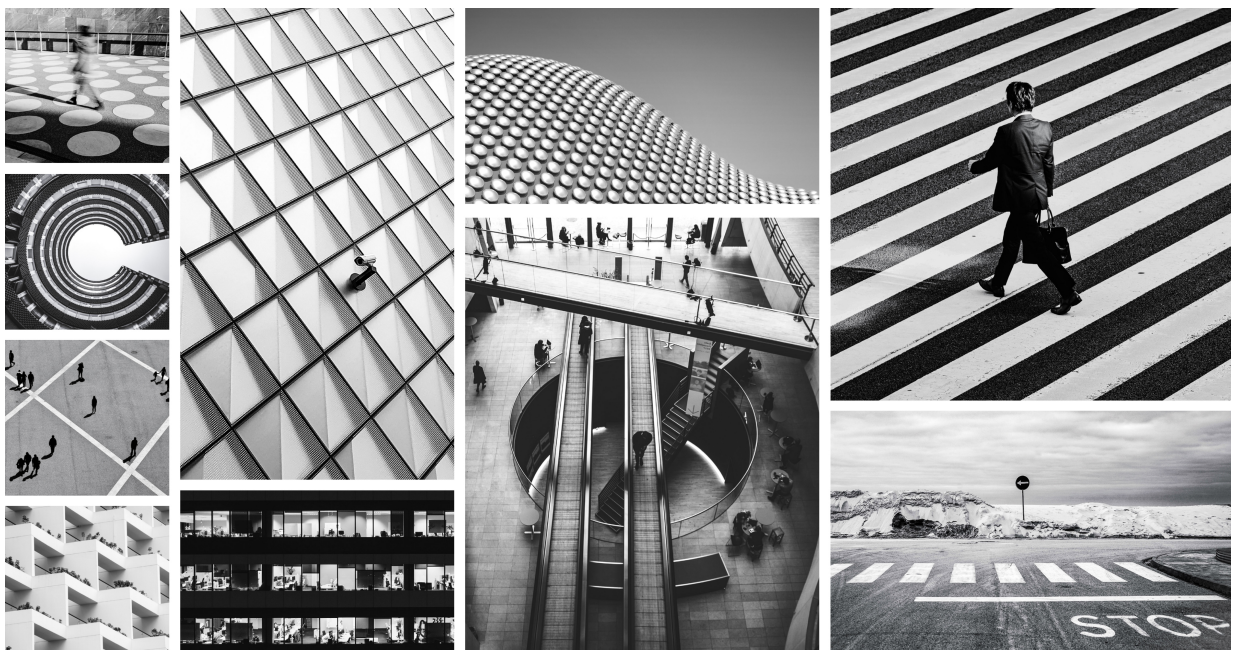


Using Xpress

Published: November, 2024



Please be advised that Edge and Xpress are planned for end-of-life. For more information and assistance, reach out to our Support team.

Table of Contents

- Legal Notice 4
- Xpress 5
 - About Xpress 5
 - Using the Xpress Runbook 5
 - About the Xpress Dashboard 7
 - Protecting Servers Overview 9
 - Protecting Endpoints Overview 15
 - Recommendations 18
 - VEN Compatibility Check 20
 - Xpress Visualization 22

Legal Notice

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

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

Resources

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

Contact Information

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

Xpress

About Xpress

This guide describes how to use the Xpress features. The goal of Xpress is to allow quick onboarding of servers and endpoints through fully guided wizards that analyze your network traffic and give you rule recommendations that minimize risk.



IMPORTANT

Please be advised that Illumio products Edge and Xpress are planned for end-of-life. For more information, reach out to the Illumio Support team.

Using the Xpress Runbook

This section provides an overview of the Xpress Runbook.

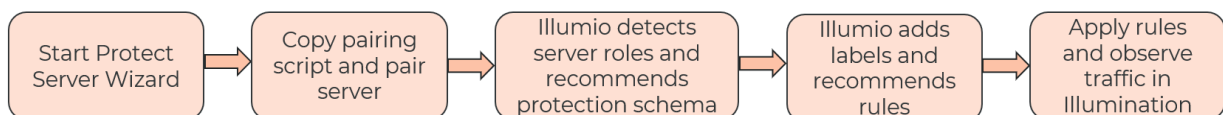
Protecting Servers

The use case for protecting servers with Xpress is to apply targeted segmentation and ringfencing to critical Windows servers, thereby protecting them from compromise. At time of writing, these include: Active Directory, Active Directory Federation Services, File Server, Windows Server Update Services, and Print Services.

Please review the 'What's New' in-app guide for new schemas, which protect different types of servers, as they are made available. If you have a recommendation, please email us with your suggestions at xpress-feedback@illumio.com.

In addition to improving the user experience, Illumio Core has added server role detection and a protection template for server roles. Furthermore, the system automatically labels these servers and recommends rules for the server roles.

The following flow lists the key events in the server protection process:



Illumio recommends that you on-board Active Directory and domain controller servers first.

If you haven't already, open a command terminal for the machine you want to protect by pairing an agent (VEN) to the workload.

1. From the dashboard, select **Add Servers**.
The Let's start by installing agents on your servers page of the wizard appears.
2. Once you select **Copy Script** for your operating system, you will paste the copied script into the command prompt of the machine and press **Enter**. This will install an agent on the server, which will start communication with Illumio Core. If you first wish to see what the script contains, select **Preview Script**.
3. After you select **Next**, the wizard will recommend protection schemas based on windows server roles.
4. In the Choose protection schemas to apply page, select the **Summary of Rules** link in the Policies column to review the recommended rules for any server with a recommended or selected protection schema.
If you do not want to confirm the recommended protection schemas for a given server, select **Change** in the Protection Schema column and choose different schemas that will apply different sets of rules and labels.
5. When you are satisfied with the selections, choose **Save**. The wizard will then show you traffic that will be potentially blocked. Any saved schemas will still need to be enforced to provide protection for the servers.
6. From the Xpress Dashboard, select the **Protection Ready** link to continue to enforcement.

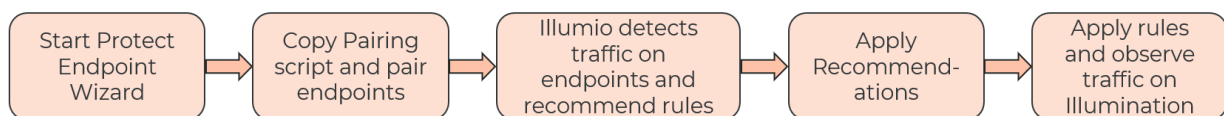
For more information on protecting servers, see [Protecting Servers \[9\]](#).

Protecting Endpoints

The use case for protecting endpoints with Illumio Core is to block all inbound traffic to all endpoints, making sure nothing is getting into your endpoints unless explicitly allowed (Admin access to User endpoints; access based on observed inbound traffic from services).

Illumio Core supports the use of endpoint groups to allow and deny traffic from different paired endpoints. The wizard will suggest security recommendations to apply to endpoints such as tablets or laptops.

The following flow lists the key events in the endpoint protection process:



If you haven't already, open a command terminal for the machine you want to protect by pairing an agent (VEN) to the workload.

1. From the dashboard, select **Add Endpoints**.
The Let's start by installing agents on your endpoints page of the wizard appears.
2. Once you select **Copy Script** for your operating system and selected user role (user or administrator), you will paste the copied script into the command prompt of the machine and press **Enter**.
This will install an agent on the endpoint, which will start communication with Illumio Core. If you first wish to see what the script contains, select **Preview Script**.
If you wish to later pair an endpoint with the same script, such as when a new person joins the department with the applicable endpoint, you can re-enter the endpoint onboarding wizard or do it manually.

3. The wizard will present recommendations based on your environment when you select **Next**. However, you should evaluate your network traffic load (no more than 24 hours are necessary) prior to accepting recommendations and selecting **Next**.
The Endpoint Traffic page of the wizard appears.
4. This page shows details about administrator access, observed services and traffic, and what inbound traffic is blocked. For observed services and traffic, Illumio will note what traffic it recommends allowing and blocking.
5. When you have reviewed or modified the recommended settings, select **Save Rules**.
This provisions the endpoint group and associated components. A Success dialog will appear. From there you can return to the Xpress Dashboard. The provisioned endpoint group and associated components will still need to be enforced to provide protection for the endpoint.
6. From the Xpress Dashboard, select the **Protection Ready** link to continue to enforcement.

For background information on protecting endpoints, see [Protecting Endpoints \[15\]](#).

Network Flow Visibility

Illumio Core map is a real-time map that shows how your systems are connecting and communicating with each other and the outside world. This map can be accessed using the Explore > Map link on the side navigation bar. It provides a visually intuitive way for you to review the traffic as affected by the policies (rules and schemas) you applied using the Xpress wizards. Draft view lets you predict how the policies would affect connections between your servers and/or endpoints, including potentially blocked traffic. Reported view lets you see how the enforced policies affect connections between your servers and/or endpoints, including actually blocked traffic. See [Xpress Visualization \[22\]](#).

Xpress Support & Troubleshooting Assistance

Please contact xpress-feedback@illumio.com if you need onboarding guidance, need clarification, or want to provide feedback. We are excited to assist you as you explore the guided workflows.

About the Xpress Dashboard

The top portion of the Illumio Core Dashboard includes quick snapshots of Servers and Endpoints. It also features links for adding, enforcing, or installing agents upon, servers or endpoints. It also has links for viewing workloads.

The remaining portion includes provides a quick way to view your information security posture at a glance.

A note about top-level navigation tabs in Illumio Core:

- Protect: This tab is the default active tab if you do not have protected endpoints or servers. If on a different tab, use the dropdown menu to add servers or endpoints.
- Dashboard: This tab is the default active tab if you do have protected endpoints or servers. This tab is described here.
- Illumination: Select this tab to view the Illumination Map.

Using the Illumio Core Dashboard

Illumio Core dashboard is organized into the following sections:

- Server and Endpoint Tiles
- VEN and Policy Tiles
- Traffic Explorer

Server and Endpoint Tiles

Servers

This tile lists the number of servers you have, including unlabeled, unprotected, and total protected servers.

- Click the **Protected** link to go to the Workloads page. This shows the workloads and VENs on your protected machines, along with connectivity, enforcement state, time of last policy application, VEN version, and so on.
- Click the **Unlabeled** link to also go to the server pairing wizard, but with the Include previously paired servers checkbox marked by default, and without the ability to re-install the agent on the previously servers from that wizard. You will be able to install agents on any remaining unpaired servers. You will also be able to review the servers and select **Next** to proceed to the Labeling page, where you can review or change the recommended protection schemas.
- Click the **Protection Ready** link to go to the server enforcement wizard.
- Click the **Add Servers** link to go to the server pairing wizard. This shows your workloads that are ready for pairing, along with a pairing script and recommendations for protection.

Endpoints

This tile lists the number of endpoints you have, including unlabeled, unprotected, and total protected endpoints.

- Click the **Protected** link to go to the Workloads page. This shows the workloads and VENs on your protected machines, along with connectivity, enforcement state, time of last policy application, VEN version, and so on.
- **Unlabeled** does not contain a link. This metric is populated only when a user manually removes a label, using the Classic UI. Illumio does not recommend removing endpoint labels.
- Click the **Protection Ready** link to go to the endpoint enforcement wizard.
- Click the **Add Endpoints** link to go to the endpoint pairing wizard. This shows the observed services and traffic, along with a pairing script and recommendations for protection.

VEN and Policy Tiles

These tiles provide broad, visualized information about your Illumio setup, including the following:

- Active VENs: Click on the numeral in the Active VENs widget to go to Workloads > VENs. This shows your VENs and their status, labels, operating system, etc.
- Active Policy: Click on the numeral in the Active Policy widget to go to Policy > Rulesets and Rules. This shows the rules and their status, modification date, etc.
- Draft Policy Changes: Click on the numeral in the Draft Policy widget to go to Policy > Draft Changes > Drafts. This shows policy changes (rulesets) that are still in draft form.
- Blocked / Simulated Block Flow: Click on the numeral in the Blocked / Simulated Block Flow widget to go to the Explore > Traffic page, filtered by **Blocked** and **Simulated Block**

policy decisions. This shows blocks, simulated or otherwise, with their source, source label, source process, destination, destination labels, destination ports and processes, as well as their flows and connections.

- **VEN count by Status / Health:** To view your VENs filtered by **Health** on the Workloads > VENs page, click on the numerals in the Health entries. To view your VENs filtered by **Status** on the Workloads > VENs page, click on the numerals in the Status entries.
- **VEN count by OS:** To view your VENs filtered by operating system on the Workloads > VENs page, click on the colored lines in the VEN Count by OS widget.
- **VEN count by Version:** To view your VENs filtered by version on the Workloads > VENs page, click on the colored lines in the VEN Count by Version widget.
- **VEN count by Enforcement Mode:** Click on the circle in the VEN Count by Enforcement Mode tile to go to Workloads > All Workloads filtered by enforcement mode. If you click the **Visibility Only** portion, for example, the page will display only those workloads set to **Visibility Only** enforcement. If you click the **Selective** portion, the page will display only those workloads set to **Selective Enforcement**.

Dashboard Traffic Mini-Explorer

This feature provides a quick way to explore ports and workloads. For a more complete visualization of traffic, with more filters, see [Xpress Visualization \[22\]](#).

- **Ports:** This tab contains a table with ports and their associated flows, sources, and policies.
- **Workloads:** This tab contains a table with workloads and their associated flows, ports, and policies.

Illumination: Click on the **Go to Illumination** link in the Illumination tile to go to the Illumination page. This provides a way to reveal the traffic flows in your network and to help you configure policies to secure your applications. See [Xpress Visualization \[22\]](#).

Protecting Servers Overview

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

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

A note about top-level navigation tabs in Illumio Core:

- **Protect:** This tab is the default active tab if you do not have protected endpoints or servers. If on a different tab, use the dropdown menu to add servers or endpoints.
- **Dashboard:** This tab is the default active tab if you do have protected endpoints or servers.
- **Illumination:** Select this tab to view the Illumination Map.

About Server Pairing

Illumio Core supports the use of server pairing to identify and protect your critical applications using best-practices for ring-fencing, tailored to your network traffic. Pairing a workload requires running the pairing script on it to install the VEN.

When you first log into the Illumio Core, a default pairing profile containing a pairing script is provided so you can begin pairing workloads. You also have the option to create a new

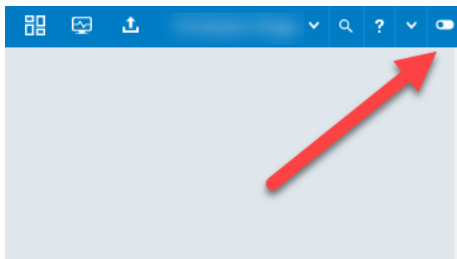
pairing profile if you want to configure your own workload pairing settings. However, the easiest way to pair a Windows server workload is to use the default pairing profile. It gets you started quickly and reduces the work associated with managing multiple pairing profiles. For instructions, see [Xpress Runbook \[5\]](#).

Pairing Servers

To pair servers:

If you haven't already, open a command terminal for the machine you want to protect by pairing an agent (VEN) to the workload.

1. If you are not already in Illumio CoreProtect or Landing page, from the PCE web console main menu, choose the **Toggle** switch in the upper right-hand corner.



If you do not yet have any workloads paired, the Illumio CoreProtect page appears. If you already have workloads paired, the Illumio CoreLanding page appears. The following instructions assume that you are on the Landing page, and are virtually identical to what you would do if you begin from the Protect page.

2. Under Servers, select **Add Servers**.
The Let's start by installing agents on your servers page of the wizard appears. It shows hostnames, status, and roles of current paired servers.
3. Select your operating system.
4. Once you select **Copy Script**, you will paste the copied script into the command prompt of the machine whose workload you want to pair with a VEN. If you wish to later pair a server with the same script, such as when a new server is added, you can re-enter the server pairing wizard or do it manually. If you want to see what the script contains, select **Preview Script**.
5. If you want to refresh the list of servers, you can either select **Refresh** to do it manually, or you can let the Auto Refresh do it automatically every 30 seconds. If you do not wish the list to automatically refresh, toggle the **Auto Refresh** switch.
6. The wizard will present recommendations based on your environment when you select **Next**.
7. The Choose protection schemas to apply page of the wizard appears. To review the recommended rules for any server with a recommended or selected protection schema, select the **Summary of Rules** link in the Policies column.
If you do not want to confirm the recommended protection schema for a given server, select **Change** in the Protection Schema column and choose a different schema that will apply a different set of rules and labels.
8. When you are satisfied with the selections, choose **Save**. Illumio will then show you traffic that will be potentially blocked. Any saved schemas will still need to be enforced in order to provide protection to the servers.

More Information About Pairing Servers

The following information provides some background on what happens when pairing servers in Illumio Core.

Rule Creation and Protection Schemas

When first opening Illumio Xpress, it will automatically create default labels, a default pairing profile, and a default ruleset.

When pairing and protecting servers, you need to replace these defaults with new rules and labels suited to your specific environment. The easiest way to do this is to use the Server Wizard. It will provide recommendations that will label your workload and create appropriate rules via protection schemas.

Protection Schemas

As part of the latest version of the Server Wizard, after workloads are paired, the PCE will automatically detect which server roles are on the machine and match them against the available protection schemas. A protection schema represents a way to associate ('protect') a workload with a given application, and Illumio Xpress supports up to 10 protection schemas per server workload. This support for multiple protection schemas is called the Multiple Server Role feature. The PCE will recommend the protection schemas that have been detected, and you have the option to choose whether to accept or override the provided recommendations. See [Recommendations \[18\]](#).

By selecting a given protection schema, corresponding labels will be applied to your workload, and corresponding rulesets will be created. After selecting the protection schemas for a given workload, the associated policies (if they exist) will appear in hyperlinks in the Server Wizard. If a protection schema does not yet have an associated policy, selecting the protection schema will still result in the appropriate labeling and inclusion of the workload into policies that will be added in near future.

Illumio Xpress Server Roles

This list is updated as additional server roles, protection schemas, and rulesets become available.

Server Role/Application	Protection Schema Available	Rulesets Available
Active Directory	X	X
Active Directory Federation Services	X	X
Active Directory Certificate Services	X	X
Active Directory Lightweight Directory Services	X	X
File Server	X	X
Windows Server Update Services	X	X
Print Server	X	X
Windows Deployment Services	X	X
Active Directory Rights Management Services	X	
Hyper-V	X	

Remote Desktop Services	X
Remote Access	X
DNS	
DHCP	
Web-Server	
VolumeActivation	
NPAS	
DeviceHealthAttestationService	
HostGuardianServiceRole	
Fax	

How the Multiple Server Role Feature Works

Illumio's enterprise policy model uses many different constructs to allow for users to write security policies with great flexibility.

Labels are the foundation of these constructs. With labels, you can specify a dimension (such as environment, role, etc.) and a value. These labels can be assigned to workloads, and policy rules can be written using these labels. Rules can also be written with label groups, which represent a collection of labels, each with the same dimension.

The Multiple Server Role feature uses these two constructs to apply the appropriate policies to your workloads. Each protection schema is associated with multiple label group objects, and these label groups will now be used in the accompanied policy rulesets.

When a protection schema, or group of protection schemas, are selected for a workload, the PCE processes this set by producing a new label that represents this grouping of schemas.

By selecting these protection schemas, the workload will now have appropriate policies to protect it. After saving your selections, you can view the dynamically created labels on the workload by going to the workload page. Illumio Xpress automatically adds these labels to the label groups used in the rulesets associated with the selected protection schemas. The API provisions the label group update in which we dynamically create the label and move it into the label group.

Dynamically Created Labels

When one protection schema is used, the full label name is applied. If multiple protection schemas are used, Illumio Xpress represents each protection schema with a short code and groups them together to make labels.

Protection Schema	App Whole Name	App Short Code	Role Whole Name	Role Short Code

Active Directory	Active Directory	AD	Domain Controller	DC-SVR
Active Directory Federation Services	Active Directory Federation Services	ADFS	ADFS Server	ADFS-SVR
Active Directory Certificate Services	Active Directory Certificate Services	ADCERT	CA Server	CA-SVR
Active Directory Lightweight Directory Services	Active Directory Lightweight Directory Services	ADLDS	AD LDS Server	ADLDS-SVR
File Server	File Servers	FILE	File Server	FILE-SVR
Windows Server Update Services	Windows Update Services	WSUS	WSUS Server	WSUS-SVR
Print Server	Print Services	PRINT	Print Server	PRINT-SVR
Windows Deployment Services	Windows Deployment Services	WDS	WDS Server	WDS-SVR
Active Directory Rights Management Services*	Active Directory Rights Mgmt Services	ADRMS	AD RMS Server	ADRMS-SVR
Hyper-V*	Hyper-V	HYPERV	Hypervisor	HYPERV-SVR
Remote Desktop Services*	Remote Desktop Services	RDS	RDS Server	RDS-SVR
Remote Access*	Remote Access Services	RA	RA Server	RA-SVR

*These do not have rulesets at time of writing.

For example, if you select the following protection schemas together:

- Active Directory
- File Server
- Windows Server Update Services

This will result in the following two labels being dynamically created and subsequently applied to your workload:

- App Label: "AD | FILE | WSUS"
- Role Label: "DC | FILE-SVR | WSUS-SVR"

Rule Enforcement

For rules (and protection schemas) to be enforced, they must be in the correct enforcement state. You can put them in the correct enforcement state by selecting the **Protection Ready** link from the Server tile on the Illumio Xpress Dashboard.

Re-onboarding Servers to Accommodate New Traffic

If you installed new applications or added new functionality to a server after onboarding (applying protection schemas, labels, etc.), you may need to re-onboard the server. If you wish to re-onboard a server, wait for at least 24 hours after new application installation or functionality modification to give Xpress time to recognize the change before using the steps listed below.

For example, if you went through the Server Pairing Wizard and selected an Active Directory (AD) protection schema, but later configured that server to do double-duty as a print server as well, your print traffic would be blocked by default. This is because you had originally selected a protection schema that allowed only that traffic necessary for AD server functionality.

To use the Server Pairing Wizard and select additional protection schemas after you have previously applied protection schemas, do the following:

1. From the Xpress Dashboard, browse to **Workloads > Servers** and select the server in question in the Name column.
2. Select **Edit**, remove all the assigned labels, and select **Save**. Keep note of any custom labels, as you may need to manually reapply them later. The server will now appear in the Server Pairing Wizard again.
3. From the Xpress Dashboard, start and complete the Server Pairing Wizard (select all the appropriate protection schemas for the server).
4. After completing the Server Pairing Wizard, add any necessary custom labels, and move the server to an enforced state using the Server Enforcement Wizard as described above in [Rule Enforcement \[13\]](#).

Guidance for Preexisting Customers

Adapting Existing Rulesets to the Multiple Server Role Workflow

You may disregard this section if you are a new customer. This guidance is of importance to only those customers who have been using Illumio Xpress prior to the inclusion of the Multiple Server Role feature.

If you have already gone through Server Wizard in full before the Multiple Server Role feature became available, some of the associated rulesets have already been created. If this has happened, there are two options in the event that you would like to use the new feature.

Option One: Modifying the Existing Ruleset

Imagine an Active Directory default ruleset

Each label within the ruleset can be replaced with the corresponding label group of the same name.

Note that not all labels need to be replaced, only the ones that have corresponding label groups. The following is a representative list of all label to label group conversions that may need to occur:

- "Active Directory",
- "Domain Controller",
- "Active Directory Federation Services",
- "ADFS Server",
- "Active Directory Certificate Services",
- "CA Server",
- "Active Directory Lightweight Directory Services",
- "AD LDS Server",
- "Active Directory Rights Mgmt Services",

- "AD RMS Server",
- "Hyper-V",
- "Hypervisor",
- "File Servers",
- "File Server",
- "Windows Update Services",
- "WSUS Server",
- "Windows Deployment Services",
- "WDS Server",
- "Remote Desktop Services",
- "RDS Server",
- "Remote Access Services",
- "RA Server",
- "Print Services",
- "Print Server"

Option Two: Deleting the Existing Ruleset

Re-use the Server Wizard after deleting the existing ruleset. This will re-create the ruleset with the label groups as expected. Any modifications to the existing ruleset would need to be re-applied.

Caveats

- Do not delete or modify any of the objects (e.g., labels, label groups, pairing profiles, etc.) associated with a server pairing. This will break the onboarding, pairing, etc., which may result in unexpected behavior.
- If you encounter issues with policy being applied, make sure that you have the correct VEN version installed.

Protecting Endpoints Overview

Endpoint groups let you apply rulesets to endpoints such as tablets or laptops.

About Endpoints

Illumio Core supports the use of endpoint groups to allow and deny traffic from different paired endpoints. An endpoint group is essentially a logical grouping of endpoints. For background information, including caveats and what gets created when you pair endpoints, see [More Information About Pairing Endpoints \[17\]](#). For instructions on pairing endpoints, see [Xpress Runbook. \[5\]](#)

A note about top-level navigation tabs in Illumio Core:

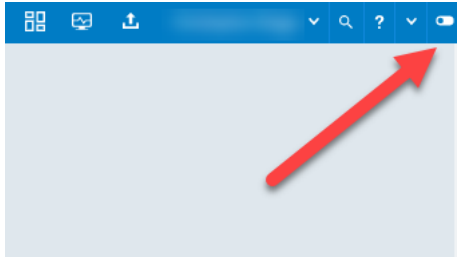
- Protect: This tab is the default active tab if you do not have protected endpoints or servers. If on a different tab, use the dropdown menu to add servers or endpoints.
- Dashboard: This tab is the default active tab if you do have protected endpoints or servers.
- Illumination: Select this tab to view the Illumination Map.

Pairing Endpoints

To Pair an Endpoint:

If you have not already, open a command terminal for the machine you want to protect by pairing an agent (VEN) to the workload.

1. If you are not already in Illumio CoreProtect or Landing page, from the PCE web console main menu, choose the **Toggle** switch in the upper right-hand corner.



If you do not yet have any workloads paired, the Illumio CoreProtect page appears. If you already have workloads paired, the Illumio CoreLanding page appears. The following instructions assume that you are on the Landing page, and are virtually identical to what you would do if you begin from the Protect page.

2. Under Endpoints, select **Add Endpoints**.
The Endpoint Pairing page of the wizard appears.
3. Select your operating system user level. For example, Windows User.
4. Once you select **Copy Script**, you will paste and enter the copied script into the command prompt of the machine whose workload you want to pair with a VEN. If you first wish to see what the script contains, select **Preview Script**.

When the installation succeeds, that workload will appear in the table on the next UI page.

If you wish to later pair an endpoint with the same script, such as when a new person joins the department with the applicable endpoint, you can re-enter the endpoint onboarding wizard or do it manually.



NOTE

To pair an Admin endpoint go to Pairing Profiles and find the “End-point Group: Admin” pairing profile. Copy the pairing script and append “-endpoint true” before the final “;” in the script.

5. Illumio will present recommendations based on your environment when you select **Next**.
The Endpoint Traffic page of the wizard appears.
6. This page shows details about administrator access, observed services and traffic, and what inbound traffic is blocked. For observed services and traffic, Illumio will note what traffic it recommends allowing and blocking.
7. When you are satisfied with the recommended settings, select **Save Rules**.
This provisions the endpoint group and associated components. A Success dialog will appear. From there you can return to the Protect page.

Viewing and Modifying Endpoint Groups

Once you create them, you can view or modify your endpoint groups’ attributes in a variety of ways:

- Browse to **Workloads and VENs > Pairing Profiles** to view, stop, or edit the pairing profile for the endpoint group
- Browse to **Rulesets and Rules > Rulesets** to add, remove, disable, or enable the rules for the endpoint group

- Browse to **Policy Objects > Labels** to view, edit, or remove the label for the endpoint group

At time of writing, some modification actions may be unavailable.

Deleting or renaming the following objects are not supported:

- Pairing Profiles associated with pre-assigned endpoint groups
- Labels associated with pre-assigned endpoint groups
- Rulesets associated with pre-assigned endpoint groups

About Pairing Endpoints

What Gets Created When Onboarding Endpoints

The following information provides some background on what happens when onboarding an endpoint.

- Groups are Created:
Two Groups are created by default during onboarding: Endpoint Group: User and Endpoint Group: Admin.
When a group is created, Illumio Core automatically creates a label, ruleset, and pairing profile. Each one of these is named after the group. Services may also be created during onboarding if Illumio Core encounters a new unique service. If re-entering onboarding, it simply updates the existing groups ruleset
- Services are Created:
These created services are based on observed allowed traffic and will appear in the groups' respective ruleset if the traffic API returns a process name for them. For Windows environments, these services are created with the port and protocol, or a process.
- Rules are Created:
During onboarding Illumio Core adds certain allow rules to both groups (Endpoint Group: User and Endpoint Group: Admin.). These rules are dynamically based off of known allowed traffic in the past 24 hours. By default, both groups share the allow rule entries that are created based on traffic with process names. These allow rules include services that are not explicitly blocked in the static list of services to block. The main difference between the two default groups' rulesets is that the Endpoint Group: Admin group receives another entry in the allow rules to allow traffic from any IP over port 3389 in addition to the dynamic traffic-based service entries.

Caveats

- By default the VEN is not paired in Visibility Only or Selective Enforcement mode. If you wish to begin with workloads already in an enforced state, move your default user or administrator group pairing profiles into Selective Enforcement. Otherwise, you will need to move the endpoint (workload) into the desired enforcement level for policy to be enforced.
- Do not delete any of the objects (e.g., labels, rulesets, pairing profiles, or services) associated with an endpoint group. This will break the onboarding, pairing, etc., which may result in unexpected behavior.
- If you encounter issues with policy being applied, make sure that you have the correct VEN version installed.
- Endpoint groups cannot be deleted in the UI.
- Endpoint groups outside of the defaults cannot be created in the UI.

- You cannot rename a group. Groups cannot be directly updated; only their constituent parts (label, ruleset, pairing profile) can. However, do *not* update the names of these constituent parts.

Recommendations

When you use either of the Illumio Core Endpoint or Server Wizards, they examine your traffic and make recommendations for you to apply certain policies, and sometimes labels, to the identified service or server role. They present the option to accept, modify, or deny recommendations depending on the situation.



NOTE

Once the recommendations are saved (accepted), in order to protect your machines, you will need to manually enforce the recommended policies.

Purpose

The purpose of recommendations is to assist you in quickly protecting your network with best-practices instead creating policies by hand.

Workflow

The endpoint protection workflow allows you to install agents on endpoints on your network, and accept or decline the recommendations.

The server protection workflow allows you to install agents on detected servers, and modify, accept, or decline the recommendations.

About Recommendations

Recommendation Components

Recommendations are made of ruleset-based policies. Each rule in a ruleset specifies sources and destinations, as well as the allowed or denied source processes/services and destination services. Each source or destination must have a selected policy object (label, label group, service, IP list, or user group) that is either allowed or denied.

Rules define which workloads are allowed to communicate. Labels allow you to categorize the aspects of workloads that you wish to include in your rules. All of this is handled automatically in the wizard.

The Endpoint Wizard lists observed processes, ports, and protocols, along with a recommendation for you to allow or disallow them.

The Server Wizard lists servers by hostname, along with a protection schema recommended based on server roles, as well as listing the labels and policy rules that make up the schema (server-specific policy). Illumio Xpress supports up to 10 protection schemas per server workload. The Server Wizard lets you examine these labels and rules.

Rejecting Recommendations

Rejecting Endpoint Wizard Recommendations

If you wish to reject Endpoint Wizard recommendations, do not select **Save Rules** at the end. This will leave the endpoints without any applied security policy until you do the following:

- Restart the Endpoint Wizard and select **Save Rules** at the end of the wizard
- Manually create policies, rules, etc.

Rejecting Server Wizard Recommendations

If you wish to reject Server Wizard recommendations, you can select **Change** in the Protection Schema column and deselect any and all protection schemas. Alternatively, do not select **Save** at the end.

If a particular server is not given a protection schema, or you change the protection schema to None, selecting **Save** will *not* update it to be protected. This will leave the server without any applied security policy until you do the following:

- Restart the Server Wizard, choose a schema, and select **Save** at the end of the wizard
- Manually create policies, rules, etc.

Modifying Recommendations

You can modify Server Wizard recommendations by clicking **Change** in the Protection Schema column and selecting up to 10 different protection schemas in the pop-up dialog, each supporting multiple roles for the server.

Endpoint Server recommendations are not modifiable at this time.

Accepting Recommendations

In the Endpoint Wizard, you accept the recommendations by selecting **Save Rules** at the end of the wizard.

In the Server Wizard, with or without changing the recommended protection schemas, you accept the listed protection schemas by selecting **Save** at the end of the wizard. Note that a protection schema may create new labels in the system.

To protect your endpoints or servers, manually enforce the policies after accepting the recommendations.

Recommendation Caveats

Endpoint Caveats

Do not delete any of the objects (e.g., labels, rulesets, pairing profiles, or services) associated with an endpoint group. This will break the onboarding, pairing, etc., which may result in unexpected behavior.

Server Caveats

If you use the classic user interface to "unlabel" a server that had been protected using the Server Wizard, this will leave the server unprotected, and may also result in unexpected behavior.

VEN Compatibility Check

This topic explains how to use the VEN Compatibility Check feature after installing VENs on workloads.

About Compatibility Checks

When you initially pair a VEN (install an agent on a workload), but before you apply any rules or move the workload to the Visibility Only or Selective Enforcement states, or after you move a workload back to its original pairing state, Xpress performs a VEN Compatibility Check that may take a few minutes. This check will run at any time that you perform the actions and will run on any workload. The check evaluates whether the pre-existing workload state will have issues when the rules are applied to the VEN. The results are sent to the Xpress service. After this initial VEN Compatibility Check, it automatically repeats every 24 hours.

After reviewing the results of the VEN Compatibility Check, you can determine if the VEN is ready to have rules applied, or you can resolve any detected issues, such as by backing up any system firewall rules.



NOTE

The VEN Compatibility Check is performed per-workload, and is unavailable for the Visibility Only or Selective Enforcement states. If a workload reverts from any of these states to the Idle policy state, the VEN Compatibility Check is performed.

All detected issues are categorized as:

- **Red:** Major incompatibility detected
- **Yellow:** A potential incompatibility detected
- **Green:** No major incompatibilities detected

The Compatibility Check results are displayed in the Server Wizard. To view the results, select the **Agent Report** link for a workload that has an agent installed. You may need to first check the box next to Include previously paired servers in order to display such workloads.

If no incompatibilities have been detected on the VEN, the Server Wizard displays "Compatible configuration." This means that the workload is ready to move to Visibility or Selective Enforcement Mode. The Server wizard will use the report to automatically move the workload to Visibility Mode if user allows it.

After viewing the results, you can export them as a text file by clicking **Export**.

The checks performed vary by the workload's operating system.

Windows Workloads

This table contains a list of compatible values and the recommended actions if your report indicates an incompatibility.

Incom- patibili- ty Type	Reason for incom- patibility with Illu- mio Core	Possible Results and Recommended Action
Group Pol- icy	<p>Windows firewall Group Policy Object (GPO) is detected.</p> <p>For more information, see KB Article #3545, Firewall GPO Warning Under Compatibility Report (login required).</p>	<p>Possible results are listed below:</p> <ul style="list-style-type: none"> • No firewall GPOs (this is the compatible value) • Domain firewall GPO found • Local firewall GPO found • Local and Domain firewall GPOs found <p>Recommend Action:</p> <p>This is only a warning message. The presence of a firewall GPO does not affect the VEN's behavior.</p>
Teredo tunneling enabled	Unsupported tunneling mode.	<p>Possible results are listed below:</p> <ul style="list-style-type: none"> • True • False (this is the compatible value) <p>Recommend Action:</p> <p>If the result is "True," consider the following:</p> <p>Teredo's relay and port addresses may change frequently, which in turn causes excessive policy re-computation for the Illumio PCE. Therefore, the VEN agent will not report the Teredo IP addresses back to the PCE. If you do not want to see this warning message in the future, disable the interface. Otherwise, treat this message as a warning only.</p>
Unsuppor- ted NICs	Unsupported interfaces detected. Untested and unsupported configura- tion.	<p>Possible results are listed below:</p> <ul style="list-style-type: none"> • None (this is the compatible value) • True <p>Recommend Action:</p> <p>If the result is "True," consider the following:</p> <p>The VEN detected a untested and unsupported network interface such as a Virtual loopback interface. If you do not want to see this warning message in the future, disable the unsupported interface. Otherwise, just treat this message as a warning only.</p>

Linux Workloads

Incompatibility Type	Reason for incompatibility with Illumio Core	Compatible Value
IPv4 forwarding enabled	At least 1 iptables forwarding rule is detected in the forwarding chain. VEN removes existing iptables rules in the non-Idle Visibility Only or Selective Enforcement policy state.	False
IPv4 forwarding packet count	Complementary check whether IPv4 forwarding is enabled.	0
iptables rule count	At least 1 iptables filter rule is detected. VEN removes existing iptables rules in the non-Idle Visibility Only or Selective Enforcement policy state.	0
IPv6 global scope enabled	IPv6 is enabled for the workload.	False
IPv6 active connection count	Complementary check whether IPv6 global scope is enabled.	0
ip6tables rule count	At least 1 iptables filter rule is detected. VEN removes existing ip6tables rules in the Visibility Only policy state	0
Routing table conflict	The StrongSwan routing table setting conflicts with exiting networking routing tables. Do not enable SecureConnect for the workload.	False

Xpress Visualization

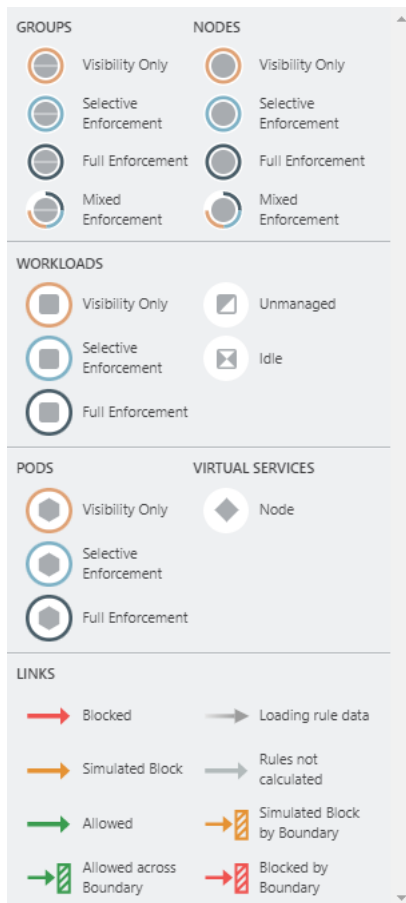
Xpress visualization tools provide a unique new way to reveal the traffic flows in your network and to help you configure policies to secure your applications.

This page provides an overview of Xpress visualization tools. For more information, see:

- [Xpress Visualization Panels \[24\]](#)
- [Xpress Visualization Reported and Draft Views \[26\]](#)
- [Xpress Visualization Search Example \[31\]](#)

How to read the Xpress Map

Legend



Pay attention to the following:

- Workloads and groups inside full dark lines depict the FullEnforcement mode
- Workloads and groups inside light blue lines depict the SelectiveEnforcement mode
- Workloads and groups inside light orange lines depict theVisibility only mode
- The ring around a group denotes the proportions of different enforcement states

Traffic links are presented with arrows in different colors:

- **Green:** Traffic is allowed
- **Yellow:** Traffic is simulated blocked
- **Red:** Traffic is blocked
- **Grey:** Rules are not calculated
- **Gradient arrows:** The light color is next to the source and dark next to the destination. Gradient arrows are used while the rule data is still loading from the traffic.

Visualization Views

This section describes the features under the Explore category of left navigation.

Map View

The Xpress Map view lets you group by labels, locations, etc. It also lets you choose layouts and split the view by selecting items on the map.

Configurable Grouping

Using the Group by menu, you can add different levels of grouping, such as grouping by types of labels and their order. You might want grouping by OS and then by environment. If you do not specify a particular grouping, Illumio will group workflows by the default, which is by workloads with the same set of labels. You can change your organization's default grouping using the same dropdown menu. This dropdown menu is also available in Mesh View.

Traffic View

The Xpress Traffic view lets you view the same items in tabular view. It also gives you the options to resolve fully qualified domain names (FQDNs) and to export the table.

Mesh View

The Xpress Mesh view lets you view the same items in a mesh view. Like the Map view, it lets you configure grouping. It also gives you the option to use a brush slider to select ranges of source and destination items.

How Xpress Visualization Tools Work with Fully Qualified Domain Names

Xpress visualization tools map the outbound connections from workloads to unknown IP addresses to FQDNs or DNS-based names. For example, it could display that the outbound connections from a workload are going to `maps.google.com` instead of 100s of different IP addresses. The FQDNs used are reported by the VEN to the PCE in the flow summaries. The VEN learns about the FQDNs by snooping the DNS responses on the workloads, which is the FQDN for the IP address as seen by the workload.

The map visualizes the workloads that form logical groups (based on labels attached to workloads) and provides an understanding of the traffic flows between workloads.

Xpress Visualization Panels

The following sections describe the Summary, Connections, and Workloads panels.

Summary Panel

The Summary panel in the map displays information about a selected item. To view the Summary panel, select an item, such as a traffic line, on the map. There are a few types of summary panels:

- Traffic detail
- Group detail
- Workload/VirtualService/Container Workload/Virtual Server

Summary

Connections

Workloads

Labels

Application

A appLabel_8082669

Environment

E Production

Location

L Denver

Role

R Web

General

Workloads

1

Pods

0

Virtual Services

0

Vulnerability

Total V-E Score

None

Highest V-E Score

None

Highest Vulnerability

None

Connections Panel

The Connections panel is a summary version of the main Table view and displays the following information:

- Reported Policy Decisions
- Sources
- Source Processes
- Source Labels
- Destinations
- Destination Port Processes
- Destination Labels
- Flows/Bytes
- First Detected
- Last detected

Summary	Connections	Workloads			
Customize columns ▾ 50 per page ▾ 1 – 3 of 3 Total ▾ < >					
<input type="checkbox"/>	Source	Source Labels	Destination	Destination Labels	Flows/Bytes
Reported Policy Decision	Source Process [User]	→	Destination Port Process [User]		First Detected ↑ Last Detected
<input type="checkbox"/> Unknown	1 Source IP ⓘ [Corporate] <div><div>IPL TEST</div></div>	→	1 Destination IP ⓘ [Corporate] Visibility Only <div><div>localhost.localdomain</div></div> 22 TCP sshd [root]	<div><div>A appLabel_808 2669</div><div>E Production</div><div>L Denver</div><div>R Web</div></div>	1 Connection 1 Flow 1 Bytes → 1 Bytes ← 07/12/2022, 16:18:57 07/12/2022, 16:18:57
<input type="checkbox"/> Allowed	1 Source IP ⓘ [Corporate] Visibility Only <div><div>localhost.localdomain</div></div> [chrony]	<div><div>A appLabel_808 2669</div><div>E Production</div><div>L Denver</div><div>R Web</div></div>	→	1 Destination IP ⓘ [Corporate] <div><div>IPL TEST</div></div> 53 UDP	1 Connection 8 Flows 07/12/2022, 16:22:32 07/12/2022, 23:33:35
<input type="checkbox"/> Simulated Block	1 Source IP ⓘ [Corporate] Visibility Only <div><div>localhost.localdomain</div></div> [chrony]	<div><div>A appLabel_808 2669</div><div>E Production</div><div>L Denver</div><div>R Web</div></div>	→	11 Destination IPs ⓘ [Corporate] <div><div>IPL TEST</div></div> 123 UDP	11 Connections 987 Flows 07/12/2022, 16:22:59 07/12/2022, 23:34:03

You will notice that the columns are configurable using the Customize Columns dropdown menu.

Workloads Panel

The Workloads panel displays the following information:

- Workload Name
- Enforcement Mode
- Labels

Summary	Connections	Workloads
Customize columns ▾ 50 per page ▾ 1 – 1 of 1 Total ▾ < >		
Name	Enforcement	Labels
localhost.localdomain	Visibility Only	A appLabel_8082669 E Production L Denver R Web

Xpress Visualization Tools Reported and Draft Views

The Illumio Core visualization tools provide two views into your organization: Reported and Draft.

Reported View

The Reported view visualizes your policy coverage as reported by your workloads, so you can examine the current state of your provisioned policy. This view displays the traffic using red, orange, or green lines to indicate whether the VEN had a rule that allows the traffic when the connection was attempted.

- A green line indicates that the VEN had an explicit rule to allow the traffic when the connection was attempted
- A red line indicates that the VEN did not have an explicit rule to allow the traffic when the connection was attempted
- An orange line indicates that no explicit rule exists, but because of the enforcement state of the workloads, the traffic is not blocked when provisioned.



NOTE

When a policy change occurs, only flows that are created after the policy change are displayed in red or green based on the new policy. Flows created before the policy change might continue to be displayed in red or green using the old policy.

If multiple rules allow traffic between entities, only one green line is displayed.

This view provides visibility for the actual traffic handling (rather than the expected traffic handling provided by the Draft view) and loads more quickly, especially when you have a large number of workloads and traffic flows.

Rules created for existing or live traffic don't change the color of the traffic lines in the Reported view, even when they are provisioned, until new traffic is detected.

The Reported view is a view-only map. You can view all the rulesets that apply to the workloads from the Reported view but you must change to the Draft view to add rules. The Reported view does not immediately reflect the latest changes to the policy. It is updated only after you provision a change to the policy and when new traffic flows that use the updated policy are reported from the VEN.

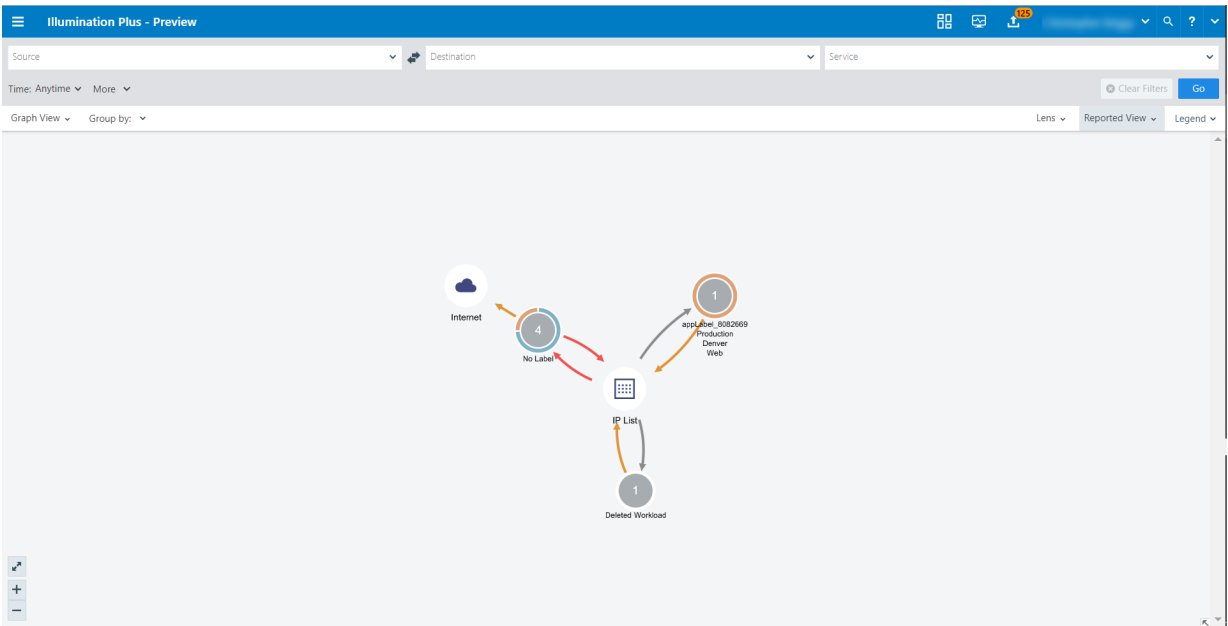
Reported and Draft view handle unmanaged workloads differently. In Draft view, rule coverage (the connections that have been included in draft rules) has limited support for traffic between unmanaged workloads. The Reported view always provides accurate rule coverage for traffic between unmanaged workloads.

Reported View (Table)

Table View

Reported Policy Decision	Source	Source Labels	Source Process [User]	Destination	Destination Labels	Destination Port Process [User]	Flows/Bytes	First Detected	Last Detected
<input type="checkbox"/> Unknown	1 Deleted Workload IP [Corporate]		msiexec.exe msiserver [SYSTEM]	3 Destination IPs [Corporate]		80 TCP	3 Connections 4 Flows 4 Bytes → 4 Bytes ←	06/24/2022, 09:30:06	06/24/2022, 09:30:06
<input type="checkbox"/> Simulated Block	1 Deleted Workload IP [Corporate]		svchost.exe WinDefend [NT AUTHORITY\SYSTEM]	9 Destination IPs [Corporate]		443 TCP	9 Connections 12 Flows 1 Bytes → 1 Bytes ←	06/24/2022, 09:30:06	06/24/2022, 09:39:55
<input type="checkbox"/> Allowed	1 Source IP [Corporate]			1 Destination IP [Corporate]		68 UDP svchost.exe [NT AUTHORITY\LOCAL SERVICE]	1 Connection 2 Flows	06/14/2022, 17:20:45	06/24/2022, 16:52:50
<input type="checkbox"/> Simulated Block	1 Source IP [Corporate]		System [NT AUTHORITY\SYSTEM]	1 Destination IP [Corporate]		IGMP	1 Connection 2 Flows	06/14/2022, 17:20:48	06/24/2022, 16:52:51
<input type="checkbox"/> Simulated Block	4 Source IPs		System [NT]	6 Destination IPs		ICMPv6	12 Connections 40 Flows	06/14/2022, 17:20:45	06/24/2022, 16:52:54

Reported View (Graph)



The Reported view helps you to understand your traffic patterns. If you click the View Rulesets link, the Rulesets page displays.

For each flow with a unique port/protocol, if there is a policy service created for that port/protocol, the name of that policy service displays, in addition to the names of the actual services that reported the flows. The Reported view shows reported rule coverage for the latest reported flow with that port/protocol in the command panel.

Different services can be running on the same port at different times or on different interfaces. The Reported view shows reported rule coverage of each flow separately, as well as its timestamp. In both cases, the Draft view shows the calculated rule coverage for traffic. For

Windows, it looks at the port, protocol, the process name (but not the process path), and the Windows service name. For Linux, it looks at only the port and protocol.

Draft View

The Draft view immediately visualizes the potential impact of your draft policy. This view displays the traffic using red or green lines to indicate whether the PCE has a rule to allow the connection that was reported by the VEN. This way, you can add rules and see their anticipated effect in real-time before the rules are implemented. Specifically:

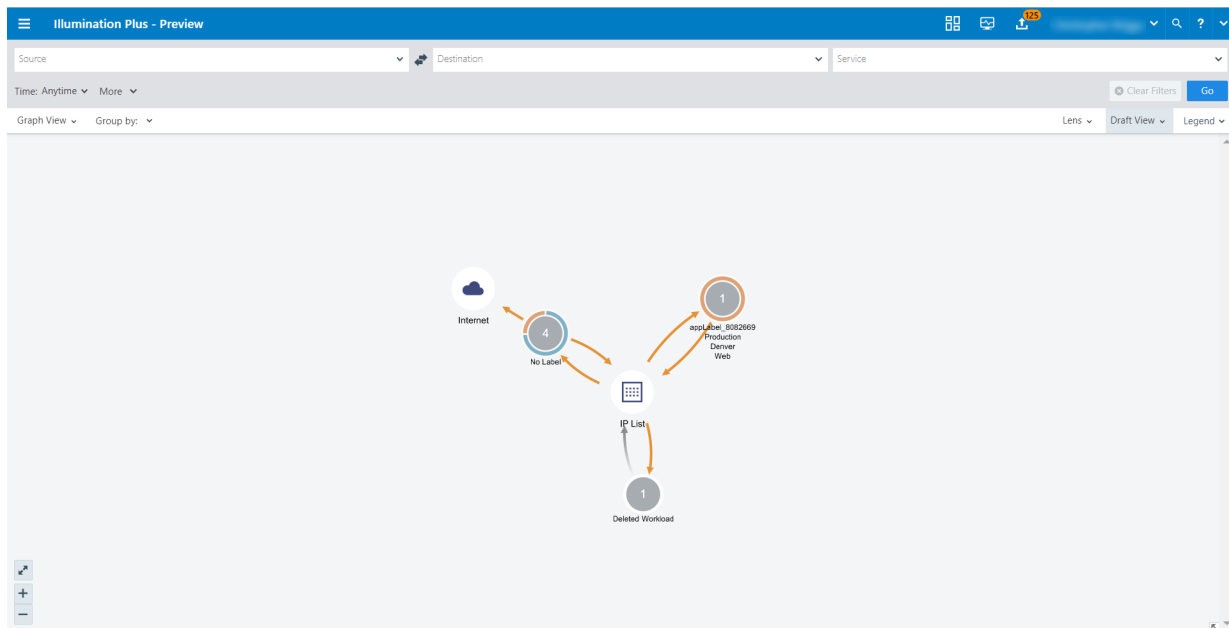
- A green line indicates that the PCE had an explicit rule (in either a draft or an active policy) to allow traffic when the connection was attempted.
- A red line indicates that the PCE did not have an explicit rule (in either a draft or an active policy) to allow traffic when the connection was attempted.
- An orange line indicates that no explicit rule exists, but because of the enforcement state of the workloads, the traffic will not be blocked when the rules are provisioned.

This view helps provide an understanding of the expected traffic handling (rather than the actual traffic handling provided by the Reported view) and considers both recently provisioned policy and draft policy. This map can take longer to load than the Reported view, especially if you have a large number of workloads and traffic flows, since the PCE has to compute the expected coverage for each traffic flow.

In Draft view, you can either view the rule that would permit traffic (turning the color of the line from red to green) or add a rule to allow a specific flow. In this view, you can immediately see the impact of the latest changes to the active or draft policy as they are reflected in the color of the traffic lines.

Draft View (Table)

Draft View (Graph)



Limitations of Draft View

The Draft view is the result of a “what-if” analysis conducted by the PCE. It is a modeling tool that depicts whether flows known to the PCE will be allowed or blocked, based on the configured policy. The modeling might not work entirely correctly for the following types of rules configured on the PCE:

- **Process-based rules:** Process-based rules are written using the process name or service name that sends or receives the traffic on the workload.
- **User-based rules:** User-based rules allow administrators to leverage the Microsoft Active Directory User Groups to control access to computing resources.
- **Custom iptables rules:** Custom iptables rules are configured on each workload and can include processes that are not known to the PCE.
- **System rules:** The VEN has implicit rules to permit necessary traffic (for example, rules permitting DHCP and DNS outbound traffic on the workload).

In most cases, the Reported view provides an accurate representation of what will be allowed or blocked by the VEN, so the Reported view should be used to verify your changes.

Changing Views

You can switch between the two views by selecting the view from the top right corner of the Illumio Core UI.



NOTE

For optimal scale and performance, if there are 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 map. The process or service name that was part of the most recently reported connection is displayed.

Xpress Visualization Search Example

Before you write policy rules to either allow or block this traffic, you will want to determine if there are any traffic flows between them.

Using Xpress visualization tools you can query, for example, the following:

"Any traffic flows during the last week between my Development and Production environments, over any port except port 80, excluding any workloads that have a Role label named 'Domain Controller'"

You would use the dropdown menus to select the above values. Once you are ready you would select **Run**. The results appear when the search criteria are met, and will default to the Table view. You can also select **Map** or **Mesh** from the drop-down list if you prefer.