Cisco Secure Workload Quick Start Guide for Release 3.8

First Published: 2023-04-12

About This Guide

This document is applicable for Secure Workload release 3.8:

- Introduces the key Secure Workload concepts: Segmentation, Workload labels, Scopes, Hierarchical scope trees, and Policy discovery.
- Explains the process of creating the first branch of your scope tree using the first-time user experience wizard.
- Describes the automated process of generating policies for the chosen application based on actual traffic flows.

Introduction

Traditionally, network security is aimed at keeping malicious activities out of network with firewalls around the edge of your network. However, you also need to protect your organization from threats that have breached your network or originated within it. Segmentation (or microsegmentation) of the network helps to protect your workloads through controlling traffic between workloads and other hosts on your network; therefore, allowing only traffic that your organization would require for business purposes, and deny all other traffic.

For example, you can use policies to prevent all communication between the workloads that host your public-facing web application from communicating with the research and development database in your data center, or to prevent non-production workloads from contacting the production workloads.

Cisco Secure Workload uses the organization's flow data to suggest policies that you can evaluate and approve before enforcing them. Alternatively, you can also manually create these policies for segmenting your network.

Tour of the Wizard

Welcome to Secure Workload. Labeling and grouping your workloads is essential to the power of Secure Workload.

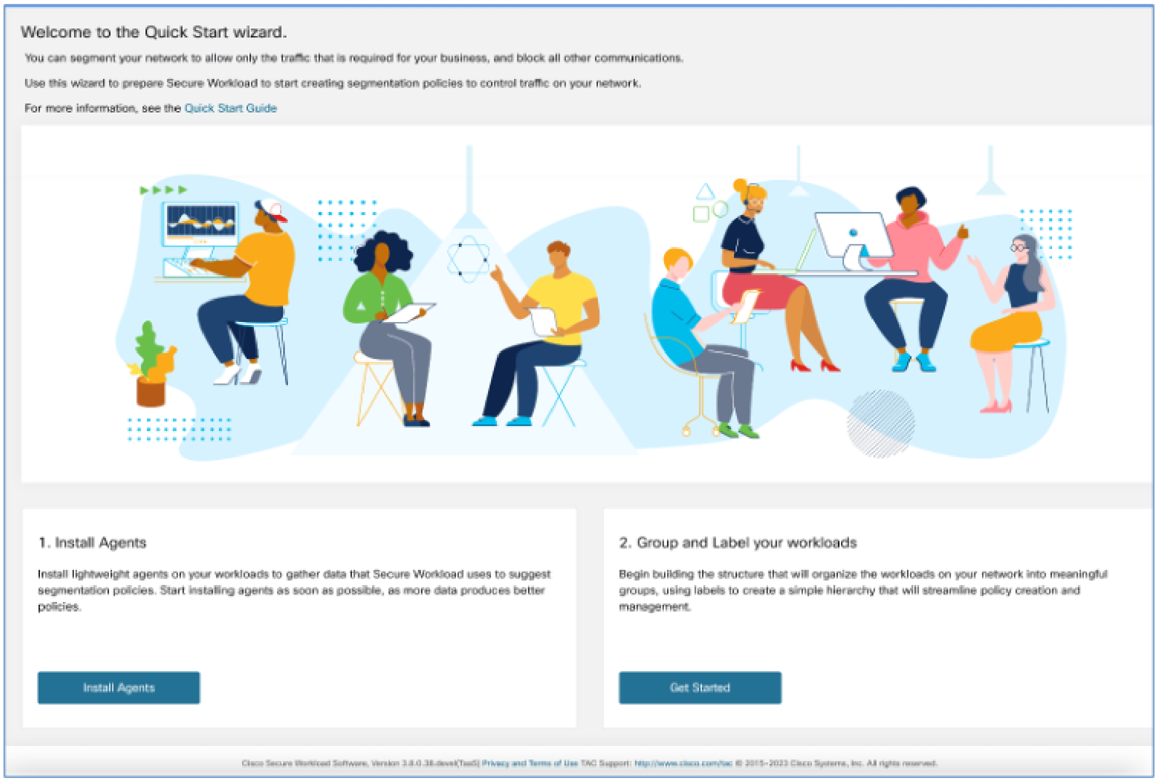
Onboarding is a user-friendly and guided approach to help you set up and deploy applications securely in your environment. You can segment your network to allow only the traffic that is required for your business, and block all other communications.

To help you get started, choose Overview on the left menu to navigate to the Quick Start Wizard. The wizard typically prepares Secure Workload to start creating segmentation policies to control traffic on your network, presents a series of steps, each focusing on a specific security aspect, and prompts users to make informed choices for configuring their workload securely.

The following user roles can access the wizard:

- site administrator
- customer support
- scope owner

Figure 1: Welcome window



Welcome to the Quick Start wizard.

You can segment your network to allow only the traffic that is required for your business, and block all other communications.

Use this wizard to prepare Secure Workload to start creating segmentation policies to control traffic on your network.

For more information, see the Quick Start Guide

1. Install Agents

Install lightweight agents on your workloads to gather data that Secure Workload uses to suggest segmentation policies. Start installing agents as soon as possible, as more data produces better policies.

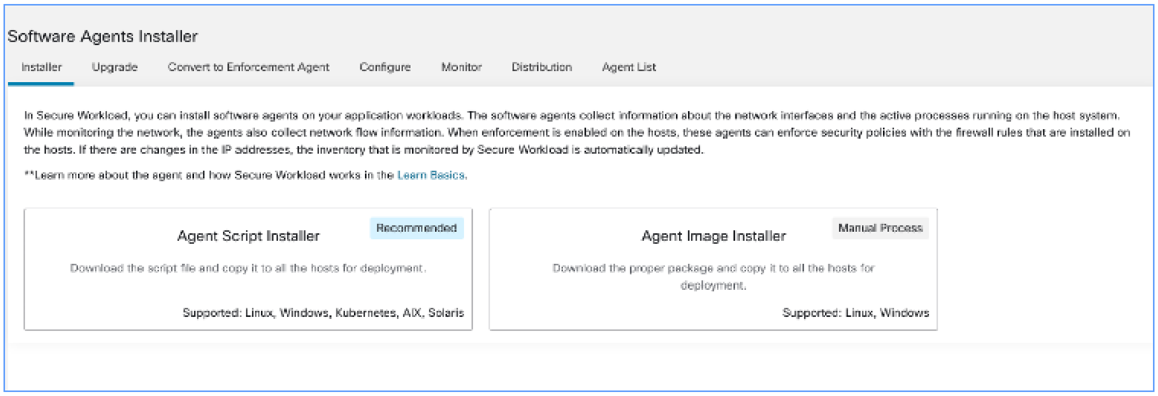
2. Group and Label your workloads

Begin building the structure that will organize the workloads on your network into meaningful groups, using labels to create a simple hierarchy that will streamline policy creation and management.

Cisco Secure Workload Software, Version 3.8.0.38.devel(TaaS) Privacy and Terms of Use TAC Support: http://www.cisco.com/tac © 2015–2023 Cisco Systems, Inc. All rights reserved.

Install Agents

In Secure Workload, you can install software agents on your application workloads. The software agents collect information about the network interfaces and the active processes running on the host system.



Software Agents Installer

In Secure Workload, you can install software agents on your application workloads. The software agents collect information about the network interfaces and the active processes running on the host system. While monitoring the network, the agents also collect network flow information. When enforcement is enabled on the hosts, these agents can enforce security policies with the firewall rules that are installed on the hosts. If there are changes in the IP addresses, the inventory that is monitored by Secure Workload is automatically updated.

**Learn more about the agent and how Secure Workload works in the Learn Basics.

Agent Script Installer

Download the script file and copy it to all the hosts for deployment.

Supported: Linux, Windows, Kubernetes, AIX, Solaris

Agent Image Installer

Download the proper package and copy it to all the hosts for deployment.

Supported: Linux, Windows

There are two ways how you can install the software agents:

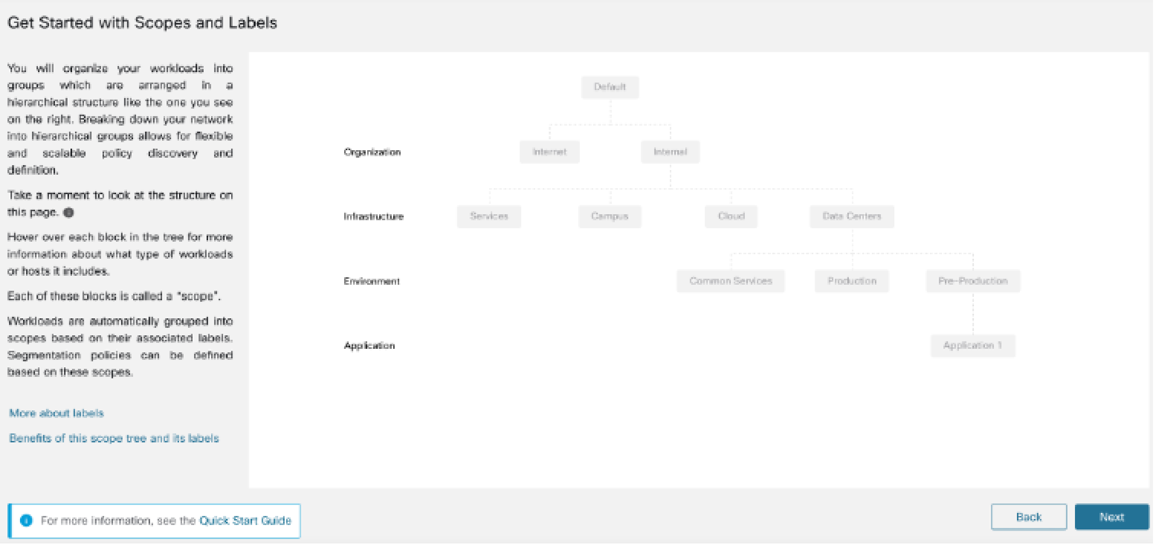
- Agent Script installer-Use this method for installing, tracking, and troubleshooting of issues while installing the software agents. Supported platforms are Linux, Windows, Kubernetes, AIX, and Solaris
- Agent Image installer-Download the software agent image to install a specific version and type of software agent for your platform. Supported platforms are Linux and Windows.

The onboarding wizard walks you through the process of installing the agents based on the selected installer method, see the installation instructions on the UI and the user guide for additional details on installing software agents.

Group and Label your Workloads

Assign labels to a group of workloads to create a scope. The hierarchical scope tree helps to divide the workloads into smaller groups. The lowest branch in the scope tree is reserved for individual applications.

Select a parent scope from the scope tree to create a new scope, which contains a subset of the members from the parent scope.



Get Started with Scopes and Labels

You will organize your workloads into groups which are arranged in a hierarchical structure like the one you see on the right. Breaking down your network into hierarchical groups allows for flexible and scalable policy discovery and definition.

Take a moment to look at the structure on this page.

Hover over each block in the tree for more information about what type of workloads or hosts it includes.

Each of these blocks is called a "scope".

Workloads are automatically grouped into scopes based on their associated labels. Segmentation policies can be defined based on these scopes.

More about labels

Benefits of this scope tree and its labels

For more information, see the Quick Start Guide

On this window, you can organize your workloads into groups, which are arranged in a hierarchical structure. Breaking down your network into hierarchical groups allows for flexible and scalable policy discovery and definition.

Labels are key parameters that describe a workload or endpoint, it is represented as a key-value pair. The wizard helps to apply the labels to your workloads, and then groups these labels into groups called scopes. Workloads are automatically grouped into scopes based on their associated labels. You can define segmentation policies based on the scopes.

Hover-over each block or scope in the tree for more information about the type of workloads or hosts it includes.

Note In the Get Started with Scopes and Labels window, Organization, Infrastructure, Environment and Application are the keys and the text in the gray boxes in-line with each key are the values.

For example, all workloads belonging to Application 1 are defined by these set of labels:

- Organization = Internal
- Infrastructure = Data Centers
- Environment = Pre-Production
- Application = Application 1

The Power of Labels and Scope Trees

Labels drive the power of Secure Workload, and the scope tree created from your labels is more than just a summary of your network:

- Labels let you instantly understand your policies:

  ```
  "Deny all traffic from Pre-Production to Production"
  ```

  Compare this to the same policy without labels:

  ```
  "Deny all traffic from 172.16.0.0/12 to 192.168.0.0/16"
  ```

- Policies based on labels automatically apply (or stop applying) when labeled workloads are added to (or removed from) inventory. Over time, these dynamic groupings based on labels greatly reduce the amount of effort required to maintain your deployment.

- Workloads are grouped into scopes based on their labels. These groupings let you easily apply policy to related workloads. For example, you can easily apply policy to all applications in the Pre-Production scope.

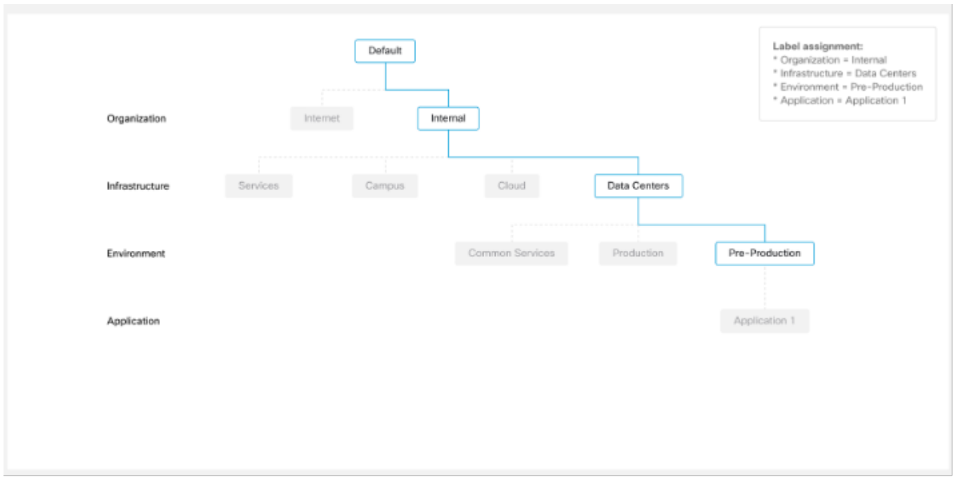
- Policies created once in a single scope can automatically be applied to all workloads in descendant scopes in the tree, minimizing the number of policies you need to manage.

  You can easily define and apply policy broadly (for example, to all workloads in your organization) or narrowly (to just the workloads that are part of a specific application) or to any level in between (for example, to all workloads in your data center.

- You can assign responsibility for each scope to different administrators, delegating policy management to the people who are most familiar with each part of your network.

Build the Hierarchy for Your Organization

Start to build your hierarchy or scope tree, this involves identifying and categorizing the assets, determining the scope, defining roles and responsibilities, developing policies and procedures to create a branch of the scope tree.



The wizard guides you through creating a branch of the scope tree. Enter IP addresses or subnets for each blue-outlined scope, the labels are automatically applied based on the scope tree.

Pre-requisites:

- Gather IP Addresses/Subnets associated with your Pre-Production environment, your data centers, and your Internal network.
- Gather as many IP addresses/subnets as you can, you can the additional IP addresses/subnets later.
- Later, as you build your tree, you can add IP addresses/subnets for the other scopes in the tree (the gray blocks).

To create the scope tree, perform these steps:

Define the Internal Scope

The internal scope includes all IP addresses that define your organization's internal network, including public and private IP addresses.

The wizard walks you through adding IP addresses to each scope in the tree branch. As you add addresses, the wizard assigns labels to each address that defines the scope.

For example, on this Scope Setup window, the wizard assigns the label

```
Organization=Internal
```

to each IP address.

By default, the wizard adds the IP addresses in the private internet address space as defined in RFC 1918

Note All the IP addresses need not be entered at once, but you must include the IP addresses associated with your chosen application, you can add the rest of the IP addresses at a later time.

Define the Data Center Scope

This scope includes the IP addresses that define your on-premises data centers. Enter the IP addresses/subnets that define your internal network

Note Scope names should be short and meaningful.

On this window, enter the IP addresses that you have entered for the organization, these addresses must be a subset of the addresses for your internal network. If you have multiple data centers, include all of them in this scope so you can define a single set of policies.

Note You can always add more addresses at a later stage. For instance, the wizard assigns these labels to each of the IP addresses:

```
Organization=Internal
```

```
Infrastructure=Data Centers
```

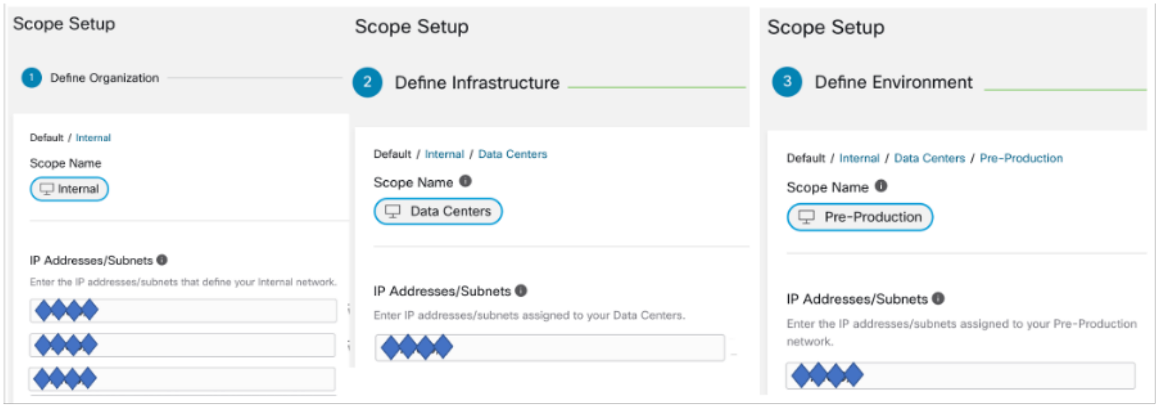
Define the Pre-Production Scope

This scope includes IP addresses of non-production applications and hosts, such as development, lab, test, or staging systems.

Note Ensure you do not include addresses of any applications that are used to conduct actual business, use them for the production scope that you define later.

The IP addresses you enter on this window must be a subset of the addresses you entered for your data centers, include the addresses of your chosen application. Ideally, they should also include pre-production addresses that are not part of the chosen application.

Note You can always add more addresses at a later stage.



Scope Setup

1 Define Organization

Default / Internal

Scope Name: Internal

IP Addresses/Subnets

Enter the IP addresses/subnets that define your Internal network.

[redacted]

[redacted]

[redacted]

Scope Setup

2 Define Infrastructure

Default / Internal / Data Centers

Scope Name: Data Centers

IP Addresses/Subnets

Enter IP addresses/subnets assigned to your Data Centers.

[redacted]

Scope Setup

3 Define Environment

Default / Internal / Data Centers / Pre-Production

Scope Name: Pre-Production

IP Addresses/Subnets

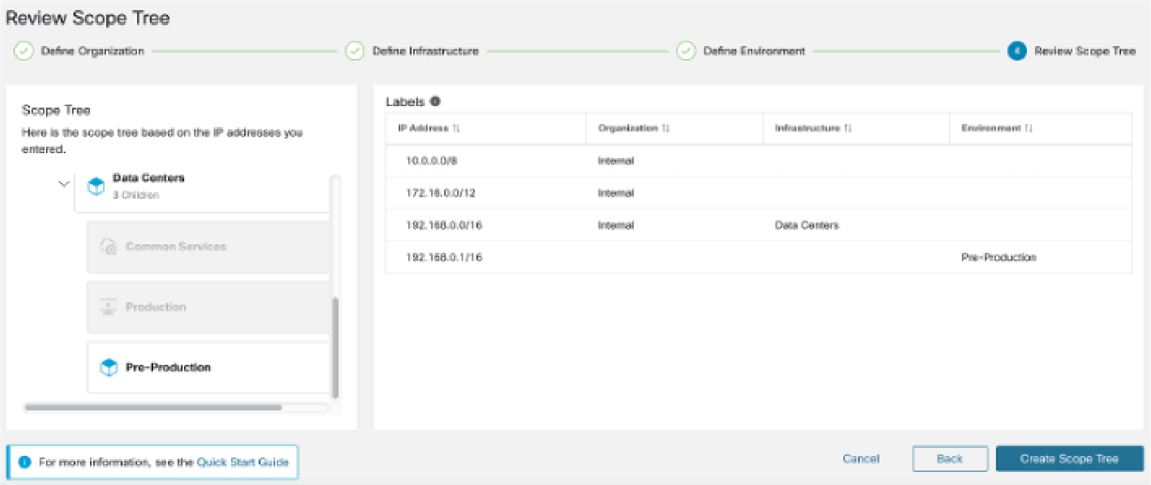
Enter the IP addresses/subnets assigned to your Pre-Production network.

[redacted]

Review Scope Tree, Scopes, and Labels

Before you start creating the scope tree, review the hierarchy that you can see on the left window. The root scope shows labels that were automatically created for all configured IP addresses and subnets. At a later stage in the process, applications are added to this scope tree.

Figure 2:



Review Scope Tree

Define Organization — Define Infrastructure — Define Environment — 4 Review Scope Tree

Scope Tree

Here is the scope tree based on the IP addresses you entered.

- Data Centers
  3 Children
  - Common Services
  - Production
  - Pre-Production

Labels

IP Address	Organization	Infrastructure	Environment
10.0.0.0/8	Internal		
172.16.0.0/12	Internal		
192.168.0.0/16	Internal	Data Centers	
192.168.0.1/16			Pre-Production

For more information, see the Quick Start Guide

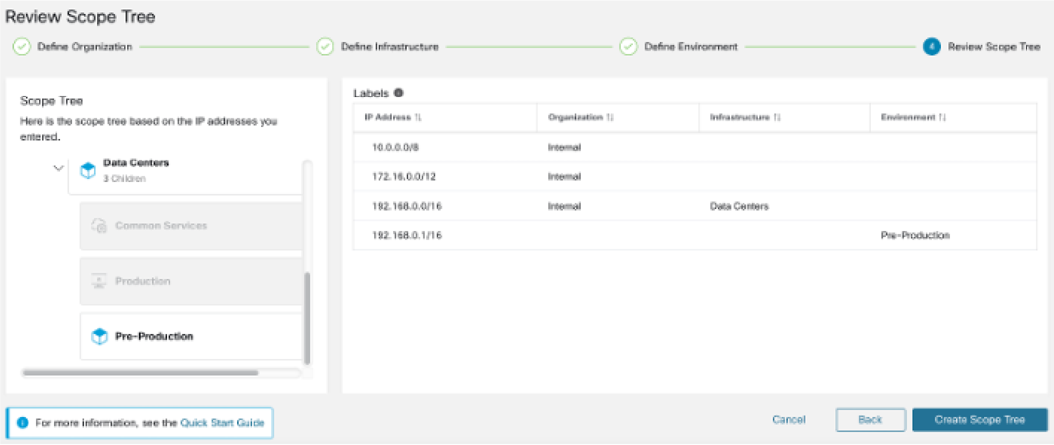
Cancel | Back | Create Scope Tree

You can expand and collapse branches and scroll down to choose a specific scope. Onthe right pane, you can see the IP addresses and labels assigned to the workloads for the specific scope. On this window, you can review, modify the scope tree before you add an application to this scope.

Note If you want to view this information after you exit the wizard, choose Organize > Scopes and Inventory from the main menu,

Review Scope Tree

Before you start creating the scope tree, review the hierarchy that you can see on the left window. The root scope shows labels that were automatically created for all configured IP addresses and subnets. At a later stage in the process, applications are added to this scope tree.



Review Scope Tree

Define Organization — Define Infrastructure — Define Environment — 4 Review Scope Tree

Scope Tree

Here is the scope tree based on the IP addresses you entered.

- Data Centers
  3 Children
  - Common Services
  - Production
  - Pre-Production

Labels

IP Address	Organization	Infrastructure	Environment
10.0.0.0/8	Internal		
172.16.0.0/12	Internal		
192.168.0.0/16	Internal	Data Centers	
192.168.0.1/16			Pre-Production

For more information, see the Quick Start Guide

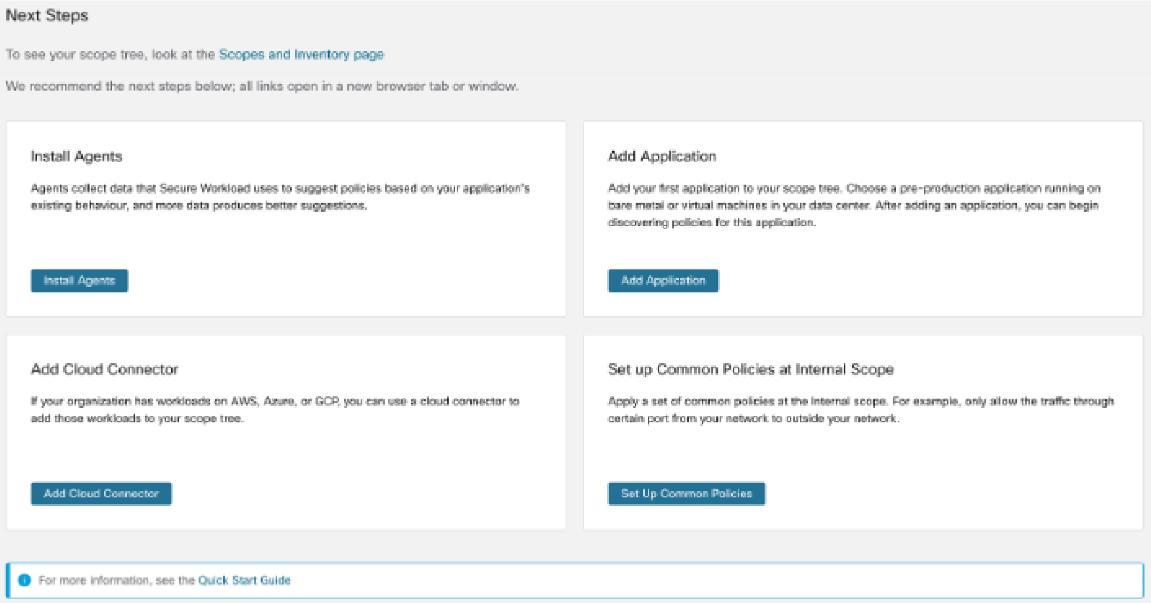
Cancel | Back | Create Scope Tree

You can expand and collapse branches and scroll down to choose a specific scope. On the right pane, you can see the IP addresses and labels assigned to the workloads for the specific scope. In this window, you can review and modify the scope tree before you add an application to the scope.

> **Note** If you want to view this information after you exit the wizard, choose **Organize** > **Scopes** and **Inventory** from the main menu.

Create Scope Tree

After you review the scope tree, create the scope tree.



Next Steps

To see your scope tree, look at the Scopes and Inventory page

We recommend the next steps below; all links open in a new browser tab or window.

Install Agents

Agents collect data that Secure Workload uses to suggest policies based on your application's existing behaviour, and more data produces better suggestions.

Add Application

Add your first application to your scope tree. Choose a pre-production application running on bare metal or virtual machines in your data center. After adding an application, you can begin discovering policies for this application.

Add Cloud Connector

If your organization has workloads on AWS, Azure, or GCP, you can use a cloud connector to add those workloads to your scope tree.

Set up Common Policies at Internal Scope

Apply a set of common policies at the Internal scope. For example, only allow the traffic through certain port from your network to outside your network.

For more information, see the Quick Start Guide

For information on the scope tree, see the Scopes and Inventory sections in the user guide.

Next Steps

Install Agents

Install the SecureWorkload agents on the workloads associated with your chosen application.The data that the agents gather is used to generate suggested policies based on the existing traffic on your network. More the data, more accurate policies are produced. For details, see the Software Agents section in the Secure Workload user guide.

Add Application

Add the first application to your scope tree. Choose a pre-production application running on bare metal or virtual machines in your data center. After adding an application, you can begin discovering policies for this application. For more information, see the Scopes and Inventory section of the Secure Workload user guide.

Set up Common Policies at Internal Scope

Apply a set of common policies at the Internal scope. For example, only allow the traffic through certain port from your network to outside your network.

Users can define policies manually using Clusters, Inventory Filters and Scopes or these can be discovered and generated from flow data using an Automatic Policy Discovery.

After you have installed agents and allowed at least a few hours for traffic flow data to accumulate, you can enable Secure Workload to generate ("discover") policies based on that traffic. For details, see Automatically Discover policies section of the Secure Workload user guide.

Apply these policies at Internal (or Inside or Root) scope to effectively review policies.

Add Cloud Connector

If your organization has workloads on AWS, Azure, or GCP, use a cloud connector to add those workloads to your scope tree. For more information, see the Cloud Connectors section of the Secure Workload user guide.

Quick Start Workflow

Step	Do This	Details
1	(Optional) Take an annotated tour of the wizard	Tour of the Wizard, on page 1
2	Choose an application to start your segmentation journey.	For best results, follow the guidelines in Choose an Application for this Wizard, on page 10.
3	Gather IP addresses.	The wizard will request 4 groups of IP addresses. For details, see Gather IP Addresses, on page 9.
4	Run the wizard	To view requirements and access the wizard, see Run the Wizard, on page 11.
5	Allow time for the agents to gather flow data.	More data produces more accurate policies. The minimum amount of time required depends on how actively your application is used.
6	Generate ("discover") policies based on your actual flow data.	See Automatically Generate Policies, on page 12.

Gather IP Addresses

You will need at least some of the IP addresses in each bullet below:

- Addresses that define your internal network

  By default, the wizard uses the standard addresses reserved for private internet use.

- Addresses that are reserved for your data centers.

  This does not include addresses used by employee computers, cloud or partner services, centralized IT services, etc.

- Addresses that define your non-production network
- Addresses of the workloads that comprise your chosen non-production application

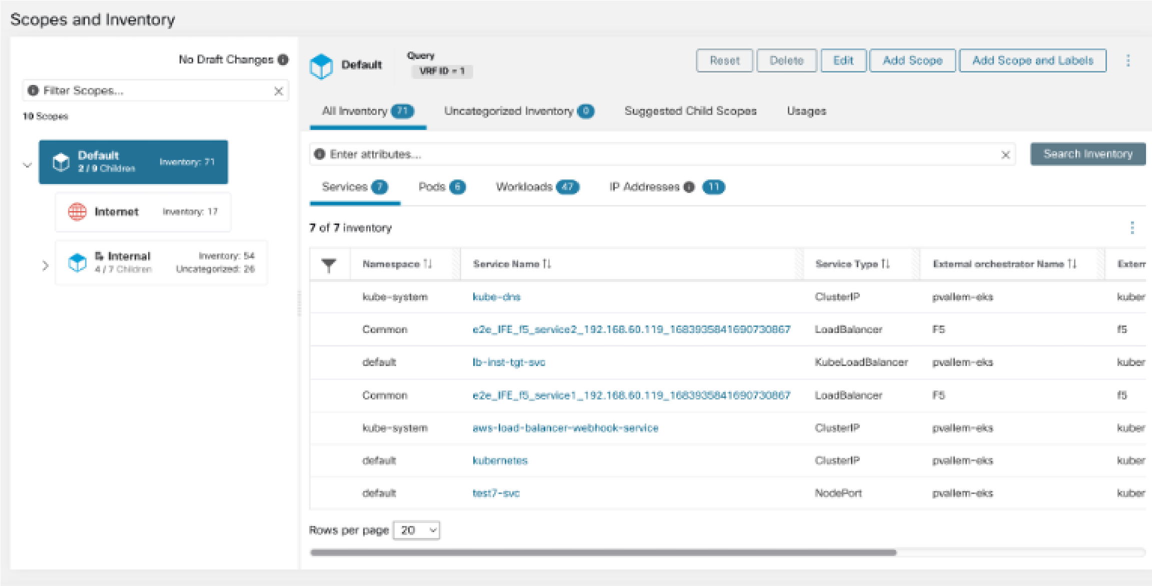
For now, you do not need to have all of the addresses for each of the above bullets; you can always add more addresses later.

Important Because each of the 4 bullets represents a subset of the IP addresses of the bullet above it, each IP address in each bullet must also be included among the IP addresses of the bullet above it in the list.

Choose an Application for this Wizard

For this wizard, choose a single application.

An application typically consists of multiple workloads that provide different services, such as web services or databases, primary and backup servers, etc. Together, these workloads provide the application's functionality to its users.



Namespace	Service Name	Service Type	External orchestrator Name	Extern
kube-system	kube-dns	ClusterIP	pvallem-eks	kuber
Common	e2e_IFE_f5_service2_192.168.60.119_1683935841690730867	LoadBalancer	F5	f5
default	lb-inst-tgt-svc	KubeLoadBalancer	pvallem-eks	kuber
Common	e2e_IFE_f5_service1_192.168.60.119_1683935841690730867	LoadBalancer	F5	f5
kube-system	aws-load-balancer-webhook-service	ClusterIP	pvallem-eks	kuber
default	kubernetes	ClusterIP	pvallem-eks	kuber
default	test7-svc	NodePort	pvallem-eks	kuber

Guidelines for Choosing Your Application

SecureWorkload supports workloads running on a wide range of platforms and operating systems, including cloud-based and containerized workloads. However, for this wizard, choose an application with workloads that are:

- Running in your data center.
- Running on bare metal and/or virtual machines.
- Running on Windows, Linux, or AIX platforms supported with Secure Workload agents, see https://www.cisco.com/go/secure-workload/requirements/agents.
- Deployed in a pre-production environment.

Note You can run the wizard even if you have not chosen an application and gathered IP addresses, but you cannot complete the wizard without doing these things.

Note If you don't complete the wizard before signing out (or timing out) or navigate to a different part of the Secure workload application (use the left navigation bar), the wizard configurations are not saved.

For details about how to add a scope/add Scope and Labels, see the Scopes and Inventory section of the Cisco Secure Workload User Guide.

Run the Wizard

You can run the wizard whether or not you have chosen an application and gathered IP addresses, but you won't be able to complete the wizard without doing these things.

Important If you don't complete the wizard before signing out (or timing out) of Secure Workload, or if you navigate to a different part of the application using the left navigation bar, wizard configurations are not saved.

Before you begin

The following user roles can access the wizard:

- site admin
- customer support
- scope owner

Procedure

Step 1 Sign in to Secure Workload.

Step 2 Start the wizard:

If you do not currently have any scopes defined, the wizard appears automatically when you sign in to Secure Workload.

Alternatively:

- Click the **Run the wizard now** link in the blue banner at the top of any page.
- Choose **Overview** from the main menu on the left side of the window.

If you have already created scopes, you cannot access the wizard again unless you delete all existing scopes. To do this, (Optional) Reset the Scope Tree, on page 12.

Step 3 The wizard will explain the things you need to know.

Don't miss the following helpful elements:

- Hover over the graphic elements in the wizard to read their descriptions.
- Click any links and info buttons (ⓘ) for important information.

Automatically Generate Policies

Secure Workload generates/discovers policies based on existing traffic between workloads and other hosts. You can modify, supplement, analyze, and eventually approve and enforce policies on the workloads.

Before you begin

- Install agents on your application's workloads
- Allow some time after agent installation for flow data to accumulate.

Procedure

Step 1 On the **Next Steps** page of the quick start wizard, click **Automatically Generate Policies**.

Alternatively, you can do the following:

a) Choose **Defend** > **Segmentation**on the left menu bar.
b) On the left pane, in the scope tree or list of scopes, scroll down to the application scope.
c) Choose **Primary** in that scope.

Step 2 Choose **Manage Policies**.

Step 3 Choose **Automatically Discover Policies**.

Step 4 Choose the time range for the flow data that you want to include:

Step 5 Choose **Discover Policies**, the generated policies appear on this page.

(Optional) Reset the Scope Tree

You can delete the scopes, labels, and scope tree you created using the wizard and run the wizard again (optional).

Tip If you only want to remove some of the created scopes and not run the wizard again, delete individual scopes instead of resetting the entire scope tree. To delete a scope, choose Scope and click **Delete**.

Before you begin

Scope owner privileges for the root scope are required.

If you have created additional workspaces, policies, or other dependencies, see the Secure Workload user guide for complete information about resetting the scope tree.

Procedure

Step 1 From the navigation menu on the left, choose **Organize** > **Scopes and Inventory** .

Step 2 Click the scope at the top of the tree.

Step 3 Click **Reset**.

Step 4 Confirm your choice.

Step 5 If the Reset button changes to Pending Reset, you may need to refresh the browser page.

More Information

For more information about concepts in the wizard, see the Secure Workload user guide.