Hewlett Packard Enterprise

HPE GreenLake Account Home User Guide

Abstract

This guide contains information for customer administrators and customer users about using HPE GreenLake. HPE GreenLake is an advanced software-as-a-service platform that provides you with a consistent cloud experience for all your applications and data—on-premises or off-premises. It provides you with insights and controls to manage your hybrid IT estate, complementing your use of public clouds and data centers. This guide describes how to use HPE GreenLake to access your existing software services, request and experience trials of new services, and manage user roles and permissions.

Published: December 2025

© Copyright 2025 Hewlett Packard Enterprise Development LP

Notices

The information provided here is subject to change without notice. Hewlett Packard Enterprise's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hewlett Packard Enterprise is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hewlett Packard Enterprise to possess, use, or copy the software. In accordance with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under the vendor's standard commercial license.

Links to third-party websites will take you outside of the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for the information outside the Hewlett Packard Enterprise website.

Acknowledgments

Ampere®, Altra®, and the A®, and Ampere® logos are registered trademarks or trademarks of Ampere Computing.

DLTtape logo and SDLTtape logo are trademarks of Quantum Corporation in the U.S. and other countries.

All third-party marks are the property of their respective owners.

Contents

Welcome to HPE GreenLake Account Home 5

Home 6

Personalizing your HPE user account 6
HPE GreenLake Account Home cloud header 7

Devices 12

Auto-subscribe 12
Managing auto-subscribe for devices 12
Inventory 13
Example scenario: adding device subscriptions 13
Adding managed devices 13
Searching and filtering the device inventory 16
Managing tags for devices 17
Adding tags to devices using a CSV file 18
Applying subscriptions to devices 19
Removing subscriptions from devices 20
Adding device subscriptions to your workspace 21
Removing device subscriptions from your workspace 22
Managing tags for subscriptions 23
Managing auto-reassign for device subscriptions 24
Device subscription expiration dates 25
Transferring a single device or multiple devices between workspaces 25
Viewing subscription expiry dates 26
Viewing devices 27
Archiving devices 28
Claiming subscription from the subscription notification email message 29
Audit logs 30
Viewing audit logs 30
Searching and filtering audit logs 31
Configuring columns in the audit log 31
Exporting audit logs 32
Identity & access management 33
Users 33
Viewing user details 33
Inviting users 35
Deleting a user 35
Viewing audit logs for users 36
Roles & permissions 36
Roles 36
Creating user roles 43
Resource restriction policies 44
Viewing resource restriction policy details 44
Creating a resource restriction policy 44
Editing resource restriction policies 46
Editing resource restriction policy assignments 47

Deleting a resource restriction policy from a user role assignment ... 47
Assign roles ... 48
Assigning roles to users in standalone or MSP tenant workspaces ... 48
Editing a user role assignment ... 49
Authentication ... 50
SAML SSO Elements for HPE GreenLake Account Home ... 50
SAML SSO workflows ... 51
Service provider-initiated SSO ... 51
Identity provider-initiated SSO ... 52
SSO authorization options ... 53
How to configure HPE GreenLake Account Home SAML SSO ... 54
Configuring SSO authentication with local authorization ... 55
Configuring SSO authentication with SSO authorization ... 55
Configuring SAML SSO on your identity provider ... 55
HPE GreenLake Account Home SAML attribute for SSO authorization ... 56
Configuring SAML SSO on HPE GreenLake Account Home ... 63
Reviewing and managing a SSO connection ... 67
Viewing SSO configuration details ... 67
Editing a SSO connection for a domain ... 68
Updating x.509 certificate details for a SSO connection ... 69
Considerations when changing the SSO authorization type ... 69
Deleting a SSO connection ... 70
Notifying users that SSO is enabled ... 71
Specifying SAML configuration details for Microsoft Entra ID ... 71
Configuring SSO attributes and claims ... 72
Downloading the SAML SSO XML token signing certificate ... 74
Verifying the SSO user has administrator privileges on HPE GreenLake Account Home ... 74
Verifying the SSO user has access to HPE GreenLake Account Home with observer privileges ... 75
Configuring SAML SSO using the Okta identity provider ... 75
SSO testing and troubleshooting ... 77
SSO FAQ ... 78
API access ... 79
Creating a personal API client ... 79
Generating an access token ... 80
Viewing code samples for generating an access token ... 81
Resetting your client secret ... 82
Deleting a personal API client ... 83
Tags ... 83
Viewing all tags in your workspace ... 84
Managing tags in your workspace ... 84

Welcome to HPE GreenLake Account Home

HPE GreenLake Account Home is a secure, cloud-based platform that allows you to view and control your hybrid cloud estate. The platform unifies and simplifies IT operations by providing an intuitive, self-service home page where you can run cloud services and provision and manage infrastructure.

Using HPE GreenLake Account Home, you can do the following:

- Administrators can:
  - Create and manage workspaces, and invite users to join a workspace.
  - Manage user access to services and resources by creating and setting up user roles and assigning permissions to them.
- Users can:
  - Explore, deploy, and manage services from the service catalog.
  - Configure, deploy, and manage the devices in their workspace.

This guide introduces you to HPE GreenLake Account Home and the services and features it enables you to access.

Home

The home page is what you see when you first log in to the HPE GreenLake Account Home, where you can access key features and services instantly.

Click the following links to explore some of the tasks you can perform from the home page as you begin using the platform:

Getting Started

The cards in the **Getting Started** section help you to initially set up your services and configure your workspace.

- Manage certificates
- Manage devices
- Manage users
- Manage roles

Quick Links

Use these links to quickly access different pages in HPE GreenLake Account Home and start configuring your workspace.

NOTE: Remember that on any screen in HPE GreenLake Account Home, what you see depends on the following:

- The services and tools that are available to your organization
- The permissions you have, based on your role

Personalizing your HPE user account

About this task

Select preferences for your HPE GreenLake user account and for individual workspaces on the **User Preferences** page.

You can set global or workspace preferences:

- **Global**

  General user account preferences apply across all your workspaces. You can set your preferred unit of measure, temperature, language, and set the session timeout.

- **Workspace**

  Workspace preferences apply to the current workspace only. At the workspace level, you can choose your preferred landing page and customize your **Home** page layout. If you have access to multiple workspaces for your HPE GreenLake user account, set your preferences for each workspace separately.

Procedure

1. On the HPE GreenLake Account Home header, click the **User** icon
2. Set your user account preferences in the **Global** section.

   a. Change the language of the HPE GreenLake Account Home UI pages by selecting your preferred language from the **Language** drop-down menu.

The UI pages and messages display in the new language immediately.

b. Change the session timeout value for your HPE user account by entering a new value in the **Session Timeout** field.

NOTE: HPE GreenLake Account Home allows you to set an idle session timeout. If you are inactive for longer than the timeout value set, you must log in again. If you use SSO, your administrator sets an idle session timeout value when they configure SAML SSO. HPE GreenLake Account Home updates your user preferences idle session timeout according to the SAML SSO configuration when you log in via SSO.

c. Change the **Unit of Measure** (UOM) for your account by selecting a value from the drop-down menu. The default value is **Feet**.

d. Change the **Temperature unit** for your account by selecting a value from the drop-down menu. The default value is **Fahrenheit**.

3. Set your workspace-specific preferences in the **Home** section.

NOTE: The preferences you select on the **Workspace** section apply only to the current workspace.

a. Set your preferred landing page.

The preferred landing page option allows you to set one of your provisioned services as your default landing page. If you set a service to be your default landing page, the service will launch immediately after you log into your workspace. You can select any service that you have permission to access and is provisioned for the workspace.

- To set the landing page, select the service in the **Preferred landing page** drop-down menu. The next time you log into your workspace, your chosen service will immediately launch.
- To return to the default **Home** page setting, select **GreenLake home page**.

b. Display or hide the **Getting Started** section on the **Home** page using the toggle button in the **Workspace** section. If you close the **Getting Started** section by selecting **Dismiss** on the **Home** page, you can restore it from here.

c. Enable or disable push notifications for what's new posts using the toggle button in the **Workspace** section. When enabled, what's new posts appear in a pop-up dialog box after you sign in and access a workspace.

d. Enable or disable the **Widgets** section on the **Home** page using the toggle button in the **Workspace** section. When enabled, a **Widgets** section is added to your **Home** page where you can select widgets from the widgets library in HPE GreenLake Account Home. For details, see .

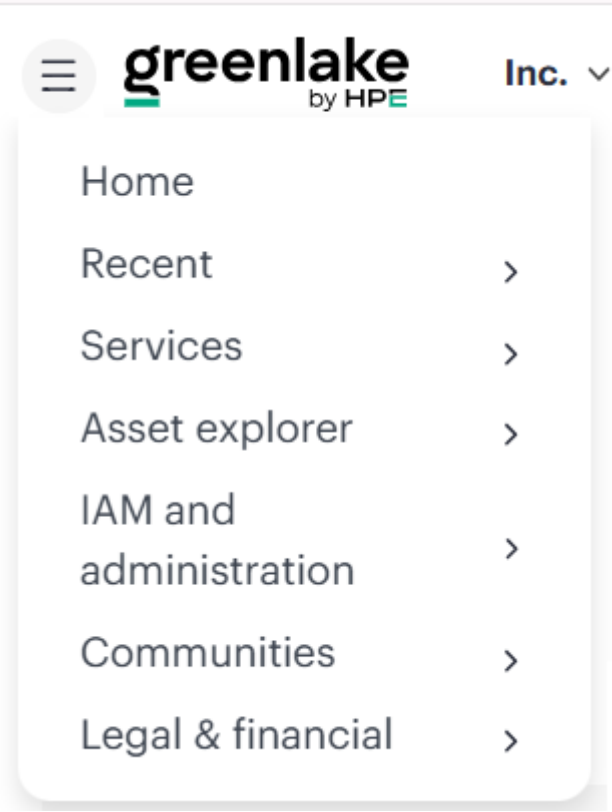
4. To save your preferences, click **Save Changes**.

HPE GreenLake Account Home cloud header

The global navigation header appears on every page and includes a global navigation menu, a workspace menu, and icons to access various resources.

Global navigation menu ☰

The global navigation menu, identified by a three-bar icon ☰ on the left of the HPE GreenLake logo, is your central location for services, workspace administration, identity and access management, assets, and recent activity.



Click the **Global navigation menu** ☰ to view and manage the following resources and information:

Menu option	Action
Home	Use to return to the HPE GreenLake Account Home **Home** page.
Recent	Use the **Recent** menu option to quickly view or open the last five services that you accessed.
Services	Use the **Services** menu option to: • View and launch your services. • Open the **Service catalog**.
Tenants	(For managed service provider (MSP) workspaces). Use the **Tenants** menu option to: • View and open a recent customer workspace (the last five workspaces that you accessed are shown in the menu). • Open the **Tenants workspaces** page.

Table Continued

Menu option	Action
Asset explorer	Use the **Asset explorer** menu option to open the following pages: • **Overview** • **Devices** • **Subscriptions** • **Settings**
IAM and administration	Use the **IAM and administration** menu option to manage workspace settings, configure identity and access management (IAM), and administration tasks such as the following: • Roles and permissions • User management • Organization management • IP access • Audit logs • Reporting • Personal API clients • Single sign-on • Audit logs • Personal API clients
Communities	Use the **Communities** menu option to go to the HPE Communities or HPE Developer Community websites.
Legal & financial	Use the **Legal & financial** menu option to view additional resources: • HPE privacy policy • HPE cookies policy • Terms of use • Do Not Sell My Personal Information • Financial services

Side navigation menu

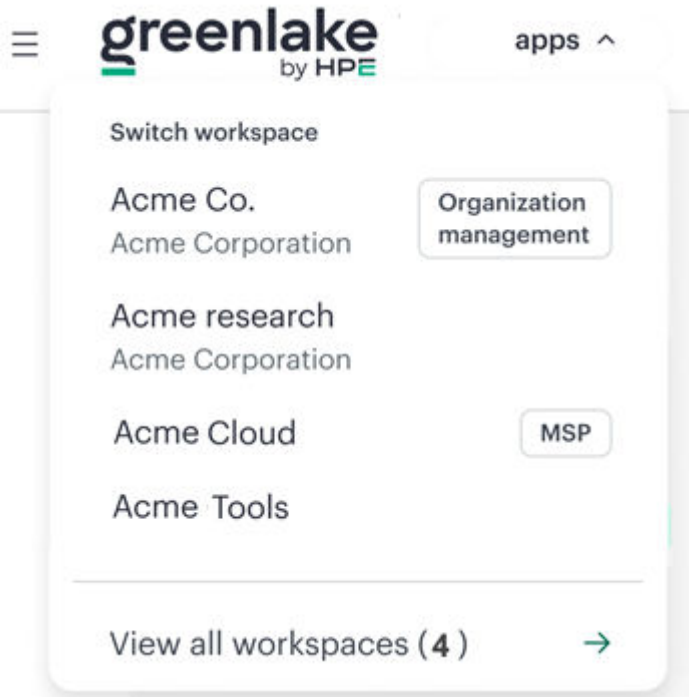
NOTE: The side navigation menu is available only in workspaces that have enhanced IAM.

Each page in HPE GreenLake Account Home has a side navigation menu which provides access to the related options for that topic.

To show or hide the side menu, click .

Workspace menu

The workspace menu appears on the right side of the GreenLake logo. Click the workspace name to access the drop-down menu, where you can switch to another workspace or open the **My workspaces** page.



Notifications

Click this icon to go to the **Notification center**, where you can view and manage your notifications. A red dot beside the bell icon indicates unread notifications.

Help & support

Click **Help & support** and select a service to view help and support options.

NOTE: The help and support options vary by service.

For HPE GreenLake Account Home, the help and support options are as follows:

Option	Description
Help	• **Videos and tutorials**—view videos about getting started with HPE GreenLake Account Home. • **Documentation**—visit the HPE GreenLake Account Home User Guide User Guide on Hewlett Packard Enterprise Support Center.
Support	• **Support Hub**—visit Support Hub—our unified support center. For more information about Support Hub, see . • **Manage support access**—when requested, use this link to give an HPE engineer access to your workspace. For more information about support access, see . • **View cases**—view your support cases in Hewlett Packard Enterprise Support Center.
Give feedback	Open the **Give feedback** form. Use the form to request a feature or send us feedback about the platform or services.
Create case	Open the **Create support case** panel to create a support case for HPE GreenLake Account Home support. **NOTE:** You can also create a support case on Support Hub. For more information, see .

Help for this page

The **Help for this page** icon opens and closes the help panel. The help panel displays targeted help for the current page, allowing you to get help without leaving the platform. Use the **Pin this topic** icon to keep any help topic open while you move to other pages in the platform.

User

Click the **User** icon to access your HPE user account details and HPE GreenLake user preferences.

- On the **HPE User account details** page, edit your personal information for your HPE GreenLake account or set up multifactor authentication (MFA).
- On the **HPE GreenLake preferences** page, select your preferred language and set the session timeout for your account. You can also choose preferences for your **Home** page.

Devices

The device inventory in asset explorer allows you to view all your devices including HPE devices and non-HPE devices. View, manage, and onboard devices to your workspace from the device inventory. Devices are categorized by factors such as type, source, and management (for managed service provider (MSP) workspaces).

You can view all your devices in a single table or grouped by source. To learn more about device sources, see .

Data Ops Manager users can also manage Data Ops Manager devices directly within the service. For more information, see the Data Ops Manager user guide.

Auto-subscribe

Configure auto-subscribe and auto-reassign for device subscriptions:

- Auto-subscribe for devices

  Devices that have auto-subscribe configured are automatically assigned subscriptions. An auto-subscribed device with a valid license is automatically enabled for use with HPE GreenLake Account Home. You can configure auto-subscribe for supported devices including switches, gateways, and access points.

- Auto-reassign for device subscriptions

  When a device subscription expires, auto-reassign assigns another subscription of the same type to prevent disruptions. Auto-reassign helps to ensure continuous coverage and avoid service disruptions.

  Auto-reassign is enabled by default for device subscriptions.

Tag-based rules for auto-subscribe and auto-reassign

HPE GreenLake Account Home provides APIs to apply tag-based rules to auto-subscribe and auto-re-assign feature. Tag-based rules allow administrators to reserve subscriptions for devices with specific tags by assigning tags to the subscription key. During auto-subscription and auto-re-assignment, devices are automatically assigned subscriptions from the available subscriptions. Using tags in this way can prevent unrelated subscriptions being assigned to devices during auto-subscription or auto-reassignment. For more information about setting up tag-based rules, see **HPE GreenLake for Subscription Management** on the HPE GreenLake Developer Portal.

Managing auto-subscribe for devices

About this task

An auto-subscribed device with a valid license is automatically enabled for use with HPE GreenLake Account Home.

When a subscription assigned to a device expires or is canceled, HPE GreenLake Account Home checks the subscription keys in your workspace and assigns the subscription key that expires first to the device.

If your workspace does not have an adequate number of subscriptions, you might have to manually assign subscriptions to as many devices as possible.

NOTE: To view the subscription utilization details and the number of subscriptions available in your workspace, on the **Devices** page click the **Managed** tab, then select **Assigned & subscribed** in the drop-down menu.

Tag-based rules for auto-subscribe

HPE GreenLake Account Home provides APIs to apply tag-based rules to auto-subscribe and auto-re-assign feature. Tag-based rules allow administrators to reserve subscriptions for devices with specific tags by assigning tags to the subscription key. During auto-subscription and auto-re-assignment, devices are automatically assigned subscriptions from the available subscriptions. Using tags in this way can prevent unrelated subscriptions being assigned to devices during

auto-subscription or auto-reassignment. For more information about setting up tag-based rules, see **HPE GreenLake for Subscription Management** on the HPE GreenLake Developer Portal.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Settings**.

   The **Settings** page opens. In the **Auto-subscribe** section, you can configure auto-subscribe for eligible device types.
3. In the **Auto-subscribe** section, click **Add**.
4. On the **Auto-subscribe** panel, use the drop-down lists to select the device type and the corresponding subscription tier.

   View the available subscription seats indicated to ensure that you have enough subscription seats to cover your devices. Updating the subscription tier could affect your auto-subscribe configuration.
5. Click **Configure device**.
   Devices of the selected type are automatically assigned subscriptions.

Inventory

The Inventory section on the **Devices** page summarizes your device information and provides a set of actions to manage all your devices and their subscriptions.

Example scenario: adding device subscriptions

A typical scenario for adding a device and subscription to your workspace in order to use a service may include the following sequence of actions.

1. Onboard a device to your workspace. See **Adding managed devices**.
2. Associate it with a service instance. See .
3. Add a device subscription key to your workspace. See **Adding device subscriptions to your workspace**.
4. Assign a device subscription to the device that you onboarded. See **Applying subscriptions to devices**.
5. Go to the **Services** page, launch the service that you need, and begin using the service.

Adding managed devices

Prerequisites

Identify a service delivery contact and create a location for the device if you want to use Service Delivery Information (SDI) to automate support and services for added device. For information about locations, see .

Applies to: Managed devices

About this task

Managed devices are HPE devices you own and manage in HPE GreenLake Account Home. You can add a managed device to your workspace by selecting the device type and providing device details including the serial number and other identifying information. You can enter device details directly on the UI or, for networking and compute devices only, by uploading a CSV file you create using a sample file provided.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Devices**.
3. Select the **Managed devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. Click **Add devices**.
5. Follow the directions on the **Add devices** wizard to complete the device setup. See the field descriptions table for help on each step of the wizard.
6. Click **Finish** to add the device.

Field	Description
Step 1: Specify device details	
Choose a device category	Select the type of device that you are adding, either **Compute**, **Storage**, or **Networking**. In the next steps, you add details about the device. The details and number of steps vary for each type of device and entry method. **NOTE:** You can find the serial number of devices on the front or back of the hardware.

Table Continued

Field	Description
Choose a method to specify details (for compute and networking devices)	For compute devices, click **View prerequisites for adding compute devices** to see if you meet the requirements. Choose one of the following methods: • **CSV file** Upload the device serial number and product ID from a CSV file as follows: **a.** Click **Download sample file** then edit the file to add the serial number and product ID of each device you want to add. You can also specify tags for the device. If you want to automate SDI services, add a location and a service delivery contact for each device. **b.** Save the file. **c.** Drag and drop the file into the box or click **Select file** to upload the file. **d.** Click **Finish**. After the device is validated, it is added to the inventory. • **Serial number & product ID** (for compute devices) Enter the serial number and product ID from the order confirmation email. • **Serial number & MAC address** (for networking devices) Enter the serial number from the order confirmation email and the MAC address of the device. **NOTE:** For Edge Connect-SD WAN Gateways, enter the same number for both serial number and MAC address fields. The MAC address is the same number entered in the MAC address format.
Select the ownership type (storage devices)	**a.** Select one of the following options: • **Infrastructure as a service**. • **Purchase or lease**. **b.** Enter the serial number and the product number that you received in the confirmation email. **c.** Click **Add** to review the information you entered. **d.** Click **Next**. **NOTE:** • You can enter the subscription key to subscribe to one or more storage devices from the **Device subscriptions** tab on the **Subscriptions** page. See **Applying subscriptions to devices**. After you add a storage device subscription, you must assign it to the device. • See table to know the number reference for your product.

Table Continued

Field	Description
Step 2: Add additional details (optional)	
Tags	Optionally assign tags to the devices that you added in the previous step. Select the name of an existing tag or create a tag to assign to the device. Add tags as follows **a.** Select a name and value. **b.** Click **Assign** to assign the tag to the device. **c.** Repeat to add more tags.
Device support contact To use Service Delivery Information (SDI) to automate support and services for the device, add a contact and location.	Assign a user from the workspace as the support contact for the device or, enter an email address of someone outside of HPE GreenLake Account Home **NOTE:** If you enter an email address of someone outside the platform, a warning is displayed. You can continue if you trust the email address. If not specified, the primary contact of the location that the device is assigned as the default service delivery contact for that device.
Location	Select an existing location from the list. **NOTE:** You can assign the location of a new device that you are on-boarding to the location of the existing devices in the same workspace. See for the steps to assign locations to devices.
Click **Next**.	
Step 3: Review add devices	
• Verify the settings for your devices. If you want to change any of the values, return to the relevant step in the wizard and update the values as required. • Click **Finish** to add the device.	

Searching and filtering the device inventory

About this task

The devices table includes a filter, and a search box, making it easier to find specific devices.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Devices** .
3. Select a vertical tab to view all devices, managed devices, or discovered devices.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. In the **Managed devices** tab, you can filter devices by assignment status using the drop-down box above the table.
5. In any tab, filter the inventory as follows:
   a. Click **Filters** .
   b. Select one or more criteria in the filter panel and click **Apply filters**.

   NOTE: The available filter options depend on the selected tab.
6. In any tab, search for a specific device as follows:
   a. Enter a full or partial serial number, model number, or MAC address in the **Search** box.

      If the device is a compute device, you can use the **Search** box to search by name and secondary name.
   b. Press **Enter**.

Managing tags for devices

Prerequisites

Applies to: Managed and discovered devices.

About this task

Create, assign, or remove tags for managed and discovered devices in your inventory. For information about tags and tag specifications, see **Tags**.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **Asset explorer** > **Devices**.
3. Select the **All devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.
4. Use the search and filter to find the devices you want to edit.

   To learn more about searching and filtering in the device table, see **Searching and filtering the device inventory**.
5. Select the checkboxes for the devices that you want to edit.
6. Click **Actions** > **Manage tags**.

   The **Managing tags** dialog box appears.

   If you selected:

   - One device: all tags assigned to the device are displayed.
   - Multiple devices: tags that are common to all the selected devices are displayed.

   NOTE: Changes you make to tags in the **Managing tags** dialog box apply to all the selected devices.

7. To assign a tag:

   a. Select the name of an existing tag or create a tag.

   b. (Optional) Select the name of an existing value or create a value.

   c. Click **Assign**.

   d. Repeat to add more tags.

      You can assign up to 50 tags.

8. To remove a tag, click the **x** icon for the tag.

   NOTE: If the tag is not assigned to any other resources, it is deleted from the workspace.

9. To apply the changes, click **Save changes**.

- The **Tags** column of each device is updated.
- You can view all tags for the workspace on the **Tags** page. For more information, see **Viewing all tags in your workspace**.

Adding tags to devices using a CSV file

Prerequisites
Applies to: Managed devices (compute and networking devices)

About this task
You can manually assign tags to devices once you have added the devices to your workspace. Alternatively, you can assign tags to networking and compute devices using a CSV file when you add these devices to your workspace.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Devices**.
3. Select the **Managed devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. Click **Add devices** to add devices to your inventory.

   The **Add devices** wizard opens.

5. In **Choose device category**, select the **Compute** or **Networking** device category.
6. Select the method **CSV file**.
7. Click **Download sample file** and review the device information required.

   The details required vary according to the device type.

8. Edit the sample file to add details for each of the devices you want to add. You can also specify tags for each device.

NOTE: If you specify a tag name for a device in the CSV file but leave the tag value cell empty, the corresponding device is not assigned the tag. If you want to assign the tag without a value, use **<blank>** as the tag value. See the example CSV format below showing how to add empty tags and valueless tags.

Serial Number	Part Number	tag:location	tag:company	tag:app	tag:env
1CU8422KH5	part1	san jose	hpe		<blank>
2CU8422KH5	part156	houston	hpe	oracle	
KU78422TS8	partAF34	houston	hpe	sfdc	dev

The above CSV file generates these device-tags:

- For **serialNum:** 1CU8422KH5, **partNum:** part1

  Tags generated are: location:san jose, company:hpe, env
- For **serialNum:** 2CU8422KH5, **partNum:** part156

  Tags generated are: location:houston, company:hpe, app:oracle
- For **serialNum:** KU78422TS8, **partNum:** partAF34

  Tags generated are: location:houston, company:hpe, app:sfdc, env:dev

9. Save the CSV file.
10. On the **Add devices** wizard, click **Select file** to select the CSV file you prepared for the device upload.
11. Click **Finish** to add the devices to the inventory.
12. On the **Adding devices to your inventory** dialog, click **View audit log** to verify that the devices are added successfully. When you navigate back to the devices table, you see your new devices and the tags you assigned to them.

Applying subscriptions to devices

About this task

You must assign a subscription to a device before you can activate and use the device.

Each device expires individually. If you have multiple devices and the expiration date varies, the devices are unsubscribed from HPE GreenLake Account Home according to the device expiration dates. Users receive an expiry notification at the subscription expiration date.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Devices**.
3. Select the **Managed devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.
4. In the drop-down list, select **Requires subscription** to display all devices requiring subscriptions.
5. Select the device or devices to which you want to apply a subscription.

6. Click **Actions** > **Apply subscription**.
7. On the **Apply subscription** page, select the subscription tier.
   A list of base subscriptions for the chosen tier is displayed.
8. (Optional) To choose which columns to view in the subscription key list, click the **Column selector** icon .
9. (Optional) To filter the list of subscription keys by tag, select one or more tags in the **Tags** drop-down list.
10. Select the subscription key to assign it to the device.

    NOTE: Go to **this link** to view the map for device type to the corresponding subscription tier for network devices (AP, IAP, switch, or gateway devices).

11. Click **Apply subscription**.

    NOTE: The **Apply subscription to your device** dialog informs you if the device is eligible for add-on subscriptions.

    The **Applying subscription to your device** dialog appears. The transaction is recorded in the audit log and you can view the audit logs from the confirmation dialog.
12. Click **X** to exit the confirmation dialog.
    The **Devices** page opens and you can view the updated device details in the inventory list.

    NOTE: UXI -LTE services have prebuilt subscriptions with a validity of 90 days.

Removing subscriptions from devices

Prerequisites

- Ensure that the Auto-Subscribe option is turned off before removing device subscriptions to prevent them from being licensed again automatically. For more information about the Auto-Subscribe option, see **Auto-subscribe**.
- You have a workspace administrator role or a role with permissions to change subscriptions.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **Asset explorer** > **Devices**.
3. Select the **Managed devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.
4. In the drop-down list, select **Assigned & subscribed**.
5. Select the check boxes for one or more devices that you want to change.
6. Click **Actions** > **Detach subscription**.
   The **Detach base subscription** dialog appears, warning you of the effects of the detachment.
7. On the **Detach base subscription** dialog, click **Yes, detach subscription**.
   A dialog appears to notify the process of detaching.

8. Click **View audit log** on the **Detach subscription** dialog to view the status in the audit log, or click **Close** to close the dialog.
9. (Optional) To verify the subscriptions have been removed, select the **Managed** tab, and select **Requires subscription** in the drop-down list to see a list of devices that have no subscription.

Adding device subscriptions to your workspace

Prerequisites

You have a workspace administrator role or a role with permissions to modify subscriptions.

About this task

You must add a device subscription key to your workspace independently of adding a specific device.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Subscriptions**.
3. Select the **Device subscriptions** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. Click **Add subscription**.
5. Follow the steps in the wizard to add the device subscription. See the field descriptions table for help on each step of the wizard.

Field	Description
Step 1 **Add subscription**	
Subscription key	Enter the subscription key that was emailed to you.
Step 2 **Assign tags (Optional)**	
Assign tags	**a.** Select an existing name from the list or type in the box to create a tag. **b.** (Optional) Select an existing value from the list or type in the box to create a value for the tag. **c.** Click **Assign** to assign the tag to the device subscription. **d.** Repeat to add more tags. You can add up to 50 tags. For more information about tag specifications, see **Tags**.

Table Continued

Field	Description
Step 3 **Manage showback rates (Optional)**	
NOTE: • Showback rates entry is optional and applies only to services where usage monitoring is available. • When this option is available, you can choose to skip this step: clear the **Add showback rates** check box and click **Next** to review and finalize your entry. To enter showback rates later, see . • For more information about showback rates, see and *Working with showback reporting* in **Consumption Analytics User Guide for HPE GreenLake Account Home**. • Adding showback rates and effective dates will update a large number of records, which can take 30 minutes or more.	
Enter rates	**a.** Enter an **Effective date** for the first meter shown. You can enter the current date or paste a date. Cost is calculated at the rate that you enter from the effective date forward. **b.** Enter the **rate** for the first volume tier (rate band). **c.** Repeat for the second rate band if there is one. **d.** Repeat these steps for any additional meter. **e.** Click **Next** to review and add your device subscription.
Step 4 **Confirmation**	
Verify entries	**a.** Verify the settings for your device subscription. **b.** If you want to change any of the values, return to the relevant step in the wizard and update the values as needed. **c.** Click **Finish** to add the device subscription.

6. You can continue adding subscription keys as needed.
   The subscriptions are now available to assign to devices in your workspace. See **Applying subscriptions to devices**.

Removing device subscriptions from your workspace

Prerequisites

You are a workspace administrator or have a user role with permissions to modify subscriptions.

About this task

Device subscriptions can be removed from workspaces, allowing you to organize your subscriptions between your workspaces. After a device subscription has been removed from a workspace, you can then add it to another workspace.

NOTE: Removing a device subscription from a workspace automatically removes any linked devices from the subscription.

Example scenario: moving device subscriptions between workspaces.

While adding a device subscription to **Workspace A**, a message tells you that the device subscription is already added to **Workspace B**.

Your actions depend on your user role and workspace access:

- If you have a workspace administrator role (or a role with permission to modify subscriptions) for **Workspace B**:
  - Log into **Workspace B** and remove the device subscription.
  - Log into **Workspace A** and add the device subscription.
- If you have access to **Workspace B** but you do not have a workspace administrator role (or a role with permission to modify subscriptions), you can:
  - Ask the workspace administrator of **Workspace B** to remove the device subscription from the workspace.
  - Log into **Workspace A** and add the device subscription.

NOTE: If you do not have access to **Workspace B**, the onscreen messages do not display the name of the workspace. In this case, you will be directed to get assistance from HPE Support.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Subscriptions**.
3. Select the **Device subscriptions** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.
4. (Optional) To check if any devices are assigned to a subscription, click the subscription key to open the details page.

   Any devices assigned to the subscription are displayed in the **Subscribed devices** section.
5. In the device subscriptions table, select the check boxes for one or more subscriptions.
6. Click **Actions** > **Remove subscriptions**.
7. On the **Remove subscriptions?** confirmation box, confirm that you want to remove the subscriptions.
   - The subscription is removed from your workspace and can be added to another workspace if needed.
   - Any assigned devices are unassigned from the subscription.
   - Any tags that were added to the subscription are removed.
   - The removal of the subscription is recorded in the Audit Log.
8. (Optional) To verify that the subscription has been removed, enter the subscription key in the search box.
   If the subscription has been removed, the search results will be empty.
9. If you want to add the subscription to another workspace, log in to the workspace and add the subscription.

   For more information about adding device subscriptions to workspaces, see **Adding device subscriptions to your workspace**.

Managing tags for subscriptions

About this task

Create, assign, or remove tags for one or more subscriptions. For information about tags and tag specifications, see **Tags**.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Subscriptions**.
3. Select the **Device subscriptions** or **Service subscriptions** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. In the subscriptions table, select the checkboxes for one or more subscriptions that you want to add tags to.
5. Click **Actions** > **Manage tags**.

   The **Manage tags** dialog box appears.

   Any tags already assigned to the subscription are shown in the dialog box. The tags displayed depend on the selected subscriptions:

   - One subscription: all tags assigned to the subscription are displayed.
   - Multiple subscriptions: tags that are common to all the selected subscriptions are displayed.

   NOTE: Changes you make to tags in the **Manage tags** dialog box apply to all the selected subscriptions.

6. To assign a tag:

   a. Select the name of an existing tag or create a name.

   b. (Optional) Select the name of an existing value or create a value.

   c. Click **Assign**.

   d. Repeat to add more tags.

      You can assign up to 50 tags.

7. To remove a tag, click the **x** icon for the tag.

   NOTE: If the tag is not assigned to any other resources, it is deleted from the workspace.

8. To apply the changes, click **Save**.

- The **Tags** column of each subscription is updated.
- You can view all tags for the workspace on the **Tags** page. For more information, see **Viewing all tags in your workspace**.

Managing auto-reassign for device subscriptions

Prerequisites

- You must already have a device subscription.
- You must have administrator permissions in HPE GreenLake Account Home.

About this task

You can enable or disable the auto-reassign feature for your device subscriptions per device type. When a subscription expires, auto-reassign applies the device to another subscription of the same type to prevent disruptions. This is enabled by default.

HPE GreenLake Account Home provides APIs to apply tag-based rules to auto-subscribe and auto-re-assign feature. Tag-based rules allow administrators to reserve subscriptions for devices with specific tags by assigning tags to the subscription key. During auto-subscription and auto-re-assignment, devices are automatically assigned subscriptions from the available subscriptions. Using tags in this way can prevent unrelated subscriptions being assigned to devices during auto-subscription or auto-reassignment. For more information about setting up tag-based rules, see **HPE GreenLake for Subscription Management** on the HPE GreenLake Developer Portal.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Settings**.
   The **Settings** page opens.
3. In the **Auto-reassign** section, click the **Configure** button and use the toggles to enable or disable auto-reassignment for each device type.

Device subscription expiration dates

Device subscriptions expire individually. If you have multiple devices and the expiration date varies, the devices are unsubscribed from HPE GreenLake Account Home according to the device expiration dates.

Transferring a single device or multiple devices between workspaces

Prerequisites

- You must have access to both the workspaces you want to work with.
- You must have permissions to add a managed device in the workspace you want to transfer the device to.
- Applies to: Managed devices.

About this task

You can transfer a single managed device or bulk transfer devices from the **Devices** page. You must assign a service and apply subscriptions to the device in the new workspace for it to work.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Devices**.
3. Select the **Managed devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. Use the **Actions** menu to **Remove assignment** and **Detach subscription** for the device or devices that you want to transfer.
5. Select the devices that you want to transfer and then click the **Actions** menu.

NOTE: For a single device, you can use the Serial Number and MAC Address of the Device in step 2 of the **Add devices** wizard in the workspace you are transferring the device to.

6. Click **Export** .
7. In **Recipient**, enter the email address you want to export the device data to.
8. Click **Create report**. The report is sent to the recipient email.
   a. Download the CSV file from your email.
   b. Go to the **Managed devices** page on the workspace where you want to add this device.
   c. Click **Add devices**.
   d. Follow the wizard and upload the downloaded CSV file to add the device or devices.
9. On the original workspace, select the device or devices that you transferred.
10. Select **Remove assignment** from the **Actions** menu to delete the device or devices from the workspace.

NOTE:

- Do not archive the device or devices that you want to transfer.
- The HPE StoreOnce system used with an HPE Alletra Storage MP B10000 system can only be onboarded to one workspace at a time.

  Contact HPE Support for assistance if you want to:
  - Change the workspace of an HPE Alletra Storage MP B10000 system with backups on HPE StoreOnce systems.
  - Move HPE StoreOnce system to a different workspace.

Viewing subscription expiry dates

About this task

Notification emails are sent to the workspace administrator 90, 60, 30, and 1 days before subscription expiry. You can visually track the expiry from the widgets on the **Home** page.

NOTE: If you have already renewed your subscription and have received a new subscription key, you will continue receiving the expiry notifications for the subscription that is due to expire.

When a device subscription expires, and no other valid or compatible subscription exists, all devices licensed with that subscription key are unlicensed. If a second valid and unexpired subscription is available, it is automatically assigned when the subscription expires. If you have multiple subscriptions with varying end dates, different devices might have different subscription expiry dates.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **Asset explorer** > **Subscriptions**.
3. Select the **Service subscriptions** or **Device subscriptions** vertical tab.

NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. To view subscription expiry dates, check the **Expiration date** column.

Viewing devices

About this task

Use the device inventory to manage all devices in your workspace. You can use it to:

- Search for a specific device.
- Manage tags for devices.
- Check the subscription status of managed devices.
- View configuration details of any storage devices that are composed of multiple modules in one or more chassis.
- Check the device location.
- Onboard managed devices and set up integrations for discovered devices.

Each device has a **Details** page that shows all information about the device in a single view.

You can configure each table to show or hide columns, change the column order, and sort the columns.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **Asset explorer** > **Devices**.
   The **Devices** page opens on the **All devices** tab.
3. Select tab:

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

   - **All devices**: All devices in the workspace. This includes Flex devices, managed devices, and discovered devices.
   - **Managed devices**: HPE devices you own and you manage in HPE GreenLake Account Home.
   - **Discovered devices**: Discovered devices are all other devices in your infrastructure that are not managed devices. They can be third-party devices or HPE devices.

   NOTE: Some actions are available only for certain device types or selections.

4. To view detailed information about a device, click the serial number in the **Device** column to open the **Details** page.

   The **Details** page shows the complete information about a device such as the location, service instance, part number, support, and other information.

   For block storage devices with multiple modules, you can view the configuration in the **Chassis** section, and you can expand each chassis to view the module information.

   For more information about each field in the device inventory, see .

5. To configure the table layout, click **Column selector** .

   For more information, see .

6. To refine the table view, use the filter and search box.
   For more information, see **Searching and filtering the device inventory**.

7. To export the inventory to a CSV file or PDF, click **Export** .
   For more information on exporting the inventory, see .

8. To see the device locations on a map, click **Map view** .
   For more information about the device map view, see .

Archiving devices

Prerequisites

- You have a **Workspace Administrator** role or a similar role with permission to manage devices.
- Applies to: Managed devices

About this task

You can archive managed devices. When you archive a device it is no longer connected to a service.

When you archive a device:

- It is not visible in the default view of the **Device** table.

  The filter option **Show archived devices only** allows you to see all archived devices in the **Devices** table.
- It is not included in the totals shown in the drop-down list the top of the **Devices** table.
- It cannot be assigned subscriptions or added to services.

You can remove a device from the archive (unarchive) a device if you want to assign it to a service again. For more information, see .

To delete a device from your workspace, use the remove devices option. For more information, see .

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **Asset explorer** > **Devices**.
3. Select the **Managed devices** vertical tab.

   NOTE: If your workspace does not use enhanced IAM, the tabs might appear in a different location on the page (for example, as horizontal tabs). The functionality is the same.

4. Use the search and filter to find the devices you want to archive.

   To learn more about searching and filtering the device table, see **Searching and filtering the device inventory**.

5. Click the check boxes to select the devices you want to archive.

6. Click **Actions** > **Archive**.
7. Click **Archive devices** to confirm your action.

   The devices are archived. The are no longer visible in the default view of the devices table and cannot be assigned to a service.

Viewing all archived devices in your inventory.

8. To see all your archived devices, click **Filters** and select **Show archived devices**.
9. (Optional) View details of the change in the Audit Log.

   For more information about viewing audit logs, see **Viewing audit logs**.
10. If you need the device again, you can remove it from the archive.

    For more information, see .

Claiming subscription from the subscription notification email message

Prerequisites

- An account in HPE GreenLake Account Home
- Purchased subscriptions licenses to be used in HPE GreenLake Account Home.

About this task

You can now click the easy onboarding link from the details section of the subscription notification email message, to claim subscription licenses under one order into your account. You can start using the subscriptions as soon as you claim them.

You can find the easy onboarding link with a unique identifier in your email after you purchase the subscription license.

Procedure

1. Click **Access Instructions** on the email.
   The subscription contract receipt is displayed.
2. On the subscription contract receipt, click **Manage Your Subscription**.
   The HPE GreenLake Account Home logon page is displayed.
3. Click the workspace where you want to onboard your licenses.
   The **Add Subscription** wizard is displayed.
4. Select one or all the licenses that you have imported, and then click **Next**.
   The licenses are added successfully.
5. On the **Review and finish** page of the wizard, review your licenses and then click **Finish**.
   A request is sent for the product to be added to your workspace and to your inventory.
6. Click **Go to dashboard** to go back to the landing page.

   NOTE:

   - You can now view these licenses in the **Service Subscriptions** page.
   - If the subscriptions are not added, you can go back to step **2**.

Audit logs

The audit log is a chronological record of user and system activity in HPE GreenLake Account Home and any provisioned services. You can filter, search, configure, and export the log entries to determine the who, what, when, and where of activity in the platform. Activities are grouped in the audit log by service type and each log entry is categorized, making it easier to search for a certain type of action.

The following information is logged for all activities.

- Category—Type of activity that was logged.
- Description—Short description of the activity, such as subscription assignment, firmware upgrade, or configuration updates.
- IP Address—IP address of the client device.
- Target—Group or device to which the changes were applied.
- Time—Date and time of the activity.
- Username—User that performed the activity.
- Source—Tenant name (for Managed Service Provider accounts).
- Workspace—Name of the workspace in which the activity took place.
- Workspace type.

Additional information is logged for some services.

NOTE: By default, the audit log table displays a subset of this information. You can configure the table to see different information, or if you need to see all information in a single view, you can export the audit log to a CSV file.

Audit log access

By default, all built-in user roles have access to the audit log and can view their own user logs. Workspace administrators can view all logs for the workspace. This includes entries for other users and system-generated entries. Workspace administrators can also control access to the audit log by creating custom roles and removing the audit log permissions. See **Creating user roles** for more information about creating and configuring custom roles.

Retention period

Audit logs are retained for one year. The audit log table displays logs for the previous three months. If you want to view logs for the preceding 4–12 months, you can download the logs.

Return merchandise authorization details for HPE Aruba Networking devices

Details of HPE Aruba Networking devices that have been deleted from your workspace as part of the return merchandise authorization (RMA) process are logged in the audit logs. Thirty days after your RMA support case is closed, the device is deleted from your workspace, and the details of the deleted device are recorded in the audit logs. The device deletion is categorized as **Device Management** and the description includes the serial number, part number, and support case details. You can use the search to find the device by any of the details in the description.

Viewing audit logs

Prerequisites

You have the appropriate role assigned to your user. For more information about user role permissions for the audit log, see .

About this task

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Audit log**.
   The **Audit log** page opens, displaying logs for the last three months to a maximum of 10,000 records.
3. To choose which services you want to view audit logs for, click the **Service** drop-down list and select one or more services.

   You can select up to five services.
4. To view complete details about a log entry, select a row.

Searching and filtering audit logs

About this task

The **Audit log** page includes a filter and search, making it easier to find specific entries.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Audit log**.
   The **Audit log** page opens, displaying logs for the last three months to a maximum of 10,000 records.
3. To choose which services you want to view audit logs for, click the **Service** drop-down list and select one or more services.

   You can select up to five services.

To search for keywords:

4. Enter one or more words in search box.
   The search results show all log entries that contain the keywords. All columns (except the **Time** column) are searched, including columns not displayed in the table.

To filter the entries:

5. Click the **Filter** ▽ to open the filter panel.
6. Select one or more categories and click **Apply filters**.

   The filter categories that you can see depend on the selected services.

Configuring columns in the audit log

About this task

Customize your view of the audit log by selecting which columns to display in the table and the order of the columns. The available columns depend on the selected service.

NOTE: Your customized layout applies only to your view of the audit log and is reset to default when you log out of the platform.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **IAM and administration** > **Audit log**.
   The **Audit log** page opens, displaying logs for the last three months to a maximum of 10,000 records.
3. Select a service in the **Service** drop-down list.
4. Click **Manage columns** to select and sort columns:
   - In **Select columns**, select or clear checkboxes to choose columns for the table.

     As you select and clear checkboxes, you can see the new layout on the table. Some columns are selected by default and cannot be cleared.
   - In **Order columns**, click the up or down arrows to rearrange the columns in the table.

     As you click the up and down arrows, you can see the new layout on the table

NOTE: The configuration applies only to the selected service. The layout is reset to default when you log out of the platform.

Exporting audit logs

Prerequisites

You must hold specific roles associated with reporting permission for a given workspace to be able to view and download reports for that workspace. These roles include:

- Workspace Administrator
- Administrator
- Workspace Administrator and Activate Administrator
- Activate Administrator
- Operator
- Any custom role created with the Download permission edit permission of the reporting service.

About this task

You can export all or a filtered set of entries to a CSV or PDF file for your chosen service. The CSV option allows you to export all columns, while the PDF option allows you to include a maximum of six columns.

Procedure

1. On the HPE GreenLake Account Home header, click the workspace menu and then select **Manage Workspace**.
2. Click **Audit Log**.
   The **Audit Log** page opens, displaying logs for the last three months.
3. Select the service in the **Service** drop-down list.
4. Use the filters to further refine the list of entries.
5. Click **Actions** > **Export Log**.

6. In the **Export Log** pane, enter the following details:
   - The **Report name**.
   - Enter the **Recipient email** address to receive the file.
   - Optionally enter a **Description**.
   - Select the **File type**.
   - In the **Included Entries** section, you can choose to include the entire audit log or just the current search results.
   - In the **Table columns** list, select the check boxes for the data you want to include in the report.
7. Click **Export report**.
   - A notification message appears at the top of the screen with the status of your report. When your report is ready, a report banner notification appears with a link to download or share the report. Click **X** to close these messages.
   - The report is sent to the email address provided in the previous step. Click the **Download Report** link in the email to download the report.

     NOTE: If you are not logged in to HPE GreenLake Account Home, the download link opens the HPE GreenLake Account Home login page. After you log in, the report automatically downloads to your computer.
   - The download link is valid for seven days.
   - The notification message is also available in the **Notifications Center** page where it is visible to the author and the recipient email user.
   - The report status is also available on the **Audit Log** page.

Identity & access management

Identity and access management in HPE GreenLake Account Home allows you to manage users and their access to services and resources in a workspace. You can define how users manage and access HPE GreenLake Account Home resources, invite users, assign roles, manage permissions, and view access history for users in your workspace.

Users logged in to HPE GreenLake Account Home have single sign-on access to other service portals for which they have an account and have access.

NOTE: HPE GreenLake Central identities (users, user groups, and API clients), roles, and access to resources are managed from within HPE GreenLake Central. For more information, see **Users and their access to resources**.

Users

On the **Users** page, you can view users and their activity status and roles. You can also invite users to your workspace or delete them.

Viewing user details

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.

The **Users** page shows a list of users and their information. The list view details include:

Field	Description
Name	Name of the user
Email	Email address of the user
Status	Status of the user: verified or unverified
Platform role	The role assigned to the user on the platform
Last login	The last time or date the user signed in to the workspace

3.

4. You can select multiple users and then click the **Actions** button to perform bulk actions such as deleting or resending email invitations.

5. Select a user to view their details. The details vary according to the user type, such as MSP user or a user in MSP tenant or standalone workspace. The page consists of a **Details** section and a **Roles** section.

Field	Description
Details	
Email	Email address of the user
Joined Date	Date on which the user joined the workspace
Last Session	Last session of the user
Roles	
Application	Lists all the applications where this user has an assigned role
Role	Lists the roles assigned to the user for the application in the same row
Role	Lists the level of access this user has to application resources for the given role (and any restrictions that might apply) and application. This column is available in the MSP tenant or standalone workspace view.
Resource Access	Lists the resource access level for the role assigned to this user. This column is available for MSP users in the MSP workspace view.

Inviting users

About this task

Account administrators can easily invite team members to join HPE GreenLake Account Home by sending them a sign-up link in an email.

NOTE: In an MSP environment, user access and privileges are based on the workspace from which the invite is issued. Users invited from a tenant workspace are tenant users and users invited from the MSP workspace are MSP users.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.

   All the existing members of the workspace are listed on the **Users** page.
3. On the **Users** page, click **Invite users**.
   The **Invite user** window opens.

Field	Description
Email address	Enter the email address of the user
HPE GreenLake role	From the drop-down list, select the role you want to assign to the user. Roles fall within the broad categories of Administrator, Observer, or Operator and vary depending on the service you select.
Contact email address (Optional)	Optionally, enter a contact email address. This is visible on the email invitation.

4. Click **Send invite**.
   An email notification is sent to the user address specified. When the user clicks the **Accept Invite** link in the notification email, they can access the HPE GreenLake Account Home and start creating an account.

   NOTE: If the user does not accept the invitation within 10 days, the **Accept Invite** link expires and the user is removed from the workspace.

Deleting a user

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.

   All the existing members of the workspace are listed on the **Users** page.
3. Select the check box next to the name of a user and click the ellipses (...) and then select **Delete**.
4. Confirm the user deletion in the **Delete user** action dialog.

Viewing audit logs for users

About this task

Audit logs are generated when a new user is created or an existing user is modified or deleted from the HPE GreenLake Account Home workspace. It also records the login and logout activities of users.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **IAM and administration** > **Audit log**.
3. To filter audit logs about user activity, use the filter, search, or both.
4. To view hidden columns or to rearrange columns, click **Manage columns** .
5. To sort audit logs by user name, click the **Username** column heading.

Roles & permissions

In the **Roles & permissions** page, you can view options for viewing, creating, and managing roles in your workspace.

A role is a group of permissions that you can specify and assign to users in your HPE GreenLake Account Home workspace. There are 3 basic role types distinguished by the privileges defined in the authorization service:

- Administrator—has view, edit, and delete privileges in the workspace.
- Operator—has view and edit privileges in the workspace.
- Observer—has only view privileges in the workspace.

Additionally, there are two major categories of roles across the platform: built-in and custom roles. As the names suggest, built-in roles are predefined roles with permissions already enabled for the platform or applications to which they apply and cannot be edited or deleted. Custom roles are roles that you create and for which you define privileges; you can duplicate or edit these roles based upon your needs.

On the **Roles & permissions** page, you can see a list of all the defined roles in your workspace along with their description, the number of assigned users, and the applications in which they are used. On this page, you can:

- View a list of all the defined roles in your workspace along with their description, the number of assigned users, and the applications in which they are used
- Use specific keywords or other text to search within the list of roles on the page
- Use the page numbers at the bottom of the list to tab through and locate a specific role
- Click a role name or select the ellipsis (**...**) to view a slide-out panel with more details; and for custom roles, to take further actions such as duplicating or deleting the role
- Create new roles using the **Create role** link

Roles

There are multiple permissions that are specific to certain roles. Permissions in the built-in roles cannot be modified or duplicated. You can create roles and assign specific permissions to that role. Here is a list of built-in roles that are available in HPE GreenLake Account Home along with their permissions.

NOTE: It takes a few minutes to update role permissions. If you receive an error to access the service after an update, try to access the service again after a few minutes.

Workspace Administrator

Administers all accounts in HPE GreenLake Account Home. This is a service role in the platform and has maximum privileges in the platform. Account administrator has the following permissions:

Permission	View	Edit	Delete
Authorization Service	✓	✓	✓
Platform Customer Account	✓	✓	✓
SAML Configuration	✓	✓	✓
Platform Customer Account Toggle MSP	✓	✓	✓
User Account	✓	✗	✓
Service Catalog	✓	✗	✗
API-Group	✓	✗	✗
Reporting Service	✓	✓	✗
Service Provision	✓	✓	✗
Audit Trail	✓	✗	✗
Billing Account	✓	✓	✓

Table Continued

Permission	View	Edit	Delete
Billing Documents	✓	✗	✗
Consumption Data service	✓	✗	✗
Devices and subscription service	✓	✓	✗
Devices Profile Management Service	✓	✓	✗
Geo	✓	✗	✗
Invoicing API	✓	✗	✗
Location Management	✓	✓	✗
Order	✓	✓	✓
Telemetry Data Service	✓	✗	✗
Wellness Dashboard	✓	✗	✗

Workspace Observer

Observes information in HPE GreenLake Account Home. Observer has the following permissions.

Item	View	Edit	Delete
Wellness Dashboard	✓	✗	✗
Location Management	✓	✗	✗

Table Continued

Item	View	Edit	Delete
Billing Account	✓	✗	✗
Order	✓	✗	✗
Consumption Data service	✓	✗	✗
Telemetry Data Service	✓	✗	✗
Devices Profile Management Service	✓	✗	✗
Geo	✓	✗	✗
Devices and subscription service	✓	✗	✗
Audit Trail	✓	✗	✗
API-Group	✓	✗	✗
Service Catalog	✓	✗	✗
Service Provision	✓	✗	✗
User Account	✓	✗	✗
Portal Customization	✓	✗	✗

Table Continued

Item	View	Edit	Delete
Platform Customer Account Toggle MSP	✓	✗	✗
SAML Configuration	✓	✗	✗
Platform Customer Account	✓	✗	✗
Authorization Service	✓	✗	✗
Reporting Dashboard Service	✓	✗	✗

Workspace Operator

Operates the customer accounts to view and edit information in HPE GreenLake Account Home based on the permissions. Operator has the following permissions.

Item	View	Edit	Delete	Download
Wellness Dashboard	✓	✗	✗	✗
Location Management	✓	✗	✗	✗
Billing Account	✓	✓	✗	✗
Order	✓	✓	✗	✗
Consumption Data service	✓	✗	✗	✗
Telemetry Data Service	✓	✗	✗	✗
Devices Profile Management Service	✓	✓	✗	✗

Table Continued

Item	View	Edit	Delete	Download
Invoicing API	✓	✗	✗	✗
Geo	✓	✗	✗	✗
Devices and subscription service	✓	✓	✗	✗
Audit Trail	✓	✗	✗	✗
API-Group	✓	✗	✗	✗
Service Catalog	✓	✗	✗	✗
Service Provision	✓	✓	✗	✗
User Account	✓	✗	✗	✗
Portal Customization	✓	✓	✗	✗
Platform Customer Account Toggle MSP	✓	✗	✗	✗
SAML Configuration	✓	✗	✗	✗
Platform Customer Account	✓	✓	✗	✗
Authorization Service	✓	✗	✗	✗
Reoorting Dashoard Service	✗	✗	✗	✓

Orders Administrator

Administers the billing accounts and orders life cycle of the customers for HPE GreenLake Account Home. Orders administrator has the following permission.

Item	View	Edit	Delete
Billing Account	✓	✓	✓
Billing Documents	✓	✗	✗
Order	✓	✓	✓
Reporting Dashboard Services	✓	✗	✗

Orders Observer

Observes the billing accounts and order life cycle of the customers in HPE GreenLake Account Home. Orders observer has the following permissions.

Item	View	Edit	Delete
Billing Account	✓	✗	✗
Billing Documents	✓	✗	✗
Order	✓	✗	✗
Reporting Dashboard Service	✓	✗	✗

Orders Operator

Operates billing accounts and orders of the customers in HPE GreenLake Account Home. Orders operator has the following permission.

Item	View	Edit	Delete
Billing Account	✓	✓	✗
Billing Documents	✓	✗	✗
Order	✓	✓	✗
Reporting Dashboard Service	✓	✗	✗

Creating user roles

About this task

You can create custom roles for specific services on the HPE GreenLake Account Home and add permissions to define the access privileges for users assigned the role.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Roles & permissions**.
3. On the **Roles & permissions** page, click the **Create role** button.

   NOTE: Use the **Duplicate existing role** option to make a copy of an existing custom role and modify it to suit your needs. Built-in or predefined roles cannot be duplicated or edited.

4. From the **Service** drop-down list, select the service to which the role applies.
5. Click **Next**.
   The **Create role** wizard appears.
6. Follow the directions on the **Create role** wizard to complete the role setup.
   a. **Add name & description** screen—add a role name and description and click **Next**.
   b. **Add <Service> permissions** screens—click **Add permissions** to access the permissions screens where you can select the actions that a user with this role can perform in the selected service. After adding permissions, click **Next** to continue.
   c. **Review & create** screen—this screen shows you the role details, including the permission granted for each role. Use this screen to review your role configuration before creating it. You can change the role name and permissions using the **Modify** link.
   d. Click **Finish** to create the role.
   The new role is added to the **Roles & permissions** page. Use the search or sort the list by name to find the newly created role in the list.

Resource restriction policies

In HPE GreenLake Account Home, each service defines its own scopes and uses the authorization service to control access to the various scope resources. These scope resources must be linked to the user role assignments to enforce the permissions on them. HPE GreenLake Account Home uses Resource Restriction Policies (RRPs) to group these scope resources and facilitate the role assignment process. An RRP is a named group of a list of scope resources. RRPs provide a central place where all role assignments or a group of role assignments can be updated in one place without the need to update multiple users individually. This removes the need to maintain each role assignment whenever a new scope resource is created.

The AllScopes RRP covers all the scopes, old and new, defined by the application to be included in the role assignment.

Use the **Resource Restriction Policies** page to manage RRPs, including creating, viewing, and deleting them.

NOTE:

- You cannot delete an RRP if it has been used in a user role assignment.
- The **Resource Restriction Policies** page is not available in MSP workspaces.

Viewing resource restriction policy details

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Resource restriction policy**.

   The **Resource restriction policies** page displays a list of resource restriction policies (RRP) and their information.

   Name

   The name of the RRP

   Description

   A brief description of the RRP

   Service

   The service for which the RRP defines access limits

   Date Created

   The date the RRP was created
3. The **Create resource restriction policy** button accesses a wizard that steps you through the process for creating a new RRP.
4. Click an RRP to display its details.

   The **Details** section provides basic information from the table view on the main RRP page.

   The **Resources** section lists the resources included in the RRP. Scope resources are listed in bold with their member scope instances below them.

   The **Role assignments** section lists the users and the role assignments where this RRP is applied. The list displays up to ten role assignments on the page; use the page numbers to view additional roles assigned to the user.

Creating a resource restriction policy

Prerequisites

Users with edit permissions through the authorization service can create resource restriction policies (RRPs) in Standard Enterprise workspaces.

About this task

RRPs are named groups of resources that you can create and customize to manage who can access your resources. You can limit access to resources by applying these policies when you make user role assignments.

Create resource restriction policy wizard

When you create an RRP, the **Create resource restriction policy** wizard guides you through a four-step resource selection procedure. In this procedure, you can name the policy, associate it with a service in a region, select the resources and scope instances, review, and save it. After the RRP is created, you can apply it to user roles to restrict the resources users can access.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Resource restriction policy**.
3. On the **Resource restriction policies** page, click **Create resource restriction policy**.
   The **Create resource restriction policy** wizard screen appears where you can enter details for the new policy.
4. In the (Step 1) **Add name & description** screen, enter a **Name** and a **Description** for the RRP and click **Next**.
5. In the (Step 2) **Choose a service** screen, select the service for which you want to limit access and click **Next**.
   The **Add resources** screen appears.
6. In the (Step 3) **Add resources** screen, click the **Add resources** button.
   The **Add <service> resources** screen appears.
7. Select the service that your policy can access. The resource options vary by service.
   a. Click to select a service region from the list. The number of available services for the region are displayed on the screen.
   b. Click a scope resource name in the left pane to view its constituent scope instances listed in the right pane.

      NOTE: There can be more than one level of resource groupings. In such cases, click the scope resource name to show the next sub-resource group.

   c. Next, select the check boxes for the scope instances that you want to include in the policy. You can select a predefined group filter from the top right section of the **Add <service name> resources** screen, or individual scope instances from the **All Resources** section below it.

      NOTE:

      - Group filters include multiple scope instances. Selecting a group filter disables the check boxes in the **All resources** section. If you prefer to select individual scope instances from the **All resources** section, you must first clear the group filter check box.
      - The **All resources** (scopes) section shows up to 200 scope instances. If your workspace has additional scope instances that are not shown on the page, you can use the search field to find them.

      As you add them, the number of scopes added to the policy are incremented and displayed on the bottom of the screen.

   d. When you have finished selecting scopes, click **Add**.
      The **Selected resources** section on the **Add resources** screen lists the resources selected for this new policy: scope resources are displayed in bold font with their member scope instances listed below them.
   e. At this point, you can click the **Add resources** button to repeat these steps and add more resources to the policy.
   f. When you have completed adding resources, click **Next**.
      The **Review & Create** screen appears.

8. In the (Step 4) **Review and create** screen, verify the settings for your RRP. Use the **Modify** links to change the policy name, description, service, or resources.
9. Click **Finish** to create the RRP.
   The **Resource restriction policies** page displays the newly created policy.

Editing resource restriction policies

Prerequisites

Users with edit permissions through the authorization service can edit existing resource restriction policies (RRPs).

About this task

Resource restriction policies (RRPs) are resource groupings that you can use to customize and limit permissions when you make user role assignments. When you edit an RRP, you can update the policy name, description, service, and scopes associated with it.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Resource restriction policy**.
3. On the **Resource restriction policies** page, click a resource restriction policy in the list.
   The RRP details screen appears.

Edit Details

4. In the **Details** section, click **Edit** to update the RRP name and description.
   The name and description fields become editable and you can make your changes in the text fields.
5. Click **Save Changes** to update the information.

Edit Resources

6. In the **Resources** section, click **Edit**.
   The **Add Resources** and **Save Changes** buttons appear. Delete icons appear next to each listed resource.
7. Click the delete icon next to a resource to remove it from the policy.
8. Click **Add Resources** to begin selecting new resources for this policy.
   The **Add <service name> Resources** screen appears.
9. Click to select a service region from the list. The number of available services for the region are displayed on the screen.
10. Click a scope resource name in the left pane to view its constituent scope resources listed in the right pane.

    NOTE: There can be more than one level of resource groupings. In such cases, click the resource name to show the next sub-resource group.

11. Next, select the check boxes for the scopes that you want to include in the policy. You can select a predefined group filter from the top right section of the **Add <service name> Resources** screen, or select individual scopes from the **All Resources** section.

NOTE:

- Group filters include multiple scopes. If you prefer to select individual scope resources from the **All Resources** section, you must clear the group filter check box.
- The scopes section shows up to 200 scopes. If your workspace has additional scopes that are not shown on the page, use the search field to find scopes defined in your workspace.

As you add them, the number of resources added to the policy are incremented and displayed on the screen.

12. When you have finished selecting scopes, click **Add**.
    The **Add Resources** screen closes and you can see the updated resources listed in the **Resources** section of the policy details page.
13. Click **Save Changes** to save the updated policy.

Editing resource restriction policy assignments

About this task

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.
3. On the **Users** page, click a name to select a user from the list.
   The user details screen appears.
4. In the **Roles** section, click the ellipsis **(...)** next to the service resource you want to modify.
   A pop-up window displays the available actions (options vary depending on the selected service and role).
5. Select the **Edit Resource Access** link.
   The **Edit Resource Access** dialog appears and the number of assigned resource restriction policies (RRPs) are listed in the **Resource Restriction Policy** field.
6. Click the down arrow to access and select the policies from the drop-down list. Use the check boxes to select new policies or clear existing assignments.

   NOTE: You can select multiple RRPs for the user role.
7. Click **Save Changes**.
   The dialog closes and a confirmation notification for the policy updates appears. Click **X** to dismiss the notification.
8. To verify the change, select the **Limited Access** link In the user details screen.
   The **Limited Access** pop-up window lists the policies applied to the role assignment.

Deleting a resource restriction policy from a user role assignment

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.
3. On the **Users** page, click a name to select a user from the list of available users.

The user details screen appears.

4. Click the ellipsis **(...)** next to the service resource that you want to modify.
5. Select the **View details** link.
   The **Details** page appears.
6. In the **Roles** section, click the ellipses **(...)** against the service you want to modify.
7. Select **Edit resource access**, if you want to remove all RRP limitations for the user, slide the **Limit resource access** toggle to the left.
8. Click **Save changes**.
   The dialog closes and in the **Roles** section, the **Resource access** column for the role shows a value of **Full access**. A confirmation notification for the update appears; click **X** to dismiss the notification.

Assign roles

The **Users** page is where you give users access to the HPE GreenLake Account Home services. Here you can add, edit, delete, and update role assignments. You can also apply resource restriction policies to user roles to limit their access or permissions to specific resources. The following restrictions apply:

- MSP account administrators can assign roles to users in the MSP workspace and limit resource access through predefined access rules. They cannot assign roles to tenant users within a tenant workspace.
- Tenant users cannot change role assignments for MSP users within the tenant workspace.
- Users cannot update or add role assignments for federated users within HPE GreenLake Account Home workspaces.

Assigning roles to users in standalone or MSP tenant workspaces

About this task

This procedure applies to users in a standalone or Managed Service Provider (MSP) tenant workspace. Account administrators or users with edit permissions through the Authorization service can assign roles. All tenant user role assignments take place and are managed within the tenant workspace.

NOTE:

- Tenant users cannot change role assignments for MSP users within the tenant workspace.
- Users cannot update or add role assignments for federated users within HPE GreenLake Account Home workspaces.
- Resource restriction policies (RRPs) are resource groupings that you can use to customize and limit permissions when you make user role assignments.

When assigning roles to users within standalone or MSP tenant workspaces, you can limit resource access through RRPs that you define in the workspace. In MSP tenant workspaces, these RRPs cannot be shared across tenants and can only be used for role assignment to users within the individual tenant workspace.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.
3. On the **Users** page, select the user you want to assign roles to.
4. On the user details page, review the user's current role assignments.

5. Click **Assign role**.
6. From the **Service** drop-down list, select the service for which you want to grant permission.
7. In the **Role** field, select a role for the user. You can enter text to search for a role or pick one from the list.

   NOTE: The options vary depending on the service that you select.

8. To further limit the scope of resources this user role can access, slide the **Limit resource access** toggle to the right and select the RRP you want to assign. Use the check boxes to select multiple RRPs from the list. As you select RRPs, the number of selections is incremented and is shown on the bottom of the **Assign role** screen.

   NOTE:

   - The options vary depending on the service that you select.
   - If the **Limit resource access** toggle is not used, all access permissions are enabled for the user role.
   - If there are no RRPs defined, you can create them by clicking the **Create policy** link. You are redirected to the **Create Resource Restriction Policy** wizard which takes you through the policy creation procedure. For more details, see **Resource restriction policies**.

9. Click **Assign role** to add the assignment.
   The **Change role assignment?** confirmation box shows the current assignments and the requested assignments.
10. Review the requested role assignment details and click **Change Role Assignment**.
    The updated role assignment is saved.

    NOTE: Role assignment changes can take up to 15 minutes to take effect.

11. To verify the update, go to the **Users** page and click the name of the user to view their newly added role in the **Details** screen.

Editing a user role assignment

About this task
Federated users do not have access to role assignment or modification.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Users**.
3. On the **Users** page, click the name of a user to view their role assignments in the user details screen.
4. To add role assignments for the user, click **Assign role** and follow the steps in the **Assign role** screen.
5. To modify existing role assignments, click **More** (...) in the row of the role you want to modify. Options include:

   - **Edit Resource Access**—use this option to limit resource access for this role. For more information, see .
   - **Remove role**—use this option to remove the role assignment for the user.

6. Click **Save changes**.

Authentication

HPE GreenLake Account Home uses Security Assertion Markup Language (SAML) to provide single sign-on (SSO) access to resources that are in different security domains. SAML is an XML-based open-standard for exchanging authentication and authorization data between trusted partners, particularly between a services provider and identity management system used by an enterprise. SAML-SSO works by passing information about the user's identity and authorization status between the identity provider and the service provider.

SAML-SSO authentication allows an authorized user to access multiple services with one set of credentials, which reduces the number of passwords a user has to remember. It also improves security by reducing the number of places where passwords are stored.

To provide a seamless login experience for users whose identity is managed by an external authentication source, HPE GreenLake Account Home offers a federated SSO solution based on the SAML 2.0 authentication and authorization framework. With the HPE GreenLake Account Home SAML SSO solution, organizations can manage user access using a single authentication and authorization source.

NOTE: The following authentication sections use:

- HPE Aruba Networking Central as the sample service in configuration examples.
- Generic service provider identifier and SSO URLs, such as **https://sso.common.cloud.hpe.com**. Replace these with URL's that apply to your solution. For example, in HPE GreenLake Dedicated Platform use Dedicated Platform URL's.

SAML SSO Elements for HPE GreenLake Account Home

HPE GreenLake Account Home SAML SSO consists of the following key elements:

Service Provider (SP)

The provider of a business function or service; for example, HPE GreenLake Account Home or any other service on the platform. The service provider requests and obtains an identity assertion from the Identity Provider (IdP). The service provider uses the identity assertion to provide services to the user.

Identity Provider (IdP)

The identity management system maintains the user's identity information and authenticates the user.

SAML Request

A request sent by the service provider to the IdP to authenticate the user. The authentication request is generated when a user tries to access HPE GreenLake Account Home.

SAML Assertion

The authentication and authorization information issued by the IdP to allow access to HPE GreenLake Account Home.

Relying Party

The business service that relies on SAML assertion for authenticating a user. For example, HPE GreenLake Account Home.

Asserting Party

The identity management system or the IdP creates SAML assertions for a service provider.

Metadata

Data in XML format exchanged between the IdP and HPE GreenLake Account Home to establish interoperability.

SAML Attributes

The attributes associated with the user; for example, username, customer ID, role, and group in which the devices belonging to a user account are provisioned. The SAML attributes must be configured on the IdP according to specifications associated with a user account in HPE GreenLake Account Home. These attributes are included in the SAML assertion when HPE GreenLake Account Home sends a SAML request to the IdP.

Entity ID

A unique string to identify the service provider that issues a SAML SSO request. SAML specifies this string is a URL, although all providers do not have the same requirement.

User

User with SSO credentials.

SAML SSO workflows

HPE GreenLake Account Home supports the following type of SAML SSO workflows:

- SP-Initiated SSO
- IdP-Initiated SSO

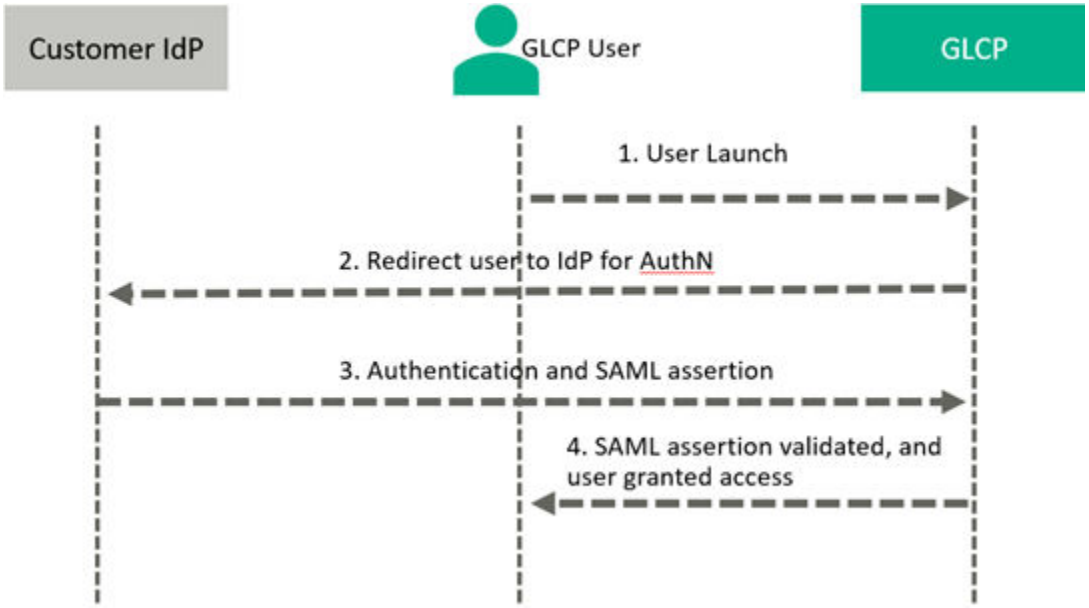
Service provider-initiated SSO

In a service provider (SP)-initiated SSO workflow, the SSO request originates from the service provider domain, for example, HPE Aruba Networking Central. When a user tries to access HPE Aruba Networking Central, a federation authentication request is created and sent to the identity provider (IdP) server.

The SP-Initiated SSO workflow with HPE GreenLake Account Home is supported through the HTTP redirect POST method. HPE GreenLake Account Home sends an HTTP redirect message with an authentication request to the IdP through the user's browser. The IdP sends a SAML response with an assertion to HPE GreenLake Account Home through HTTP POST.

The SP-Initiated SSO workflow with HTTP Redirect POST includes the following steps:

1. The user tries to access HPE GreenLake Account Home and the request is redirected to the IdP.
2. HPE GreenLake Account Home sends an HTTP redirect message with the SAML request to the IdP for authentication through the user's browser.
3. The user logs in with the SSO credentials.
4. On successful authentication, the IdP sends a digitally signed HTML form with SAML assertion and attributes to HPE GreenLake Account Home through the web browser.
5. If the digital signature and the attributes in the SAML assertion are valid, HPE GreenLake Account Home allows access to the user.

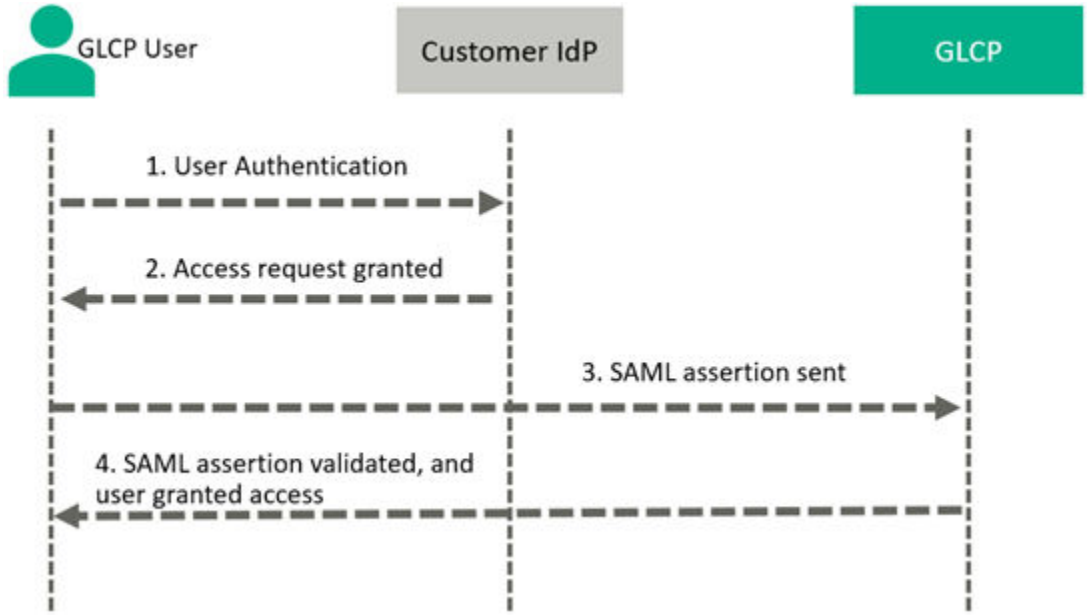


Identity provider-initiated SSO

In an identity provider (IdP)-initiated workflow, the SSO request originates from the IdP domain. The IdP server creates a SAML response and redirects the users to HPE GreenLake Account Home.

The HPE GreenLake Account Home SAML SSO deployments support the IdP-Initiated SSO workflow through the HTTP POST method. The IdP-Initiated SSO workflow consists of the following steps.

1. The user is logged in to the IdP and tries to access HPE GreenLake Account Home.
2. The IdP sends a digitally signed HTML form with SAML assertion and attributes to HPE GreenLake Account Home through the web browser.
3. If the digital signature and the attributes in the SAML assertion are valid, HPE GreenLake Account Home allows access to the user.



SAML SSO single logout

HPE GreenLake Account Home supports Single Logout (SLO) of SAML SSO users. SLO allows users to terminate server sessions established using SAML SSO by initiating the logout process once.

NOTE: HPE GreenLake Account Home supports IdP-initiated SLO only.

The IdP-Initiated SAML SLO workflow includes these steps:

1. User logs out of the IdP.
2. The IdP sends a logout request to HPE GreenLake Account Home.
3. HPE GreenLake Account Home validates the logout request from the IdP, terminates the user session, and sends a logout response to the IdP.
4. The user is logged out of HPE GreenLake Account Home. After the IdP receives a logout response from all service providers, the IdP logs the user out.

SSO authorization options

Once you have configured SSO, when users sign in with their SSO credentials they are authenticated. The access users then have to workspaces and other resources is determined by the roles and permissions they are authorized to use. The following options are available for managing user authorization when you configure a SSO connection for a workspace on HPE GreenLake Account Home.

Authorization option	Description
Manage authorization locally via the GreenLake platform	User authorization is configured in HPE GreenLake Account Home (local authorization).
Use the SAML SSO response for session-based authorization	User authorization is configured in the hpe_ccs_attribute in your IdP (session-based authorization). This attribute is returned in the SAML authentication response.

Select the SSO authorization option according to where you want to manage your users access to HPE GreenLake Account Home resources.

NOTE: The workspaces associated with a domain must all be configured to use the same method of SSO authorization; either static or session.

SSO for local authorization

If you configure SSO for local authorization, when users sign in to HPE GreenLake Account Home using their SSO credentials, their identity is authenticated but they are not created as users or assigned permissions to a workspace. To give users the access they need, invite users to the workspace and assign roles to them on HPE GreenLake Account Home.

For information about creating users and roles, see **Identity & access management**.

SSO for session-based authorization

If you configure SSO for session-based authorization, when users sign in using their SSO credentials they are authenticated and assigned roles in HPE GreenLake Account Home on a per-session basis.

The workspaces, roles, and services a user has access to each time they sign in are defined using the custom SAML attribute, hpe_ccs_attribute, which you create in your identity provider. If you want to change a user's access, edit the attribute; you cannot change a user's access using the HPE GreenLake Account Home UIs.

NOTE: The default name of the custom SAML attribute is hpe_ccs_attribute but you can choose a different name for the attribute when you create it. You specify the attribute name when you configure a SSO connection on the HPE GreenLake Account Home Add SAML Connection wizard. Make sure the name you enter on the wizard matches the attribute name in the identity provider.

For information about creating the hpe_ccs_attribute, see **HPE GreenLake Account Home SAML attribute for SSO authorization**.

For information on configuring a SSO connection, see **Configuring SAML SSO on HPE GreenLake Account Home** . For information on changing the type of authorization defined for an existing SSO connection, see **Changing the authorization method for a SSO connection**.

How to configure HPE GreenLake Account Home SAML SSO

To configure SAML SSO authentication, you must complete tasks on your IdP and on HPE GreenLake Account Home. If you have different administrators for HPE GreenLake Account Home and your IdP, ensure they coordinate to complete the steps.

There are some differences in how you configure SSO authentication depending on whether you choose to use session-based or static local authorization:

- When you configure SSO authentication, you select the type of user authorization you want to implement by selecting an option on the **Add SAML Connection** wizard. The option you select determines where you manage your SSO users and their access to GLCP workspaces and resources.

  The following table shows the option to select for each authorization type.

User authorization type	Add SAML Connection wizard option to select
Session-based authorization	Use the SAML SSO response for session-based authorization.
Local authorization	Manage authorization locally via the GreenLake Platform.

- Providing users with access to HPE GreenLake Account Home workspaces and roles.
  - If you use session-based authorization, the IdP administrator creates users and provides them with access to HPE GreenLake Account Home workspaces and roles by configuring a SAML attribute, by default the hpe_ccs_attribute, on the IdP.

    With session-based authorization, a SSO user's access to HPE GreenLake Account Home is valid only for the duration of the SSO session and you can only change a user's access to HPE GreenLake Account Home resources by updating the hpe_ccs_attribute for the user.
  - If you are using static local authorization, the workspace administrator manages users access to workspaces and assign roles on HPE GreenLake Account Home.

Depending on the type of authorization you want to use for your SSO configuration, perform the steps in one of the following procedures:

- **Configuring SSO authentication with local authorization**
- **Configuring SSO authentication with SSO authorization**

Configuring SSO authentication with local authorization

Procedure

1. Configure SSO on the identity provider. See **Configuring SAML SSO on your identity provider**.
2. Configure the SAML authorization profile by running the Add SAML Connection wizard. See **Configuring SAML SSO on HPE GreenLake Account Home** .

   When prompted by the wizard for the authorization type to select, choose the option **Manage authorization locally via the GreenLake Platform**.
3. On HPE GreenLake Account Home, invite users to your workspace and assign roles to them.

   For information on adding users to a workspace, see **Inviting users**. For information on role assignments, see **Assigning roles to users in standalone or MSP tenant workspaces**.
4. Verify that users can sign in to HPE GreenLake Account Home using their SSO credentials.

   For troubleshooting information, see **SSO FAQ**.

Configuring SSO authentication with SSO authorization

Procedure

1. Configure SSO on the identity provider. See **Configuring SAML SSO on your identity provider**.
2. Configure the SAML authorization profile by running the Add SAML Connection wizard. See **Configuring SAML SSO on HPE GreenLake Account Home** .

   When prompted by the wizard for the authorization type to select, choose the option **Use the SAML SSO response for session-based authorization**.
3. Assign roles to users on the IdP.

   For information, see **Configuring SAML SSO on your identity provider** and **HPE GreenLake Account Home SAML attribute for SSO authorization**.
4. Verify that users can sign in to HPE GreenLake Account Home using their SSO credentials.

   For troubleshooting information, see **SSO FAQ**.

Configuring SAML SSO on your identity provider

About this task

To set up SSO for HPE GreenLake Account Home, first configure SSO in your identity provider (IdP). An IdP administrator performs this task.

For examples of configuring an IdP for SAML SSO, see the following:

-
- **Configuring SAML SSO using the Okta identity provider**

Procedure

1. Create a new SSO application on your organization's IdP.
2. Configure the service provider identifier URLs in the application. Ensure you have the following service provider URLs available:

- Entity ID: https://sso.common.cloud.hpe.com
- Reply URL: https://sso.common.cloud.hpe.com/sp/ACS.saml2
- Relay State: https://common.cloud.hpe.com

NOTE: You must specify a Relay State URL if you are configuring an IdP-initiated SSO work flow in which the user is authenticated by the IdP before being redirected to HPE GreenLake Account Home.

3. Configure the format and value of each of the following SAML attributes in the IdP.

   - Email address. For example, **NameId**.
   - User first name. For example, **FirstName**.
   - User last name. For example, **LastName**.
   - User country code. If specified, the country code must be defined in a custom attribute named **CountryCode**.

     If the IdP does not provide a CountryCode attribute, in HPE GreenLake Account Home the user's country code is set to **US** (United States) by default.

     For additional information, see .

   You configure SAML attributes on the IdP according to specifications associated with a user account. These attributes are included in the SAML assertion when HPE GreenLake Account Home sends a SAML request to the IdP.

4. **SSO role assignments only.** Configure the hpe_ccs_attribute.

   Configure the hpe_ccs_attribute for each SSO user only if you are implementing SSO role assignments. This attribute specifies the user's access to resources on HPE GreenLake Account Home.

   For information on the format for this attribute, see **HPE GreenLake Account Home SAML attribute for SSO authorization**.

5. Create the SAML SSO response signing certificate, then download and save the file.

   You require the certificate data when you configure a SSO connection for a workspace in HPE GreenLake Account Home.

HPE GreenLake Account Home SAML attribute for SSO authorization

The HPE GreenLake Account Home SAML attribute, hpe_ccs_attribute, defines the access to services each user is assigned. Create the hpe_ccs_attribute on the IdP only if you are configuring SSO with SSO authorization. If you plan on using SSO for authentication only (local authorization), and will manage user access on HPE GreenLake Account Home, you do not have to create the hpe_ccs_attribute.

When configuring the hpe_ccs_attribute, the format to use varies depending on whether you are in a standard workspace environment or an MSP environment:

- In a standard enterprise workspace, use this format:

  ```
  {version_1}#{workspace id}:{service id}:{role_name}:{resource_
  restriction_policy_name1,resource_ restriction_policy_name2|ALL_SCOPES}
  ```

- In an MSP workspace, use the following format.

  NOTE: In MSP workspaces, you must specify an access type for the role element and resource restriction policies are not supported.

  ```
  {version_1}#{workspace id}:{service id}:{role_name|{accessType}|}:{ALL_SCOPES}
  ```

The table describes each element in the attribute hpe_ccs_attribute.

Syntax	Description
`version`	Defines the version of the assertion attribute; currently, only version_1 is supported.
`workspace id`	The identifier assigned to your workspace.
`service id`	The identifier of the service to access, for example, the ID assigned to HPE Aruba Networking Central or the ID assigned to HPE GreenLake Account Home. If you have multiple services, define attributes separately for each service ID with a colon (:) delimiter. **NOTE:** Users must be assigned access to the HPE GreenLake Account Home before they can access a service on the platform. Therefore you usually have to specify at least two service IDs in the hpe_ccs_attribute: one to access the HPE GreenLake Account Home, and one to access a service on the platform, such as HPE Aruba Networking Central. Specify the HPE GreenLake Account Home service ID first; the ID is 00000000-0000-0000-0000-000000000000 but this value can be abbreviated to 0 if you want to minimize the overall size of the attribute.

Table Continued

Syntax	Description
`role_name` `accessType` (MSP workspaces only)	• **Role** The name of a role defined in HPE GreenLake Account Home that you want to assign to the user for the service you specified. To view the role names available, on the HPE GreenLake Account Home header, click the Global navigation menu and then select **IAM and administration** > **Roles & permissions**. The role defines the access level for a particular Name ID returned in the response. Name ID is a valid email address used as the user name to log into HPE GreenLake Account Home. • **accessType** In an MSP environment, the access type specifies where the role you have specified is assigned. The role can be assigned to the user in a tenant workspace or an MSP workspace.

`resource_ restriction_policy_name`
 	
`ALL_SCOPES`
	• If you specify the name of a custom resource restriction policy (RRP) defined for a service in HPE GreenLake Account Home, the user can access only the specific groups of resources specified within the RRP. You can specify more than one RRP for a combination of user, service and role. Separate each RRP name with a comma.
	
	NOTE: HPE GreenLake Account Home roles do not support RRPs. When assigning an HPE GreenLake Account Home role, the role is scoped to all workspace resources by default.
	
	• ALL_SCOPES. Provides access to all resources associated with a service without any restriction. You can use the ALL_SCOPES RRP If you did not define a custom RRP.
	
	The ALL_SCOPES value can be abbreviated to ALL if you want to minimize the overall size of the attribute.

Size limits of the hpe_ccs_attribute

SAML imposes a limit on the length of content that can be sent in a single SAML request and this in turn imposes restrictions on the length of the hpe_ccs_attribute. It's recommended that the hpe_ccs_attribute does not exceed 2048 characters.

In general, if you define a maximum of eight workspaces in the attribute, the character limit will not be exceeded and SSO will be successful. However, depending on the number of roles and services specified for each workspace, you might be able to specify more than eight workspaces without reaching the limit.

If the number of workspaces you need to specify for a user exceeds the allowed character limit, it's recommended that you contact HPE GreenLake Account Home Support for assistance.

TIP: Minimize the size of hpe_ccs_attribute by substituting the following values with their abbreviated versions when configuring the attribute.

Value	Abbreviation
ALL_SCOPES	All
HPE GreenLake Account Home service ID: 00000000-0000-0000-0000-000000000000	0

Location of the workspace id and service id values

You can locate the workspace ID and service ID values for your workspaces and services from the UI. You need this information in constructing the hpe_ccs_attribute.

- **Workspace ID**

  To locate the identifier assigned to a workspace, select the **IAM and administration** > **Workspace details** option on the HPE GreenLake Account Home header **Global navigation** menu.

  On the workspace details page, the workspace ID is listed along with other details about the workspace such as the workspace type and any associated address information.

- **Service ID**

  1. To locate the identifier of your service, on the HPE GreenLake Account Home header, click the **Global navigation** menu .
  2. Select **Services** > **Service catalog**.

     The **Services catalog** page shows services that are available for your workspace.
  3. To see information about any service, click the service card.

     The service detail page appears. The **Overview** tab provides details about the service including the Service ID.

After configuring a SAML SSO connection, you can view all the SAML attributes, including the workspace ID and the service ID, used in the configuration. For information on how to do this, see **Viewing SSO configuration details** .

Example configurations for the hpe_ccs_attribute

This topic provides examples of how to configure the HPE GreenLake Account Home SAML attribute, hpe_ccs_attribute, for different types of workspace environments. The format of the attribute is always the same but the values you specify for each element vary according to the workspace and services you are provisioning. The format of the attribute is as follows:

Standard workspaces:

```
{version_1}#{workspace id}:{service id}:{role_name}:{resource_
restriction_policy_name|ALL_SCOPES}
```

MSP workspaces:

```
{version_1}#{workspace id}:{service id}:{role_name|accessType}:{ALL_SCOPES}
```

For additional information about the hpe_ccs_attribute, see **HPE GreenLake Account Home SAML attribute for SSO authorization**.

NOTE: The workspace ID values shown in the examples are for illustrative purposes only. When you configure the hpe_ccs_attribute, substitute these values for your workspace ID.

Standard Enterprise Workspace

The following hpe_ccs_attribute grants federated SSO users access to a standard workspace on HPE GreenLake Account Home with one role. Users are granted the following permissions:

Orders Operator access to all resources in HPE GreenLake Account Home (Orders Operator role, All Scopes access)

Example attribute:

```
version_1#77e31a38775411ee857d7ea612b4de9e:00000000-0000-0000-0000-000000000000:
Orders Operator:ALL_SCOPES
```

The example attribute uses the values shown in the table.

Workspace ID	Service	Service ID	Role	Scope
77e31a38775411ee857d7ea612b4de9e	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Orders Operator	All scopes

Standard Enterprise Workspace with Multiple Roles

The following hpe_ccs_attribute grants federated SSO users access to HPE GreenLake Account Home with more than one role in a standard workspace. Users are granted the following permissions:

- Orders Operator access to all resources in HPE GreenLake Account Home (Orders Operator role, All Scopes access)
- Workspace Observer access to all resources in HPE GreenLake Account Home (Workspace Observer role, All Scopes access)

Example attribute:

```
version_1#77e31a38775411ee857d7ea612b4de9e:00000000-0000-0000-0000-000000000000:
Orders Operator:ALL_SCOPES:00000000-0000-0000-0000-000000000000:Workspace
Observer:ALL_SCOPES
```

The attribute uses the values shown in the table.

Workspace ID	Service	Service ID	Role	Scope
77e31a38775411ee857d7ea612b4de9e	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Orders Operator Workspace Observer	All scopes

Standard Enterprise Workspace with Multiple Services

The following hpe_ccs_attribute grants federated SSO users access to the HPE GreenLake Account Home and the HPE Aruba Networking Central services in a standard workspace. Users are granted the following permissions:

- Aruba Central Administrator access to the resources specified in two RRPs that are defined in HPE GreenLake Account Home based on resources created in the HPE Aruba Networking Central service (Aruba Central Administrator role, RRP1,RRP2 access)
- Workspace Administrator access to all resources in HPE GreenLake Account Home (Workspace Administrator role, All Scopes access)

Example attribute:

```
version_1#77e31a38775411ee857d7ea612b4de9e:00000000-0000-0000-0000-000000000000:
Workspace Administrator:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba
Central Administrator:RRP1,RRP2
```

The attribute uses the values shown in the table.

Workspace ID	Service	Service ID	Role	Scope
77e31a38775411ee857d7ea612b4de9e	HPE Aruba Networking Central	683da368-66cb-4ee7-90a9-ec1964768092	Aruba Central Administrator	RRP1,RRP2
	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Workspace Administrator	All scopes

Multiple Standard Enterprise Workspaces

The following hpe_ccs_attribute grants federated SSO users with access to services in more than one standard workspace. Users are granted the following permissions:

- For workspace with workspace id# 77e31a38775411ee857d7ea612b4de9e, Orders Operator access to all resources on HPE GreenLake Account Home (Orders Operator role, All Scopes access)
- For workspace with workspace id# edf5b71495ca11ee88d36202766a05fe, Workspace Administrator access to all resources on HPE GreenLake Account Home (Workspace Administrator role, All Scopes access)

Example attribute:

```
version_1#77e31a38775411ee857d7ea612b4de9e:00000000-0000-0000-0000-000000000000:
Orders
Operator:ALL_SCOPES#edf5b71495ca11ee88d36202766a05fe:00000000-0000-0000-0000-000
000000000:Workspace Administrator:ALL_SCOPES
```

The attribute uses the values shown in the table.

Workspace ID	Service	Service ID	Role	Scope
77e31a38775411ee857d7ea612b4de9	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Orders Operator	All scopes
edf5b71495ca11ee88d36202766a05fe			Workspace Administrator	

MSP and Tenant Workspace Access with Different Roles

The following hpe_ccs_attribute grants federated SSO users access to HPE GreenLake Account Home on an MSP workspace and on all tenant workspaces. Users are granted the following permissions:

- Workspace Observer access to all resources on HPE GreenLake Account Home (Workspace Observer role, All Scopes access) on the MSP workspace
- Workspace Observer access to all resources on HPE GreenLake Account Home (Workspace Observer role, All Scopes access) on tenant workspaces
- Aruba Central Administrator access to all resources on HPE Aruba Networking Central (Aruba Central Administrator role, All Scopes access) on tenant workspaces

Example attribute:

```
version_1#fa3d56d2982011ee9a95365bbe91047f:00000000-0000-0000-0000-000000000000:
Workspace Observer|
MSP|:ALL_SCOPES:00000000-0000-0000-0000-000000000000:Workspace Observer|
TENANT|:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central
Administrator|TENANT|:ALL_SCOPES
```

The attribute uses the values shown in the table. The |MSP| and |Tenant| elements in the hpe_ccs_attribute specify whether access is granted to MSP or tenant workspaces.

Workspace ID	Service	Service ID	Role	Access Type	Scope
fa3d56d2982011ee9a95365bbe91047f **NOTE:** This is the ID of the MSP workspace.	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Workspace Observer	MSP	All scopes
	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Workspace Observer	Tenant	All scopes
	HPE Aruba Networking Centrall	683da368-66cb-4ee7-90a9-ec1964768092	Aruba Central Administrator	Tenant	All scopes

MSP Workspace with MSP Access Only

The following hpe_ccs_attribute grants federated SSO users with access to HPE GreenLake Account Home on an MSP workspace. Users are assigned the following permissions:

Workspace Administrator access to all resources on HPE GreenLake Account Home (Workspace Administrator role, All Scopes access) on the MSP workspace

Example attribute:

```
version_1#fa3d56d2982011ee9a95365bbe91047f:00000000-0000-0000-0000-000000000000:Workspace Administrator|MSP|:ALL_SCOPES
```

The attribute uses the values shown in the table. The |MSP| element in the hpe_ccs_attribute specifies that user access is granted to the MSP workspace only.

Workspace ID	Service	Service ID	Role	Access Type	Scope
fa3d56d2982011ee9a95365bbe91047f **NOTE:** This is the ID of the MSP workspace.	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Workspace Administrator	MSP	All scopes

MSP Workspace with Tenant Access Only

The following hpe_ccs_attribute grants federated SSO users access to HPE GreenLake Account Home on tenant workspaces only. Users are assigned the following permissions:

Workspace Operator access to all resources on HPE GreenLake Account Home (Workspace Operator role, All Scopes access) on tenant workspaces

Example attribute:

```
version_1#fa3d56d2982011ee9a95365bbe91047f:00000000-0000-0000-0000-000000000000:Workspace Operator|TENANT|:ALL_SCOPES
```

The attribute uses the values shown in the table. The `|Tenant|` element in the hpe_ccs_attribute specifies that the access is granted to tenant workspaces only.

Workspace ID	Service	Service ID	Role	Access Type	Scope
fa3d56d2982011ee9a95365bbe91047f **NOTE:** This is the ID of the MSP workspace.	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Workspace Operator	TENANT	All scopes

MSP Workspace with MSP and Tenant Access to Multiple Services

The following hpe_ccs_attribute grants federated SSO users with access to HPE GreenLake Account Home and access to HPE Aruba Networking Central on the MSP workspace and all tenant workspaces. Users are assigned the following permissions:

- Workspace Operator access to all resources on HPE GreenLake Account Home (Workspace Operator role, All Scopes access) on the MSP and tenant workspaces
- Aruba Central Administrator access to all resources on HPE Aruba Networking Central (Aruba Central Administrator role, All Scopes access) on the MSP and tenant workspaces

Example attribute:

```
version_1#fa3d56d2982011ee9a95365bbe91047f:00000000-0000-0000-0000-000000000000:
Workspace Operator|
MSP|:ALL_SCOPES:00000000-0000-0000-0000-000000000000:Workspace Operator|
TENANT|:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central
Administrator|MSP|:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central
Administrator|TENANT|:ALL_SCOPES
```

The attribute uses the values shown in the table. The `|MSP|` or `|TENANT|` elements in the hpe_ccs_attribute specify whether user access is granted to MSP or tenant workspaces.

Workspace ID	Service	Service ID	Role	Access Type	Scope
fa3d56d2982011ee9a95365bbe91047f **NOTE:** This is the ID of the MSP workspace.	HPE GreenLake Account Home	00000000-0000-0000-0000-000000000000	Workspace Operator	MSP TENANT	All scopes
	HPE Aruba Networking Central	683da368-66cb-4ee7-90a9-ec1964768092	Aruba Central Administrator	MSP TENANT	All scopes

Configuring SAML SSO on HPE GreenLake Account Home

Prerequisites

Identify the SAML SSO metadata from the IdP that you need to add to HPE GreenLake Account Home. If you want to add this information from a metadata file or metadata URL, have the XML file or URL available.

About this task

During this task you must claim a domain to use for SSO and select the type of authorization that you want to implement with SSO.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Authentication**.
3. On the **Authentication** page, click **Set Up SAML connection**.
4. Enter a domain to add an authorization profile and click **Continue**.
   - Ensure that the domain has at least one verified user. The user claiming the domain must be the same user who created the account and must be logged into HPE GreenLake Account Home. For example, to claim an acme.com domain, the user must be logged in to HPE GreenLake Account Home with an @acme.com email address.
   - HPE GreenLake Account Home does not support adding other free public domain names such as Gmail.com, Yahoo.com, or Facebook.com, for SAML authorization profiles.
5. Follow the directions on the **Add SAML connection** wizard to complete the SSO setup. See the step descriptions table for help on each step of the wizard.
6. Click **Next** after each step.
7. Click **Finish** to set up your SSO domain.

   When your SSO domain is set up, click **Download Metadata File** if you want to download the metadata, then click **Exit**.
8. Click **Send Email** to send an email to users to notify them that SSO is enabled for their account, or you can select the **Skip For Now** link to send an email later.

Step	Description
Step 1 of 5 **Authorization settings**	
Authorization method	Select the authorization method for the SSO connection: • **Manage authorization locally via the GreenLake platform.** Select this option to use SSO only to authenticate users. You must create users and assign roles to them on HPE GreenLake Account Home to provide user access to workspaces. • **Use the SAML SSO response for session-based authorization.** Select this option to use SSO to authenticate and authorize users. Users are authenticated and assigned access to workspaces and roles dynamically during each SSO session.

Table Continued

Step	Description
Target workspace	If you are configuring SSO for an MSP workspace, select one or more of the folllow options to identify where the SSO profile connection applies: • **Apply the SSO connection to the MSP workspace.** Select this option to apply the SSO profile only to the MSP workspace. • **Apply the SSO connection to all customer workspaces.** Select this option to apply the SSO connection only to tenant workspaces. • Select both options to apply the SSO profile to MSP and tenant workspaces.
Step 2 of 5 **Add Identity Provider Details**	
Select a Configuration Method	Select one of the following options to add identity provider details: • **Metadata File**. The metadata file must be in XML format and must include a valid certificate and HTTPS URLs for the entity ID, login URL, and logout URL fields. **a.** Select **Metadata File**, then click **Upload Metadata File** to upload the file. HPE GreenLake Account Home extracts the entity ID, domain login URL, domain logout URL, and certificate content. **b.** Verify the details, then click **Save**. • **Metadata URL**. The HTTPS URLs for the entity ID, login URL, and logout URL fields must be valid. **a.** Select **Metadata URL** then enter the URL to the page where the identity provider details are available. **b.** Click **Validate URL**. Details are automatically filled in for valid configurations. **c.** Click **Save**. • **Manual (Enter X.509 Certificate Details)** **a.** Select **Manual (Enter X.509 Certificate Details)** then enter values in the **Entity ID**, **Domain Login URL**, **Domain Logout URL**, and **X.509 Signing Certificate** fields. **b.** Click **Save**.
Step 3 of 5 **Configure Settings**	

Table Continued

Step	Description
Map SAML Attributes	Map the SAML attributes you configured on the IdP to HPE GreenLake Account Home attributes. • **Required Attributes** **Email address**. Leave the default value of **NameId** or enter the name of the email address attribute as configured on the IdP server. The **NameId** attribute must include the email address of the user. For example, <NameId>admin@test.com</NameId>. If you use a custom attribute, make sure it contains the user's email address. **HPE GreenLake Attribute**. This is a mandatory attribute but is only required if you are configuring session-based SSO. The default value is **hpe_ccs_attribute**. You can also substitute your own custom value. For more information, see **HPE GreenLake Account Home SAML attribute for SSO authorization**. • **Optional Attributes** **First name**, **Last name** Enter the attributes for the user's first and last names, or accept the default values, **FirstName** and **LastName**. If you do not configure first and last names as optional attributes, the user's name displays as `UnknownFN` and `UnknownLN` in the user's HPE user account profile.
Manage Idle Session Timeout	Specify a value for **Idle Session Timeout**.
Step 4 of 5 **Create a Recovery User**	

Table Continued

Step	Description
Recovery User	A recovery user is a fallback user account you can use to log in and recover the account if there is an error in the SSO configuration and users are locked out. If the recovery user details are lost, the recovery user is specified in the format: `sso_re_<GLCP account ID >@yourdomain.com` **Enable Recovery User**. Enable the recovery user option if it is not already enabled by sliding the **Recovery User** toggle to the right, then enter values in the following fields. ⚠ **WARNING:** If you disable the recovery user feature, you can no longer recover your account credentials if an SSO failure occurs. • **Recovery User Email**. Copy the value in the recovery user email field. This email is auto generated and you cannot change it. • **Recovery User Password**. Enter a password for the recovery user. • **Point of Contact Email**. Enter a point of contact email in case you forget your password. This email is used for password recovery in case the recovery user's password is forgotten or has expired. It is recommended that you configure an email alias to protect against lockout if the single user with the email is not active in the company. Copy and store the recovery user details in a safe place.
Step 5 of 5 **Review & Create**	Check the information displayed and verify that all your configuration details are correct. Click **Modify** to edit your configuration details for a step.

Once the SSO domain configuration is completed, only users who log in to HPE GreenLake Account Home using the SSO credentials for the domain can access the workspace. For example, if SSO is configured for the domain acme.com, only users who log in using the acme.com email address can access the workspace. If the same users have an existing HPE GreenLake Account Home username and password, and if they log in to their HPE GreenLake Account Home account using those credentials, they cannot access the SSO-enabled workspace.

Reviewing and managing a SSO connection

Once SSO is successfully configured for a domain, review and manage the SSO connection on the **Authentication** page. Existing SSO connections for domains are listed in the SAML section of the page.

Click the ellipsis (**...**) next to a domain name to view the tasks you can perform. These include viewing and editing connection details, deleting a connection for a domain, changing the SSO authorization method, and notifying users that SSO is enabled.

Viewing SSO configuration details

About this task

The SSO connection details for a domain are available for review once SSO is set up. You can view the values you specified when setting up SSO, and the connection values assigned by HPE GreenLake Account Home.

Procedure

1. On the **Authentication** page, click the ellipsis (**...**) next to a domain.

   A domain name is listed only if you configured SSO for the domain.

2. Depending on the configuration data you want to review, select one of the following options:

- Click **View Details** to go to the domain SSO details page. The configuration values specified in the **Add Connection** wizard when you configured SSO are listed and can be updated by clicking **Edit Connection**.
- Click **Download Metadata File** to review the metadata that is exchanged between the IdP and HPE GreenLake Account Home to establish interoperability.

  The metadata XML file opens in a new tab. If you want to download the XML file to a local directory, right-click on the page then select **Save as.**
- Click **View SAML Attribute** to view the following SAML attributes defined for the SSO connection.

Value	Description
Entity ID	The entity ID specified for the SSO configuration.
Sign-On URL	The sign on URL specified during the SSO configuration.
HPE GreenLake Account Home Customer ID	The identifier assigned to the workspace where SSO is configured.
HPE GreenLake Account Home ID.	The HPE GreenLake Account Home identifier. This value is always 00000000-0000-0000-0000-000000000000.
Service	The name and identifier of each service available in the workspace.

Editing a SSO connection for a domain

Prerequisites

You must be a domain user to edit SSO connection details for the domain.

About this task

Once you have configured SSO, you can review and edit the SSO connection details if required. You cannot edit the **Domain Name** field or the URL for the **Entity ID**. If these values are incorrect, delete the existing SSO connection and create a new one.

Procedure

1. On the **Authentication** page, click the ellipsis (**...**) next to the domain you want to edit.
2. Click **View Details** to go to the domain SSO details page.
3. Click **Edit Connection** to edit the connection details.

   On the domain SSO details page, you can also delete the SSO connection, notify workspace users that SSO is enabled for their workspace, view the connection metadata in XML file format or change the type of authorization enabled for the SSO connection. Click the ellipsis (**...**) to view all the options available.
4. Update the SSO configuration details as required. For example, you might want to enable a recovery user account if you didn't do so previously.
5. Click **Save Changes** to save your updates or **Discard Changes** to delete them.

   Any changes you make are applied when SSO users next log in to the workspace. The changes do not impact SSO users who are currently logged in.

Updating x.509 certificate details for a SSO connection

About this task

When a SAML SSO connection is configured for a domain using the **Add SAML Connection** wizard, X.509 signing certificate details are uploaded for the identity provider (IdP). If you need to update the certificate details at a later time, for example, when the certificate is renewed, you can do so.

Procedure

1. On the **Authentication** page, click the ellipsis (**...**) next to the domain you want to update.
2. Select **View Details** to go to the domain SSO details page.
3. Click **Edit Connection**.
4. In the Identity Provider Information section of the domain page, update the details in the **X.509 Signing Certificate** field:
   a. Copy the updated certificate details and paste them into a text editor.
   b. Verify that the certificate does not include any extraneous white spaces at the end of each line.
   c. Copy the updated certificate details into the **X.509 Signing Certificate** field.
5. Click **Save Changes** to save your updated certificate details.

Considerations when changing the SSO authorization type

You can change the type of authorization used for an existing SSO connection by editing the connection on the **Authentication** page of the workspace. For example, you can edit the SSO connection to change from using session-based authorization to using static authorization. Before switching the authorization type for a workspace, keep in mind the following:

- Changing from static local authorization to session-based authorization.

  If you change to session-based authorization, existing SSO users are deleted from the workspace and can no longer access workspace resources. Workspace users who are currently logged in will also lose access to the workspace. To make sure users retain their access, configure the hpe_ccs_attribute on the identity provider to specify the roles a user should have on HPE GreenLake Account Home before switching to session-based authorization.
- Changing from session-based to static local authorization. The hpe_ccs_attribute is no longer used to authorize SSO users. You must create users and provision them with roles on HPE GreenLake Account Home. You can also choose whether or not any pre-existing users on HPE GreenLake Account Home are retained. For additional information on the options for managing pre-existing users, see **Changing the authorization method for a SSO connection**.

NOTE: When you switch the type of authorization used in a SSO profile for a workspace, the change is applied to any other workspaces where SSO is configured using the same domain.

Changing the authorization method for a SSO connection

About this task

When you configure a SSO connection for a workspace, you select the authorization method you want to use: either static local authorization or session-based authorization. If you want to change the type of authorization used for workspace users at a later date, you can do so. For information on the different types of SSO authorization, see **SSO authorization options**.

Procedure

1. On the **Authentication** page, click the ellipsis (**...**) next to a domain.

A domain name is listed only if you configured SSO for the domain.

2. Click **View Details** to go to the domain SSO details page.

   The configuration values specified in the **Add Connection** wizard when you configured SSO are listed.

3. To change the type of authorization used for the SSO connection, click the ellipsis (**...**) beside the domain name, then select **Change to session-based SAML authorization** (if static authorization is currently configured) or **Change to static local authorization** (if session-based authentication is currently implemented).

   A dialog is displayed describing the consequences of changing the authorization mode:

4. Review the information in the dialog and complete the fields available.

   - If you change to session-based SSO, all existing users who access the workspace through SSO are removed from the workspace and any SSO users who are currently logged in lose access. Once the authorization change process completes, when users next SSO log in to HPE GreenLake Account Home, they are created and assigned roles on a per-session basis according to the values defined in the HPE GreenLake Account Home SAML attribute.

     a. In the **HPE GreenLake Attribute** field, enter the name of the HPE GreenLake Account Home SAML attribute that is used to configure users and roles in the IdP. By default, the name is **`hpe_ccs_attribute`**.

     b. In the **Confirmation** field, enter **`CHANGE`** to confirm the change request. The SAML connection is updated to use session-based authorization.

   - If you change to static local authorization SSO, SSO users must be created and assigned roles on HPE GreenLake Account Home to have access to workspace resources. Existing SSO users might already exist on HPE GreenLake Account Home from previous SSO sessions. You can choose whether or not these pre-existing users are retained.

     NOTE: SSO users who are currently logged in are not affected by the retention option you select.

     a. In the Disposition of current users section, select one of the following options:

        I. **Least secure.** Select this option and all SSO users are retained with their existing role assignments. The access these SSO users have to workspace resources is not impacted.

        II. **More secure.** Select this option and all SSO users are retained but their existing role assignments are removed. You must create new role assignments for these users on the workspace so that they can continue to access workspace resources.

        III. **Most secure.** All existing SSO users are removed from the workspace. Re-create these users and assign roles to them if you want them to continue to have access to the workspace resources.

     b. In the **Confirmation** field, enter **`CHANGE`** to confirm the change request.

        The retention method you selected is applied and the SAML connection is updated to use static local authorization.

Deleting a SSO connection

About this task

You can delete a SSO connection that you configured for a domain if, for example, the domain name is incorrect or the entity ID is invalid.

WARNING: Deleting a SSO connection is irreversible. Make sure that deleting the connection will not interrupt users access to their workspaces before proceeding.

Procedure

1. On the **Authentication** page, click the ellipsis (**...**) next to the domain you want to edit.
2. Click **Delete** to remove the SSO connection set up for the domain.
3. Click **Delete** again to confirm the delete operation.
   The connection is deleted for the domain. Workspace users can no longer access the workspace using their SSO credentials for the domain that was removed.

Notifying users that SSO is enabled

About this task

Once SSO is enabled for a domain in a workspace, notify users that they must log in to the workspace using their SSO credentials. You can also notify users that SSO is enabled when you run the **Add SAML connection** wizard to create the SAML connection.

Procedure

1. On the **Authentication** page, click the ellipsis (**...**) next to the domain.
2. Select the **Notify Active Users** option.
3. In the **Notify All Active Users** dialog, click **Send Email**.
   All workspace users receive an email notification stating that SSO has been enabled for their account on HPE GreenLake Account Home and that they will now have to log in through their company's identity provider.

Specifying SAML configuration details for Microsoft Entra ID

About this task

When you have created a Microsoft Entra ID application for SAML SSO, configure the SAML information required to integrate with HPE GreenLake Account Home.

Procedure

1. On the **Set Up Single Sign-On with SAML** pane, click the Edit (pencil) icon on the Basic SAML Configuration section.
2. Enter the following values for the **Entity ID**, **Reply URL** and **Relay State** fields.

Field	Value
Identifier (Entity ID)	Enter the HPE GreenLake Account Home SSO sign-on URL: https://sso.common.cloud.hpe.com. This value is required for Microsoft Entra ID to exchange SMAIL receive and response token values for authentication purposes.
Reply URL (Assertion Consumer Service URL)	Enter the reply URL. Use this value: https://sso.common.cloud.hpe.com/sp/ACS.saml2.
Relay State	Enter a default relay state to indicate the URL users are redirected to after successfully signing in. Use this value: https://common.cloud.hpe.com. You must specify a Relay State URL if you are configuring an IdP-initiated SSO work flow in which the user is authenticated by the IdP before being redirected to HPE GreenLake Account Home.

Configuring SSO attributes and claims

About this task

When you have created a Microsoft Entra ID application for SAML SSO, define the attributes and claims required for Microsoft Entra ID users to sign in to HPE GreenLake Account Home using SSO authentication.

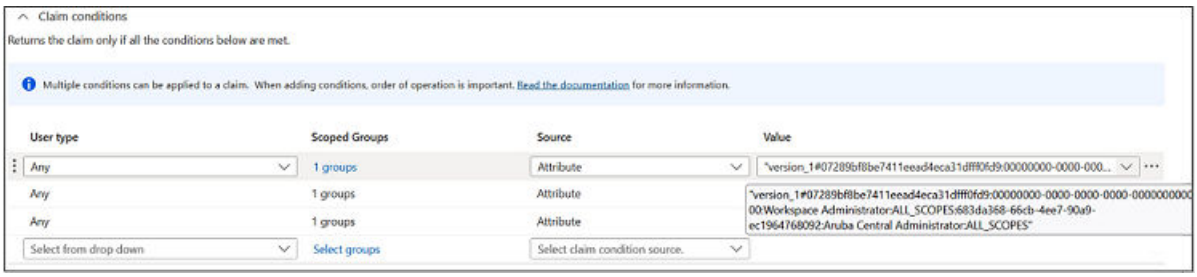
Procedure

1. In the Attributes & Claims section of the **Set Up Single Sign-On with SAML** pane, click the Edit icon.
2. Click **Add new claim**.
3. Enter values for each of the parameters shown in the table.

Field	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname
The attribute you use for the user's first name. The default value is FirstName.	SAML	user.givenname
The attribute you use for the user's last name. The default value is LastName.	SAML	user.surname
hpe_ccs_attribute	SAML	Multiple conditions

4. In the Attributes and Claims section, under Additional claims, click the **hpe_ccs_attribute** claim name. The hpe_ccs_attribute is used to specify the roles, responsibilities and workspaces each user who is part of a scoped group is assigned on HPE GreenLake Account Home when SSO is configured.

   The Manage claim console is displayed.



5. In the Claim conditions section, create a claim condition for each scoped group.

   For example, assume you have created three scoped groups in Microsoft Entra ID—Admin-homewarriors, Observer-homewarriors, and Operator-homewarriors—and you want to assign each group the following roles on HPE GreenLake Account Home.

   - Admin–homewarriors: HPE GreenLake Account Home Workspace Administrator and Aruba Central Administrator roles.
   - Observer–homewarriors: HPE GreenLake Account Home Workspace Observer and Aruba Central View Only roles.
   - Operator-homewarriors: HPE GreenLake Account Home Workspace Operator and Aruba Central Operator roles.

   Create a claim condition for each group using the following values for each claim condition.

   NOTE: The value you specify for each group must include the identifier of the workspace where the role assignments are to apply.

User Type	Scoped Groups	Source	Value
Any	Admin-homewarriors	Attribute	version_1#07289bf8be7411eead4eca31dfff0fd9:00000000-0000-0000-0000-000000000000:Workspace Administrator:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central Administrator:ALL_SCOPES
Any	Observer-homewarriors	Attribute	version_1#07289bf8be7411eead4eca31dfff0fd9:00000000-0000-0000-0000-000000000000:Workspace Observer:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central View Only:ALL_SCOPES
Any	Operator-homewarriors	Attribute	version_1#07289bf8be7411eead4eca31dfff0fd9:00000000-0000-0000-0000-000000000000:Workspace Operator:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092: Aruba Central Operator:ALL_SCOPES

NOTE: Make sure the claim condition values are entered correctly. For detailed information and examples of constructing the hpe_ccs_attribute, see **HPE GreenLake Account Home SAML attribute for SSO authorization**.

Downloading the SAML SSO XML token signing certificate

About this task

The last step in integrating Microsoft Entra ID with HPE GreenLake Account Home for SSO is to download the SSO metadata XML SAML token signing certificate. You import this metadata into HPE GreenLake Account Home later when you configure a workspace for SSO.

Procedure

1. In the SAML Certificates section of the **SAML-based Sign-on** pane, in the **Federation Metadata XML** row, select **Download** to download the SAML signing certificate.
2. Save the certificate file to be used later.

Verifying the SSO user has administrator privileges on HPE GreenLake Account Home

About this task

As a member of the Admin-homewarriors group in Microsoft Entra ID, the example user Pat Tracy is assigned administrator roles on HPE Aruba Networking Central and HPE GreenLake Account Home.

Administration users can invite co-workers to join a workspace; they can also assign roles and delete roles for users in the workspace. Verify that as an administrator user, Pat Tracy can perform these tasks.

Procedure

1. Navigate to the HPE **Sign In** page on **https://common.cloud.hpe.com**.
2. In the Username field, enter the name of the example user, for example: pat.tracy@homewarriorservices.com, then select the **Sign in with SSO** option.
3. On the **Sign In with Single Sign-On** page, enter the email of the example user, pat.tracy@homewarriorservices.com, then click **Next**.

   HPE GreenLake Account Home redirects the request to Microsoft Entra ID for SSO authentication.
4. Type in the user's password, then click **Sign In**.

   After Microsoft Entra ID successfully authenticates the user details you entered for user Pat Tracy, you can access the homewarriorservices workspace.
5. Verify that you can invite users to the workspace by clicking **Manage Workspace** on the Home page.
6. Click the **Workspace identity & access** card, then click **Users**.

   The **Invite users** option is available on the **Users** page.
7. Verify that you can assign and delete roles for users by selecting one of the users listed on the **Users** page, then click the ellipses (**...**) beside the user.

   The **Assign Roles** and **Delete Roles** options are displayed.
8. To confirm the roles Pat Tracy is assigned, select the user **Pat Tracy** from the list.
9. Click the ellipses (**...**) for the user and select **View Details**.

The details page shows that Pat Tracy is assigned the Aruba Central Administrator role and the HPE GreenLake Account Home Workspace Administrator roles.

10. Log out of the HPE GreenLake Account Home workspace.

Verifying the SSO user has access to HPE GreenLake Account Home with observer privileges

About this task

Perform the following steps to verify that when the example user, Pat Tracy, logs into HPE GreenLake Account Home using SSO, he has observer roles and privileges on the homewarriorservices workspace and no longer has administrator privileges.

Procedure

1. Log in to HPE GreenLake Account Home using the SSO credentials for the user Pat Tracy.

   When the user credentials are authenticated by Microsoft Entra ID, verify that the user can no longer perform the two administrator tasks, invite a user to the workspace, and add and remove roles for users, in the homewarriorservices workspace.

2. Navigate to the **Users** page.

   Note that the **Invite Users** option is not available.

3. Select a user from the list, then click the ellipses (**...**) for the user.

   Notice that the **Delete Roles** and **Assign Roles** options are not available.

4. On the **Users** page, select the example user, Pat Tracy then click the ellipses (**...**) and select **View Details**.

5. On the user details page, in the Roles region, notice that Aruba Central View Only and HPE GreenLake Account Home Workspace Observer roles are assigned to the user.
   You have now verified your SSO Microsoft Entra ID integration with HPE GreenLake Account Home.

Configuring SAML SSO using the Okta identity provider

The following configuration is an example of configuring SAML SSO using Okta as your IdP. Configuration steps differ if you use other IdPs.

Watch a video of this task on **HPE YouTube**.

To configure application metadata in Okta, complete the following steps.

- Create an Okta SAML application
- Configure Sign On settings
- Export the SAML 2.0 IdP metadata

Create an Okta SAML Application

1. Log in to the Okta administration console.
2. Click **Applications > Create App Integration**.
3. Select **SAML 2.0** and click **Next**.
4. Provide a name for the HPE GreenLake Account Home SSO service (Okta Application)

Configure Single Sign On Settings

1. Enter the SAML information on the General tab:

   - Single Sign on URL: **https://sso.common.cloud.hpe.com/sp/ACS.saml2**
   - Audience URI (SP Entity ID): **https://sso.common.cloud.hpe.com**
   - `Name ID format: EmailAddress`
   - `Application username: Email`
   - `NameID = user.email`
   - `FirstName = user.firstName`
   - `LastName = user.lastName`
   - `hpe_ccs_attribute` = See **HPE GreenLake Account Home SAML attribute for SSO authorization**

2. Click **Next** and select **Internal App**.
3. Click **Finish** to complete setup.

Export the SAML 2.0 IdP Metadata

1. Click **Next** – Configure the Sign On settings.
2. Scroll down to the SAML Signing Certificates section.
3. Click **Actions** and select **SHA-2** from the drop down menu.
4. Select **View IdP Metadata**.
5. Save the output to an **XML** file.

IdP Settings for Okta

Mark the box for IdP configuration.

SSO testing and troubleshooting

Procedure

1. On the HPE GreenLake Account Home **Sign In** page, click **Sign in with SSO**.
2. Enter your SSO credentials, and you are redirected to Okta to authenticate. After you successfully authenticate, you return to HPE GreenLake Account Home, where you can configure roles and permissions.

   Okta MFA example

   Okta, similar to other cloud identity providers, supports various MFA and other types of security policies.

   a. In Okta, click the **Factor Enrollment** tab and create an enrollment policy.

   b. Select the user groups you want this policy to apply to.

c. Click the **Factor Types** tab.

d. In the Okta Verify Settings region, make sure the **Enable Push Notification** option is selected. MFA enabled accounts are verified with push notifications

When the user attempts to log into HPE GreenLake Account Home they are sent a challenge through the Okta app. If this is the first log in, the user might need to enroll by installing the app and scanning a QR code. After that the user should only receive the push MFA notification.

SSO FAQ

Q: What if the SAML configuration is wrong, and I get locked out?

A: Log in using the recovery user account configured during the IdP configuration. The recovery user account bypasses the SAML federation.

Q: What do I do if I see the error `Metadata doesn't match with existing config`?

A: This error occurs if you configured the SSO domain successfully in a company workspace with metadata and you are now trying to configure the same domain in another company workspace with different metadata. This configuration is not supported. You must use the same domain and the same metadata across company workspaces. Try one of these two options to rectify the problem:

- Use the HPE GreenLake Account Home UI to delete the SSO configuration on the previous workspaces. You can then configure and claim the domain again with new metadata.
- Use the same metadata that you used for the previous configuration.

Q: What happens if the `FirstName` and `LastName` values are not configured for the optional SAML attributes?

A: If there is a mismatch in these values on the SP and IdP configurations, then you will see `UnknownFN`, `UnknownLN` displayed on the HPE **User Account Details** page.

Q: What do I do if I get the error `Bad Request` when I have configured the SSO domain and have clicked **Finish** at the last step?

A: Validate that all your inputs are correct. Check that the certificate you provided does not have any extra spaces, or newline or carriage returns, similar to this example:

MIIDyjCCArKgAwIBAgIGAYDjvKBNMA0GCSqGSIb3DQEBCwUAMIGlMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU …TIFt/6TyAwrP/Bbaa8vNcClScbHwwW5cGJNamoAwhhVjWsAyf56rLSjEUotXo1wwLMnq

Q: What do I do if I see the error `SSO Mode doesn't match with the one already configured for this domain`?

A: This error occurs if you have successfully configured a SSO domain in a workspace using one method of SSO authorization (either local or session-based) and you are now trying to configure the same domain in another workspace using a different method of authorization.

In an MSP environment, this error also occurs if you have configured a SSO domain in a workspace and are now trying to configure the same domain in another workspace using the same method of authorization but have chosen to apply the SSO profile to different targets. For example, if the original SSO profile was applied to the MSP workspace only and you attempt to create another profile with the same domain that is applied to tenant workspaces only.

Resolve the issue in either of the following ways:

- Switch to the workspace where you originally configured the SSO domain and delete the SSO connection set up for the domain. You can then configure and claim the domain again with your desired method of SSO authorization and, for MSP workspaces, your desired target workspaces.
- In your current workspace, select the same method of SSO authorization that you used in the original configuration and for MSP workspaces, the same target workspaces.

Q: I have configured SSO in a workspace but when I sign in to HPE GreenLake Account Home using my SSO credentials, the workspace is not available to launch. Why?

A: The cause of this error differs depending on the type of authorization selected during the SSO configuration.

- If you selected the local authorization option when you configured SSO, then make sure that the users have been invited to the workspace. If you cannot access the workspace, sign in using the recovery user account credentials specified during the SSO configuration. The recovery user account bypasses the SAML SSO federation.
- If you selected the session-based authorization option when you configured SSO, check that the hpe_ccs_attribute is specified correctly and includes the correct workspace identifier for the workspace where you configured SSO.

Q: After configuring SSO in my workspace, why can't I change the roles assigned to my SSO users.

A: When session-based SSO authorization is implemented, all roles are managed by the hpe_ccs_attribute. To change a user's role assignments, change the hpe_ccs_attribute for the user. If you want to be able to assign roles to users manually, change the SSO authorization method selected in the SSO configuration to local authorization.

API access

HPE GreenLake Account Home allows developers to make API requests to the platform and service instances. Using the personal API client functionality, you can create a client ID and client secret for specific service instances that are then used to generate an access token. You add the token to an API request header to make API requests.

A personal API client allows programmatic access to HPE GreenLake Account Home. Personal API clients inherit the permissions of the HPE GreenLake Account Home user or administrator that creates the personal API client. For example, if an API call requires edit permissions, the user or administrator who created the personal API client must have edit permission for that resource.

- All users can see the personal API clients in the current workspace for which they are the owner.
- Certain administrator users assigned specific permissions can be view, update, or delete personal API clients for all other users in a workspace. Refer to Managing workspace APIs.

NOTE: To learn more about HPE GreenLake Account Home roles and permissions, see **Roles & Permissions.**

HPE GreenLake Developer Portal

HPE GreenLake Developer Portal lists all available HPE GreenLake Account Home APIs and includes guides and reference documentation. To learn more, see or go directly to the **HPE GreenLake Developer Portal** to browse the API documentation.

Creating a personal API client

About this task

By creating a personal API client, you create the client ID and client secret used to access HPE GreenLake Account Home or another service's APIs. The client ID and client secret are used to generate an access token. An access token authenticates API communication between your application and HPE GreenLake.

Each user can create a maximum of seven personal API clients per workspace.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **API access**.
3. Click **Create personal API client**.
4. In **Name**, enter a name for the API client.
5. (Optional) In **Description**, add a short description outlining the purpose of the API client.
6. Select the **Service** that you want to access.
   Choose **HPE GreenLake Cloud Platform** to access APIs related to:
   - Data Services
   - HPE GreenLake Account Home services (for example, Audit Logs, Devices, Reporting, User Management, and so on)
   - HPE Compute Ops Management
   - HPE Consumption Analytics
   - HPE Sustainability Insight Center
7. Click the **Create personal API client** button to continue.
   The **Personal API client created** dialog appears, confirming that your credentials were successfully created.
8. Click **Copy** next to **Issuer URL**, **Client ID**, and **Client Secret** and save both to a safe and secure location.

   NOTE: HPE GreenLake Account Home does not store your client secret. If it is lost, you need to **reset your client secret**.

   When storing the client secret, do not assert a maximum or fixed length. Refer to **Client secret length**.
9. Click **Close** to continue.
   You are returned to the main **API access** page, where you can generate the access token.

Generating an access token

Prerequisites
You must have created a personal API client and have copied or stored the client secret.

About this task

On the **API access** page, you can view API credential details, generate access tokens, and delete personal API clients.

Access tokens are small strings of code sent in the header of your API calls. Access tokens identify whether you (or your application) have the necessary permissions to access resources securely through an API call. Access tokens inherit the permissions of the user that created the personal API client.

- In a standard enterprise workspace or in a tenant workspace, the access token applies automatically to the workspace of the logged-in user.
- In Managed Service Provider (MSP) mode, all MSP roles can configure access tokens to apply to the MSP mode workspace or to a tenant workspace.

HPE GreenLake Account Home tokens stay valid for 15 minutes. Tokens for all other HPE service managers stay valid for 120 minutes.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **API access**.
3. Click a personal API client name to go to the details page.
4. Click **Actions** > **Generate access token**.
   The **Generate access token** dialog appears. The options depend on your workspace type. Only MSPs require and see the option **Generate access token for access to workspace**.
5. From **Generate access token**, perform the following steps.
   a. The **Client ID** is prepopulated with the client ID.
   b. Paste the `client secret` into the **Client secret** field.
   c. (MSP-only) From the **Generate access token for access to workspace** drop-down, choose, or search for the workspace for which to create the access token. In MSP mode, you can choose to generate a token for the MSP workspace or a tenant workspace.
      API requests that are made using this access token can only retrieve results from or affect the chosen workspace.
6. Click **Create access token**.
   The **Access token created** dialog appears with your **Access token**.
7. Click **Copy** next to your access token.

   NOTE: HPE GreenLake does not store tokens. Therefore, you must copy and store your access token in a secure location.
8. Click **Close** when you are finished.

   NOTE: The access token can be used as an authorization bearer token to make secure REST API calls to HPE GreenLake API services. For example, if using cURL, include `-H 'Authorization: Bearer <YOUR_JWT_HERE>'` in your API request header. Replace `<YOUR_JWT_HERE>` with your token. The API reference documentation on **HPE GreenLake Developer Portal** provides example request headers, endpoint details, and instructions on how to make the API request.

Viewing code samples for generating an access token

About this task

You can generate access tokens programmatically. You can create sample code from the HPE GreenLake UI for this purpose.

Access tokens remain valid for limited periods.

- In a standard enterprise workspace or in a tenant workspace, the access token applies automatically to the workspace of the logged-in user.
- In Managed Service Provider (MSP) mode, all MSP roles can configure access tokens to apply to the MSP mode workspace or to a tenant workspace.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Personal API client**.

3. Click the arrow next to the personal API client name to display the details.
4. Click **View code sample**.
   The **Generate code sample** modal appears. The options in the **Generate code sample** modal depend on your workspace type. Only Managed Service Providers (MSP) require, and see the option **Produce sample for accessing**.
5. From the **Generate code sample** modal, perform the following steps.
   a. (MSP-only) From the **Produce sample for accessing** drop-down, select the target workspace. In MSP mode, you can choose to generate a token for the MSP workspace or a tenant workspace.
      The resulting code sample generates an access token applicable to the chosen workspace.
   b. From the **Select programming language** drop-down, select the programming language.
   c. **Personal API client** is always prepopulated with the name given to the personal API client.
   d. Paste the `client secret` into the **Enter client secret** field.

   The information you selected or entered is displayed in the code sample.
6. Click **Copy code sample**. The copied code sample can be used to generate an access token programmatically.
7. Click **Close** when you are finished.

NOTE: The access token can be used as an authorization bearer token to make secure REST API calls to HPE GreenLake API services. For example, if using cURL, include `-H 'Authorization: Bearer <YOUR_JWT_HERE>'` in your API request header. Replace `<YOUR_JWT_HERE>` with your token. The API reference documentation on **HPE GreenLake Developer Portal** provides example request headers, endpoint details, and instructions on how to make the API request.

Resetting your client secret

About this task

There may be a time when you want to reset your client secret for security purposes.

Procedure

1. Click the ellipsis ⋮ next to the **Generate access token**, then select **Reset client secret**.
2. Click **Reset client secret**.
   The **Personal API client secret reset** dialog appears.
3. Click **Copy** next to the **Client secret**.

NOTE: Save the client secret in a secure location, as HPE GreenLake Account Home does not store the client secret.

When storing the client secret, do not assert a maximum or fixed length. Refer to **Client secret length**.

4. Click **Close**.

Deleting a personal API client

Procedure

1. Click the ellipsis next to the **Generate access token**.
2. Select **Delete personal API client**.
   The **Delete personal API client** display appears.
3. Click **Delete personal API client**.

NOTE: If a user is deleted from HPE GreenLake Account Home, any personal APIclients generated and associated with any services owned by this user will not be valid.

Tags

A tag is a form of metadata applied to resources and is primarily used to categorize resources based on purpose, owner, environment, or other criteria. In HPE GreenLake Account Home, a tag has two parts: a tag name and a tag value.

You create and assign tags directly at the resource level, either during setup or later on. After a tag is created, it is stored centrally and can then be assigned to any other resources that support tagging. For example, if you create a tag while onboarding a device, you can then assign the same tag to the device subscription.

After tags are assigned to resources, you can filter and search for the resources by tag name or value.

The **Tags** page is an overview of all tags that have been created in your workspace. You can see how many resources a tag has been assigned to and you can view details of the individual resources.

The following resources support tags:

Resource	For more information about
Devices	• Assigning tags during device onboarding, see **Adding managed devices**. • Managing device tags, see **Managing tags for devices**.
Device subscriptions	• Assigning tags during device subscription setup, see **Adding device subscriptions to your workspace**. • Managing device subscription tags, see **Managing tags for subscriptions**.
Service subscriptions	• Assigning tags during service subscription setup, see . • Managing service subscription tags, see **Managing tags for subscriptions**.
Locations	• Assigning tags while adding locations, see . • Managing location tags, see .

Tag specifications

HPE GreenLake Account Home supports the following specification for tags:

NOTE: You should not store any Personal Identifiable Information (PII) in tags.

- Up to 50 tags can be assigned to a single resource.
- Tag names and values are not case-sensitive.
- Only one value can be assigned to each tag name for a single resource. For example, you could assign only one of the following tags to a particular device: **location: building 1**, **location: building 2**.
- A tag name can have between 1–128 characters.
- A tag name cannot be empty or blank.
- A tag value can have up to 256 characters.
- A tag value can be empty or blank. For example, if you want to use tags as labels, you can create tag with a name and no value.
- You cannot use **hpe** for a tag name because it is used for system tags. You can, however, use **hpe** within a tag name. For example, **hpe device: abc** is a valid tag.
- Allowed characters are letters, numbers, spaces representable in UTF-8, and the following characters: _ . : = + - @.

Viewing all tags in your workspace

About this task

The **Tags** page is an overview of all tags in your workspace. You can view all tags in your workspace and see which resources a tag is assigned to. This workspace overview can help you check if a tag has been assigned consistently across different resources.

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu ☰.
2. Select **IAM and administration** > **Tags**.
   The **Tags** page opens showing the number of resources assigned to each name-value pair.
3. To search for a specific tag, enter the name or value in the search box.
4. To see the list of resources that a tag is assigned to select the tag row.
   The **Resources** page opens, showing all resources that the tag is assigned to.
5. To see the detail page for a specific resource, click the **Detail** link.
   The **Details** page for the resource opens. The **Tags** section shows all tags that have been assigned to that resource.
6. To return to the **Tags** page from the **Details** page:
   a. Click the **Global navigation** menu ☰.
   b. Select **IAM and administration** > **Tags**.

Managing tags in your workspace

About this task

The **Tags** page shows how many resources that a particular tag is assigned to. You can see which resource types that a particular tag has been assigned to. You can also see the details of each resource and manage tags for individual resources.

You can bulk manage tags for a resource at the resource level (for example, if you want to add the same tag to several devices). For more information, see:

-
- **Managing tags for devices**
- **Managing tags for subscriptions**

Procedure

1. On the HPE GreenLake Account Home header, click the **Global navigation** menu .
2. Select **IAM and administration** > **Tags**.
   The **Tags** page opens showing the number of resources assigned to tag.
3. Click the row for the tag that you want to manage.
   The **Resources** page opens, showing all resources that the tag is assigned to.
4. To manage the tags for a specific resource, click the **Detail** link.
   The **Details** page for the resource opens. The **Tags** section shows all tags that have been assigned to that resource.
5. To manage tags for the resource, click **Actions** > **Manage tags**.
   The **Manage tags** dialog appears.
6. To assign a tag:
   a. Select an existing tag name or create a name.
   b. (Optional) Select an existing tag value or create a value.
   c. Click **Assign**.
   d. Repeat to add more tags.
      You can assign up to 50 tags.
7. To remove a tag, click the **x** icon for the tag.

   NOTE: If the tag is not assigned to any other resources, it is deleted from the workspace.
8. To apply the changes, click **Save**.

The **Tags** section is updated with the changes.