Settings

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

Threat Intelligence

To manage threat intelligence, in the left navigation pane, click **Manage** > **Service Settings** > **Threat Intelligence**.

The **Threat Intelligence** feature provides the most up-to-date datasets for the Secure Workload pipeline that identifies and quarantines threats by inspecting the datacenter workloads against externally known malware command and control addresses, security flaws in processes and geographical location.

The Threat Intelligence dashboard displays the updated status of threat intelligence datasets. These datasets are updated automatically.

Warning The Threat Intelligence feature requires a connection to Cisco Secure Workload servers to automatically update. Your enterprise outbound HTTP request may require:

- Allow the following domain from the enterprise firewall outbound rules: `uas.tetrationcloud.com`
- Configure your Outbound HTTP Connection.

In environments without an outbound connection, upload the datasets directly. See the **Manual Uploads** section.

Table 1: Datasets

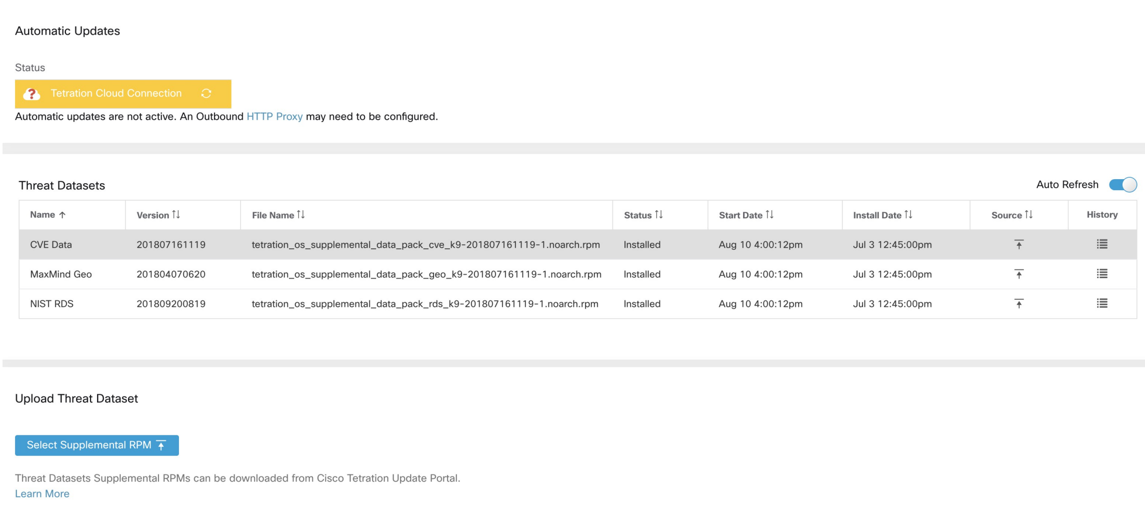
Dataset	Description
NVD CVEs	Security related software flaws, CVSS base score, vulnerable product configuration, and weakness categorization
MaxMind Geo	Identification of the location and other characteristics of source IPs
NIST RDS	NIST Reference Data Set of digital signatures of known, traceable software applications
Team Cymru	Insight on 3,000+ botnet command and control IPs
Hash Verdict	Verdict of Secure Workload on process hashes (only available with the Automatic Updates section).

Note In case the MaxMind Geo dataset is manually uploaded in an earlier release, you must reupload the corresponding RPM to view the location and related information on the Flow Visibility page.

Automatic Updates

The threat dataset updates are triggered from the appliance to synchronize with the global dataset that is hosted on the Internet at uas.tetrationcloud.com, everyday between 3-4 a.m. UTC. The global dataset is refreshed weekly on Fridays or Mondays. The Threat Intelligence dashboard lists the datasets and the date on which the dataset is last updated.

Figure 1: Dashboard



Manual Uploads

Attention **Scheduling Manual Uploads**—Dataset RPM files are published to Secure Workload Update Portal weekly. It is recommended to install the latest releases periodically by configuring a schedule for an administrator.

Downloading Updated Datasets

The datasets can be downloaded from Secure Workload Update Portal.

Uploading Datasets Manually

To upload dataset RPM files:

Before you begin

Log in as a **Site Administrator** or **Customer Support**.

Procedure

Step 1 In the left navigation pane, click **Manage** > **Service Settings** > **Threat Intelligence**.

Step 2 Under the **Upload Threat Dataset** section, click **Select Supplemental RPM**.

Step 3 Upload the RPM file downloaded from Secure Workload Update Portal.

Step 4 Click **Upload**.

The RPM upload process is initiated and the status is displayed on a progress bar. After the upload, the RPM file is processed and installed in the background. The table is updated after the installation is complete.

Figure 2: Threat Datasets

Threat Datasets

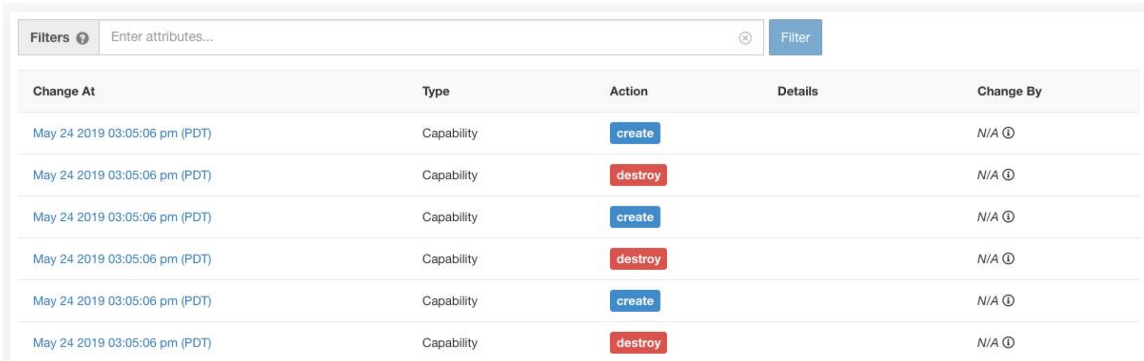
Auto Refresh

Name ↑	Version ↑↓	File Name ↑↓	Status ↑↓	Start Date ↑↓	Install Date ↑↓	Source ↑↓	History
MaxMind Geo	202108060000	tetration_os_supplemental_data_pack_geo_k9-202108060000-1.noarch.rpm	Failed	Aug 10 5:22:47pm			
Team Cymru	202108060000	tetration_os_supplemental_data_pack_zeus_k9-202108060000-1.noarch.rpm	Failed	Aug 10 5:23:12pm			

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.

Figure 3: Change Log Page

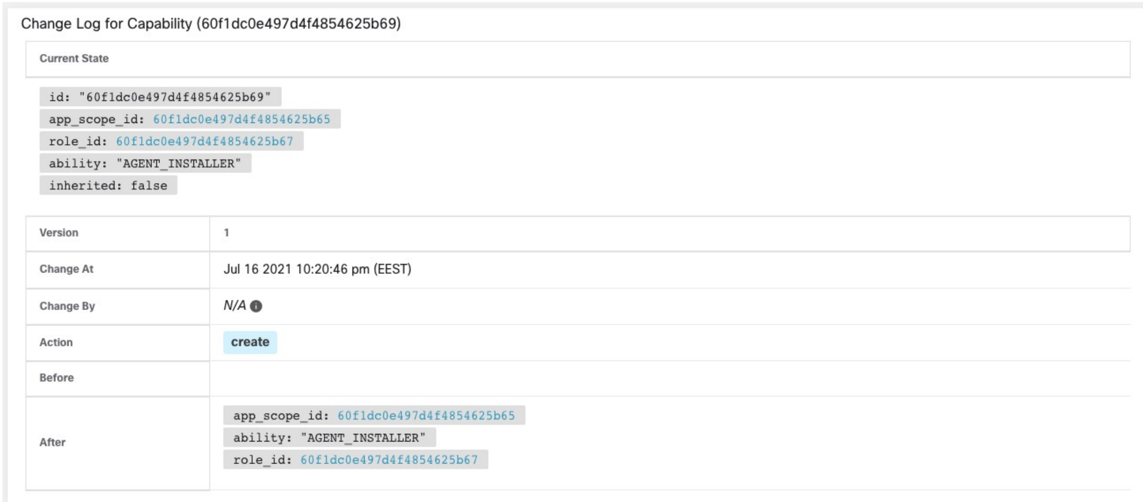


The details of each change log entry can be viewed by clicking on the link in the **Change At** column. This page includes a **Before** and **After** snapshot of the fields changed. The fields may include technical names that require some interpretation to understand how they are surfaced elsewhere throughout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

Figure 4: Change Log Details Page

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 5: Full Change Log for Entity



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.

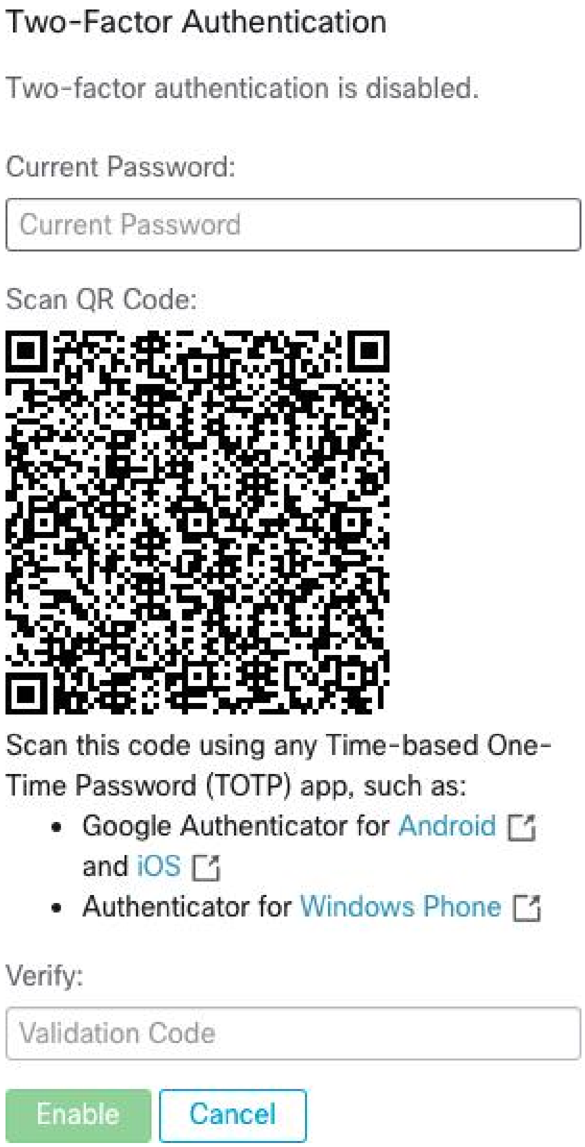
Step 4 Enter your password.

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 6: Two-Factor Authentication Pane



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.

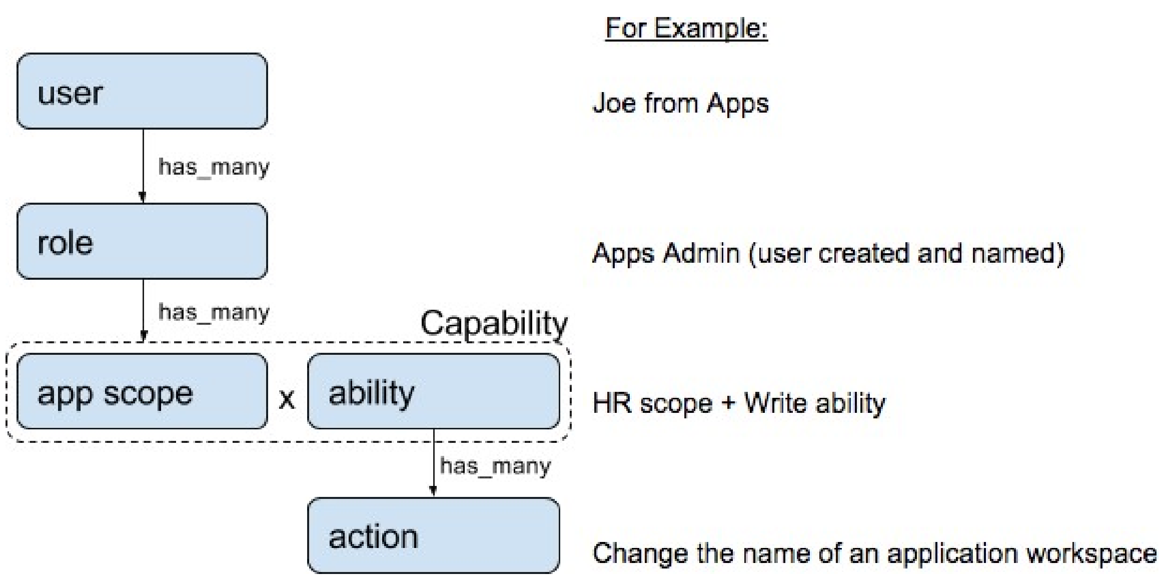
You will no longer be required to enter a two-factor verification code during login.

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 7: 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.

Roles contain sets of Capabilities and are assigned to users on the **Users** page. A user can have any number of roles. Roles can have any number of capabilities.

Seven 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.
Customer Support	For Technical Support or Advanced Services. Provides access to cluster maintenance features. Allows the same access as Site Admin, but **cannot** modify users.
Customer Support Read Only	For Technical Support or Advanced Services. Provides access to cluster maintenance features. Allows the same access as Site Admin, but **cannot** modify users.
Site Admin	Provides the ability to manage users, agents, and so on. Can view and edit all features and data. There must be at least one site admin.
Global Application Enforcement	Provides the Enforce ability on every scope.
Global Application Management	Provides the Execute ability on every scope.
Global Read Only	Provides the Read ability on every scope.

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.
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.

Ability	Description
Owner	Required to toggle an application workspace from secondary to primary. Access to Data Tap Admin abilities, such as managing User App sessions, adding Data Taps, and creating Visualization Data Sources.

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 menus a user can see and use depend on the user's assigned role:

Table 2: Overview Menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Overview	Overview	Yes	Yes	Yes	Yes	Yes	Yes	No
Reporting	Overview	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 3: Organize Menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Organize	Scopes and Inventory	Yes	Yes	Yes	Yes	Yes	Yes	No
Organize	Label Management	Yes	Yes	Yes	Yes	Yes	Yes	No
Organize	Inventory Filters	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 4: Defend Menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Defend	Segmentation	Yes	Yes	Yes	Yes	Yes	Yes	No

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Defend	Enforcement Status	Yes	Yes	Yes	Yes	Yes	Yes	No
Defend	Policy Templates	Yes	Yes	Yes	Yes	Yes	Yes	No
Defend	Forensic Rules	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 5: Investigate Menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Investigate	Traffic	Yes	Yes	Yes	Yes	Yes	Yes	No
	Alerts	Yes	Yes	Yes	Yes	Yes	Yes	No
	Vulnerabilities	Yes	Yes	Yes	Yes	Yes	Yes	No
	Forensics	Yes	Yes	Yes	Yes	Yes	Yes	No

Table 6: Manage Menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Manage	Agents	Yes	Yes	Yes	No	No	No	Yes
Manage	Alerts Configs	Yes	Yes	Yes	Yes	Yes	Yes	No
Manage	Change Logs	Yes	No	Yes	No	No	No	No
Manage	Connectors	Yes	Yes	No	No	No	No	No
Manage	External Orchestrators	Yes	Yes	No	No	No	No	No
Manage	Secure Connector	Yes	Yes	No	No	No	No	No
Manage	Virtual Appliances	Yes	Yes	No	No	No	No	No
Manage	Users	Yes	Yes	No	No	No	No	No

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Manage	Roles	Yes	Yes	Yes	No	No	No	No
Manage	Threat Intelligence	Yes	Yes	Yes	No	No	No	No
Manage	Licenses	Yes	No	No	No	No	No	No
Manage	Collection Rules	Yes	Yes	Yes	Yes	Yes	Yes	No
Manage	Session Configuration	Yes	Yes	No	No	No	No	No
Manage	Usage Analytics	Yes	Yes	No	No	No	No	No
Manage	Data Tap Admin	Yes	No	No	No	No	No	No

Table 7: Platform menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Platform	Tenants	Yes	Yes	No	No	No	No	No
Platform	Cluster Configuration	Yes	Yes	No	No	No	No	No
Platform	Outbound HTTP	Yes	Yes	No	No	No	No	No
Platform	Collectors	Yes	Yes	No	No	No	No	No
Platform	External Authentication	Yes	Yes	No	No	No	No	No
Platform	SSL Certificate	Yes	Yes	No	No	No	No	No
Platform	Login Page Message	Yes	Yes	No	No	No	No	No
Platform	Federation	See below	See below	No	No	No	No	No
Platform	Data Backup	See below	See below	No	No	No	No	No

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Platform	Data Restore	See below	See below	No	No	No	No	No
Platform	Upgrade/ Reboot/ Shutdown	Yes	Yes	No	No	No	No	No

Note

- The Federation option is available to Site Admin and Customer Support roles if Federation is enabled.
- Data Backup and Restore options are available to Site Admin and Customer Support roles if data backup and restore are enabled.

Table 8: Troubleshoot Menu

Menu	Option	Site Admin	Customer Support	Customer Support Read Only	Global Application Enforcement	Global Application Management	Global Read Only	Agent Installer
Troubleshoot	Service Status	Yes	Yes	Yes	No	No	No	No
Troubleshoot	Cluster Status	See below	See below	No	No	No	No	No
Troubleshoot	Virtual Machine	Yes	Yes	Yes	No	No	No	No
Troubleshoot	Snapshots	Yes	Yes	No	No	No	No	No
Troubleshoot	Maintenance Explorer	Yes	Yes	No	No	No	No	No
Troubleshoot	Resque	Yes	Yes	No	No	No	No	No
Troubleshoot	Hawkeye (Charts)	Yes	Yes	Yes	No	No	No	No
Troubleshoot	Abyss (Pipeline)	Yes	Yes	Yes	No	No	No	No

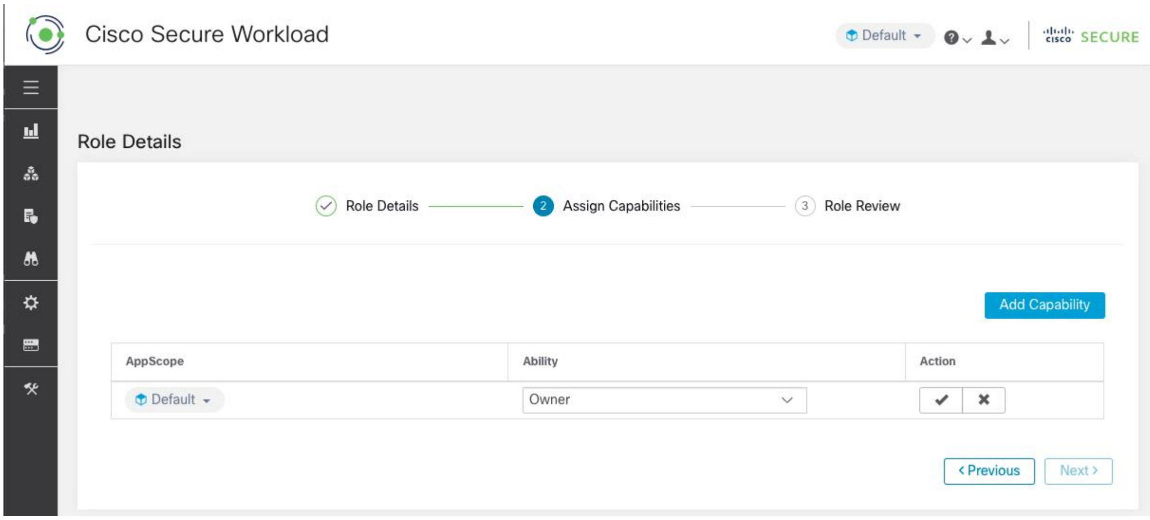
Note The Cluster Status option is available to Site Admin and Customer Support roles if the cluster type is ‘Physical’ or ‘OCI’.

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.



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

Procedure

Step 1

a) Enter the appropriate values in the following fields:

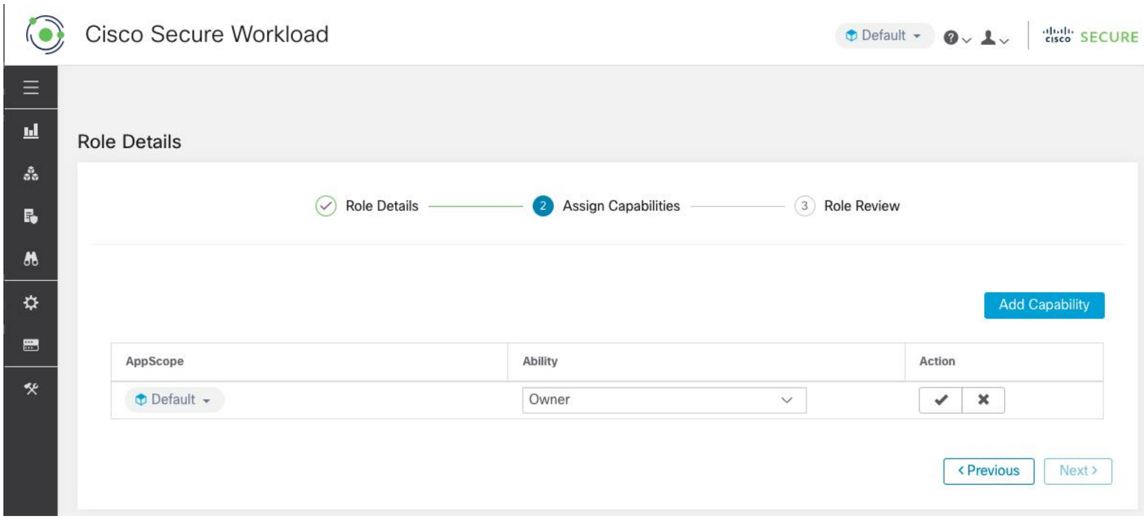
Field	Description
Name	The name to identify the role.
Description	A short description to add context about the role.

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

Step 2

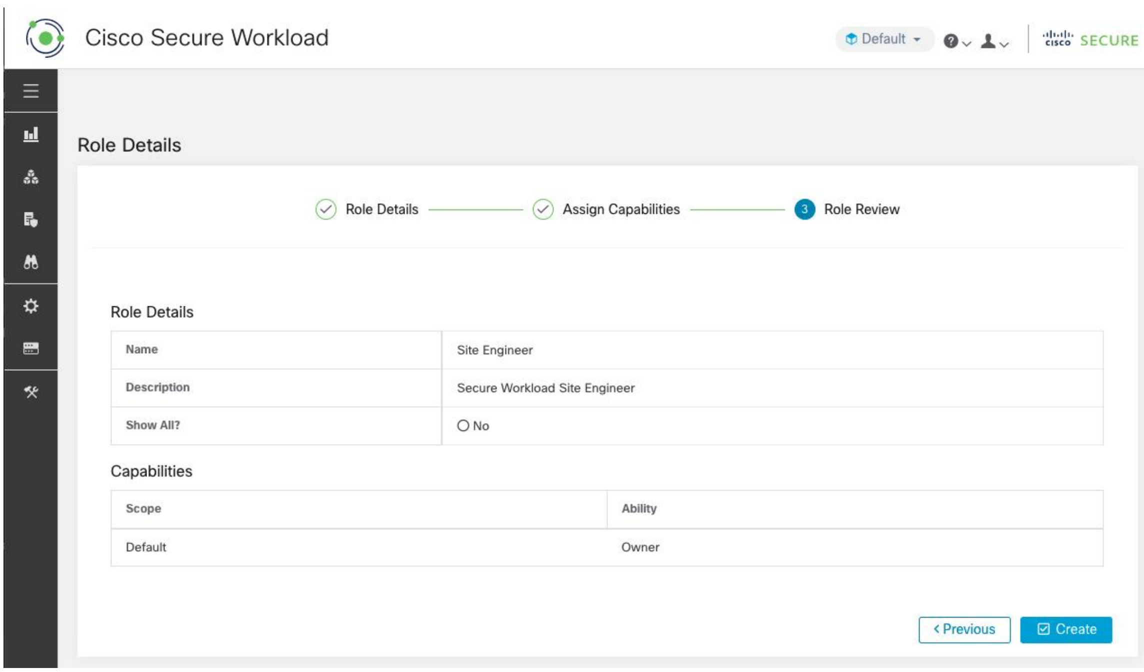
a) Click the **Add Capability** button to show the creation form in the top row.
b) Select scope and ability.
c) Click the **Checkmark** button to create a new capability or **Cancel** button to cancel.
d) Click **Next** to review role details or **Previous** to go back and edit.

Figure 8: Capability Assignment



Step 3
a) Review the role details and capabilities.
b) Click **Create** to create role.

Figure 9: Role Review



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 – Roles

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

Figure 10: Change Log

These users can also view a list of deleted roles by clicking on the **View Deleted Roles** link below the table.

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.

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 in the navigation bar at the left side of the window.

This page shows all Service Provider users and those associated with the scope that is selected on the page header.

Multitenancy

To support multitenancy, users can be assigned to a root scope. These users can be managed by users with the ‘Owner’ ability on the root scope and can only be assigned roles that are associated with the same scope.

Users without a scope are called ‘Service Providers’ and they can be assigned any role allowing 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 9: User Details Field Descriptions

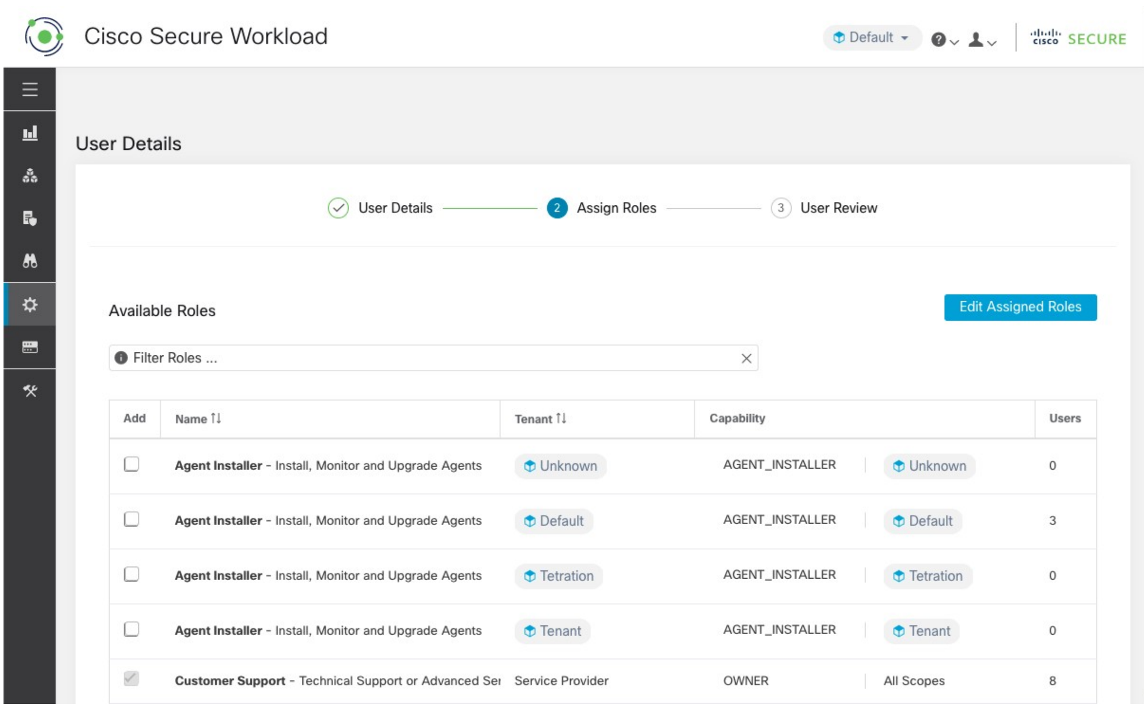
Field	Description
Email	Enter the email ID of the user. It is non case-sensitive. We use the lower case version of your email if it contains letters.
First Name	Enter the user’s first name.
Last Name	Enter the user’s last name.
Scope	Root scope that is assigned to the user for multitenancy. (Available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

Step 5 Click **Next**.

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

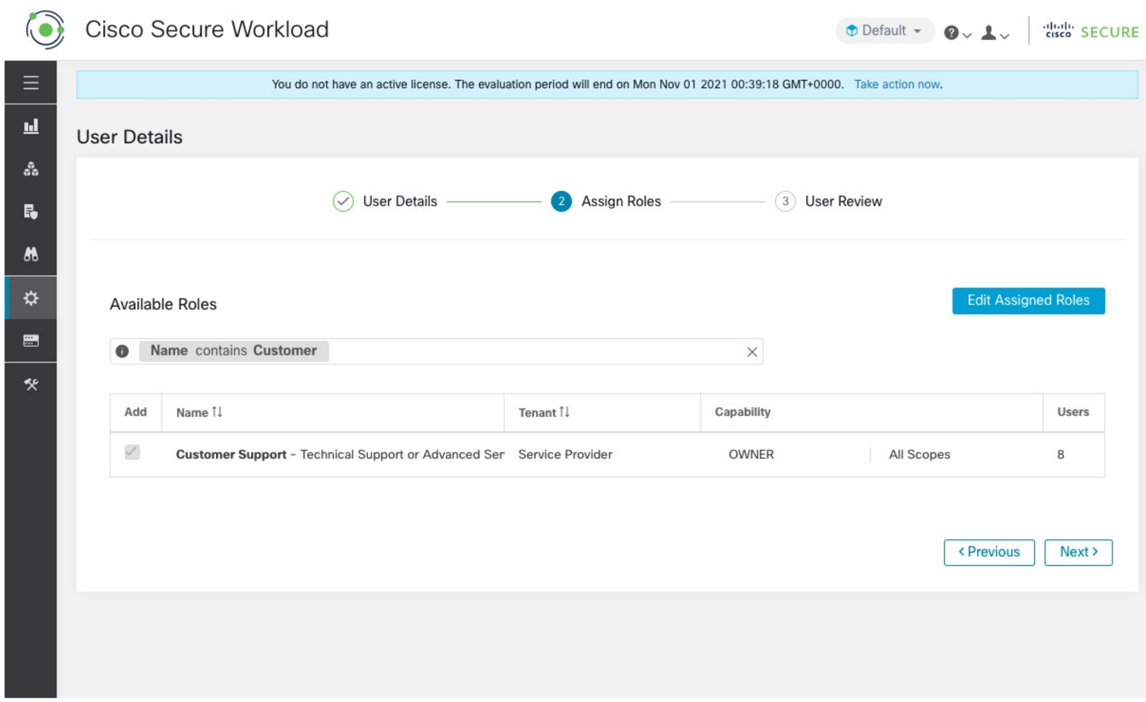
- Click **Add Roles** to assign new roles, and then click the **Add** check box.

Figure 11: Assigned User Roles



- 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 12: Filter User Roles



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 10: 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.

Import SSH Public Key

To enable SSH access as **ta_guest** user via one of the collector IP addresses, SSH public key can be imported for each user. This menu will only be available to **Site Admins** and users with the `SCOPE_OWNER` ability on the root scope. The SSH Public Key automatically expires in 7 days.

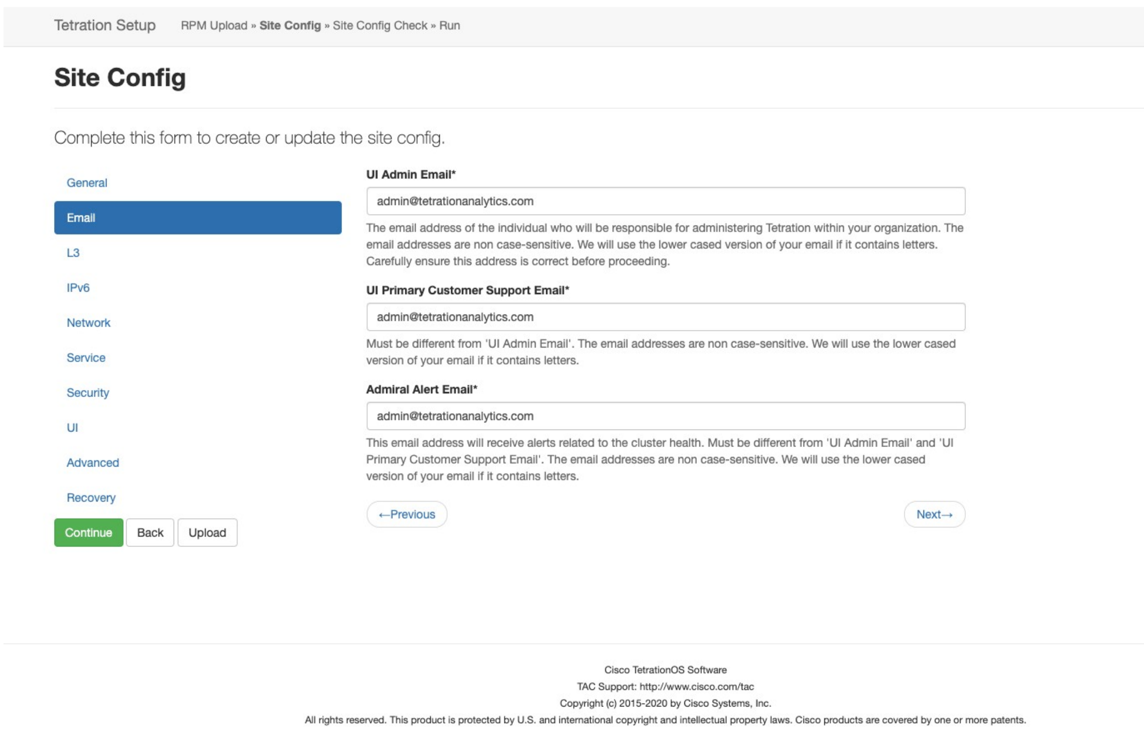
Site Configuration in Secure Workload Setup

This section explains how **Site Admins** can set up a site during the Secure Workload Setup process.

Field	Description
UI Admin Email	The email address of the individual who will be responsible for administering Secure Workload within your organization.
UI Primary Customer Support Email	The email address of primary support. Must be different from UI Admin Email.
Admiral Alert Email	This email address receives alerts that are related to the cluster health. Must be different from UI Admin Email and UI Primary Customer Support Email.

The email addresses are non case-sensitive. We use the lower cased version of your email if it contains letters.

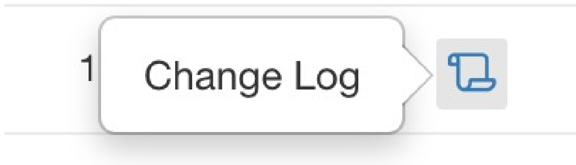
Figure 13: Configure UI Admin, Primary Customer Support, and Admiral Admin Alert Emails



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 14: 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.