Set up System Configurations in Secure Workload

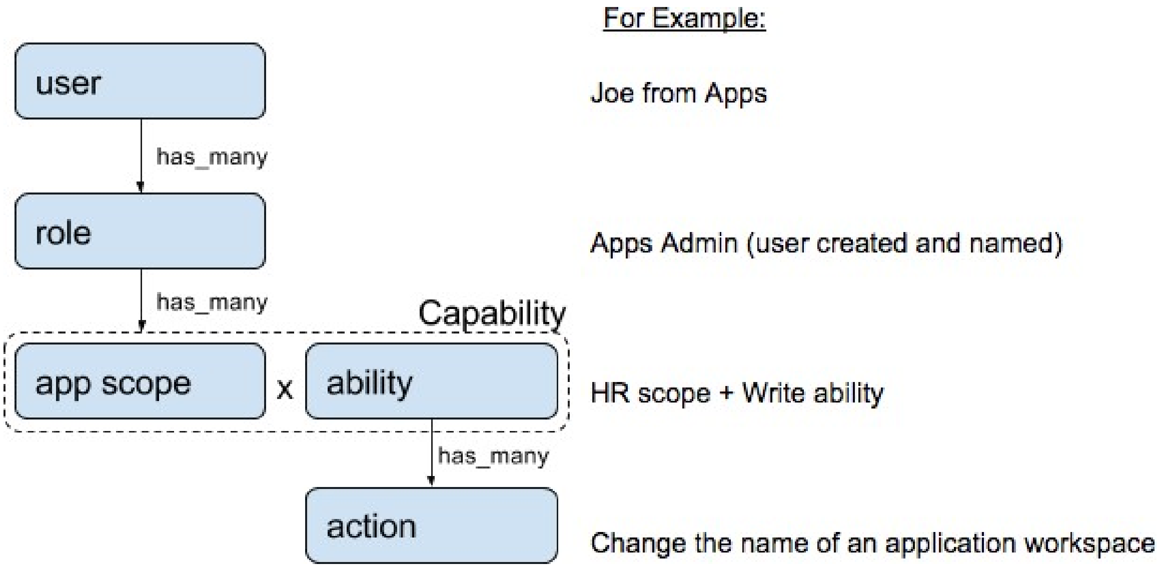
System-level settings are available to you depending on your role. For example, only users with **Site Administrator** and **Customer Support user** role, can view the **Users** option.

Roles

You can restrict access to features and data using role-based access control (RBAC) model.

- User - someone with login access to Cisco Secure Workload.
- Role - user created set of capabilities that is assigned to a user.
- Capability - scope + ability pair
- Ability - collections of actions
- Action - low-level user action such as “change workspace name”

Figure 1: Role Model



A user can have any number of roles. Roles can have any number of capabilities. For example, the "HR Search Engineer" role could have two capabilities: "Read on the HR Scope" to give visibility and context and "Execute on "HR:Search" capability to allow the engineers assigned this role to make specific changes that are related to their applications.

Use the **Users** page to assign users to the different roles. Roles have several capabilities and you can assign users to any number of roles.

System roles are defined to allow users to get started more quickly. They define different levels of access to **all Scopes**, that is, all data on the system. These system roles are defined below.

Role	Description
Agent Installer	Provide the ability to manage agents life cycle including install, monitor, upgrade, and convert, but **cannot** delete agents and access agent config profile.

Abilities and Capabilities

Roles are made up of capabilities which include a scope and an ability. These define the allowed actions and the set of data that they apply to. For example, the (HR, Read) capability should be read and interpreted as "Read ability on the HR scope". This capability would allow access to the HR scope and all its children.

Ability	Description
Installer	Install, monitor, and upgrade software agents.
Audit	Global appliance data read support and access to change logs.
Read	Read all data including flows, application, and inventory filters.
Write	Make changes to applications and inventory filters.

Ability	Description
Execute	Perform Automatically discover policies run and publish policies for analysis.
Enforce	Enforce policies that are defined in application workspaces that are associated with the given scope.

Important Abilities are inherited, for example, the Execute ability allows all the Read, Write, and Execute actions.

Important Abilities apply to the scope and all the scope's children.

Menu Access by Role

The menu items that you see and use on the navigation pane depend on the assigned role:

Table 1: Overview Menu

Menu	Option	Tenant Owner	Agent Installer
Overview	Overview	Yes	No

Table 2: Organize Menu

Menu	Option	Tenant Owner	Agent Installer
Organize	Scopes and Inventory	Yes	No
Organize	Use Uploaded Labels	Yes	No
Organize	Inventory Filters	Yes	No

Table 3: Defend Menu

Menu	Option	Tenant Owner	Agent Installer
Defend	Segmentation	Yes	No
Defend	Enforcement Status	Yes	No

Menu	Option	Tenant Owner	Agent Installer
Defend	Policy Templates	Yes	No
Defend	Forensic Rules	Yes	No

Table 4: Investigate Menu

Menu	Option	Tenant Owner	Agent Installer
Investigate	Traffic	Yes	No
	Alerts	Yes	No
	Vulnerabilities	Yes	No
	Forensics	Yes	No

Table 5: Reporting Menu

Menu	Option	Tenant Owner	Agent Installer
Reporting	Reporting Dashboard	Yes	No

Table 6: Manage Menu

Menu	Option	Tenant Owner	Agent Installer
Manage	Agents	Yes	Yes
Manage	Alerts Configs	Yes	No
Manage	Change Logs	Yes	No
Manage	Connectors	Yes	No
Manage	External Orchestrators	Yes	No
Manage	Secure Connector	Yes	No
Manage	Virtual Appliances	Yes	No

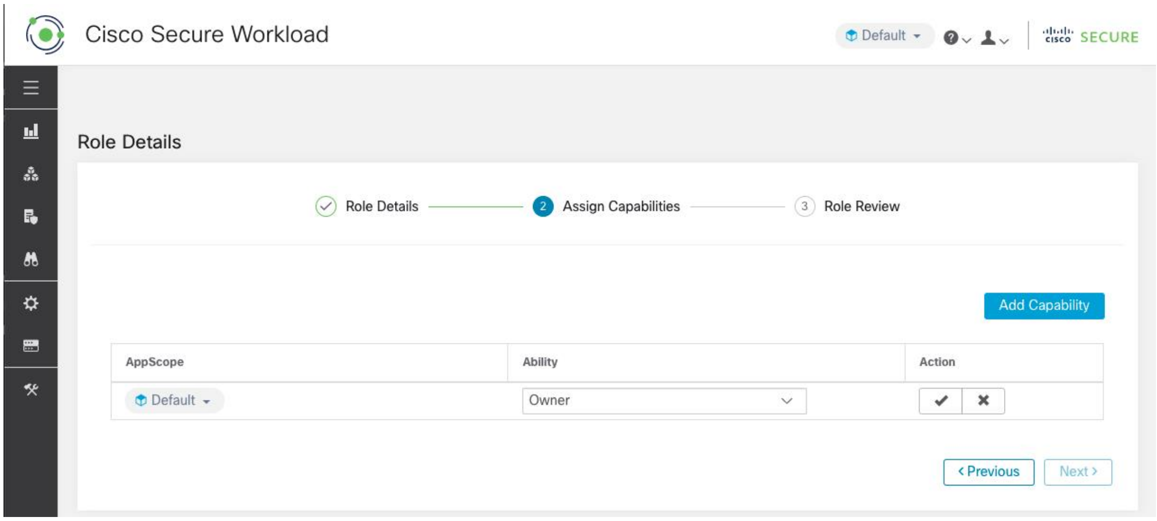
Menu	Option	Tenant Owner	Agent Installer
Manage	Users	Yes	No
Manage	Roles	Yes	No
Manage	Collection Rules	Yes	No
Manage	Session Configuration	Yes	No
Manage	Usage Analytics	Yes	No
Manage	Data Tap Admin	Yes	No

Create a Role

Before you begin

You must already have a **Site Admin** or **Customer Support** user role.

1. In the navigation bar on the left, click **Manage** > **User Access** > **Roles**.
2. Click **Create New Role**. The **Roles** panel appears.



AppScope	Ability	Action
Default	Owner	✔ ✖

Creating a role using the Create Role Wizard is three-step process.

Procedure

Step 1 a) Enter the appropriate values in the following fields:

Field	Description
Name	The name to identify the role.
Description	A short description to add context about the role.

b) Click the **Next** button to move to the next step or **Back to Roles Page** to go back to Roles Page.

Step 2

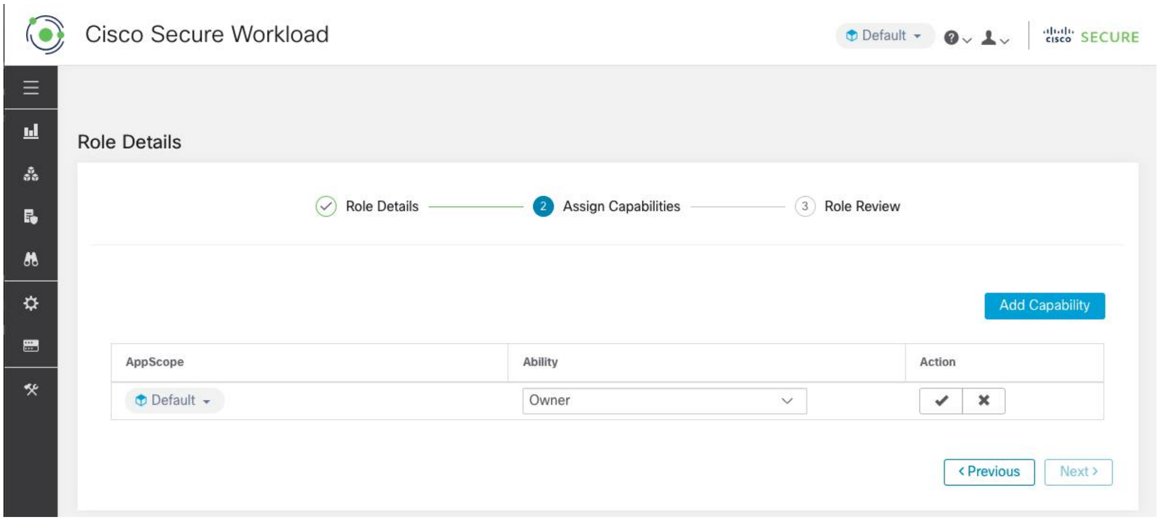
a) Click the **Add Capability** button to show the creation form in the top row.

b) Select scope and ability.

c) Click the **Checkmark** button to create a new capability or **Cancel** button to cancel.

d) Click **Next** to review role details or **Previous** to go back and edit.

Figure 2: Capability Assignment

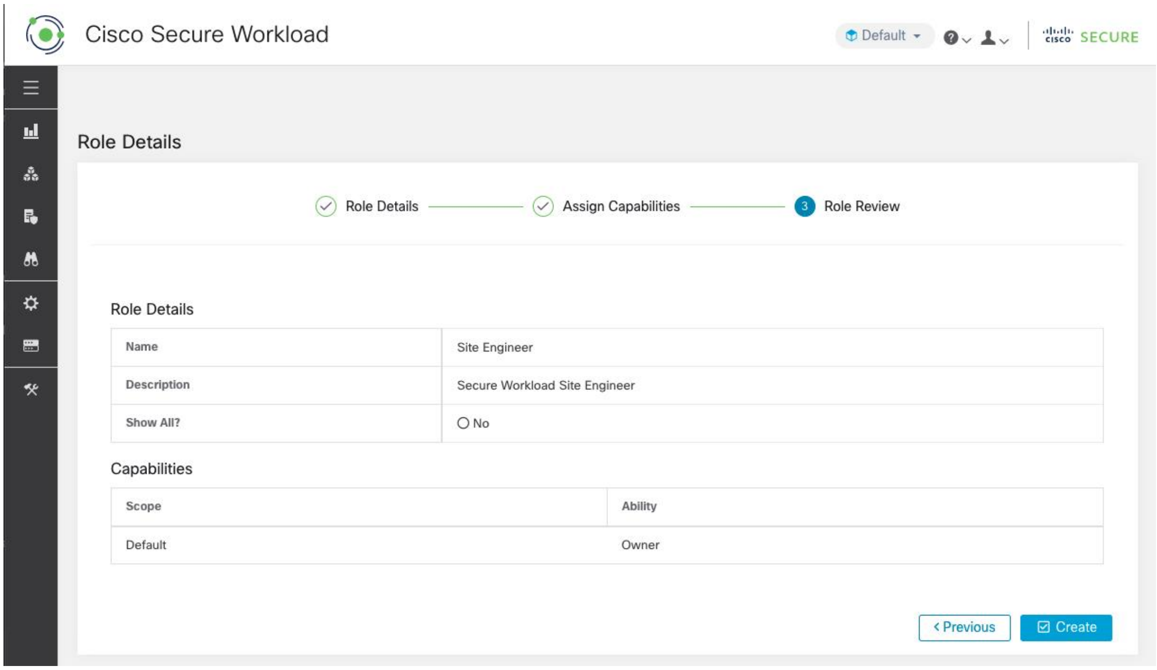


Step 3

a) Review the role details and capabilities.

b) Click **Create** to create role.

Figure 3: Role Review



Role Details

Name	Site Engineer
Description	Secure Workload Site Engineer
Show All?	○ No

Capabilities

Scope	Ability
Default	Owner

Edit a Role

This section explains how **Site Admins** and **Customer Support users** can edit roles.

Before you begin

You must be Site Admin or Customer Support User.

1. In the navigation bar on the left, click **Manage** > **User Access** > **Roles**.
2. In the row of the role to edit, click the **Edit** button in the right-hand column. The **Roles** panel appears.

Editing a role using the Edit Role Wizard is three-step process.

Procedure

Step 1

a) Update the name or description if desired.
b) Click the **Next** button to move to the next step or **Back to Roles Page** to go back to Roles Page.

Step 2

a) Remove any capability as needed. In the row of the capability to delete, click the **Delete** icon in the right-hand column.
b) To add, click the **Add Capability** button to show the creation form in the top row.
c) Select scope and ability.
d) Click **Next** to review role details or **Previous** to go back and edit.

Step 3

a) Review the role details and capabilities.

b) Click **Update** to create the role or **Previous** to go back and edit. Changes to role details and capability assignment are saved after **Update**.

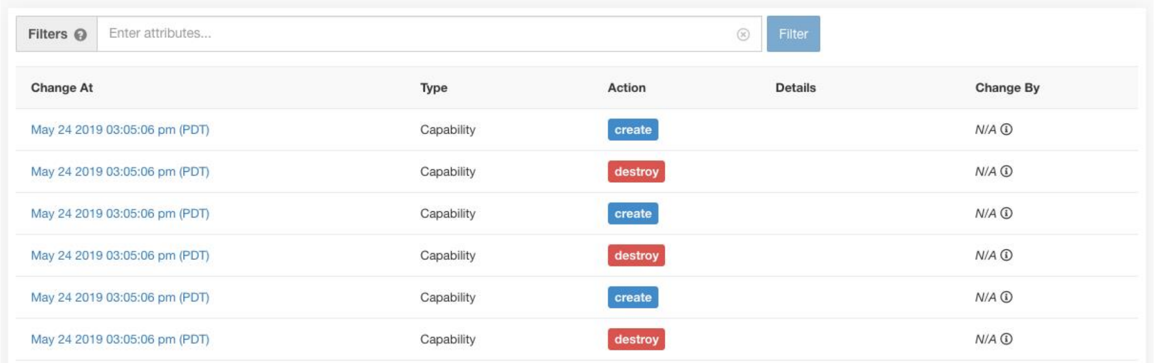
Note Capabilities cannot be edited, they must be deleted and recreated.

Change Log

Site Admins can access the **Change Log** page under the **Manage** menu in the navigation bar at the left side of the window. This page displays the most recent changes that are made within Cisco Secure Workload.

Note **Change Log Retention Period**: Secure Workload manages change logs for a duration of up to one year on both SaaS and On-premises clusters. An hourly job deletes change logs that exceed a one-year timeframe.

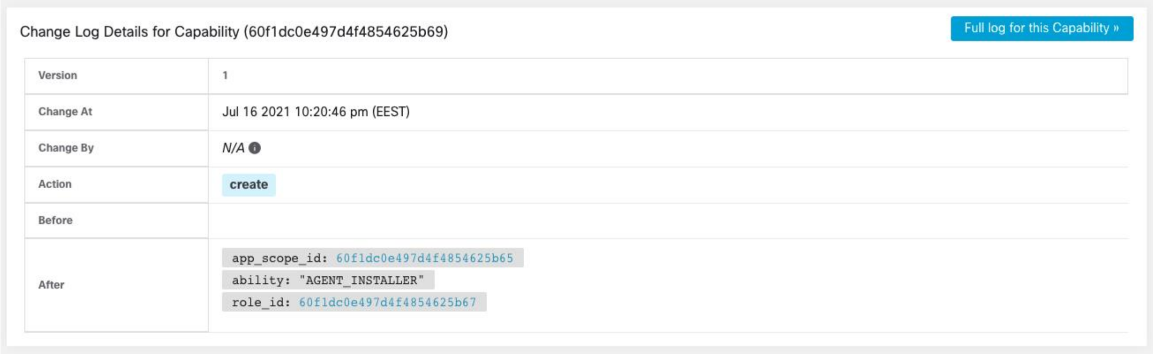
Figure 4: Change Log Page



Change At	Type	Action	Details	Change By
May 24 2019 03:05:06 pm (PDT)	Capability	create		N/A ⓘ
May 24 2019 03:05:06 pm (PDT)	Capability	destroy		N/A ⓘ
May 24 2019 03:05:06 pm (PDT)	Capability	create		N/A ⓘ
May 24 2019 03:05:06 pm (PDT)	Capability	destroy		N/A ⓘ
May 24 2019 03:05:06 pm (PDT)	Capability	create		N/A ⓘ
May 24 2019 03:05:06 pm (PDT)	Capability	destroy		N/A ⓘ

The details of each change log entry can be viewed by clicking on the link in the **Change At** column. This page includes a **Before** and **After** snapshot of the fields changed. The fields may include technical names that require some interpretation to understand how they are surfaced elsewhere throughout Secure Workload.

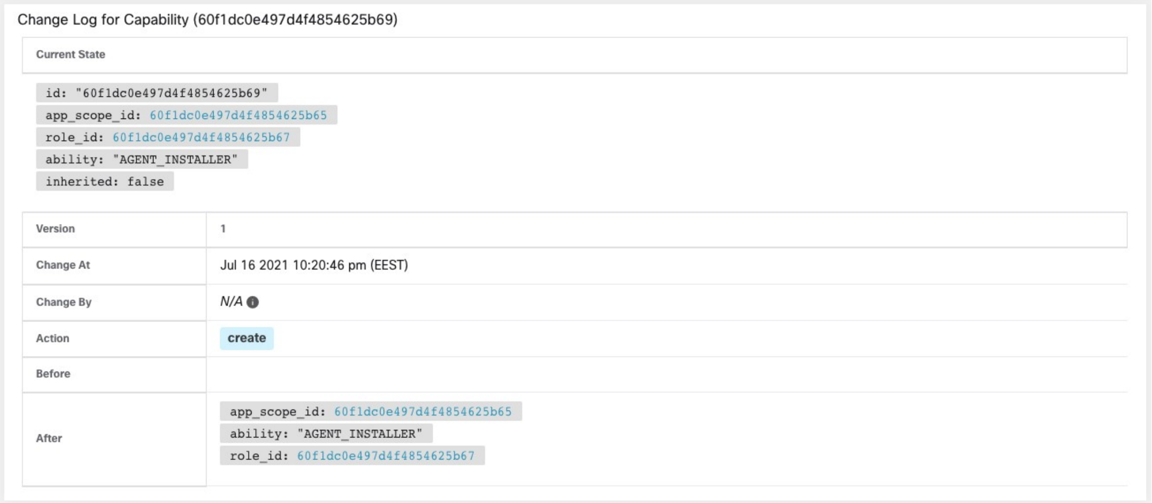
Figure 5: Change Log Details Page


Change Log Details for Capability (60f1dc0e497d4f4854625b69)

Version	1
Change At	Jul 16 2021 10:20:46 pm (EEST)
Change By	N/A ⓘ
Action	create
Before	
After	app_scope_id: 60f1dc0e497d4f4854625b65 ability: "AGENT_INSTALLER" role_id: 60f1dc0e497d4f4854625b67

The complete list of changes for an entity can be viewed by clicking the button in the upper-right corner, titled **Full log for this <entity type>**. This page displays the details of each change. It also includes the **Current State** of the entity, when available.

Figure 6: Full Change Log for Entity



Change Log for Capability (60f1dc0e497d4f4854625b69)

Current State

```
id: "60f1dc0e497d4f4854625b69"
app_scope_id: 60f1dc0e497d4f4854625b65
role_id: 60f1dc0e497d4f4854625b67
ability: "AGENT_INSTALLER"
inherited: false
```

Version	1
Change At	Jul 16 2021 10:20:46 pm (EEST)
Change By	*N/A* ⓘ
Action	create
Before	

After	`app_scope_id: 60f1dc0e497d4f4854625b65`
	`ability: "AGENT_INSTALLER"`
	`role_id: 60f1dc0e497d4f4854625b67`

Collection Rules

Site Admins and **Customer Support users** can access the **Collection Rules** page under the **Manage > Service Settings** menu in the navigation bar at the left side of the window. This page displays the hardware collection rules by VRF that is used by switches running the Cisco Secure Workload agent. There is a row in the table for each VRF.

Rules

Click the **Edit** button on a VRF to modify its collection rules. By default, every VRF is configured with two default catch-all rules, one for IPv4 `(0.0.0.0/0 INCLUDE)` and one for IPv6 `(::/0 INCLUDE)`. *These default rules can be removed, but do so with caution.*

Extra include and exclude rules can be added. Enter a valid subnet, select include or exclude, and click **Add Rule**. The priority of these rules can be adjusted via drag-and-drop. Click-and-hold on a rule in the list and drag it to adjust the order.

Changes may take several minutes to propagate to your switches. Click the **Back** button in the upper-right corner to return to the VRF list.

Priority

Collection Rules are ordered in decreasing order priority. No longest prefix match is done to determine the priority. The rule appearing first has higher priority over all the subsequent rules. Example:

1. 1.1.0.0/16 INCLUDE
2. 1.0.0.0/8 EXCLUDE

3. 0.0.0.0/0 INCLUDE

In the earlier example, all addresses belonging to 1.0.0.0/8 subnet are excluded except subnet 1.1.0.0/16 which is included.

Another Example with changed order:

1. 1.0.0.0/8 EXCLUDE
2. 1.1.0.0/16 INCLUDE
3. 0.0.0.0/0 INCLUDE

In the above example, all addresses belonging to 1.0.0.0/8 subnet are excluded. Rule number-2 does not get exercised here because of a higher-order rule already defined for its subnet.

Session Configuration

UI User Authentication idle session timeout can be configured here. This config applies to all the users of the appliance. The default idle session duration is 1 hour. The idle session duration can be set within the range of 5 minutes to 24 hours. The session timeout takes effect on a user’s authenticated session when this value is saved.

Site Admins and **Customer Support users** can access this setting. In the left navigation pane, click **Manage** > **Service Settings** > **Session Configuration**.

Idle Session

For those who are authenticating using a local database, this section explains how failed login attempts may lock the user account:

Procedure

Step 1 Five failed login attempts using email and password result in locking the account.

Note As a security measure against probing, no specific message indicating the lock will be provided in the login interface when trying to sign in a locked account.

Step 2 Lock out interval is set at 30 minutes. After the account is unlocked, use the correct password to log in or initiate password recovery by clicking *Forgot password?*

Note Once a user is successfully signed in, one hour of inactivity logs out the user. This timeout is configured from **Manage** > **Service Settings** > **Session Configuration**.

Preferences

The **Preferences** page displays your account details and enables you to update your display preferences, change your landing page, change your password, and configure two-factor authentication.

Change Your Landing Page Preference

To change the page you see when you sign in:

Procedure

Step 1 On the top-right corner of the window, click the user icon and choose **User Preferences**.

Step 2 Choose a landing page from the drop-down menu. Your preference is saved as the default or home page when you log in. To see the change, click the Secure Workload logo at the top-left corner of the page.

Changing a Password

Procedure

Step 1 Click on the user icon in the top-right corner.

Step 2 Select **User Preferences**.

Step 3 In the **Change Password** pane, enter your current password in the **Old Password** field.

Step 4 Enter your new password in the **Password** field.

Step 5 Re-enter your new password in the **Confirm Password** field.

Step 6 Click **Change Password** to submit the change.

Note **Password must be 8–128 characters and contain at least one of the each following:**

- Lower case letters (a b c d . . .)
- Upper case letters (A B C D . . .)
- Numbers (0 1 2 3 4 5 6 7 8 9)
- Special characters (! " # $ % & ’ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ‘ { | } ~), space included

Recovering Passwords

This section explains how to recover your password.

Before you begin

To reset a password, you must first have an account. A new account can be added by **Site Admins** and **Customer Support users**.

Procedure

Step 1 Point your browser to the Cisco Secure Workload URL and click the **Forgot Password** link. The **Forgot your password?** dialog box is displayed.

Step 2 Enter your email address in the **Email** field.

Step 3 Click **Reset Password**.

Password reset instructions are sent to your email.

Note The password recovery procedure for two-factor authentication requires contacting Secure Workload Customer Support because the email-based password recovery cannot contain the one-time password.

Enabling Two-Factor Authentication

This section explains how to enable two-factor authentication.

Procedure

Step 1 Click on the user icon in the top-right corner.

Step 2 Select **User Preferences**.

Step 3 In the **Two-Factor Authentication** pane, click the **Enable** button. A new **Two-Factor Authentication** pane appears.

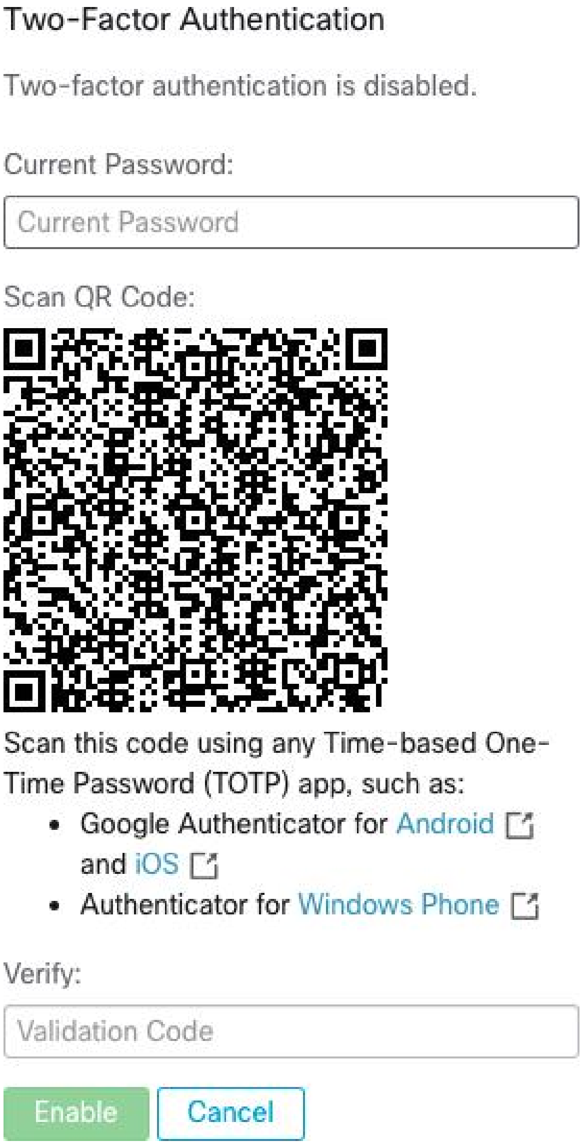
Step 4 Enter your password.

Step 5 Scan the QR code that is displayed under the **Current Password** field using any time-based one-time password (TOTP) app, such as Google Authenticator (for Android or iOS) or Authenticator (for Windows Phone).

Step 6 Enter the validation code that is shown by your chosen TOTP app.

Step 7 Click **Enable**.

Figure 7: Two-Factor Authentication Pane



Two-Factor Authentication

Two-factor authentication is disabled.

Current Password:

Current Password

Scan QR Code:

Scan this code using any Time-based One-Time Password (TOTP) app, such as:

- Google Authenticator for Android and iOS
- Authenticator for Windows Phone

Verify:

Validation Code

The next time that you log into the system, you must select the **Use two-factor authentication** check box and enter the verification code that is shown in your TOTP app to sign in.

Note The password recovery procedure for two-factor authentication requires contacting Secure Workload Customer Support because the email-based password recovery cannot contain the one-time password.

Disabling Two-Factor Authentication

This section explains how to disable two-factor authentication.

Procedure

Step 1 Click on the user icon in the top-right corner.

Step 2 Select **User Preferences**.

Step 3 Under two-factor authentication, click the **Disable** button. The **Two-Factor Authentication** pane appears.

Step 4 Enter your password.

Step 5 Click the **Disable** button again.

You will no longer be required to enter a two-factor verification code during login.

Scopes

Note The **Scopes** page is merged with **Inventory Search**. For more information, see the Scopes and Inventory page.

Users

Site Admins and Root Scope Owners can access the **Users** page under the **Manage** > **User Access** menu from the navigation pane.

This page shows all Service Provider users and users associated with the scope on the page header.

Multitenancy

To support multitenancy, assign users to a root scope. Users with the **Owner** ability on the root scope manage these users and assign roles that are associated with the same scope.

Service Providers users are without a scope; users are assigned to roles that allow them to perform actions across root scopes.

Add a User

Before you begin

- You must be a **Site Admin** or **Scope Owner** user to add users in Secure Workload.
- If a user is assigned a scope for multitenancy, only roles that are assigned to the same scope may be selected.

Note This page is filtered by the scope preference that is selected on the page header.

Procedure

Step 1 If applicable, select the appropriate root scope from the page header.

Step 2 From the navigation pane, choose **Manage** > **User Access** > **Users**.

Step 3 Click **Create New User**.
The **User Details** page is displayed.

Step 4 Update the following fields under **User Details**.

Table 7: User Details Field Descriptions

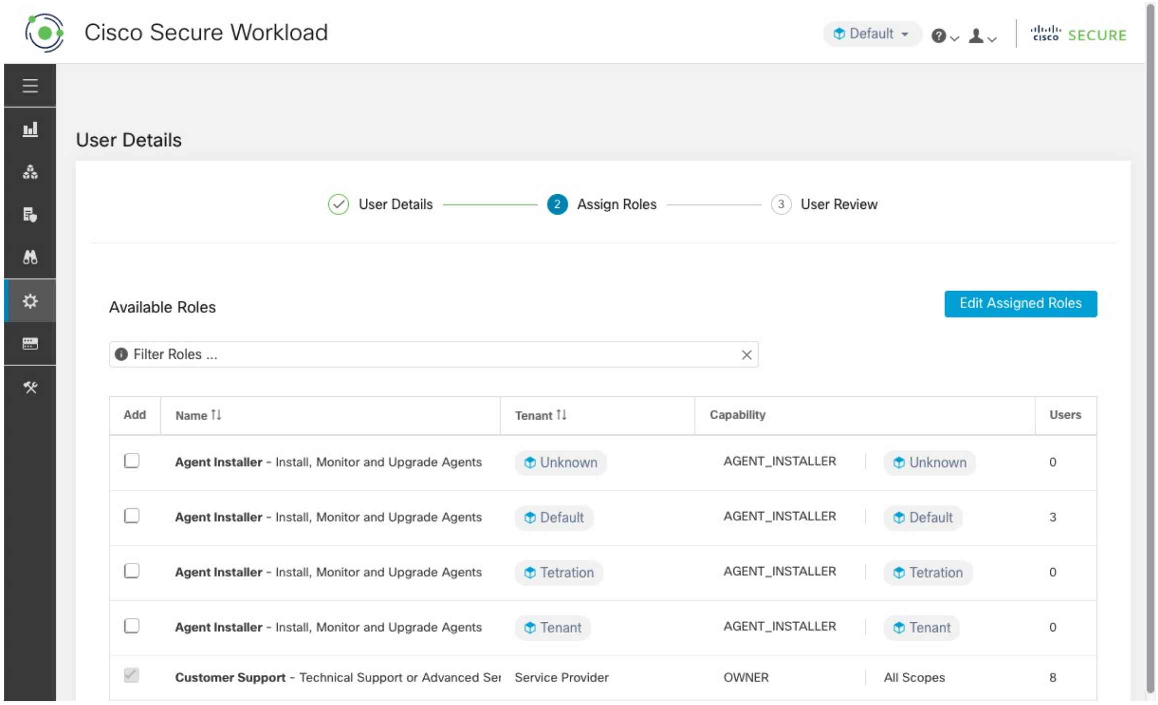
Field	Description
Email	Enter the email ID of the user. It is non case-sensitive. We use the lower case version of your email if it contains letters.
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Scope	Root scope that is assigned to the user for multitenancy. (Available to site admins)

Step 5 Click **Next**.

Step 6 Under **Assign Roles**, add or remove assigned roles to the user.

- Click **Add Roles** to assign new roles, and then click the **Add** check box.

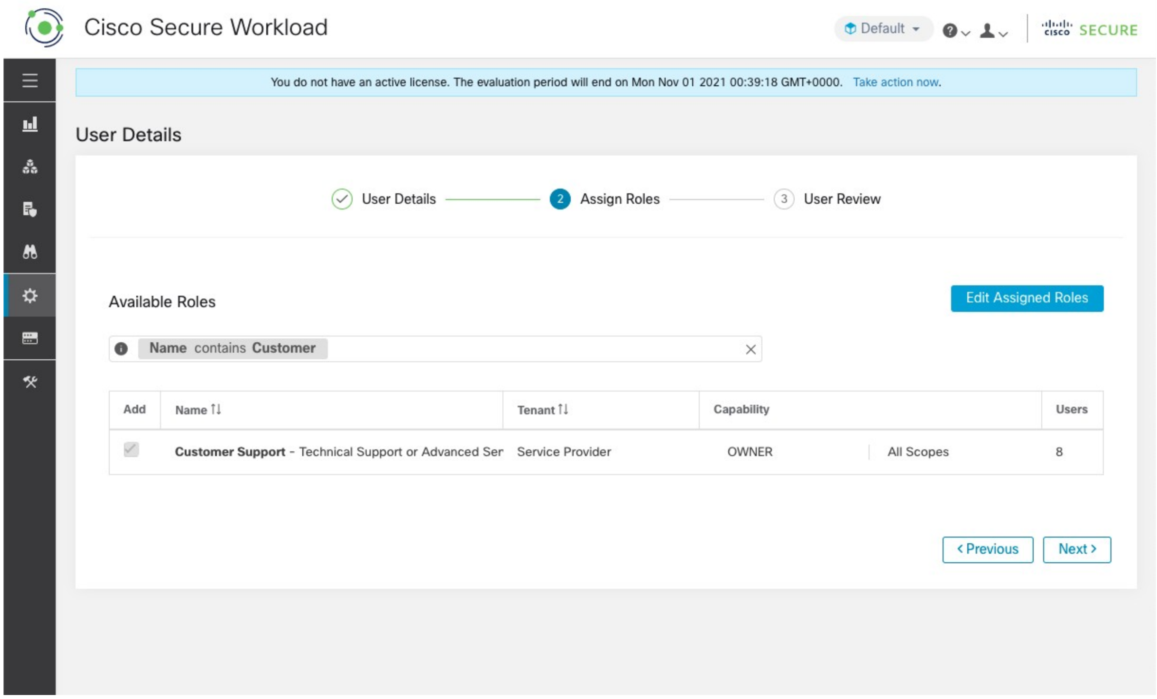
Figure 8: Assigned User Roles



Add	Name	Tenant	Capability		Users
□	**Agent Installer** - Install, Monitor and Upgrade Agents	Unknown	AGENT_INSTALLER	Unknown	0
□	**Agent Installer** - Install, Monitor and Upgrade Agents	Default	AGENT_INSTALLER	Default	3
□	**Agent Installer** - Install, Monitor and Upgrade Agents	Tetration	AGENT_INSTALLER	Tetration	0
□	**Agent Installer** - Install, Monitor and Upgrade Agents	Tenant	AGENT_INSTALLER	Tenant	0
☑	**Customer Support** - Technical Support or Advanced Se	Service Provider	OWNER	All Scopes	8

- Select the assigned roles, click **Edit Assigned Roles**, and then click the **Remove** icon.
- You can filter the user roles using **Name** or **Tenant**.

Figure 9: Filter User Roles



You do not have an active license. The evaluation period will end on Mon Nov 01 2021 00:39:18 GMT+0000. Take action now.

User Details

Available Roles

Name contains Customer

Add	Name	Tenant	Capability		Users
☑	**Customer Support** - Technical Support or Advanced Ser	Service Provider	OWNER	All Scopes	8

Step 7 Click **Next**.

Step 8 Under **User Review**, review the user details and the assigned roles. Click **Create**.

If external authentication is enabled, the authentication details are displayed.

Note After the user is added in Secure Workload, an activation email is sent to the registered email ID to set up the password.

Edit User Details or Roles

Before you begin

You must be a **Site Admin** or **Root Scope Owner** user to edit users in Secure Workload.

Note This page is filtered by the scope preference that is selected on the page header.

Procedure

Step 1 If applicable, select the appropriate root scope from the page header.

Step 2 From the navigation pane, choose **Manage** > **User Access** > **Users**.

Step 3 For the required user account, under **Actions**, click **Edit**.
The **User Details** page is displayed.

Step 4 Edit the following details.

a) Update the following fields under **User Details**.

Table 8: User Details Field Descriptions

Field	Description
Email	Update the email ID of the user.
First Name	Update the user's first name.
Last Name	Update the user's last name.
Scope	Root scope that is assigned to the user for multitenancy. (Available to site admins)
Reset MFA	If the user has lost their multifactor authentication (MFA) device or is locked out of MFA, then click **Reset MFA**. MFA of the user is reset in a few minutes.
Resend Activation Email	If a user has not received an activation email or the activation email link has expired, then click **Resend Activation Email**.

b) Click **Next**.

c) Under **Assign Roles**, add or remove assigned roles to the user.

- Click **Add Roles** to assign new roles, and then click the **Add** check box.
- Select the assigned roles, click **Edit Assigned Roles**, and then click the **Remove** icon.

d) Click **Next**.

e) Under **User Review**, review the user details and the assigned roles. Click **Update** to update the user account.

If external authentication is enabled, the authentication details are displayed.

Deactivating a User Account

Note To maintain consistency of change log audits, users can only be deactivated, they are not deleted from database.

Before you begin

You must be a **Site Admin** or **Root Scope Owner** user.

Note This page is filtered by the scope preference that is selected on the page header.

Procedure

Step 1 In the navigation bar on the left, click **Manage** > **User Access** > **Users**.

Step 2 If applicable, select the appropriate root scope from the top right of the page.

Step 3 In the row of the account you want to deactivate, click **Deactivate** button in the right-hand column.

To view deactivated users, toggle **Hide Deleted Users** button.

Reactivating a User Account

If a user has been deactivated, you can reactivate the user.

Before you begin

You must be a **Site Admin** or **Root Scope Owner** user.

Note This page is filtered by the scope preference that is selected on the page header.

Procedure

Step 1 In the navigation bar on the left, click **Manage** > **User Access** > **Users**.

Step 2 If applicable, select the appropriate root scope from the top right of the page.

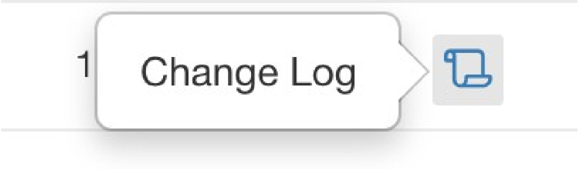
Step 3 Toggle **Hide Deleted Users** to display all users, including deactivated users.

Step 4 For the required deactivated account, click **Restore** in the right-hand column to reactivate the account.

Change Log – Users

Site Admins and users with the `SCOPE_OWNER` ability on the root scope can view the change logs for each user by clicking on the icon in the **Actions** column as shown in the following figure.

Figure 10: Change Log



For more information on the **Change Log**, see Change Log. Root scope owners are restricted to viewing change log entries for entities belonging to their scope.