Cisco Secure Workload Quick Start Guide for Release 3.7

First Published: 2022-08-17

Introduction to Segmentation

Traditionally, network security aimed to keep malicious activity out of your network by placing firewalls around the edge of your network. However, you also need to protect your organization from threats that have breached your network -- or originate inside it. Segmentation (also known in this case as microsegmentation) helps protect workloads on your network by letting you control traffic between workloads and other hosts on your network, so you can allow only traffic that your organization requires for business purposes, and deny all other traffic.

For example, you can use segmentation policy to prevent all communication between the workload that hosts your public-facing web application from communicating with your top-secret research and development database in your data center, or to prevent non-production workloads (which are often less compliant and less carefully protected) from contacting production workloads.

Cisco Secure Workload uses your organization's actual flow data to suggest segmentation policies that you evaluate and approve before enforcing them. You can also manually create policies.

About This Guide

You can use this guide with Secure Workload release 3.7.

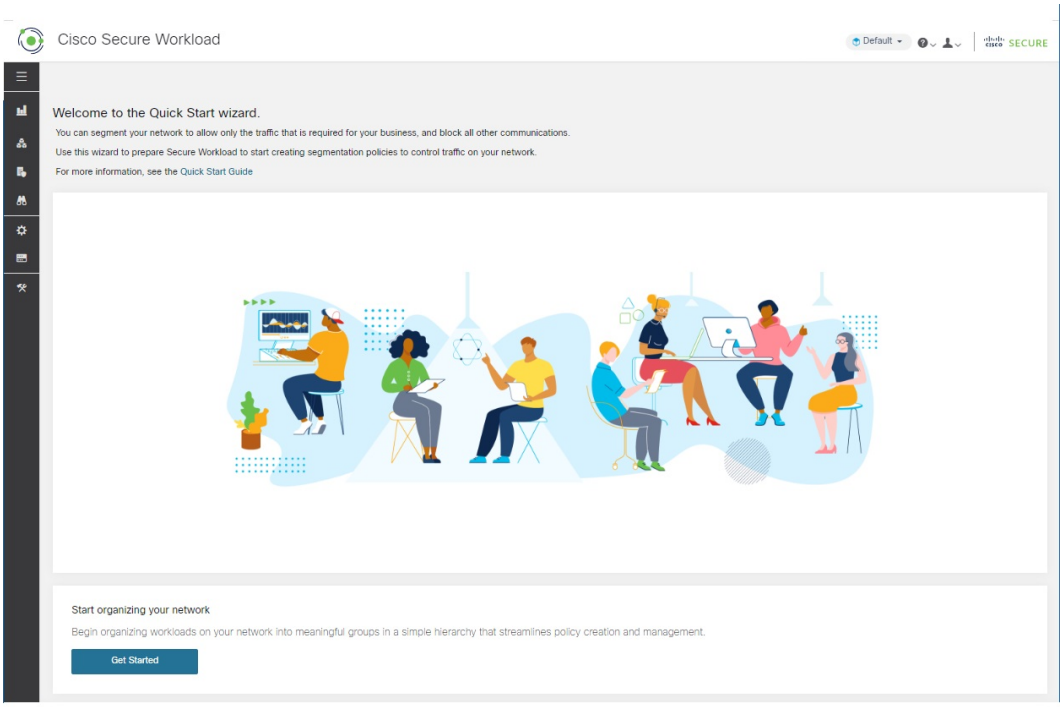
This document:

- Introduces you to key Secure Workload concepts: Segmentation, workload labels, scopes, hierarchical scope trees, and policy discovery;
- Walks you through the process of creating the first branch of your scope tree for a single application (using the first-time user experience wizard in Secure Workload); and
- Shows you how to automatically generate policies for your chosen application based on actual traffic flows.

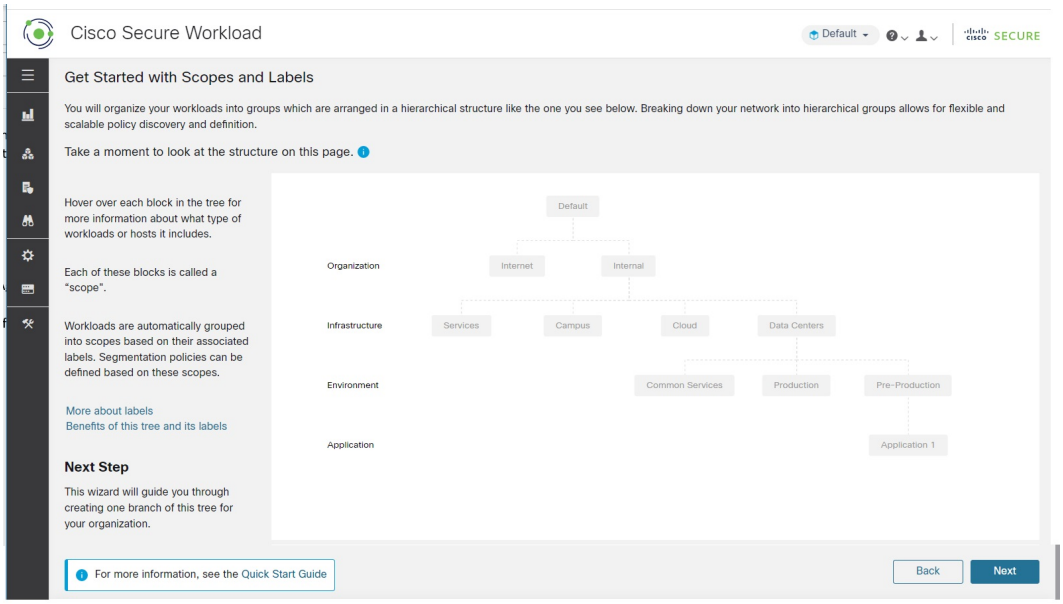
The Secure Workload quick start wizard does not require external documentation, but for those who prefer to read ahead before they work in a new product, this onboarding guide is an optional companion and supplementary source of information.

Tour of the Wizard

Start Page



Get Started with Scopes and Labels



This page explains what you'll build. It tells you (and shows you) what labels and scopes are and how they work together.

About Labels

The power of Secure Workload rests on the labels assigned to your workloads.

Labels are key-value pairs that describe each workload.

Look at the tree above. The label keys appear at the left side of the tree. The label values are the text in the gray boxes in line with each key. The wizard helps you apply these labels to your workloads.

Assigning labels to workloads lets you group them into groups called scopes. Each gray box in the tree above is a scope.

As you see in the tree above, all workloads belonging to the Application 1 scope (at the bottom right of this tree) are defined by the following 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:

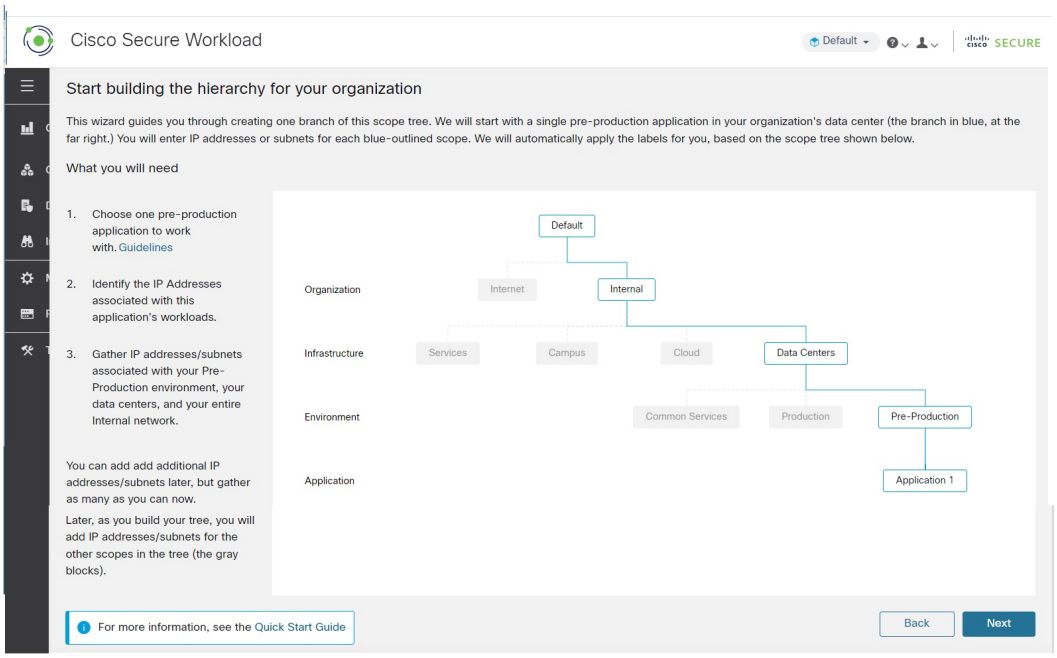
  ```
  "Deny all traffic from 172.16.0.0/12 to 192.168.0.0/16"
  ```

- 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.

Start Building the Hierarchy for Your Organization

Now that you know what you're building and why, you can start to build your own scope tree.

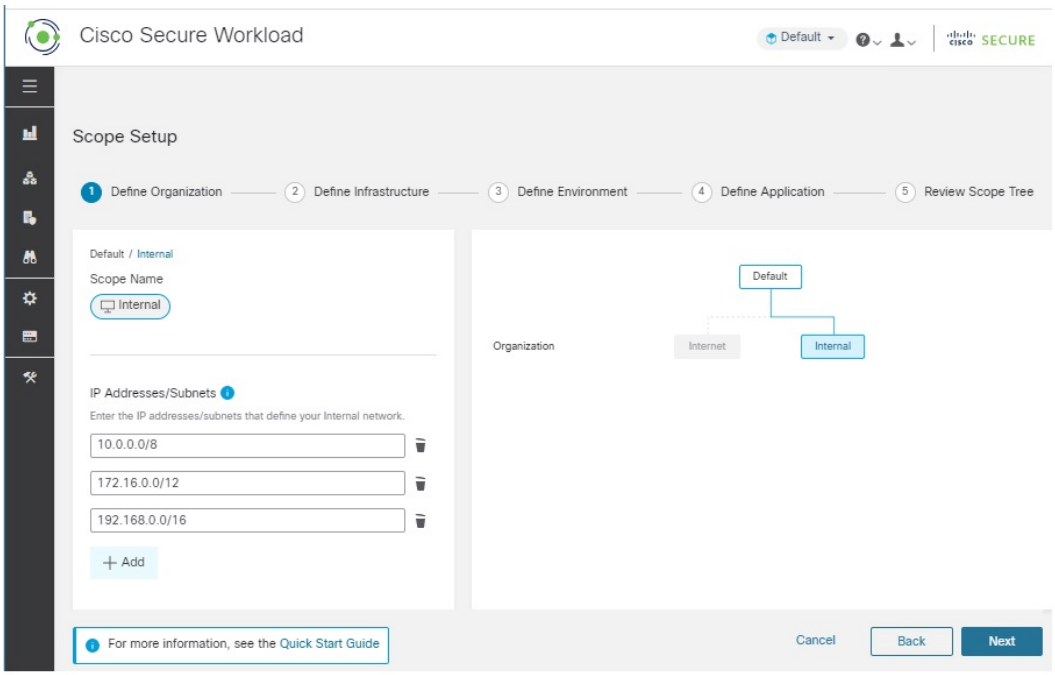


Before you continue, you need to choose the application to work with. See the guidelines at Choose An Application for This Wizard, on page 10.

Note that when you run the wizard, you won't be able to return to these informational pages unless you restart the wizard.

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 to each address the labels that define that scope.

So, on this page, the wizard assigns the label

```
Organization = Internal
```

to each IP address you enter.

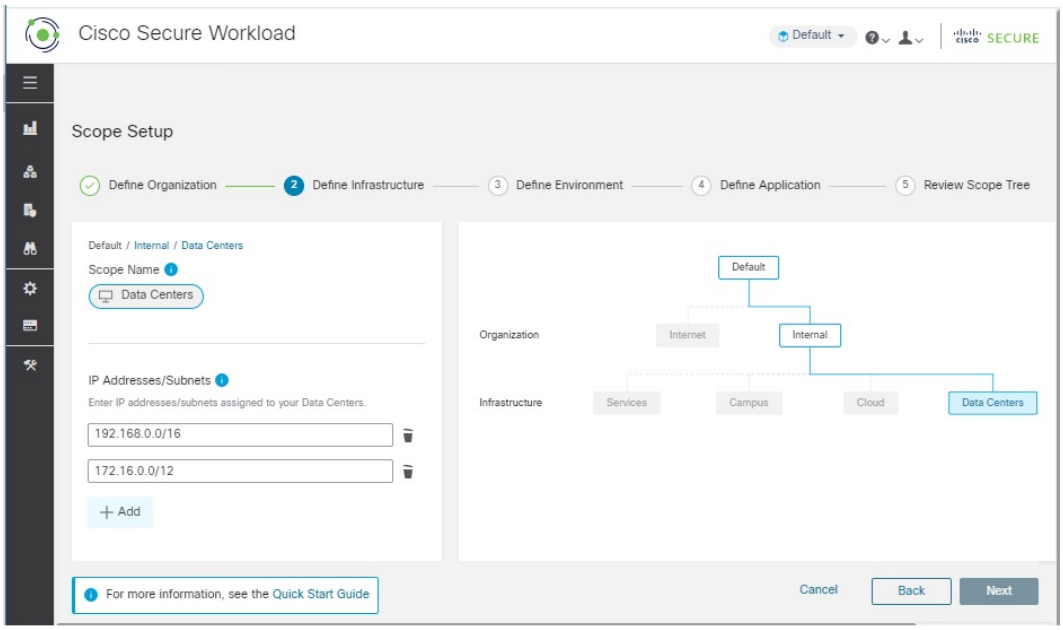
By default, the wizard adds the IP addresses in the private internet address space as defined in RFC 1918.

You don't have to add all of the IP addresses in your internal network now, but you must include the IP addresses associated with your chosen application, and you should include as many others as you can easily include. You can add the rest later.

Define the Data Centers Scope

This scope includes the IP addresses that define your on-premises data centers.

You can change the scope name, but keep the meaning the same. Scope names should be short and meaningful.



On this page, the IP addresses you enter must be a subset of the addresses for your internal network that you entered on the previous page. You must also include the IP addresses associated with your chosen application, and ideally you should include other addresses that represent workloads in your data centers – but it's OK to continue without them if you don't have those available. (If you have multiple data centers, you will include all of them in this scope so you can define a single set of policies.) You can always add more addresses later.

The wizard assigns the labels

```
Organization = Internal
```

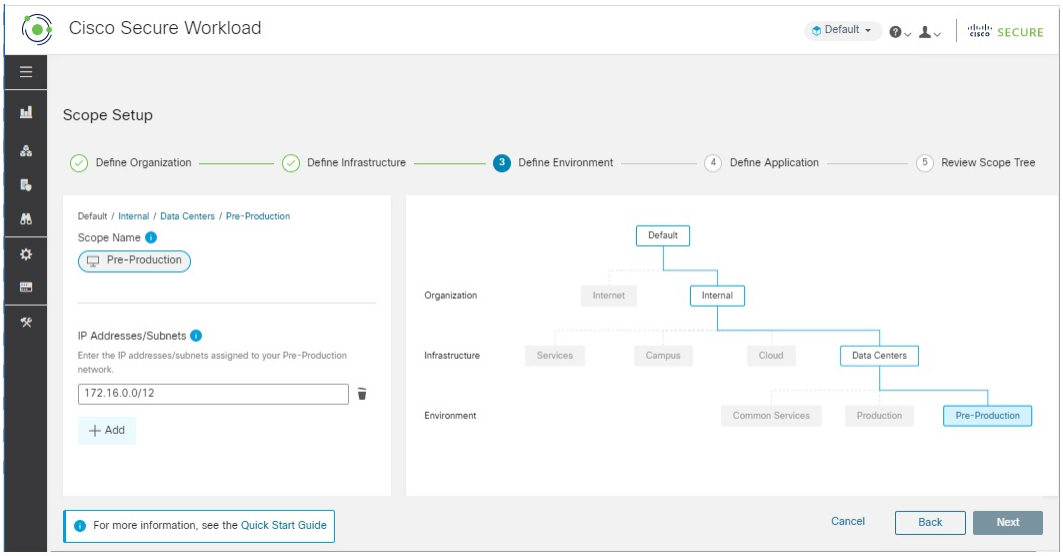
and

```
Infrastructure = Data Centers
```

to each IP address you enter.

Define the Pre-Production Scope

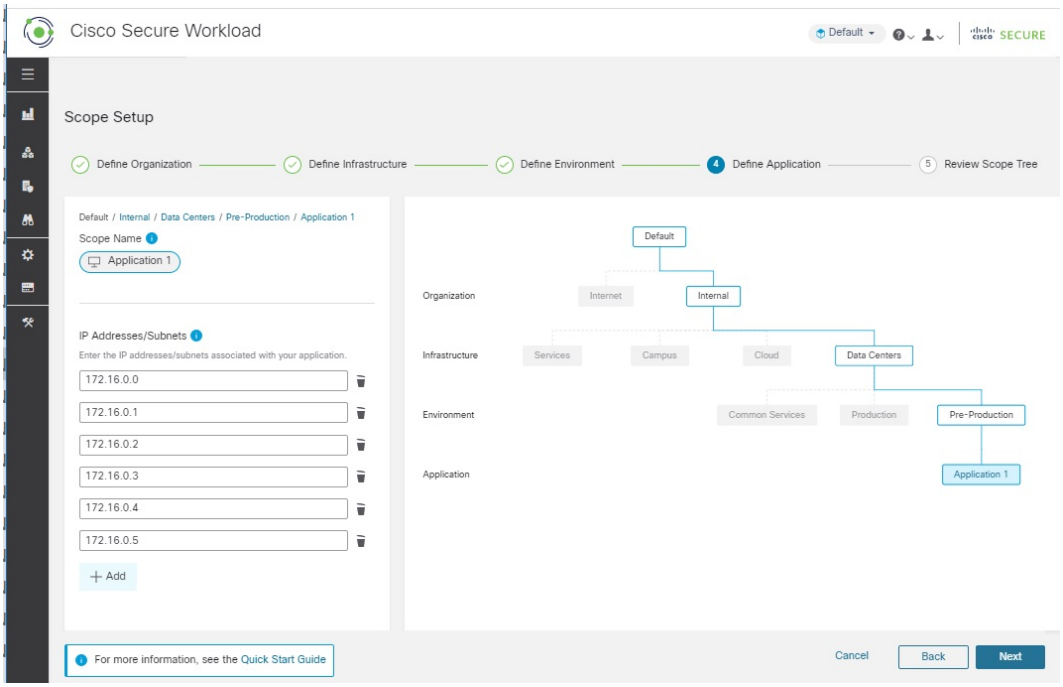
This scope includes IP addresses of non-production applications and hosts, such as development, lab, test, or staging systems. It should NOT include addresses of any applications that you're using to conduct actual business, which will be part of the Production scope that you define later.



The IP addresses you enter on this page must be a subset of the addresses you entered for your data centers, and they must again include the addresses of your chosen application. Ideally, they should also include pre-production addresses that are not part of your chosen application. Again, you can add more addresses later.

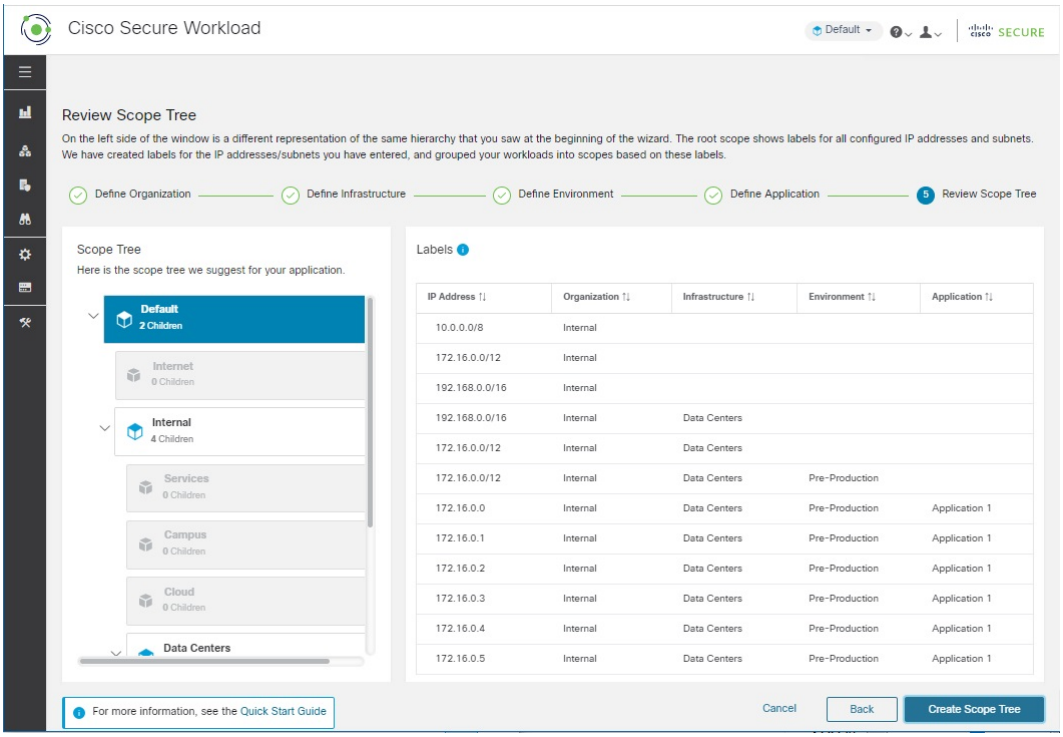
Define the Scope for Application 1

"Application 1" is an application you choose. See guidelines at Choose An Application for This Wizard, on page 10. An application consists of multiple workloads.



Add the IP addresses of the workloads that comprise your application. For example, include databases, web services, backup volumes, standby instances in high availability deployments, etc. You can add more addresses later, but you should try to include most of them now.

Review Scope Tree, Scopes, and Labels



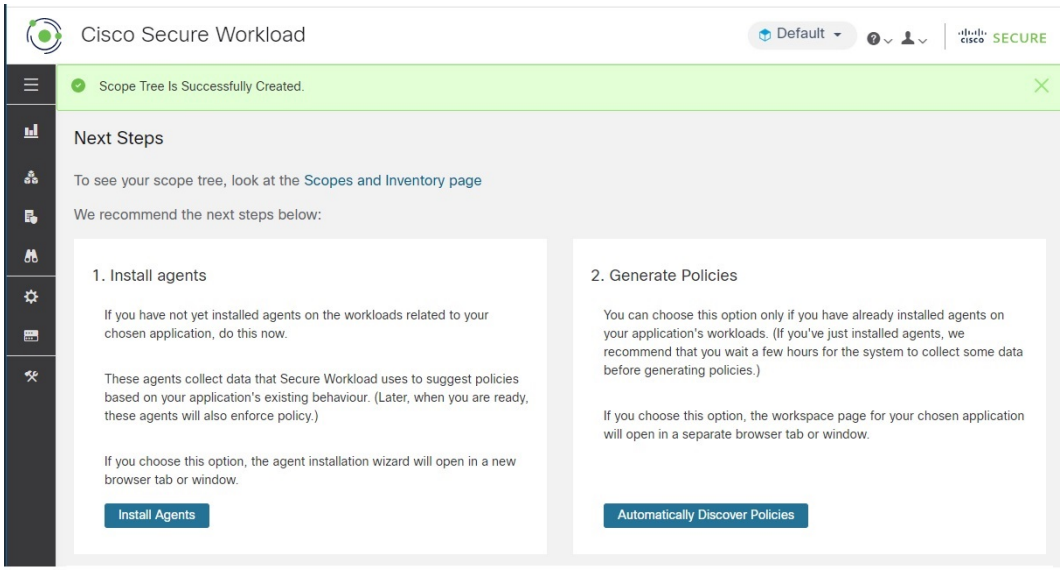
On the left, you see a different representation of the same scope tree that is shown on the other pages. You can expand and collapse branches, and scroll down to click a specific scope.

On the right, you see the IP addresses and labels assigned to the workloads in the scope you've clicked on the left. The column headings are the label keys, and the table cells show the label values.

In the image above, the top-level scope is selected, so you see the data for all IP addresses you specified in the wizard. The empty cells in the table are awaiting future labeling, for example for workloads that are not in your data center or are part of non-production applications other than your chosen application.

If you want to view this information after you've exited the wizard, choose **Organize > Scopes and Inventory** from the menu on the left side of the window.

Next Steps Page



Install Agents

You should install Secure Workload agents as soon as possible 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 data produces more accurate policies. For details, see Install Agents on Workloads, on page 12.

Generate Policies

After you've installed agents and allowed at least a few hours for traffic flow data to accumulate, you can tell Secure Workload to generate ("discover") policies based on that traffic. For details, see Automatically Generate Policies, on page 13.

Other

If you use the navigation bar at the left of the window, be sure to open new pages in a separate window or tab, or you won't be able to return to this page.

Quick Start Workflow

Step	Do This	Details
1	(Optional) Take an annotated tour of the wizard	Tour of the Wizard, on page 2
2	Choose an application to start your segmentation journey with.	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 10.
4	Run the wizard	To view requirements and access the wizard, see Run the Wizard, on page 11

Step	Do This	Details
5	Install Secure Workload agents on your application's workloads	See Install Agents on Workloads, on page 12.
6	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.
7	Generate ("discover") policies based on your actual flow data	See Automatically Generate Policies, on page 13.
8	Review the generated policies	See Look at the Generated Policies, on page 14.

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, you will choose a single application to work with.

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.

Guidelines for Choosing Your Application

Secure Workload supports workloads running on a wide range of platforms and operating systems, including cloud-based and containerized workloads. However, for simplicity, for this wizard, you should 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 by Secure Workload agents:

  See https://www.cisco.com/go/secure-workload/requirements/agents

  (In a future step, you will need to install agents on this application's workloads)

- Deployed in a pre-production environment

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) To Start Over, Reset the Scope Tree, on page 15.

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.

Next Steps

Tip After you complete the wizard, you can see and work with the scope tree you created using the wizard by going to **Organize** > **Scopes and Inventory**.

Once you have created the branch of your scope tree for your application, take the following steps:

Install Agents on Workloads

To collect flow data that is used to automatically generate policy suggestions, install agents on your workloads. Later, these agents can enforce policy, but **agents don't enforce policy until you tell them to**.

You should install agents as soon as possible, to start gathering data. More data produces more accurate policy suggestions.

Install an agent on each workload that is related to your chosen application.

Use the default settings unless you have good reason not to.

If you want additional information about agent installation, see the "Deploying Software Agents" chapter in the Secure Workload online help or user guide.

Before you begin

- Make sure all workloads on which you will install agents are running on supported platforms. See https://www.cisco.com/go/secure-workload/requirements/agents.
- Make sure you have permissions to install agents on each workload. If needed, ask someone who has the required permissions to do so.

Procedure

Step 1 Click the **Install Agents** button in the wizard.

Or, you can get to the agent installers this way:

a) Sign in to the Secure Workload web portal.
b) In the navigation bar on the left, select **Manage** > **Agents**.
c) Click the **Installer** tab.

Step 2 Click **Auto-Install Agent using an Installer**, then click **Next**.

Step 3 If you are using Secure Workload on-premises:

If you see this option: **Which tenant is your agent going to be installed under?**: Select the default unless you have a reason to choose something else.

(You see this option only if you are using on-premises Secure Workload.)

Step 4 Skip this option: **Which labels would you like us to apply to this workload? (Optional)**.

Step 5 Choose the platform on which your application is running.

Step 6 Enter the HTTP Proxy if necessary for your environment.

Step 7 Choose installer expiration options if desired.

Step 8 Click **Download Installer**.

Step 9 Click **Next**.

Step 10 Follow the installation precheck instructions, then click **Next**.

Step 11 Follow the installation instructions.

Use the default settings unless you have good reason to change them.

You should not need to change any of the flags listed for the installer script.

Step 12 Click **Next**.

Step 13 Follow the instructions on the screen to verify that the agent was installed successfully.

Step 14 Install the agent on each workload associated with your application.

Automatically Generate Policies

Secure Workload generates ("discovers") policies for you, based on existing traffic between your workloads and other hosts. (The policy discovery feature was formerly known as "ADM", so you may see or hear it called that.) You can modify, supplement, analyze, and eventually approve and enforce these policies when you are ready.

Note Policies are not enforced until you enforce them.

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 at any time:

a) Choose **Defend > Segmentation** from the left side of the Secure Workload window.
b) In the scope tree or list of scopes in the pane on the left, scroll down to your application's scope.
c) Click **Primary** in that scope.

(The wizard has created the primary workspace for your application for you.)

Step 2 Click **Manage Policies**.

Step 3 Click **Automatically Discover Policies**.

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

In general, more data produces more accurate policies.

Step 5 Click **Discover Policies**.

Generated policies will appear on this page.

What to do next

Look at the Generated Policies, on page 14.

Look at the Generated Policies

Take a look at the discovered policies. (If you have navigated away from the page, you can return to it by following the steps in View Policies, on page 14.)

Do the policies make sense? The labels should help you understand the type of hosts each workload is communicating with.

Do you see any mysteries? See if you can find out what the mystery workloads or communications are.

You can ask a colleague who is familiar with this application to evaluate the suggested policies.

As flow data accumulates, you should extend the configured time range and discover policies again, as often as needed to generate policies that address your traffic.

View Policies

If you have navigated away from the policies page after initiating policy discovery (or at any other time), you can view generated ("discovered") policies by going to the application workspace associated with the scope.

Before you begin

Discover policies. See Automatically Generate Policies, on page 13.

Procedure

Step 1 In the navigation bar on the left, choose **Defend** > **Segmentation**.

Step 2 In the list of scopes on the left side of the window, scroll to and click the scope for which you want to view policies.

Step 3 Click the workspace in which you want to view polices.

This may be the primary workspace or a secondary workspace, depending on which workspace you were in when you initiated policy discovery.

Step 4 Click **Manage Policies**.

Step 5 If you don't see a list of policy suggestions, click **Absolute and Default Policies**.

Step 6 (Optional) To view policies in a different workspace version (primary or secondary), use the drop-down list at the top of the page.

Step 7 (Optional) To view policies for a different scope, click **Workspace** at the top of the page, then click a different scope in the list at the left.

What to do next

For things to look for, see Look at the Generated Policies, on page 14.

(Optional) To Start Over, Reset the Scope Tree

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

Tip If you only want to remove some of the created scopes and you don't want to run the wizard again, you can delete individual scopes instead of resetting the entire tree: Click a scope to delete, then 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 User Guide in Secure Workload 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 Destroy Pending, you may need to refresh the browser page.

More Information

For more information about concepts in the wizard, see:

- The online help in Secure Workload
- The *Secure Workload User Guide* PDF for your release, available from https://www.cisco.com/c/en/us/support/security/tetration-analytics-g1/model.html