Hitachi Content Platform Anywhere Enterprise

v8.0

Portal Team Administration Guide

This document describes how to administer teams using HCP Anywhere Enterprise Portal to manage files securely and provide other users with access to these files.

MK-HCPAE002-01
December 2023

Contents

Contents

Preface

About this document

This book describes Hitachi Content Platform Anywhere Enterprise Portal for a team administrator. HCP Anywhere Enterprise Portal is a scalable cloud service delivery platform that you use to create, deliver and manage cloud storage applications, including a Global File System and file access via stubbing/caching. HCP Anywhere Enterprise Portal enables you to extend the Global File System to endpoints; HCP Anywhere Enterprise Edge Filers, Drive Share and Drive Connect. The HCP Anywhere Enterprise Portal ensures data consistency, maintains version history, and facilitates file sharing among users, regardless of their access method. Both global source-based deduplication and data compression are used to ensure that only incremental data changes are transferred for storage in the cloud, and that data blocks are stored only once. This dramatically reduces storage capacity needs and overall network traffic.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. • Indicates emphasized words in list items.
Italic	Indicates a document title or emphasized words in text.
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Intended audience

This document is intended for HCP Anywhere Enterprise Portal team administrators.

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: https://support.hitachivantara.com/.

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Getting Help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Chapter 1. Introduction to Team Administration

HCP Anywhere Enterprise Portal is a scalable cloud service delivery platform that you use to create, deliver and manage cloud storage applications, including a Global File System and file access via stubbing/caching.

HCP Anywhere Enterprise Portal enables you to extend the Global File System to endpoints; HCP Anywhere Enterprise Edge Filers and HCP Anywhere Enterprise Drive Connect. The HCP Anywhere Enterprise Portal ensures data consistency, maintains version history, and facilitates file sharing among users, regardless of their access method. Both global source-based deduplication and data compression are used to ensure that only incremental data changes are transferred for storage in the cloud, and that data blocks are stored only once. This dramatically reduces storage capacity needs and overall network traffic.

HCP Anywhere Enterprise Portals and endpoints are centrally managed from HCP Anywhere Enterprise Portal using a single web-based console. Template-based management, centralized monitoring, customized alerting and remote software and firmware upgrade capabilities make it easy to manage HCP Anywhere Enterprise Edge Filers of various types and sizes as well as individual endpoints – up to hundreds of thousands of connected devices – with no need for on-site IT presence in remote locations.

A team portal, also referred to as a virtual portal, is designed for the needs of a company or team with multiple members. The users in the portal are the team members. Team portals are managed by team administrators, who are team members with the Administrator role.

All users in the team portal share, by default, a single folder group, enabling cooperative deduplication between all members of the group. Furthermore, when the cloud drive feature is used, each user receives, by default, one personal folder, and can create multiple additional personal folders. Users can share personal folders. Each user also receives access to a projects folder that is visible to all the users in the portal. Users can create projects to collaborate with other team members.

In this chapter

Management Features

With the HCP Anywhere Enterprise Portal, you control all aspects of cloud storage, including:

- **Service Provisioning**
  Manage from tens to hundreds of thousands of subscribers. Control user access, subscription plans per user account, and view real-time storage usage and account status.
  Note: Add-ons are managed by the global administrator.
- **User Management**
  Manage anywhere from tens to hundreds of thousands of subscribers. Control user access,

subscription plans, and add-ons per user account, and view real-time storage usage and account status.

- **Remote Device Management and Monitoring**
  Manage HCP Anywhere Enterprise Edge Filers and HCP Anywhere Enterprise Agents remotely. This enables you to view the device status in detail, including logged events, network status, and storage volumes, as well as to set firmware upgrades, and more.
- **Real-Time Event Monitoring**
  Centrally monitor and audit all events pertaining to the cloud service.
- **Reporting**
  Run and export detailed reports on a variety of usage parameters, including storage usage, bad files, snapshot status, and more. Generate user reports that are automatically emailed as PDF attachments.

Security

HCP Anywhere Enterprise Portal incorporates multiple layered security features to ensure that your data is protected whether in transit or at rest:

- You can deploy the HCP Anywhere Enterprise Portal either on-premise or in a virtual private cloud (VPC) to keep your data within your network and 100% behind your firewall.
- HCP Anywhere Enterprise Portal uses cryptographic libraries certified with FIPS 140-2.
- All data is encrypted before it is sent to the cloud using AES-256 encryption and remains encrypted as it is stored.
- All WAN transfers use Transport Level Security (TLS) protocol over the WAN, preventing unauthorized interception of data transfers.
- Manage your own encryption keys or use personal passphrases per user to prevent privileged administrators from accessing data. Password policy enforcement ensures that passwords have a minimum length and complexity, and that the password is changed frequently.
- Use email and SMS-based two-step authentication for external file sharing to ensure only intended parties can access files. You define rules based on file size, name, or type that deny or allow files to be shared externally or uploaded to your network.
- HCP Anywhere Enterprise Portal provides role-based access control, using Active Directory or LDAP roles and groups to control access to data and set up administrator roles.
- HCP Anywhere Enterprise Portal interfaces with Single Sign-On (SSO) management tools to provide seamless user authentication and avoid duplicate credentials.
- HCP Anywhere Enterprise Portal integrates with leading Anti-Virus tools to ensure that security and governance follow the data.

Devices

HCP Anywhere Enterprise Portal connects to the following devices:

- <u>HCP Anywhere Enterprise Edge Filers</u>
- <u>HCP Anywhere Enterprise Drive Share (Agents)</u>
- <u>HCP Anywhere Enterprise Drive Connect</u>

Throughout this guide, the term device refers generically to any of the above devices.

HCP Anywhere Enterprise Edge Filers

HCP Anywhere Enterprise Edge Filers are appliances that seamlessly combine local storage, cloud storage, data protection functionality and collaboration capabilities in a single, cost-effective package. Ideal for enterprise branches, SMBs and remote offices, HCP Anywhere Enterprise Edge Filers can replace legacy file servers with significant cost savings.

HCP Anywhere Enterprise Edge Filers feature a full set of Network Attached Storage (NAS) capabilities and comprehensive sync and share functionalities, utilizing on-premises storage capabilities for speed and local sharing, while taking advantage of cloud storage for universal access, file sharing, and folder synchronization.

HCP Anywhere Enterprise Edge Filers are managed remotely by HCP Anywhere Enterprise Portal. Template-based management and remote firmware upgrades make it possible to manage numerous HCP Anywhere Enterprise Edge Filers while maintaining minimal on-site IT and reducing total cost of ownership.

See HCP Anywhere Enterprise Edge Filer documentation.

HCP Anywhere Enterprise Drive Share (Agents)

HCP Anywhere Enterprise Agents are small-footprint software agents that provide both cloud backup and enterprise file sync and share (EFSS) functions. HCP Anywhere Enterprise Agents can connect either directly to the cloud or to a HCP Anywhere Enterprise Edge Filer.

HCP Anywhere Enterprise Agents are available for Windows and Mac platforms, and are licensed for either laptop/desktop use or for servers. In all cases they provide file sync and backup capabilities. When connected to a HCP Anywhere Enterprise Edge Filer.

HCP Anywhere Enterprise Agents can be managed remotely by HCP Anywhere Enterprise Portal, where all aspects of sync and agent setup can be monitored and configured from a single console, including software upgrades.

HCP Anywhere Enterprise Drive Connect

HCP Anywhere Enterprise Drive Connect enables you to easily view all your files in the HCP Anywhere Enterprise Portal Global File System in Windows File Explorer or macOS Finder. Using HCP Anywhere Enterprise Drive Connect you mount your HCP Anywhere Enterprise Portal cloud drive as a disk in Windows File Explorer or macOS Finder so you can work on it as a local volume.

HCP Anywhere Enterprise Drive Connect caches content from the portal so that all your cloud drive content in the portal, cloud folders you own and the files and folders shared with you under Shared With Me, are presented as stubs on your local disk, with ACLs fully supported.

See HCP Anywhere Enterprise Drive Connect documentation.

Provisioning

Provisioning is the process of assigning services and quotas to users.

The team HCP Anywhere Enterprise Portal owner provisions end users with services and quotas, such as storage space and the number of HCP Anywhere Enterprise Agents. End-user provisioning is optional and is performed by team administrators.

End users must be subscribed to a subscription plan in order to obtain services. The subscription plan includes the list of services provided to the user and the quota for each service.

If a subscription plan or add-on is modified, all user accounts assigned to the plan or add-on are updated with the changes.

Note: Add-ons are managed by the global administrator.

For more details, see Provisioning.

Chapter 2. Getting Started

This chapter describes how to get started with the HCP Anywhere Enterprise Portal.

In this chapter

Browser Requirements

In order to use the HCP Anywhere Enterprise Portal, you need an Internet browser. You can use any of the latest two releases of Apple Safari, Google Chrome, Microsoft Edge, and Mozilla Firefox.

The Administration Interface

HCP Anywhere Enterprise Portal provides an administration web interface for configuring and monitoring the team, virtual, HCP Anywhere Enterprise Portal, including:

- Setting up zones so that only the relevant subset of the global file namespace is accessible by each edge location.
- Provisioning the team, virtual, HCP Anywhere Enterprise Portal.
- Managing users, including from a directory service, such as Active Directory.
- Setting up single sign-on (SSO) to the HCP Anywhere Enterprise Portal.
- Protecting the data, for example from viruses.
- Managing edge devices.

Signing In To the Administration User Interface

As an administrator, you have access to the administration Web interface. This interface lets you perform administration tasks for the HCP Anywhere Enterprise Portal.

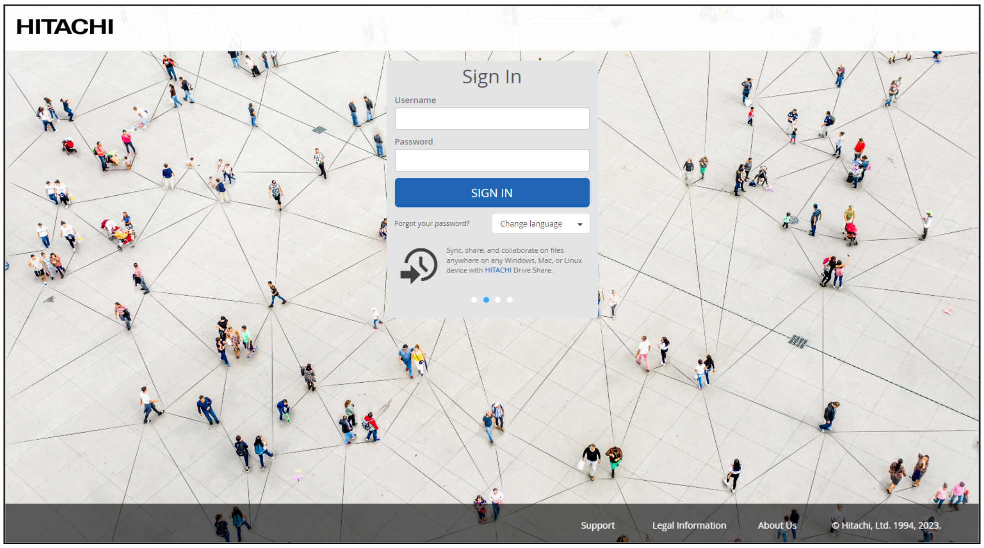
To sign in to the administration interface you use the IP address of the portal server. If the DNS service is set up, you can use it with the portal's DNS suffix and, if changed from the default, the HTTPS access port number.

To sign in to the administration user interface:

1. In a Web browser open `http://`*`virtualportal_name.DNS_Suffix`*`/ServicesPortal`
   where, *virtualportal_name* is the name of the virtual portal, and *DNS_Suffix* is the DNS suffix for the HCP Anywhere Enterprise Portal installation.
   The interface to the specified portal is displayed.
   Note: If the HCP Anywhere Enterprise Portal is set to redirect HTTP requests to HTTPS, HCP Anywhere Enterprise Portal redirects the browser to the HTTPS page. It is also

possible to set the HTTPS access port to be different from the standard 443. In this case, the address is:
`https://`*`virtualportal_name.DNS_Suffix`*`:`*`HTTPS_port`*`/ServicesPortal`
where *HTTPS_port* is a customized port.
For example, to connect to *Example*'s administration HCP Anywhere Enterprise Portal using HTTPS port 9443, use the following address:
`https://example.hcp.com:9443/ServicesPortal`.

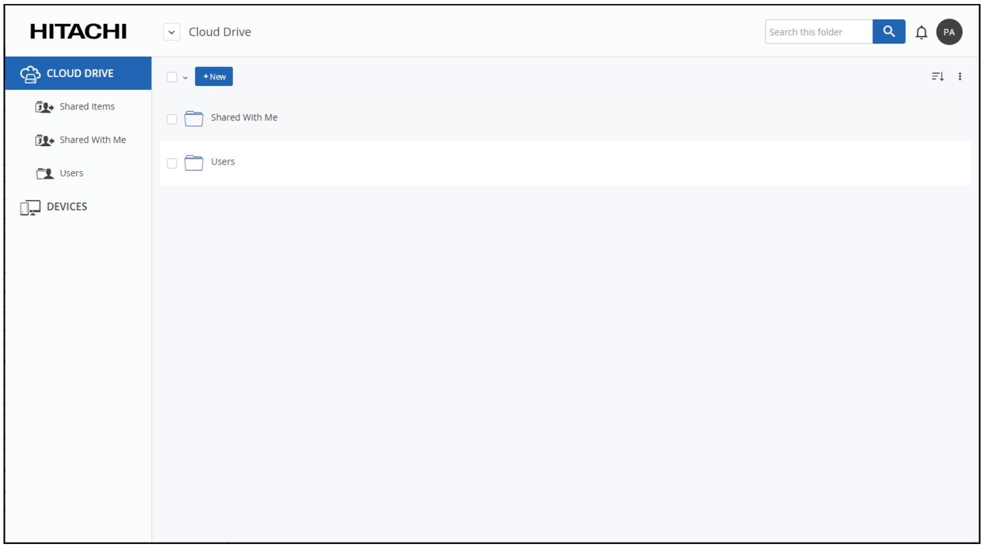
The HCP Anywhere Enterprise Portal opens, displaying the sign in page.



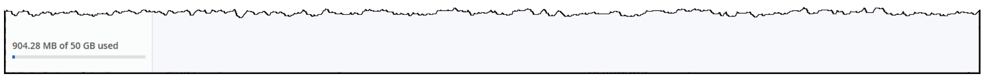
If Single Sign-on (SSO) is enabled, on your first access to the HCP Anywhere Enterprise Portal you are redirected to the SSO identity provider's login page. On subsequent log ins, you directly access the HCP Anywhere Enterprise Portal.
If CAC, Common Access Card, is implemented at the site, the login page is skipped if the card access is authorized.

2. Enter your administrator user name and password and click **SIGN IN**. If you are redirected to an identity provider's login page, enter your credentials there. The identity provider processes your authentication.

   The team administrator end user interface is displayed.

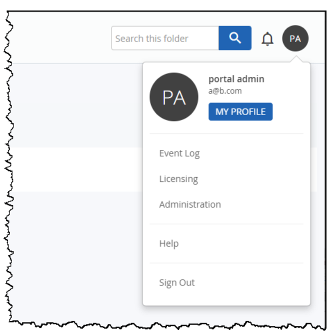


Note: The first time you sign in to the HCP Anywhere Enterprise Portal, a short tutorial starts, to guide you through using the HCP Anywhere Enterprise Portal.
If the global administrator has set a storage quota for you, this quota and the current usage is displayed at the bottom of the screen.



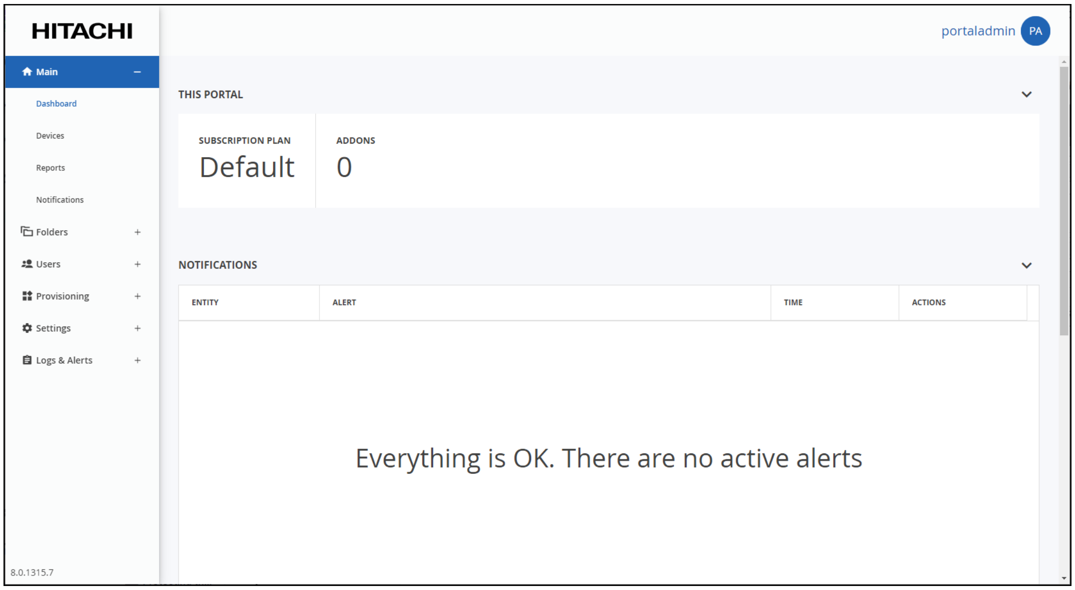
An administrator has options to manage the end users in this view, as described in Administration Options In the End User Interface.

3. To access the full administrator interface, click the avatar at the top right, or your initials, if you have not yet configured an avatar, and select **Administration**.

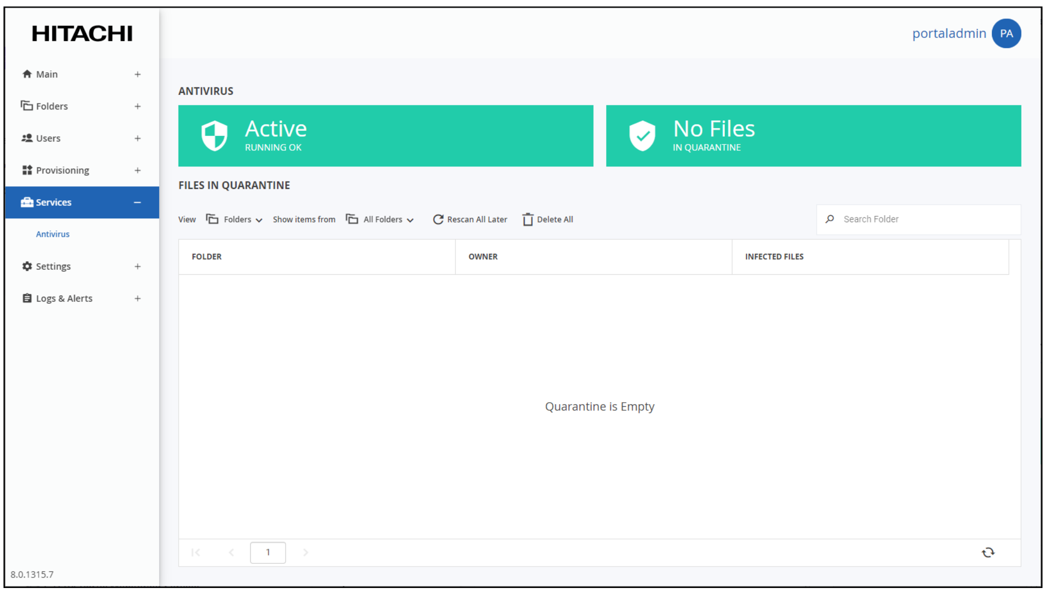


Note: Configuring an avatar is described in Changing Your Personal Details.

The administration interface opens in a new tab, displaying the **Main > Dashboard** page of the HCP Anywhere Enterprise Portal.



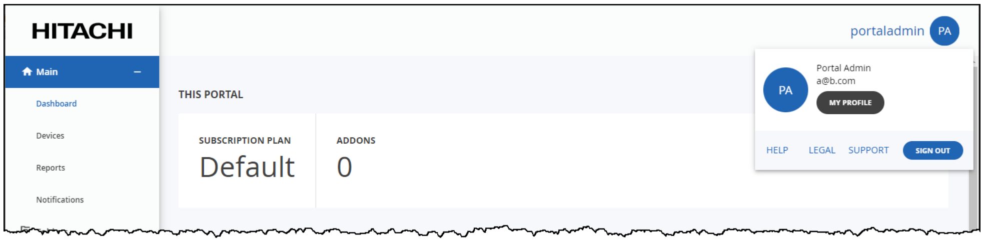
If the portal is licensed for antivirus functionality and the default provisioned plan in the global administration includes the antivirus service, the navigation pane includes a **Services** option.



Using the Administration User Interface

The HCP Anywhere Enterprise Portal interface consist of the following elements:

Top bar – The user name at the top right. Clicking the graphic next to the name displays additional controls, such as access to the portal documentation.



Navigation Pane – To navigate between pages in the HCP Anywhere Enterprise Portal.

Content – Displays the HCP Anywhere Enterprise Portal pages.

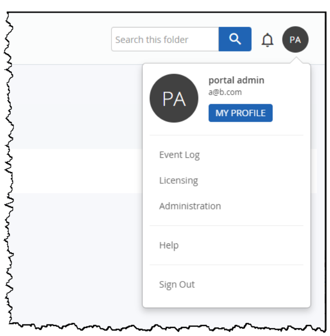
Changing Your Personal Details

You can configure the following personal details in your profile details in the end user interface:

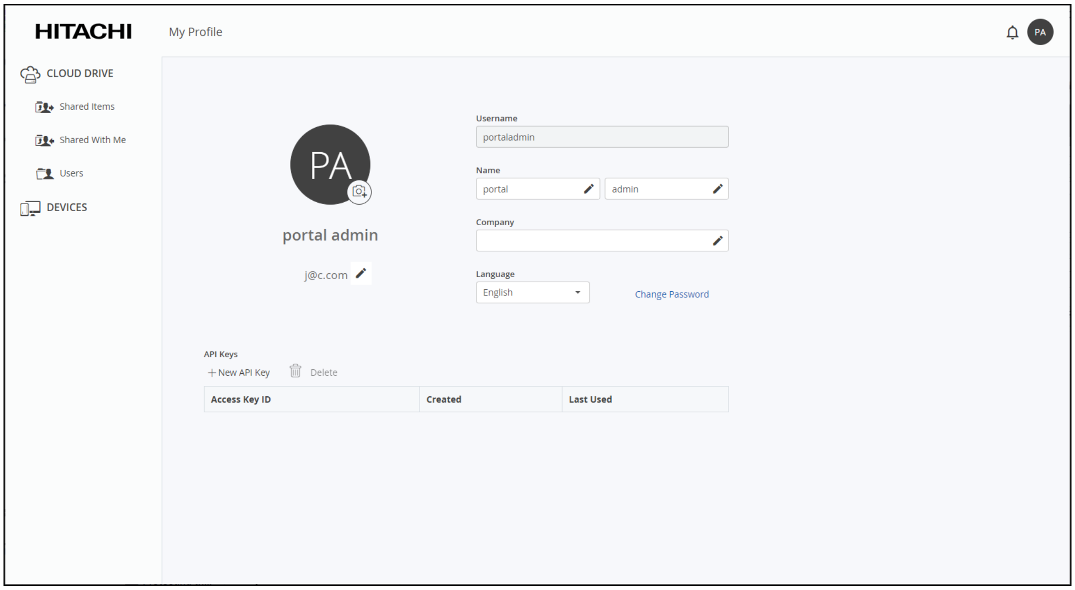
- Add or change the avatar used to identify you. If an avatar is not used, your initials are used.
- Your email address.
- Your first and last name. If you do not have an avatar, the initials of the first and last name are used.
- Your company.
- Your language for the user interface, described in Changing the User Interface Language.
- Your password, described in Changing Your Password.

To configure your user profile:

1. Click your avatar or initials in the upper-right corner and in the menu, click **MY PROFILE**.



The **My Profile** page is displayed.



Note: If Single Sign-on (SSO) is enabled, the **Change Password** option is not available.

2. You can upload an avatar by clicking and selecting your picture. The picture must be a JPEG or PNG file.

   The avatar is displayed instead of your initials.

3. To change information, click by the item to change, enter the change and click ✓ to confirm the change.

   Note: To change your email address you have to enter the and user password to the HCP Anywhere Enterprise Portal and then confirm the email change after receiving a verification email to the new email address.

To exit your profile, click on one of the options in the navigation bar.

Changing the User Interface Language

You can change the user interface language from the **My Profile** page.

Note: You can also change the language in the sign in page

To change the user interface language:

1. Click your avatar or initials in the upper-right corner and then in the menu click **MY PROFILE**.
2. Select the desired language in the **Language** drop-down list.

After a few seconds, the interface is refreshed with the chosen language.

Changing Your Password

Note: A user accessing the HCP Anywhere Enterprise Portal using Active Directory or Single Sign-on (SSO), cannot change the password from this page, but must contact the system administrator.

If access to the HCP Anywhere Enterprise Portal is by a local user, You can change your password from the **My Profile** page.

To change the password used to access the HCP Anywhere Enterprise Portal:

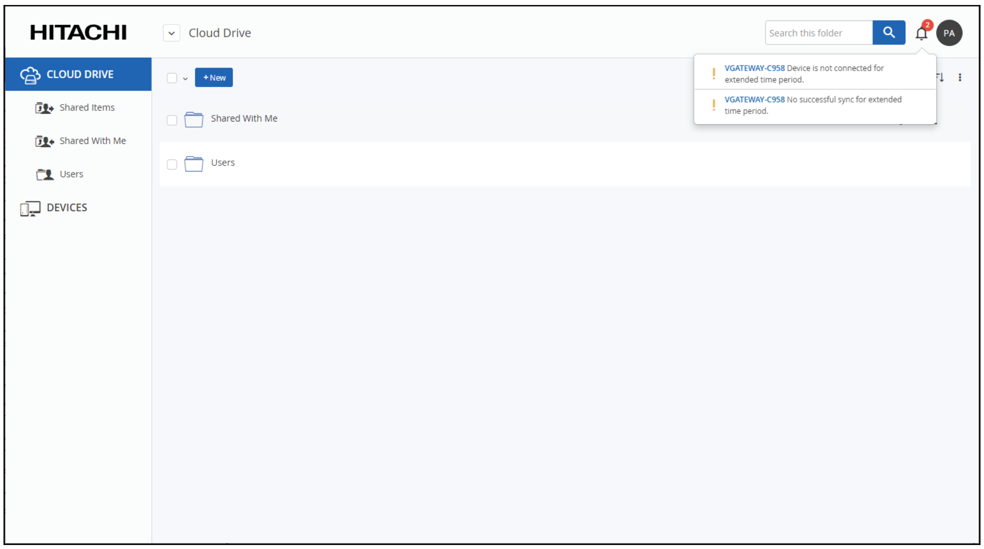
1. Click the avatar in the upper-right corner, and then in the menu click **MY PROFILE**.
2. Click the **Change Password** link.

   The **Change Password** window is displayed.
3. Complete the fields, then click **Change Password**.

Chapter 3. Administration Options In the End User Interface

Viewing Notifications

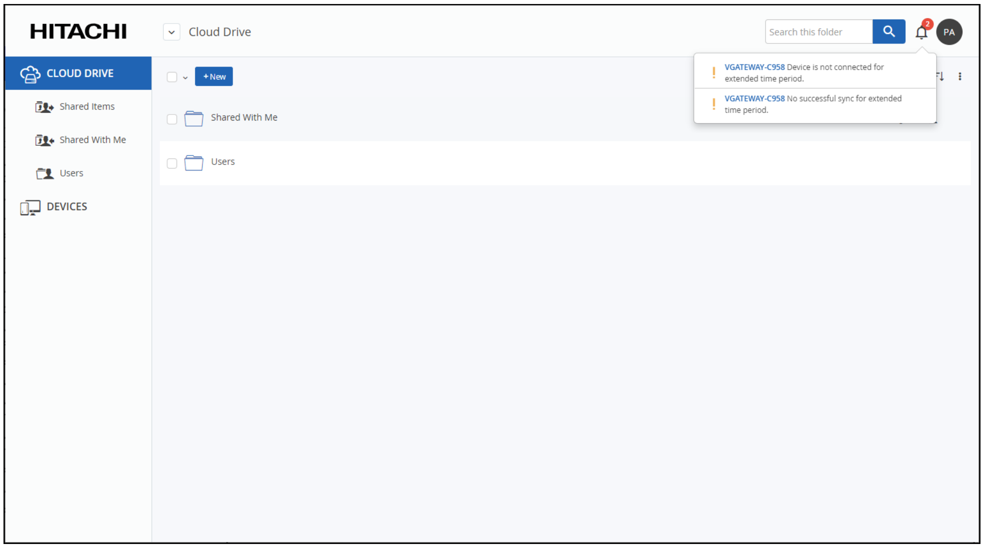
When there are notifications, the number is displayed on the notifications icon in the end user interface. Clicking the notifications  icon displays a list of notifications.



Clicking a notification in the list opens the device details to investigate the cause of the notification.

The End User Interface Navigation Pane

CLOUD DRIVE



The **CLOUD DRIVE** option in the navigation pane contains folders and files. You can add as many folders or files as you like to the cloud drive, but the **Shared Items**, **Shared With Me**, and **Users** options are available by default. If the global administrator set you up with a home folder, the default being **My Files**, then this folder contains your most frequently used content and is automatically synced to the cloud when HCP Anywhere Enterprise Agent is installed on your computer.

Shared Items

The **Shared Items** option displays all the shared items by the administrator.

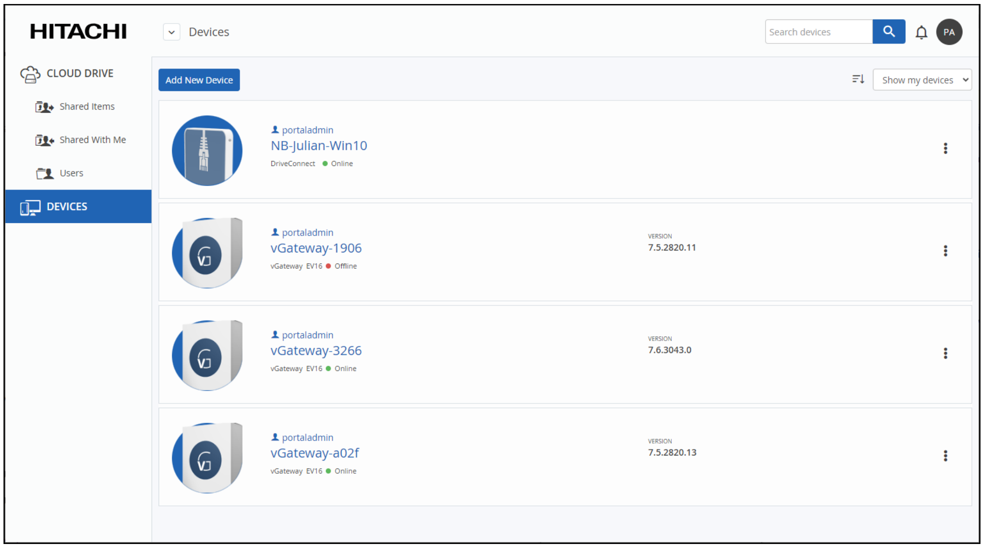
Shared With Me

The **Shared With Me** option displays all of the content that other users have shared with you.

Users

An administrator with the Read Only Administrator role can see the users and the folders for each user. An administrator with the Read/Write Administrator role can also manage the user folders and files as that user.

DEVICES



The end user HCP Anywhere Enterprise Portal displays all devices connected to the HCP Anywhere Enterprise Portal that you are managing.

To manage a device as an administrator, see Managing Devices From the End User Portal View.

Actions That Can Be Performed on Folders and Files

As an administrator, you can perform the same actions as an end user on folders and files, such as copying, moving and deleting folders and files. In addition, you can Permanent Deletion content to comply with company, national, and international data protection regulations, such as GDPR.

Permanent Deletion

You can permanently delete end user files and folders. Only a single permanent deletion operation can be performed per cloud drive and not multiple permanent deletions in parallel.

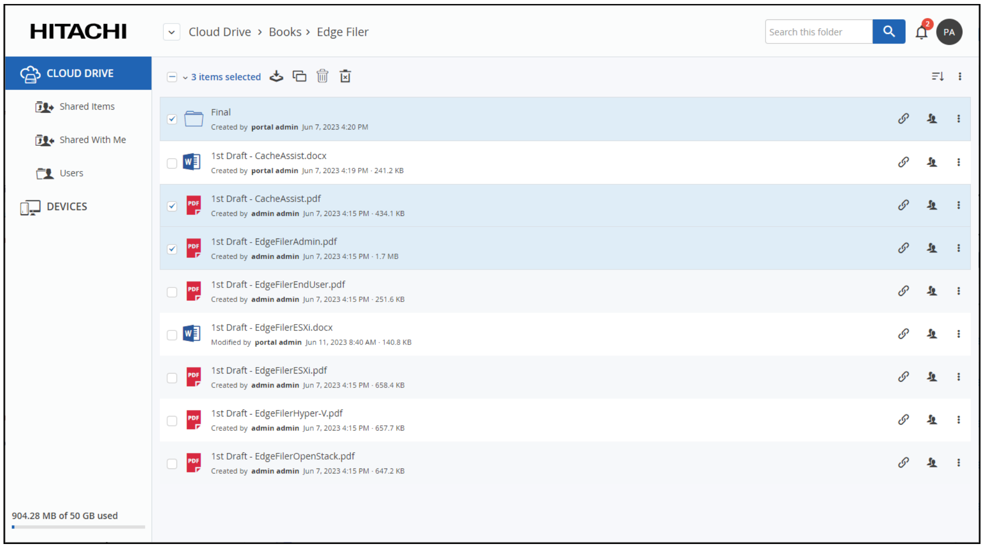
Permanent deletion means that the content is not saved as deleted content for the amount of time specified for the *The numbers of days to keep deleted files* value in the snapshot retention policy, described in The Snapshot Retention Policy Options, but it and all previous versions under the version, saved in previous snapshots, are deleted as well as the version on all devices. If the file that is permanently deleted was moved or renamed in the past, the originally named files and the versions in the original folder are also deleted.

Note: Devices that are not connected to the portal that have the content that is permanently deleted will have the content permanently deleted when the device reconnects to the portal as long as less time than 180 days has passed.
Displaying a previous version and then permanently deleting content in this previous version, deletes the content in this version and previous versions from this version but not from more recent versions. In this case, since more recent content still exists, the report that is produced indicates this by stating that zero files were removed.

To enable permanent deletion, the administrator must have the following defined:

- **Allow Files/Folder Permanent Deletion** role, described in Managing Administrator Users.
- The email SMTP server defined by the global administrator must be running.

You can permanently delete multiple items at the same time.

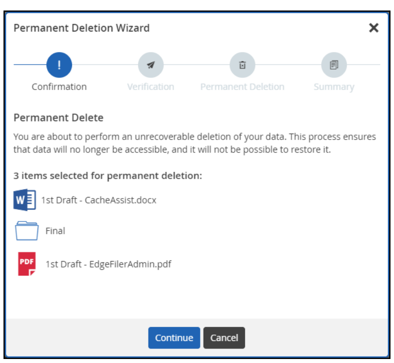


To permanently delete content:

1. In the end user view, go to the content that you want to permanently delete.
2. Select the content and click .

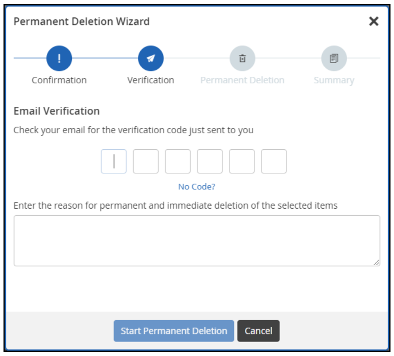
   Note: If you are only deleting one item, you can also click the 3 vertical dots on the right and chose **Delete Permanently** from the drop-down menu.

   The **Permanent Deletion Wizard** is displayed, listing the items selected for permanent deletion.

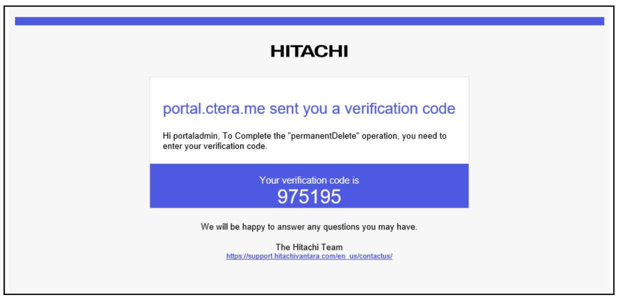
   

3. Click **Continue**.

   The **Verification** step is displayed.

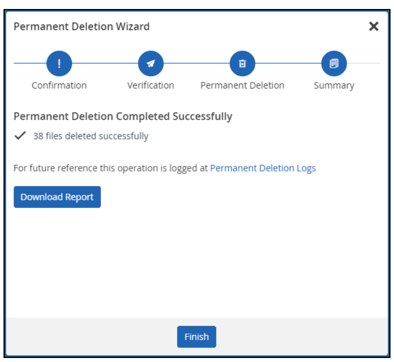


An email with the verification code is sent to the email address for the administrator.



4. Enter the verification code and a reason for the deletion. The reason must consist of letters and/or numbers only.
5. Click **Start Permanent Deletion**.

   The deletion completes and the **Summary** window is displayed with details.



   Note: When permanently deleting content from a previous version, `No files deleted` is displayed instead of the number of files deleted successfully.
6. Click **Download Report** to download a csv file that lists the files deleted, with the file path and name and snapshot, last modified and more information about the deleted file.
7. Click **Finish** to close the wizard.

The permanent deletion operation is slower than normal file deletion as all past versions are also deleted.

Note: Information about permanent deletion of folders and files is written to the Permanent Deletion Log.

Chapter 4. Configuring Team Portal Settings

By default, the HCP Anywhere Enterprise Portal inherits its settings from global virtual HCP Anywhere Enterprise Portal settings, which are set for multiple virtual HCP Anywhere Enterprise Portals by a global administrator. You can override the global settings for the HCP Anywhere Enterprise Portal and modify the settings as needed.

In this chapter

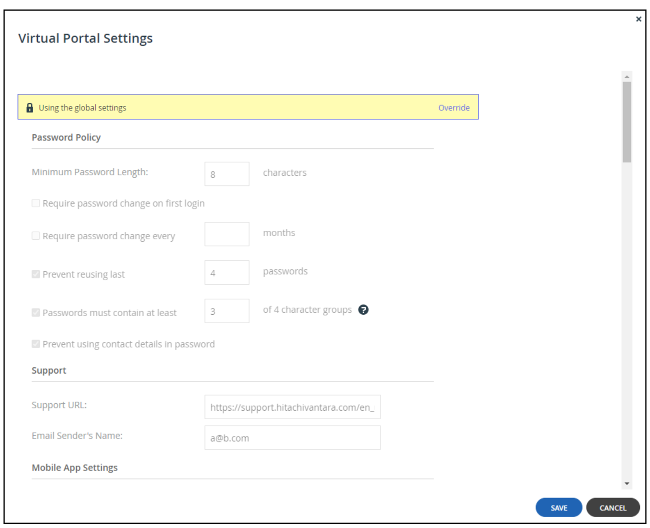
To set virtual HCP Anywhere Enterprise Portal settings:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

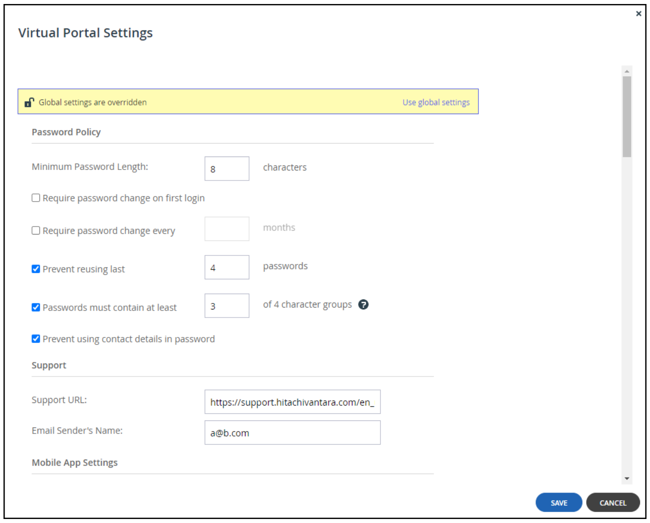
Note: The **Antivirus** option in the navigation pane is only displayed if the portal is licensed for this service.

2. Select **Virtual Portal**, under **SETTINGS** in the **Control Panel** page.

   The **Virtual Portal Settings** window is displayed.

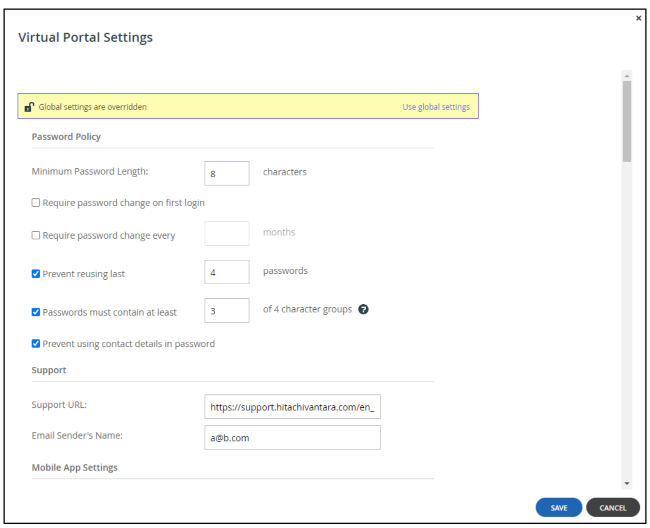


3. Click **Override** to enable changing the default settings for the virtual HCP Anywhere Enterprise Portal.



4. Change settings as required, as described below.
5. Click **SAVE**.

Password Policy



HCP Anywhere Enterprise Portal features a password strength policy to comply with security standards. You can:

- Configure a password rotation cycle (in months)
- Prevent the re-use of the last X passwords
- Determine the number of character groups required in a user's password. The available character group values are:
  - Lowercase characters
  - Uppercase characters
  - Numerical characters
  - Special characters such as "!@#$"

- Prevent users from using their personal details in their password, including first name, last name, email, username, and company name.

  Minimum Password Length – The minimum number of characters that must be used in a HCP Anywhere Enterprise Portal account password. The default value is 8 characters.

  Require password change on first login – Force users to change their password on their first login.

  Require password change every – Force users to change their password after a certain number of months: Specify the number of months. When the specified number of months has elapsed, the user's password expires, and a new password must be provided on their next login.

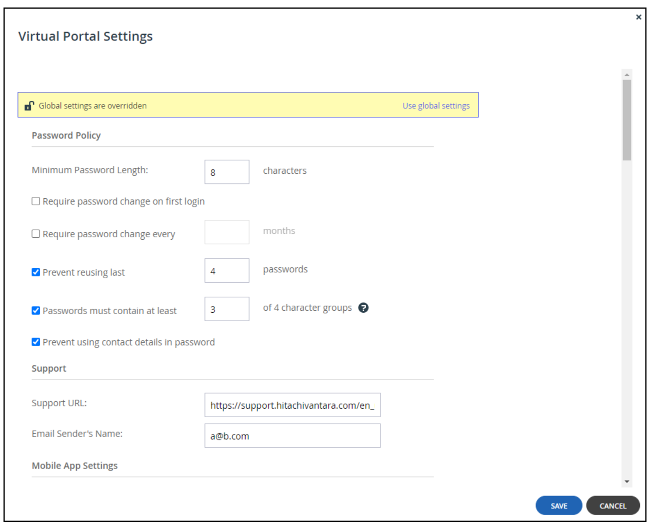
  Prevent reusing last... passwords – Prevent users from reusing a specified number of their previous passwords when they change their password. Specify the number of previous passwords you want this to apply to.

  Passwords must contain at least.... of 4 character groups – Require users to choose passwords that contain at least a specified number of the following character groups:

  - Lowercase characters
  - Uppercase characters
  - Numerical characters
  - Special characters such as “!@#$”

  Prevent using contact details in password – Prevent users from using their personal details in their password, including first name, last name, email, username, and company name.

Support Settings



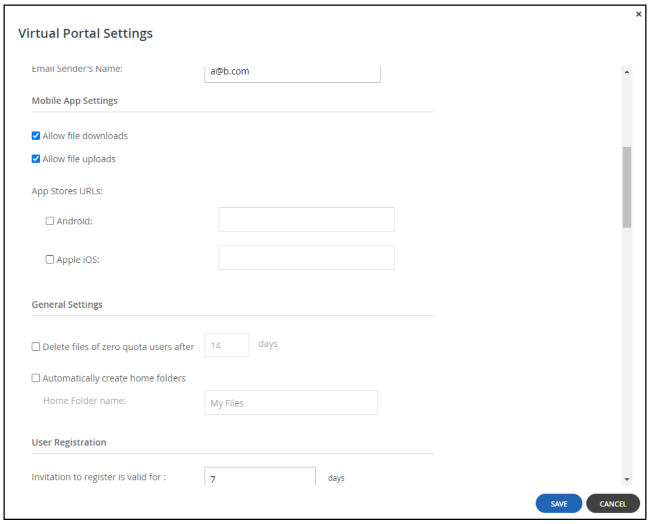
Support URL – The URL to which HCP Anywhere Enterprise Portal users browse for customer support.

Email Sender's Name – The email address that is displayed in the **From** field of notifications sent to users by the virtual HCP Anywhere Enterprise Portal.

Mobile App Settings

This feature is currently not supported.

General Settings

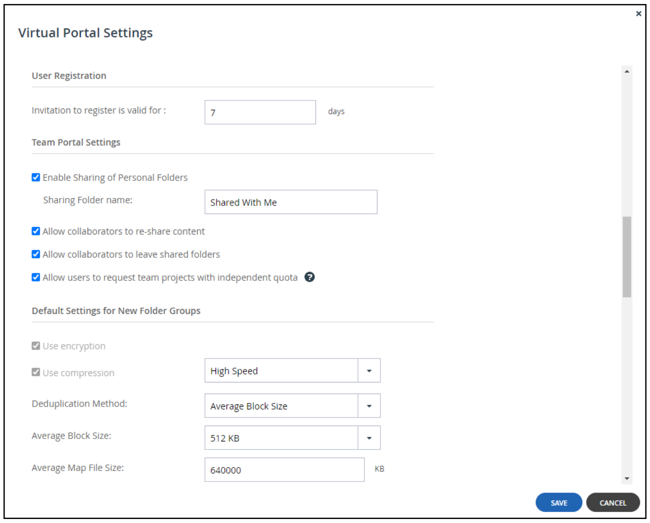


Delete files of zero quota users after – The storage folders of customers who have no quota (for example, customers with expired trial accounts) are deleted automatically after a certain number of days. Enabling this option helps free storage space. A notification is sent to the customer prior to deletion, prompting the customer to purchase cloud storage in order to avoid the scheduled deletion of their files. Storage folders of over-quota users with a non-zero quota are not deleted. The default value is 14 days.

Automatically create home folders – A personal folder is automatically created for each **new** user account. This folder is given the home folder name entered in the **Home Folder name** field.

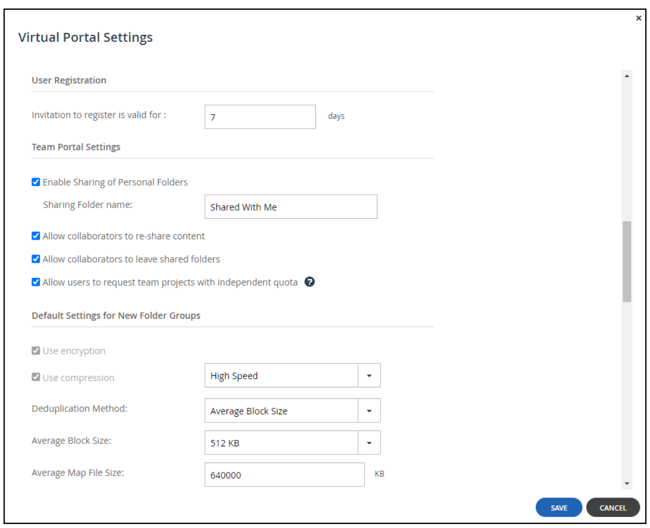
Home Folder name – The name of the personal folder created for each new user account.

User Registration Settings



Invitation to register is valid for:... days – The validity period, in days, for registration invitations sent to users by HCP Anywhere Enterprise Portal team administrators. If a user has not registered for the service after the number of days specified in this field, the invitation expires.

Team Portal Settings



Enable Sharing of Personal Folders – Enable HCP Anywhere Enterprise Portal team members to share personal folders with other HCP Anywhere Enterprise Portal team members.

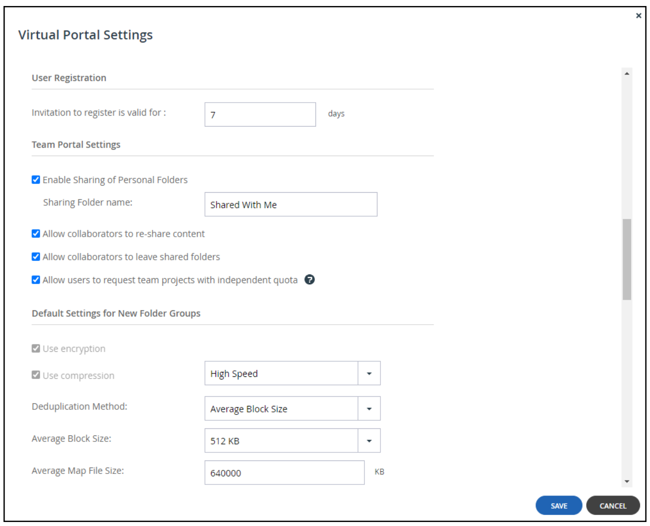
> **Sharing Folder name** – The name of the folder in each user's cloud drive folder hierarchy in which other users' personal folders that were shared with the user are displayed.

Allow collaborators to re-share content – Enable HCP Anywhere Enterprise Portal team members who are listed as collaborators for a file or folder to re-share the file or folder to other users.

Allow collaborators to leave shared folders – Enable HCP Anywhere Enterprise Portal team members to leave a folder that they have been listed as a collaborator. Once a member leaves a shared folder, they have no access to the folder unless they are re-added as a collaborator.

Allow users to request team projects with independent quota – Enable HCP Anywhere Enterprise Portal team members to request a team project, so that storage for the project does not use personal storage.

Default Settings for New Folder Groups



Note: Hitachi Vantara recommends consulting Hitachi Vantara before changing the defaults. Changes to these values do not affect existing folder groups.

Use encryption – Data in newly created folder groups is stored in encrypted format by default.

Note: Passphrase protection is only available in encrypted folders.

Use compression – Specify which data compression method is selected by default for newly created folder groups:

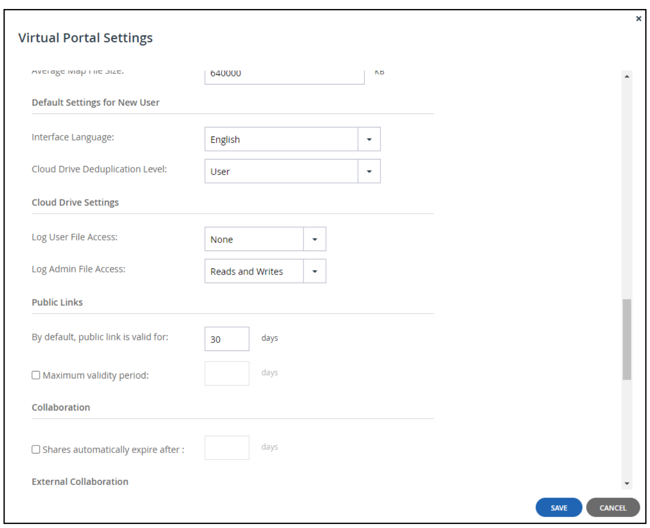
High Compression – gzip compression is used.
High Speed (default) – Snappy compression is used.

Deduplication Method – Whether to use the average block size or a fixed block size for deduplication. The options in the window change depending on what is selected to either **Average Block Size** or **Fixed Block Size**. This value applies to new folder groups only. Use Fixed Block Size if many of the folder groups that large files where deduplication is not common, such as media files. Hitachi Vantara also recommends using **Fixed Block Size** if the global administrator defined direct mode for the storage node.

Average Block Size/**Fixed Block Size** – The average block size used by the folder group or the fixed block size used by the folder group. The default value when set to **Average Block Size** is 512KB and 4MB when set to **Fixed Block Size**. HCP Anywhere Enterprise Portal deduplication splits each stored file into blocks. Increasing the **Fixed Block Size** or **Fixed Block Size** causes the files to be split into larger chunks before storage, and results in increased read/write throughput at the cost of a reduced deduplication ratio. For example, with the default 4MB fixed block size, a file of 3MB will be uploaded as a single 3MB block and a file of 5MB will be uploaded as two blocks, 4MB and 1MB. Increased block size is useful for workloads that require high performance, as well as for those that do not gain greatly from deduplication. For example, where the stored files consist mostly of videos, images, and music files that are not frequently modified. Decreasing the average block size can result in better deduplication, since the HCP Anywhere Enterprise Portal can better identify finer-grained duplicate data. If the global administrator defined direct mode for the storage node, Hitachi Vantara recommends keeping the default 4MB fixed block size.

Average Map File Size – The average map file size used by new folder groups. HCP Anywhere Enterprise Portal uses file maps to keep track of the blocks each file is made of. The Average Map File Size represents the maximum size of file that will be represented using a single file map object. For example, if the average map file size is set to 100MB, files of up to approximately 100MB will have one file map, files of up to approximately 200MB will have two file maps, and so on. Reducing the average map file size causes more file maps to be created per file. This may result in smoother streaming of files; however, it will also result in some extra overhead for creating, indexing, and fetching the additional file maps. The default value is 640,000KB. This value applies to new folder groups only and cannot be changed for existing folder groups.

Default Settings for New User



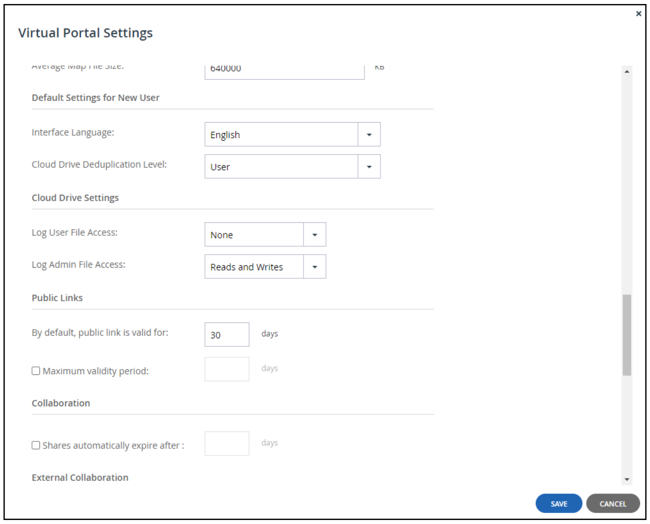
Interface Language – The default language for new users. This language can be overridden by end users in the end user portal.

Cloud Drive Deduplication Level – The default deduplication level to use for cloud folders, for all new users. Deduplication is performed on the device before the data is uploaded to the portal:

> **User** – Create a single folder group for each user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group.

Portal – Create a single folder group for each virtual HCP Anywhere Enterprise Portal, containing all of the cloud folders in the portal. Deduplication is increased but performance impacted and this setting is not recommended for large portals.
Folder – Create a folder group for each of a user account's devices, containing all of the device's cloud folders. Deduplication is performed separately for each of the user account's folder groups, decreasing the benefits of deduplication.

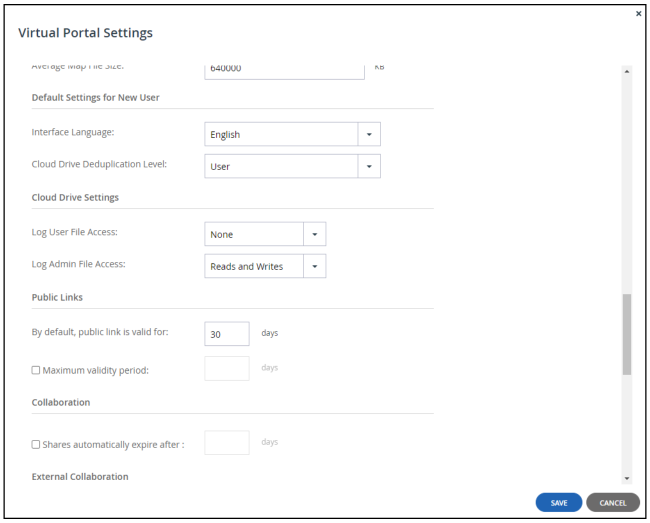
Cloud Drive Settings



Log User File Access – The logging level for the Cloud Drive accessed by end users:
None – No logging.
Writes Only – The access log only includes what files were uploaded or deleted.
Reads and Writes – The access log includes what files were uploaded, deleted, copied and moved.

Log Admin File Access – The logging level for the Cloud Drive accessed by administrators:
None – No logging.
Writes Only – The access log only includes what files were uploaded or deleted.
Reads and Writes – The access log includes what files were uploaded, deleted, copied and moved.

Public Links

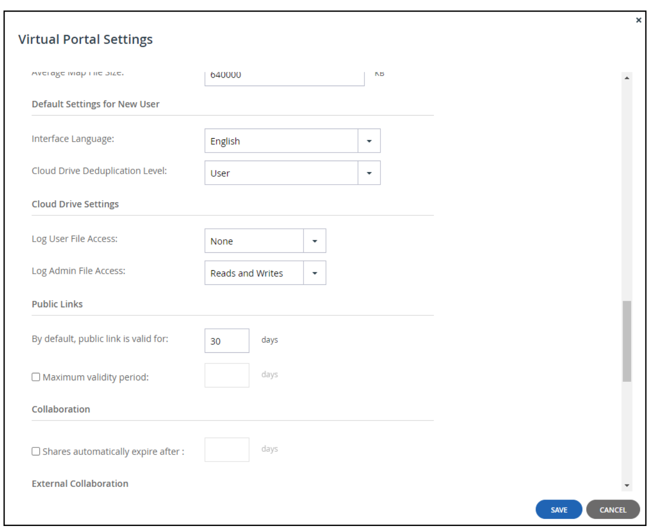


By default, public link is valid for – The number of days for which public link to a folder is valid.

Maximum validity period – The maximum validity period a user can choose for a public link when sharing a folder by public link. The default is empty; no maximum is set. If set, the maximum must be the same or greater than the **By default, public link is valid for** value.

Note: Links that you never want to expire can be set by the user who creates the link, per link. To make the default to never expire, you can set **By default, public link is valid for** to a high number, such as 36500 for a default validity of 100 years).

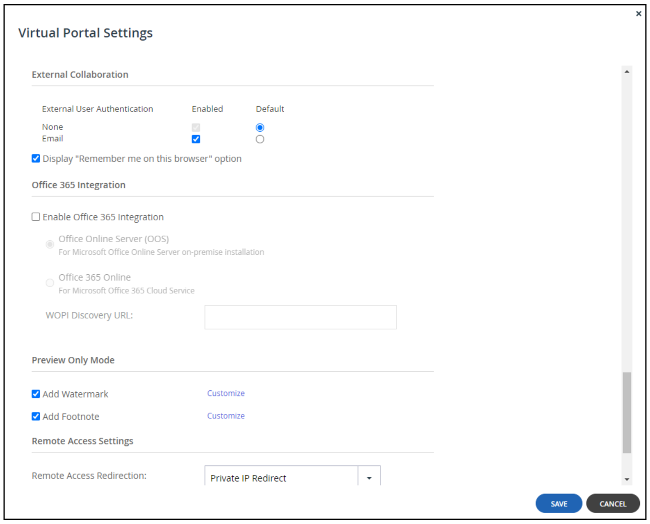
Collaboration



Shares automatically expire after – The time period after which invitations to share files expires. This time period is applied to all users.

Note: When a file is shared for collaboration, an entry is written to the **Access** log.

External Collaboration



How external collaboration is authenticated when a user sends an invitation to collaborate on files or folders. The default is applied with the end user able to select from any of the enabled options to override the default.

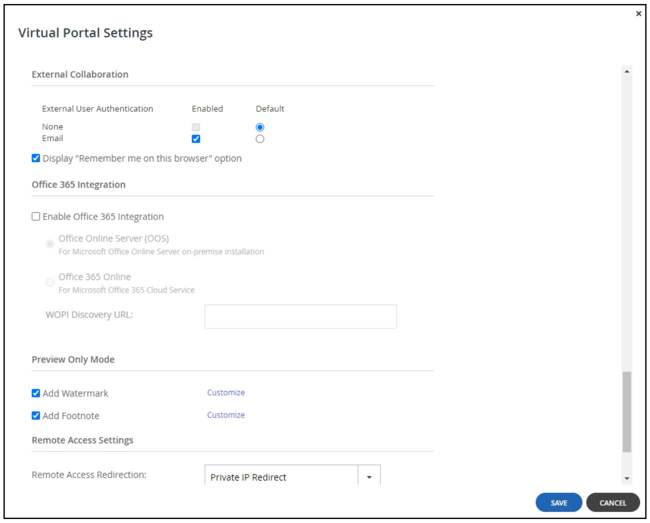
None – No user authentication is applied.

Email – The invitation recipient receives a time limited authenticated link to the file or folder. On every access, a new 6 digit passcode challenge is sent to the recipient by email. The recipient must enter the passcode before accessing the file or folder. This ensures that the invitation is not usable in case the invitation link is accidentally forwarded to another person, or posted on a public website.

> **Note:** **Email** must be enabled for the plug-in to Microsoft Outlook that enables sending email attachments as public links to files on the HCP Anywhere Enterprise Portal Cloud Drive. The plug-in syncs attached files to the HCP Anywhere Enterprise Portal Cloud Dive and inserts public links to the files into the email body.

Display "Remember me on this browser" option – When checked, a *Remember me* checkbox is displayed in the user interface when the user accesses the file or folder via the link and the user can opt to be remembered on the computer. In this case, a passcode is not sent every time the user wants to access the file or folder. If this option is not checked, a *Remember me* checkbox is not displayed and the users receive a passcode to their email or SMS on every access to the file or folder.

Office 365 Integration



Office 365 is a cloud-based office suite offered by Microsoft, which allows users to create and edit files using lightweight, web browser-based versions of Microsoft Office applications, such as Word, Excel, and PowerPoint.

Implementation of Office 365 is dependent on the type of customer:

- **Enterprise Customers** – For enterprises offering their users access to Microsoft Office applications, HCP Anywhere Enterprise supports using Office Online Server (OOS), an on-premise version, which is installed in the enterprise data center or in a private cloud.
  Note: Microsoft allows customers with a Microsoft Volume Licensing account to download OOS from the *Volume License Servicing Center* at no cost but the customer is restricted to view-only functionality. Customers that require document creation, edit and save functionality in OOS need the following from Microsoft: either an on-premises Office suite license with Software Assurance or an Office 365 ProPlus subscription.
- **CSPs** – For **CSPs** offering their customers the ability to create and edit Microsoft Office applications, HCP Anywhere Enterprise supports using Office 365 Online, hosted by Microsoft in a public cloud. This requires the CSP to directly enter into an agreement with Microsoft. For more details, contact Hitachi Vantara support.

To integrate Office Online in a HCP Anywhere Enterprise Portal:

- Install the Office Online Server (OOS), as described in:
  https://technet.microsoft.com/en-us/library/jj219455(v=office.16).aspx#DeploymentTypes,
  under the section *Deploy a single-server Office Online Server farm that uses HTTPS*.
  As part of the procedure make sure that TLS 1.2 or higher support is enabled, as described in https://technet.microsoft.com/en-us/library/mt791311(v=office.16).aspx.
  You can verify that TLS 1.2 or higher support is enabled by checking the registry keys for the server. The following registry keys must be set:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0
.30319]
```

"SchUseStrongCrypto"=dword:00000001

Note: Different HCP Anywhere Enterprise Portals can use the same OOS server.

- Make sure that ports 443 and 80 are open from the HCP Anywhere Enterprise Portal to the Office Online Server.

  Note: If you have more than one Office Online Server in the farm, Microsoft requires that port 809 is open between all the servers in the farm.

- Make sure that the certificate is recognized by the HCP Anywhere Enterprise Portal: It might need adding to the portal trust store.

In the **Virtual Portal Settings** window:

- Verify that the discovery URL, the URL for the Office Online Server, is displayed correctly, with the format `https://`*`servername`*`/hosting/discovery`.
- Configure the settings for OOS:
  Enable Office 365 Integration – If checked, Office 365 can be used to create, view and edit Microsoft Word, Excel, and PowerPoint files stored in HCP Anywhere Enterprise Portal.
  Office Online Server (OOS) – Use Office 365 on-premise: Office Online Server.
  Office 365 Online – Use Office 365 Online. This option is aimed at CSPs, who require a Microsoft O365 license.
  WOPI Discovery URL – The URL to enable using Office 365 with files stored on the HCP Anywhere Enterprise Portal. This URL is either the URL for a local server when using Office Online Server on-premise or the URL received from Microsoft when using Office Online as a service from Microsoft. Different HCP Anywhere Enterprise Portals can use the same WOPI URL.

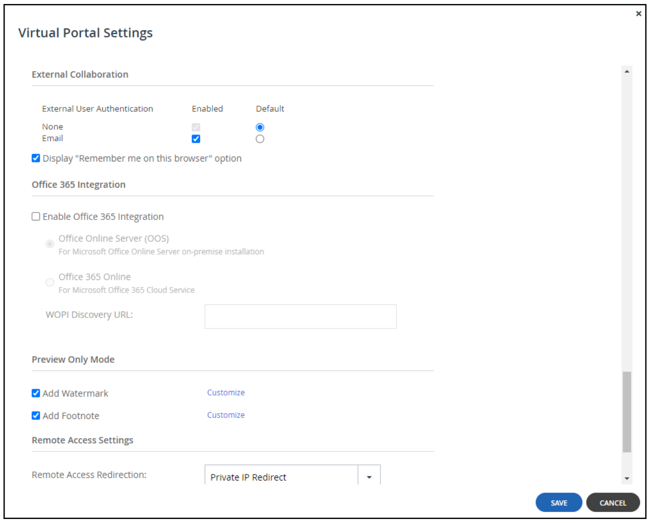
Troubleshooting

Other web sites also include instructions to install the Office Online Server (OOS), with graphics to help you, for example, https://www.getfilecloud.com/supportdocs/display/cloud/Installing+Office+Online+Server+on+Windows+2012+R2+Server to install OOS on a Windows 2012 R2 Server.

If required, import a certificate, via the *certmgr.msc* application, to **Personal > Certificates**.

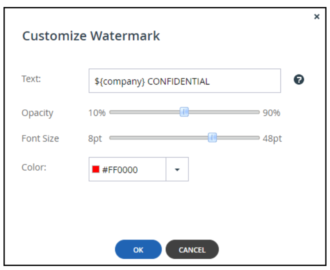
If you have problems and need to refer to the OOS logs, they are located by default on the OOS server under `C:\ProgramData\Microsoft\OfficeWebApps\Data\Logs\ULS`.

Preview Only Mode



Customize the watermark and footnote added to shared files restricted to previewing.

Adding a Customized Watermark



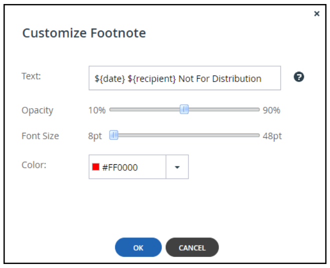
Text – The text to be displayed diagonally each page of a file restricted to previewing only. The following variables are supported in the text field: ${recipient}, ${date} and ${company}.

Opacity – The level of opacity of the watermark text. The greater the opacity the more covered the content under the watermark.

Font Size – The size of the text to use for the watermark.

Color – The watermark text color.

Adding a Customized Footnote



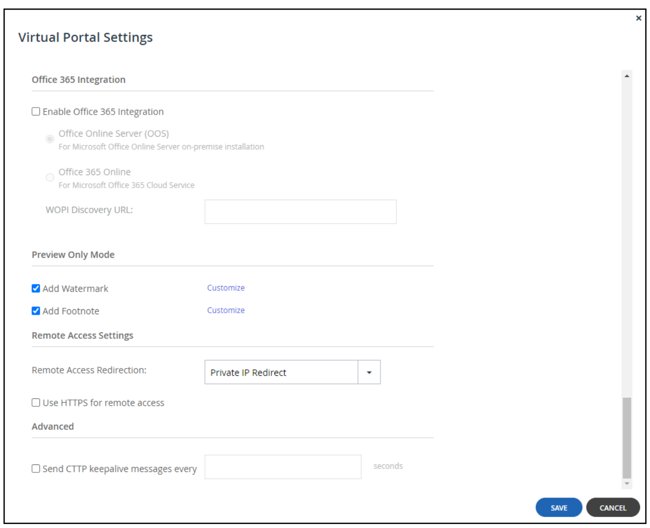
Text – The text to be displayed at the bottom of each page of a file restricted to previewing only. The following variables are supported in the text field: ${recipient}, ${date} and ${company}.

Opacity – The level of opacity of the footnote text. The less the opacity the fainter the footnote text.

Font Size – The size of the text to use for the footnote.

Color – The footnote text color.

Remote Access Settings



Remote access must be configured **On** in the HCP Anywhere Enterprise Edge Filer in **Cloud Services > Remote Access**, in the **CONFIGURATION** tab. If it is configured **Off**, when trying to access the HCP Anywhere Enterprise Edge Filer from the HCP Anywhere Enterprise Portal, the following message is displayed:

```
Remote Access is disabled
Remote access is currently not available for this device.
```

Remote Access Redirection – Whether Web clients attempting to remotely access a HCP Anywhere Enterprise Edge Filer are redirected to communicate directly with the HCP Anywhere

Enterprise Edge Filer, instead of relaying communications through the HCP Anywhere Enterprise Portal:

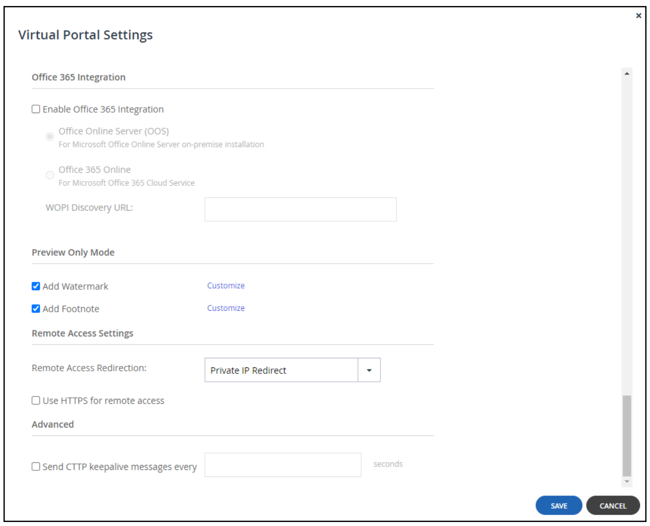
Public IP Redirect – Redirect Web clients to the device's public NAT IP. The inbound port 80 or 443 towards the endpoint device must be open.

Private IP Redirect – Redirect Web clients to the device's private IP address. The same network is used by both device and end user, who can reach the IP address. If the device is in the same network/network subnet, the redirection works.

No Redirect – Do not redirect communications between Web clients and the device. Relay all communications through the HCP Anywhere Enterprise Portal. No special ports are required. The HCP Anywhere Enterprise Portal acts as a mediator and the HTTP is tunneled to the device through the open 995 connection to the HCP Anywhere Enterprise Portal.

Use HTTPS for remote access – Use HTTPS for remotely accessing devices, using the remote access service. For example, if a device is named *dev1* and the HCP Anywhere Enterprise Portal is named *portal.mycompany.com*, then enabling this option will cause the client's browser to be automatically redirected from the HTTP URL *http://dev1.portal.mycompany.com* to the HTTPS-secured URL *https://portal.mycompany.com/devices/dev1*.

Advanced



Send CTTP keepalive messages every – Prevent proxy or load balancer servers from preemptively terminating connection between a device and the HCP Anywhere Enterprise Portal. This may be relevant if the HCP Anywhere Enterprise Edge Filer is configured to use a proxy server and there are connectivity problems during Cloud Sync. This is because some proxy servers and load balancers are configured to close open connections that are not transferring any data after a certain amount of time, thereby causing connectivity problems.

In the field provided, specify an interval, in seconds, smaller than the timeout value configured on the proxy or load balancer server.

Chapter 5. Managing Folders and Folder Groups

Cloud Folders

Cloud Folders are folders created by the Cloud Drive service for shared and personal use. Personal use can be configured by defining a home folder in the General Settings of the Virtual Portal Settings, accessed via **Settings > Virtual Portal Settings**.

Note: You can migrate your Windows file system to a HCP Anywhere Enterprise Edge Filer, maintaining the same file structure and ACLs after the migration. By connecting the HCP Anywhere Enterprise Edge Filer to a HCP Anywhere Enterprise Portal, you can extend your file system capabilities to include file sharing and sync and mobile collaboration capabilities while still maintaining the same structure and ACLs of your original file system. Every share on the HCP Anywhere Enterprise Edge Filer, must be first created as a Cloud Folder in the portal.

By default, when folders are created in a portal, they are assigned a name based on the device's name. For example, if a device is named JohnS, then this device's files will be backed up to a folder called JohnS, and its cloud files will be stored in a folder called JohnS-CloudFiles followed by a number. You can add new folders manually and can edit their properties.

Folder Groups

HCP Anywhere Enterprise Portal organizes cloud folders in *folder groups*. Each folder group acts as a deduplication realm and as a way to ensure that an edge filer writes to a specific storage node. Deduplication means that when files are written to a folder in a folder group, the files' content is compared to data already stored in *other* files in the same folder group. Only the data that *differs* from existing data in the other files is stored in the folder group so that data is only stored once.

Storage classes are groups of one or more storage nodes, defined by the HCP Anywhere Enterprise Portal global administrator. By defining a storage class for the folder group, when the edge filer writes to the cloud folder associated with the folder group, the data is then written to the specific storage class specified for that folder group.

Folder groups are organized according to each user's deduplication level for cloud folders.

For cloud folders you can set the deduplication level to any of the following. Deduplication is performed on the HCP Anywhere Enterprise Edge Filer before the data is uploaded to the HCP Anywhere Enterprise Portal:

- **User**
  A single folder group is created for each user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group. See Configuring Deduplication for a User Account. You can also change the default deduplication for all new users. For details, see Default Settings for New User.
- **Folder**
  A folder group is created for each device of a user account, containing all of the device's cloud folders. Deduplication is performed separately for each of the user account's folder groups.
- **Portal**
  A single folder group is shared by *all* user accounts in the HCP Anywhere Enterprise Portal. The folder group acts as a deduplication realm that spans the entire HCP Anywhere Enterprise

Portal. In other words, if different users' devices back up similar data, the similar data will only be stored once.

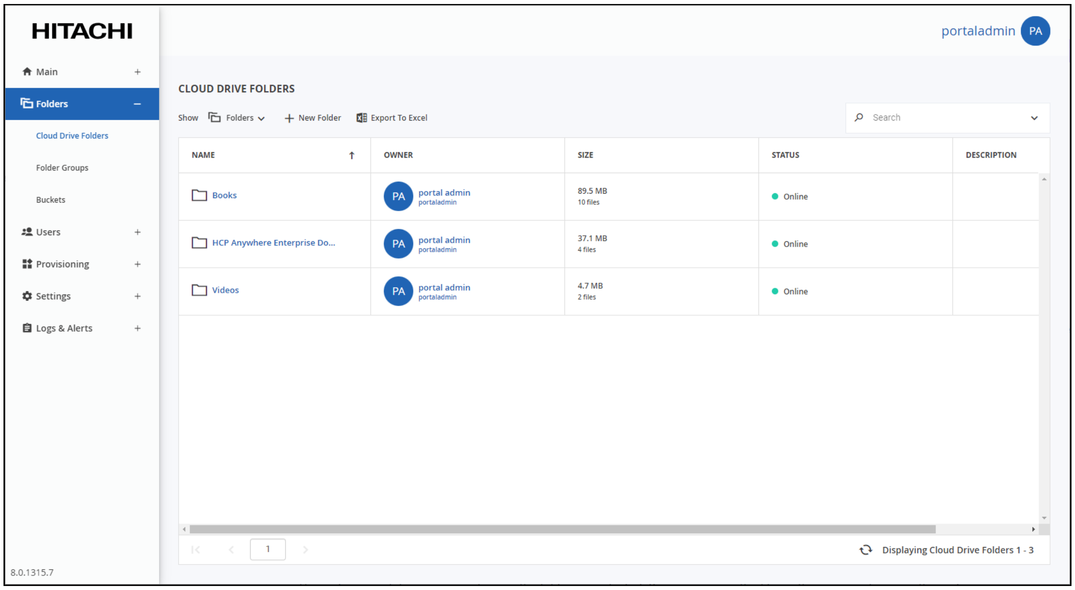
You can change the default deduplication levels for any user created in the HCP Anywhere Enterprise Portal, and you can change any user's deduplication levels.

In this chapter

Viewing Cloud Folders

To view all cloud folders:

- Select **Folders > Cloud Drive Folders** in the navigation pane.
  The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud folders.



NAME – The folder's name.
OWNER – The user name of the folder's owner.
SIZE – The current size of the folder. The total number of files in the folder is displayed under the size.
STATUS – The folder's status:
  Online – The folder is online, and it is possible to view and modify, and sync files to it.
  Offline – The folder is offline, and it is not possible to view, modify, or sync files to it. Folders may be taken offline during some maintenance operations, such as when repairing a folder.
DESCRIPTION – An optional description of the folder.

Viewing Folder Contents

Note: Viewing folder content can be managed by the *Access End User Folders* administrator role attribute. See Customizing Administrator Roles for details.

To view a folder's content:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.
2. Mouse over the folder you want to view.

   The folder icon  is displayed.
3. Click  next to the folder you want to view.

   If you don't have permission to access the folder, you are prompted for the folder owner's password. Enter the password and click **OK**.
   The end user portal view opens, showing the folder you selected. You can manage the files in

this view, as if you are the end user.

Adding or Editing Cloud Folders

You can add a folder in the cloud drive for a user, or edit an existing folder. The folder can be for a specific user or for a team project.

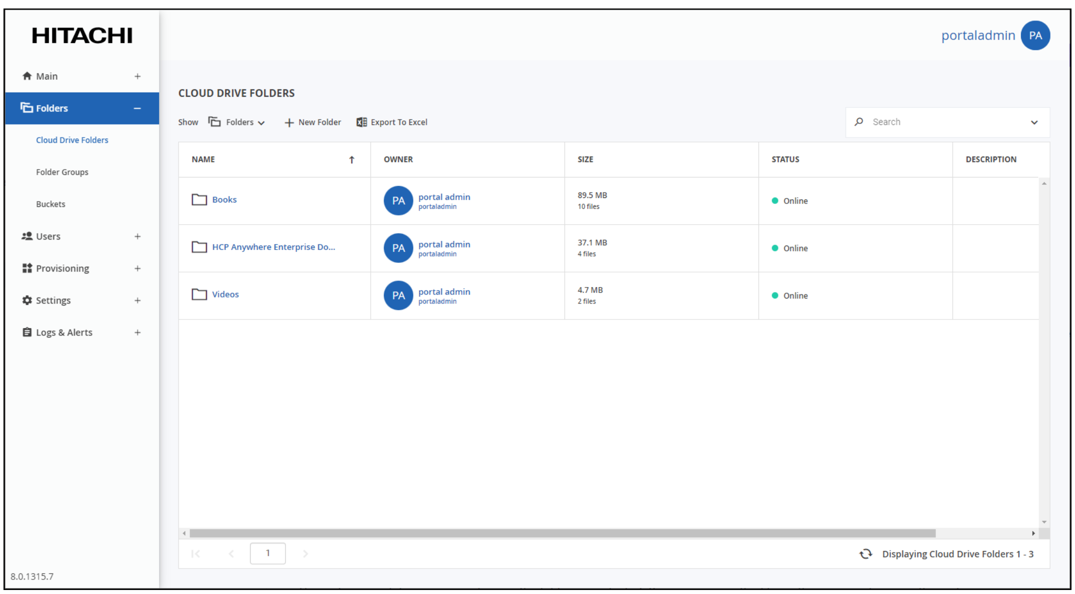
Team projects are shared equally by the collaborators and the initial owner's name is not displayed as part of the folder name. So that a user can use a team project that does not use personal storage:

- The user can request that a folder in the cloud drive to be a team project with the storage allocation taken from the storage provisioned for that team portal and not from the folder owner's storage quota.
- Administrators can define team projects in the cloud drive for a user, with the storage allocation taken from the storage provisioned for that team portal and not from the folder owner's storage quota.

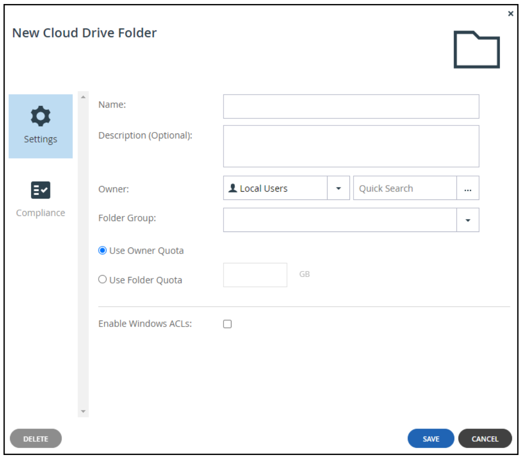
Note: The user can only request a team project if **Allow users to request team projects with independent quota** is enabled in the virtual portal settings for the team portal, described in Team Portal Settings.

To add or edit a cloud folder:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud folders.

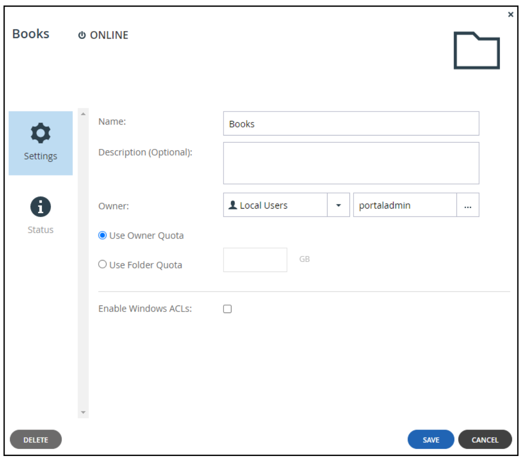


2. Either,
   - Create a new folder, click **New Folder**.
     The **New Cloud Drive Folder** window is displayed.



Or,

- Edit an existing folder, click the folder's name**.**
  The folder window is displayed with the folder name as the window title.



Note: A **Compliance** option is displayed for an existing cloud folder if compliance was set up when the cloud folder was first defined. For details, see Folder (WORM) Compliance: HCP Anywhere Enterprise VAULT.

3. Complete the fields:

Name – A name for the folder.
Renaming a nested cloud folder makes the folder inaccessible to every edge filer that includes this share.
Description (Optional) – A description for the folder.
Owner – The user to own the folder. The owner controls access to the folder.
Folder Group – A folder group for the folder.
Use Owner Quota – The storage quota allowed for this folder is taken from the storage quota of the folder owner. If the owner attempts to use more than this amount of storage, for example, by uploading a file to the folder that causes the quota to be exceeded, the file is not uploaded. The quota is also enforced on the folder on HCP Anywhere Enterprise Edge Filers.
Use Folder Quota – The amount of storage allowed for this folder, which cannot be more than the storage quota of the team portal. The value must be an integer value. If a user attempts to use more than this amount of storage, for example, by uploading a file to the folder after the folder quota has been reached, the file is not uploaded. A file that when uploaded causes the

quota to be exceeded will be uploaded, but no files after that. The quota is also enforced on the folder on HCP Anywhere Enterprise Edge Filers.

Note: The HCP Anywhere Enterprise Messaging service, described in the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*, must be implemented by the global administrator for the folder quota to be applied to HCP Anywhere Enterprise Edge Filers.

Enable Windows ACLs – Select this option if you are syncing a HCP Anywhere Enterprise Edge Filer share to a HCP Anywhere Enterprise Portal including the NT ACLs and extended attributes on the HCP Anywhere Enterprise Edge Filer. The files are saved in the Portal using the NT ACL settings defined on the files. For more information, see Maintaining Windows File Server Structure and ACLs in HCP Anywhere Enterprise Portal Folders.

4. If you are a *Compliance Officer* or a *Read/Write Administrator* with the **Manage Compliance Settings** permission, described in Managing Administrator Users, you can set the compliance that will apply to the cloud folder, described in Folder (WORM) Compliance: HCP Anywhere Enterprise VAULT.

   Note: The **Compliance** option can only be defined when first defining the cloud folder.
5. Click **SAVE**.

The cloud folder is created or updated.

Folder (WORM) Compliance: HCP Anywhere Enterprise VAULT

WORM (write once, read many) compliance ensures that data cannot be tampered with or deleted. In may industries, and especially regulated industries such as financial services and government sectors, organizations are required to store certain types of data in unalterable formats. **HCP Anywhere Enterprise Vault** uses WORM technology to prevent editing, overwriting, renaming or erasing this data.

When a cloud folder is defined with folder compliance and added to the HCP Anywhere Enterprise Vault, after an initial, optional, grace period, the contents of the folder can be protected from any attempt to change the folder content such as by renaming, moving, modifying, or deleting content for a specified retention period.

Any file in a folder in the HCP Anywhere Enterprise Vault has the same compliance restrictions when accessed by HCP Anywhere Enterprise Edge filers, HCP Anywhere Enterprise Drive Connect, and when accessed from an S3 Browser after the cloud folder is set up as a bucket, as described in Setting Up Access to Portal Content Using the S3 API: HCP Anywhere Enterprise Fusion.

HCP Anywhere Enterprise Drive Share (Agent) cannot sync content that is in the HCP Anywhere Enterprise Vault.

Enabling HCP Anywhere Enterprise Vault

Hitachi Vantara provides a role, *Compliance Officer* and a permission, *Manage Compliance Settings* that you use to manage folder compliance. You can also set the *Manage Compliance Settings* permission for a Read/Write Administrator.

Only administrators with the *Manage Compliance Settings* can set up HCP Anywhere Enterprise Vault on a folder.

To enable HCP Anywhere Enterprise Vault:

- Make sure that the administrator has the **Manage Compliance Settings** permission. For details, see Managing Administrator Users.

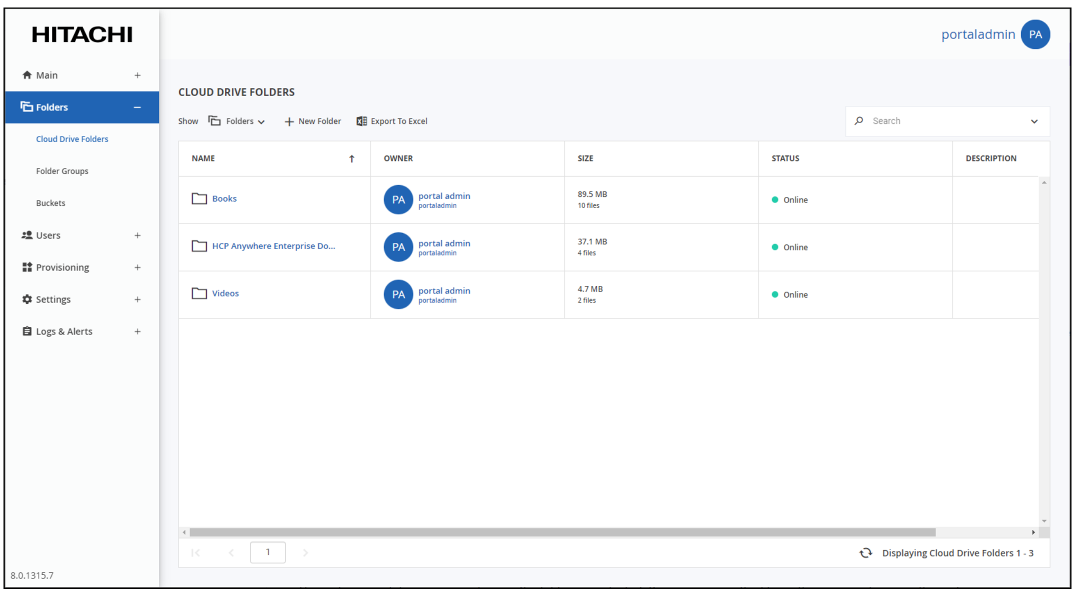
The *Compliance Officer* role automatically has the **Manage Compliance Settings** permission.

Setting Up HCP Anywhere Enterprise Vault on a Folder

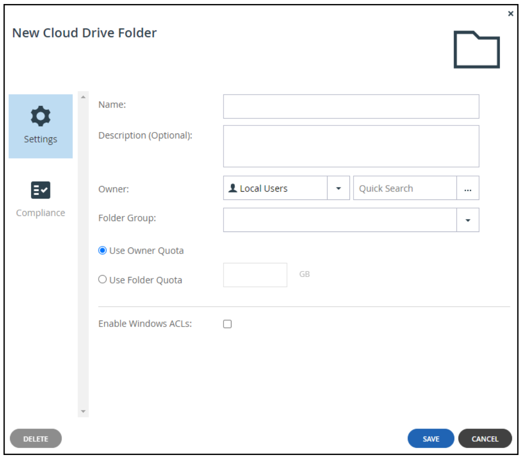
A folder can only be added to the HCP Anywhere Enterprise Vault when it is created.

To protect a cloud folder with HCP Anywhere Enterprise Vault:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud folders.



2. Click **New Folder**.
   The **New Cloud Drive Folder** window is displayed.



3. Complete the fields:

   Name – A name for the folder.

   Renaming a nested cloud folder makes the folder inaccessible to every edge filer that includes this share.

   Description (Optional) – A description for the folder.

   Owner – The user to own the folder. The owner controls access to the folder.

   Folder Group – A folder group for the folder.

   Use Owner Quota – The storage quota allowed for this folder is taken from the storage quota of the folder owner. If the owner attempts to use more than this amount of storage, for example, by uploading a file to the folder that causes the quota to be exceeded, the file is not uploaded. The quota is also enforced on the folder on HCP Anywhere Enterprise Edge Filers.

   Use Folder Quota – The amount of storage allowed for this folder, which cannot be more than the storage quota of the team portal. The value must be an integer value. If a user attempts to use more than this amount of storage, for example, by uploading a file to the folder after the folder quota has been reached, the file is not uploaded. A file that when uploaded causes the quota to be exceeded will be uploaded, but no files after that. The quota is also enforced on the folder on HCP Anywhere Enterprise Edge Filers.

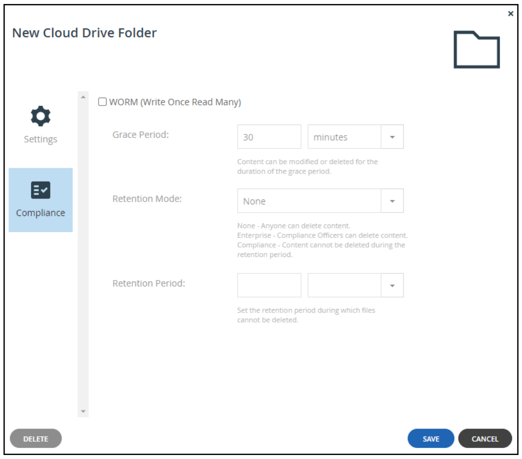
   Note: The HCP Anywhere Enterprise Messaging service, described in the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*, must be implemented by the global administrator for the folder quota to be applied to HCP Anywhere Enterprise Edge Filers.

   Enable Windows ACLs – Select this option if you are syncing a HCP Anywhere Enterprise Edge Filer share to a HCP Anywhere Enterprise Portal including the NT ACLs and extended attributes on the HCP Anywhere Enterprise Edge Filer. The files are saved in the Portal using the NT ACL settings defined on the files. For more information, see Maintaining Windows File Server Structure and ACLs in HCP Anywhere Enterprise Portal Folders.
4. If you are a *Compliance Officer* or a *Read/Write Administrator* with the **Manage Compliance Settings** permission, described in Managing Administrator Users, you can set the compliance that will apply to the cloud folder, described in Folder (WORM) Compliance: HCP Anywhere Enterprise VAULT.

   Note: The **Compliance** option can only be defined when first defining the cloud folder.
5. Click the **Compliance** option.

   Note: If you do not set up **Compliance** when creating the cloud folder, you cannot set it up later.

   The HCP Anywhere Enterprise Vault configuration is displayed.



6. Check **WORM (Write Once Read Many)** to enable HCP Anywhere Enterprise Vault.
7. Define the required compliance:

   Grace Period – The period of time before the compliance restrictions are applied.
   Retention Mode – The level of compliance:
   - **None** – Files in the cloud folder, after the **Grace Period**, cannot be renamed or modified but they can be deleted.
   - **Enterprise** – After the **Grace Period** and for the duration of the **Retention Period**, the *Compliance Officer* or a *Read/Write Administrator* with the **Manage Compliance Settings** permission can permanently delete files. This mode is useful when the enterprise does not have external compliance regulations but wants to impose enterprise-wide regulations. In this case, compliance is enforced for everyone in the enterprise except for administrators with the **Manage Compliance Settings** permission.

   Note: An administrator with the **Allow Files/Folders Permanent Deletion** permission can permanently delete folder content with the **Retention Mode** set to **Enterprise**, even if the administrator does not have the **Manage Compliance Settings** permission.
   - **Compliance** – After the **Grace Period** and for the duration of the **Retention Period** no-one can delete or make changes to files in the folder.

   Retention Period – How long the compliance is applied.
8. Click **SAVE**.

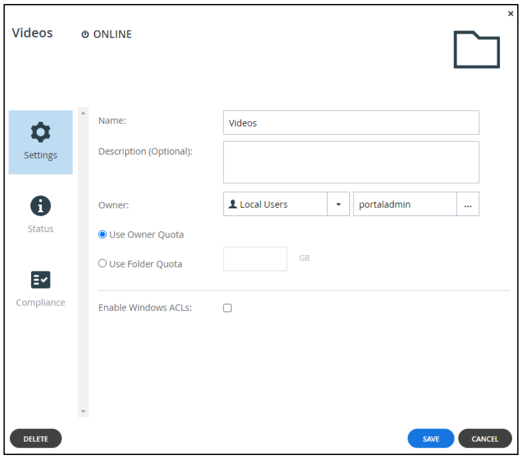
Changing the Compliance Settings for a Folder

Unless **WORM (Write Once Read Many)** in the **Compliance** option was checked when the folder was created in the **New Cloud Drive Folder** window, even if the **Retention Mode** was set to **None**, compliance cannot be set for the folder. **If WORM (Write Once Read Many)** was checked when the folder was created, you can edit the compliance settings.

To edit a cloud folder in HCP Anywhere Enterprise Vault:

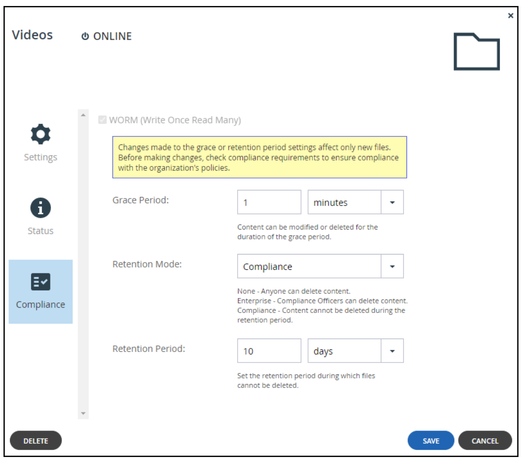
1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud folders.
2. Click the folder to edit.

   The folder window is displayed with the folder name as the window title.



3. Click the **Compliance** option.

   The HCP Anywhere Enterprise Vault configuration is displayed.



4. Edit the compliance settings:

   Grace Period – The period of time before the compliance restrictions are applied. Changes to the **Grace Period** only apply to content added to the folder after the change. Existing content complies with the old setting.
   Retention Mode – The level of compliance. The **Retention Mode** can be changed from **None** to **Enterprise** or **Compliance** and from **Enterprise** to **None** or **Compliance** but **Compliance** cannot be changed.
   Retention Period – How long the compliance has to be applied. Changes to the Retention Period only apply to content added to the folder after the change. Existing content complies with the old setting. When the **Retention Mode** is **Compliance** the **Retention Period** can be extended but not shortened.
5. Click **SAVE**.

The changes only apply to new files added to the cloud folder and not files that are already in the cloud folder.

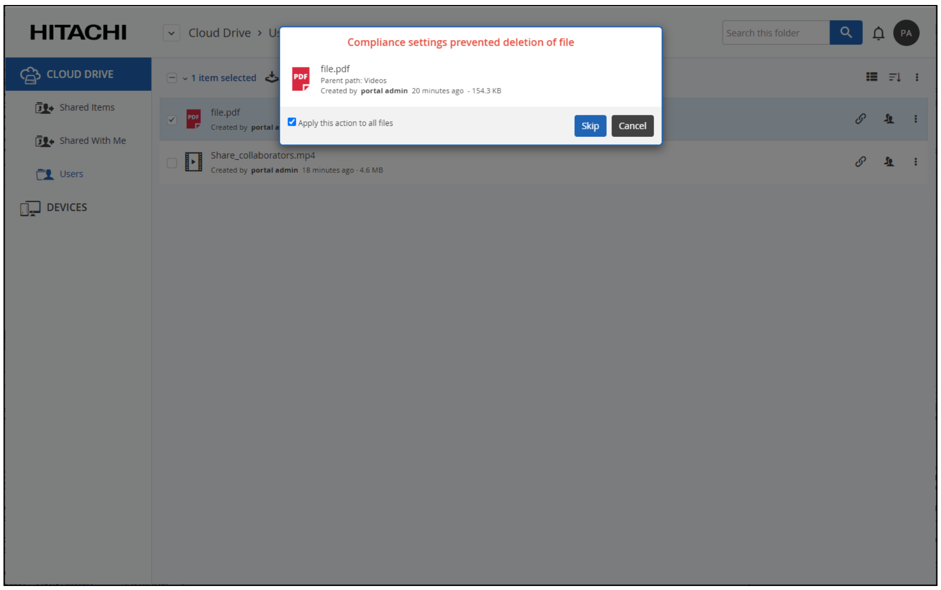
Attempting to Break Compliance

If an attempt is made to change content that is in the HCP Anywhere Enterprise Vault, an error is displayed and written to the audit log.

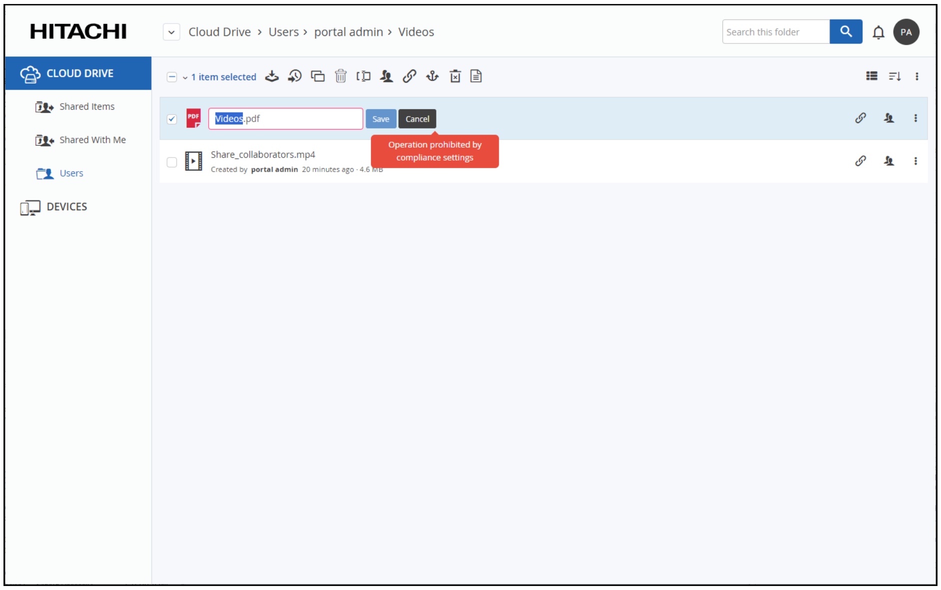
Note: When the **Retention Mode** is set to **Compliance**, when attempting to permanently delete content, the permanent deletion process will delete all the files marked for permanent deletion, including all previous versions of these files, until the first file that is in the HCP Anywhere Enterprise Vault that cannot be deleted. The permanent deletion process will then stop.

Examples

- Attempting to delete a file:



- Attempting to rename a file:

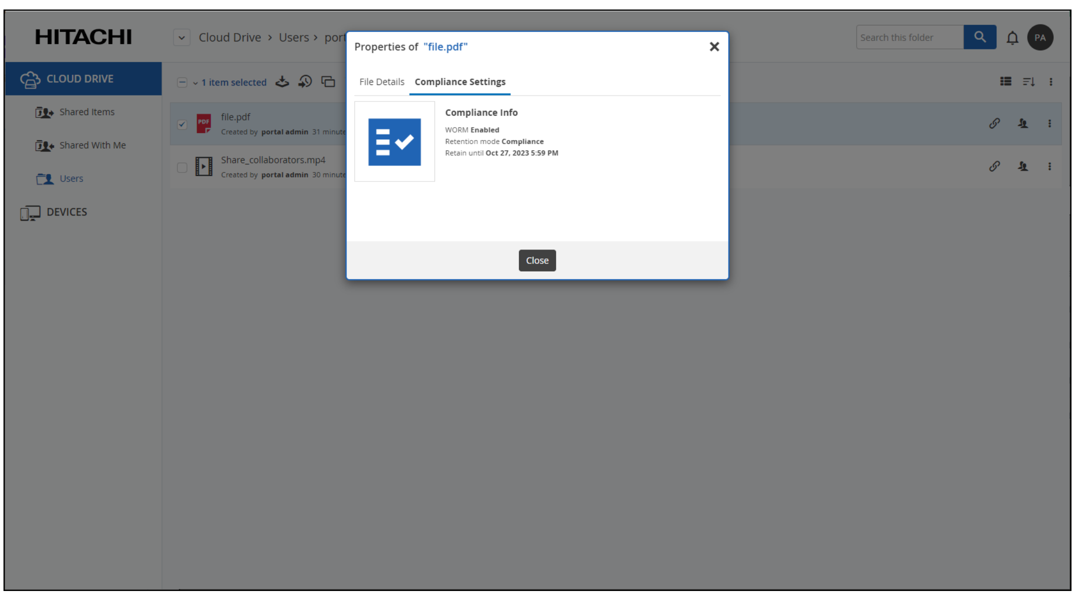


Viewing Compliance Content Details

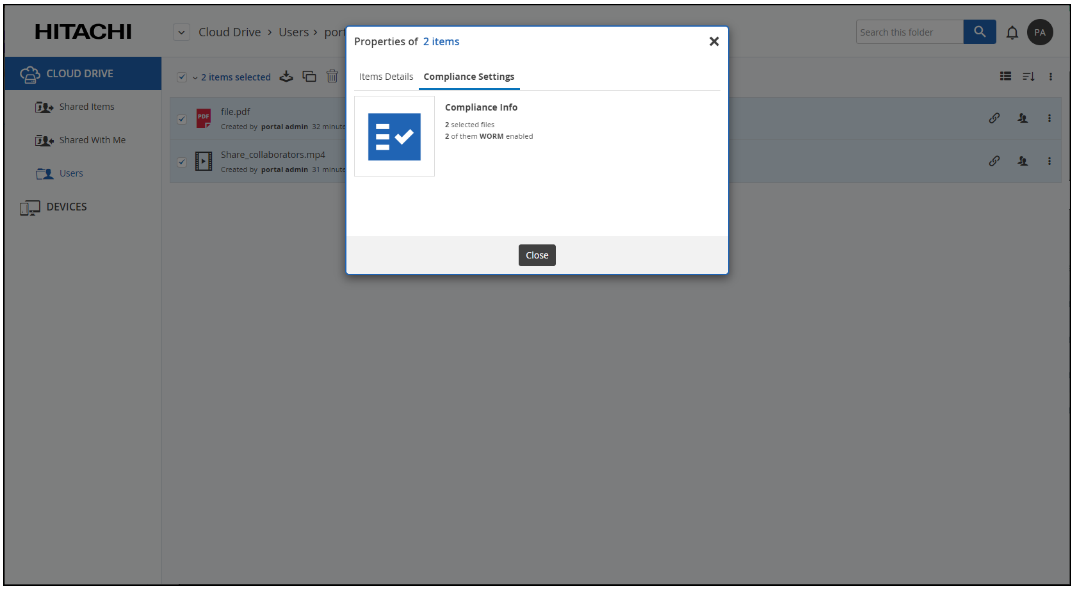
As an administrator with the Manage Compliance Settings permission you can display details of the content in the HCP Anywhere Enterprise Vault.

When displaying the folder that has compliance set, clicking the icon displays content details as well as compliance details in a separate tab.

- For a single item, which includes the retention mode and when the compliance period ends:

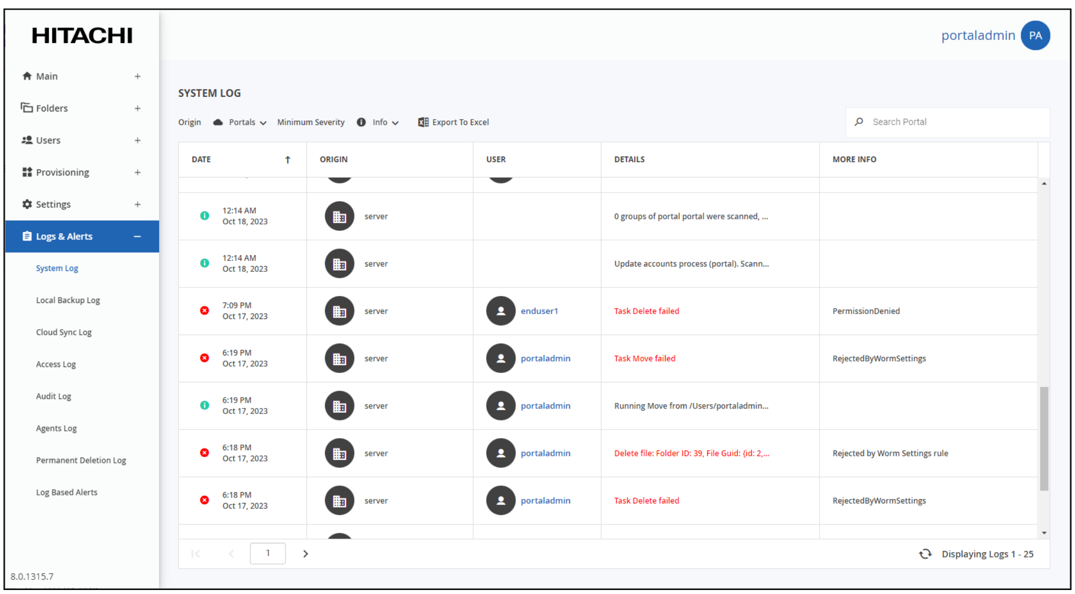


- For multiple items:



HCP Anywhere Enterprise Vault Log Entries

If an attempt is made to change content that is in the HCP Anywhere Enterprise Vault, an error is written to the System log.



Note: Attempting to rename a file in the HCP Anywhere Enterprise Vault is logged as a `Move` operation.

Maintaining Windows File Server Structure and ACLs in HCP Anywhere Enterprise Portal Folders

If you have your Windows file server structure and ACLs defined in a shared system on a HCP Anywhere Enterprise Edge Filer, as described in the Hitachi Content Platform Anywhere Enterprise *Edge Filer Administration Guide,* you can implement this structure on the HCP Anywhere Enterprise Portal.

To maintain your Windows file server structure and ACLs in a portal:

1. Set up the users that will access the file system.
2. Create a new cloud folder. You cannot edit an existing folder to emulate Windows ACLs.
3. Create the cloud share root folders in the portal, as described in To add or edit a cloud folder:, checking **Enable Windows ACLs** in step **3**.
4. Set the HCP Anywhere Enterprise Edge Filer to Caching Gateway mode, as described in the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.
5. Set up the cloud share with Windows ACL emulation in the HCP Anywhere Enterprise Edge Filer, as described in the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.
6. Use HCP Anywhere Enterprise Migrate to copy the file system from the old share in the HCP Anywhere Enterprise Edge Filer to the new share, as described in the *Hitachi Content Platform Anywhere Enterprise Edge Filer Installation Guide* for the environment.

Since you can have many users and root folders to migrate, Hitachi Vantara recommends writing scripts to perform these tasks.

A HCP Anywhere Enterprise Agent connected to the HCP Anywhere Enterprise Portal has access to the cloud drive and is able to share any of the ACL folders and files with other users accessing the HCP Anywhere Enterprise Portal. These folders and files are accessible or not accessible by the other users based on the ACLs defined. For example, if a folder is shared with a user but the folder does not have any ACL access permissions, when the user attempts to access the folder a message similar to the following is displayed: `You have no permission to view this folder`.

Approving Or Rejecting a Team Project Folder

By default, when a user has a storage quota allocated, any content that the user owns, even when shared with other users, is from the storage quota for that user. The user can request to use storage from the team HCP Anywhere Enterprise Portal quota, to share content instead of from his own storage quota. The end user requests a team project from the team administrator, specifying how much storage will be required for the project.

After a user requests a team project, an administrator who receives an email asking for the team project can click in the email **Approve** or **Reject**. Clicking **Approve** or **Reject**, displays the portal with the **CLOUD DRIVE FOLDERS** page open and the option to approve or reject the team project request.

Note: Only portal administrators defined as **Read/Write Administrators** with the **Manage Cloud Folders** role checked can accept or reject the request, as described in Customizing

Administrator Roles. The administrators that can accept or reject a request can be limited according to a set policy, described in Managing Policy for Team Projects.

The approval or rejection of a team project folder is logged in the **Audit** log with details in the **MORE INFO** column. For example:

A user request: `Name: TeamProject1 Details: Requested Team Project Quota=1 GB`

An administrator response: `Owner: enduser Name: TeamProject1 Details: Team Project request approved, Owner=End User, Message=`

Only one administrator can accept or reject the request. If another administrator attempts to accept or reject a request that has already been accepted or rejected, a window is displayed with the message that the request was handled.

To approve a team project request:

1. Click **Approve** in the email requesting the team project.
2. The portal with **CLOUD DRIVE FOLDERS** page is displayed, showing the **Approve Team Project Request** window.
3. You can edit the folder name and the storage quota before clicking **APPROVE**.
4. Click **APPROVE** to approve the request or **CANCEL** to close the **Approve Team Project Request** window without approving or rejecting the request.

Once approved, the folder is added to the list of folders in the **CLOUD DRIVE FOLDERS** page and the user who requested the team project is sent an email confirming the team project.

Note: If the administrator changes the name of the project or the amount of storage to allocate to this team project, this is specified in the email sent to the user as if this was what was requested.

To reject a team project request:

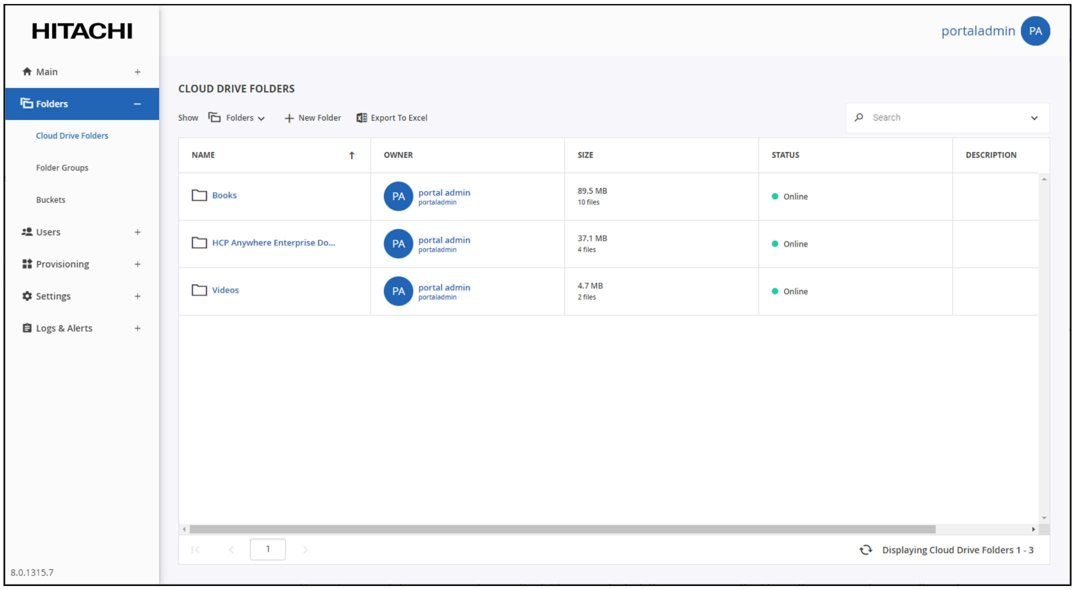
1. Click **Reject** in the email requesting the team project.
2. The portal with **CLOUD DRIVE FOLDERS** page is displayed, showing the **Reject Team Project Request** window.
3. Enter a reason why the request has been rejected in the **Reject Request** text box.
4. Click **REJECT REQUEST** to reject the request or **CANCEL** to close the **Reject Team Project Request** window without approving or rejecting the request.

The user who requested the team project is sent a rejection email.

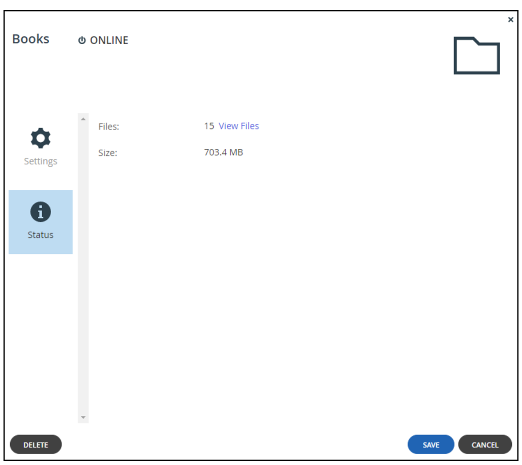
Monitoring Folder Usage

To monitor folder usage:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page opens, displaying all cloud folders.



2. Click the folder's name**.**
   The folder window is displayed with the folder name as the window title.
3. Click **Status**.
   The folder status is displayed.



You can see the following information about the folder:

- The number of files in the team project. Click **View Files** to display the folder content in a new tab. You are prompted for the user password to gain access to the files.
- The amount of storage that has been used. If the folder is a team project folder, the amount of storage used is shown as the percentage of storage allocated to the team project folder.

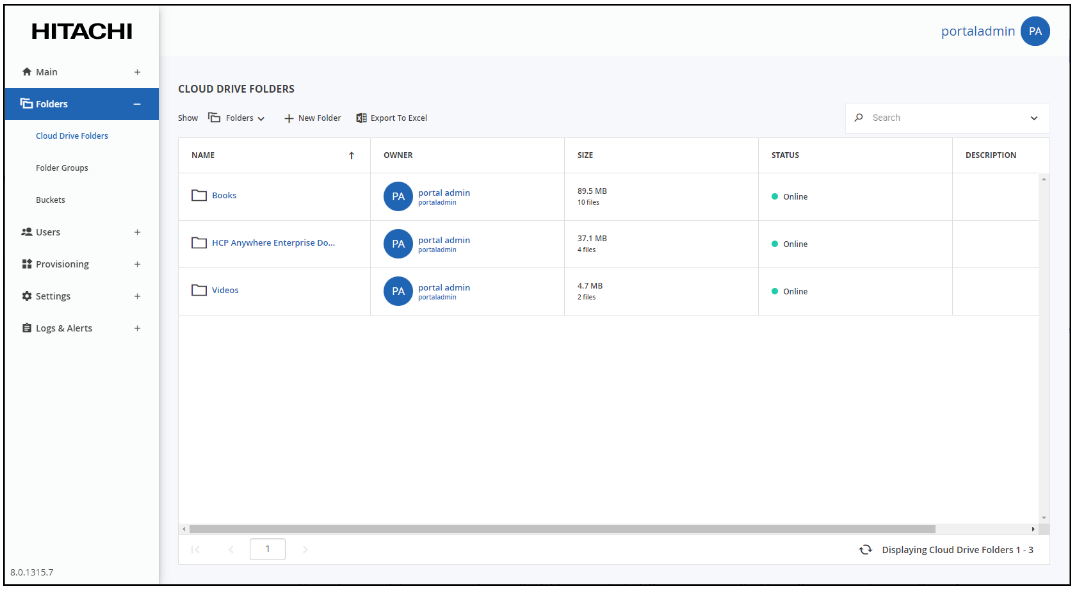
- When antivirus protection is configured, the number of files found to contain malware. Click **View Files** to view the list of infected files.

Exporting Folder Details To Excel

You can export a list of folders and their details to a Comma Separated Values (*.csv) Microsoft Excel file on your computer.

To export a folder details to Microsoft Excel:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.



2. Click **Export to Excel**.

The folder list is downloaded to your computer.

Deleting and Undeleting Folders

To delete a folder:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.
2. Either,
   a) Select the folder's row to delete and click **Delete**.
   A confirmation window is displayed.
   b) Click **DELETE** to confirm.
   Or,
   a) Click the folder.
   b) Click **DELETE**.
   A confirmation window is displayed.
   c) Click **YES** to confirm.

The folder is deleted.

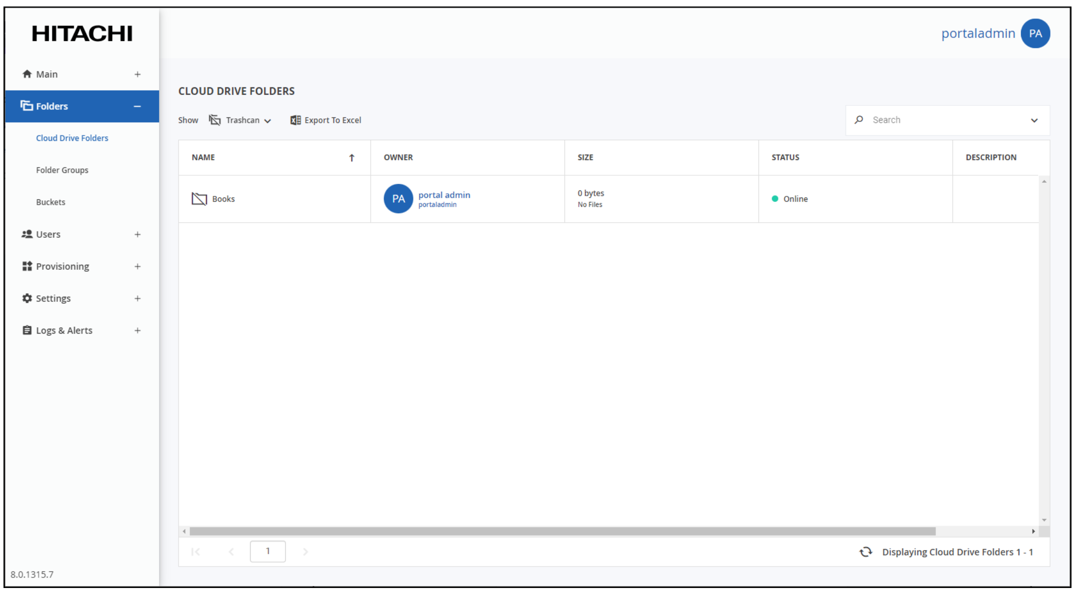
When you delete a cloud drive, it goes into the **Trashcan**. The folder is kept in the **Trashcan** for the duration of the retention policy specified for deleted files, described in The Snapshot Retention Policy Options.

Note: Snapshots of deleted folders are maintained as long as the folder is in the trashcan. To access a previous version, you must first undelete the folder.

You can review cloud folders that have been deleted, while they are still in the **Trashcan** and either undelete them or permanently delete them.

To view and manage deleted folders:

1. Select **Folders > Cloud Drive Folders** in the navigation pane.
   The **CLOUD DRIVE FOLDERS** page is displayed.
2. In the **Show** option, from the drop-down list select **Trashcan**, to display all the deleted cloud folders.

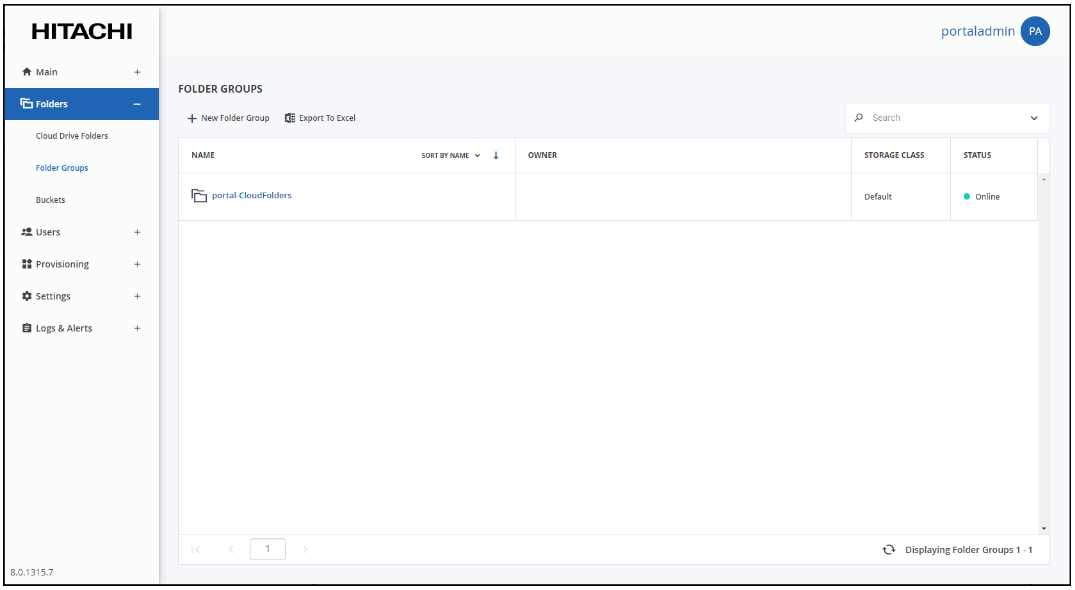


3. You can select one folder row to review the files in that folder that were deleted, as described in Viewing Folder Contents or select one or more rows to either undelete the folders, by clicking **Undelete**, or permanently delete the folders and their contents, by clicking **Delete Permanently**.

Viewing Folder Groups

To view all folders groups in the portal:

- Select **Folders > Folder Groups** in the navigation pane.
  The **FOLDER GROUPS** page opens, displaying all folder groups.



NAME – The folder group's name.
OWNER – The user name of the folder group's owner.
STORAGE CLASS – The storage class where content of the folder group is written. A storage class is a group of one or more storage nodes, defined by the HCP Anywhere Enterprise Portal global administrator, where data is written and saved.
STATUS – The folder's status:

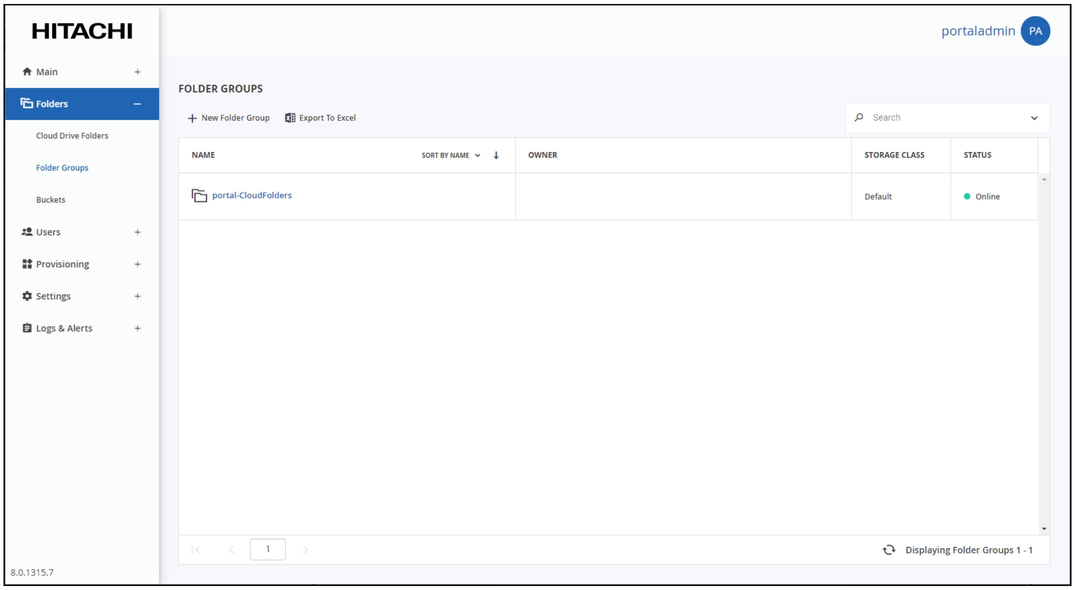
> **Online** – The folder group is online, and it is possible to view and modify, and sync files to it.
> **Offline** – The folder group is offline, and it is not possible to view, modify, or sync files to it. Folders may be taken offline during some maintenance operations, such as when repairing a folder.

Adding a Folder Group

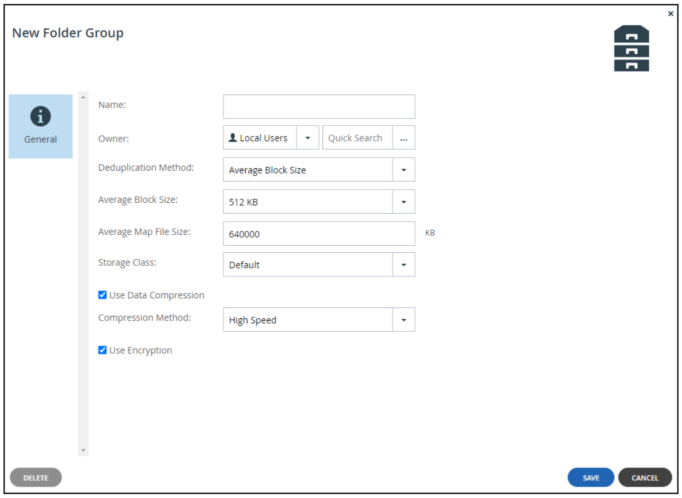
When a device first backs up files to a portal, and cooperative deduplication is enabled for the device's owner, a folder group is automatically created. By default, the folder group is assigned a name based on the device's name. You can add new folder groups manually.

To add a folder group:

1. Select **Folders > Folder Groups** in the navigation pane.
   The **FOLDER GROUPS** page opens, displaying all folder groups.



2. Click **New Folder Group**.
   The **New Folder Group** window is displayed.



3. Complete the fields in the **General** option.
   Name – A name for the folder group.
   Owner – An owner for the folder group. When editing a folder group, you can click on the

owner's name to open the User Account Manager and manage the owner's user account. For information on managing user accounts, see Managing Users.

Deduplication Method – Whether to use the average block size or a fixed block size for deduplication. The options in the window change depending on what is selected to either Average Block Size or Fixed Block Size. Use Fixed Block Size if many of the folder groups that large files where deduplication is not common, such as media files, or if the global administrator defined direct mode for the storage node.

Average Block Size/**Fixed Block Size** – The average block size used by the folder group or the fixed block size used by the folder group. The default value when set to Average Block Size is 512KB and 4MB when set to Fixed Block Size. HCP Anywhere Enterprise Portal deduplication splits each stored file into blocks. Increasing the Average Block Size or Fixed Block Size causes the files to be split into larger chunks before storage, and results in increased read/write throughput at the cost of a reduced deduplication ratio. Increased block size is useful for workloads that require high performance, as well as for those that do not gain greatly from deduplication. For example, where the stored files consist mostly of videos, images, and music files that are not frequently modified. Decreasing the average block size can result in better deduplication, since the portal can better identify finer-grained duplicate data. If the global administrator defined direct mode for the storage node, Hitachi Vantara recommends keeping the default 4MB fixed block size.

Average Map File Size – The average map file size used by new folder groups. HCP Anywhere Enterprise Portal uses file maps to keep track of the blocks each file is made of. The Average Map File Size represents the maximum size of file that will be represented using a single file map object. For example, if the average map file size is set to 100MB, files of up to approximately 100MB will have one file map, files of up to approximately 200MB will have two file maps, and so on. Reducing the average map file size causes more file maps to be created per file. This may result in smoother streaming of files; however, it will also result in some extra overhead for creating, indexing, and fetching the additional file maps.

Storage Class – The storage class where content of the folder group is written.

Note: A storage class is a group of one or more storage nodes, defined by the HCP Anywhere Enterprise Portal global administrator, where data is written and saved. When a storage class is defined, you can specify to which group of storage nodes content from the edge filer is written to. You must specify a storage class that is valid for the virtual portal and you need to check with the global administrator for the list of valid storage classes that you can chose from the list.

After the folder group is created, the storage class cannot be changed.

Use Data Compression – Data in this folder group will be stored in compressed format. Hitachi Vantara recommends only unchecking this option after consulting with Hitachi Vantara support.

- **Compression Method** – The compression method to use for file storage:
  - **High Compression** – gzip compression is used.
  - **High Speed (default)** – Snappy compression is used.

Use Encryption – The data in this folder group is stored in encrypted format.

Note: After creating the folder group the **Name** can be changed and the **state** can be changed from online to offline or offline to online.

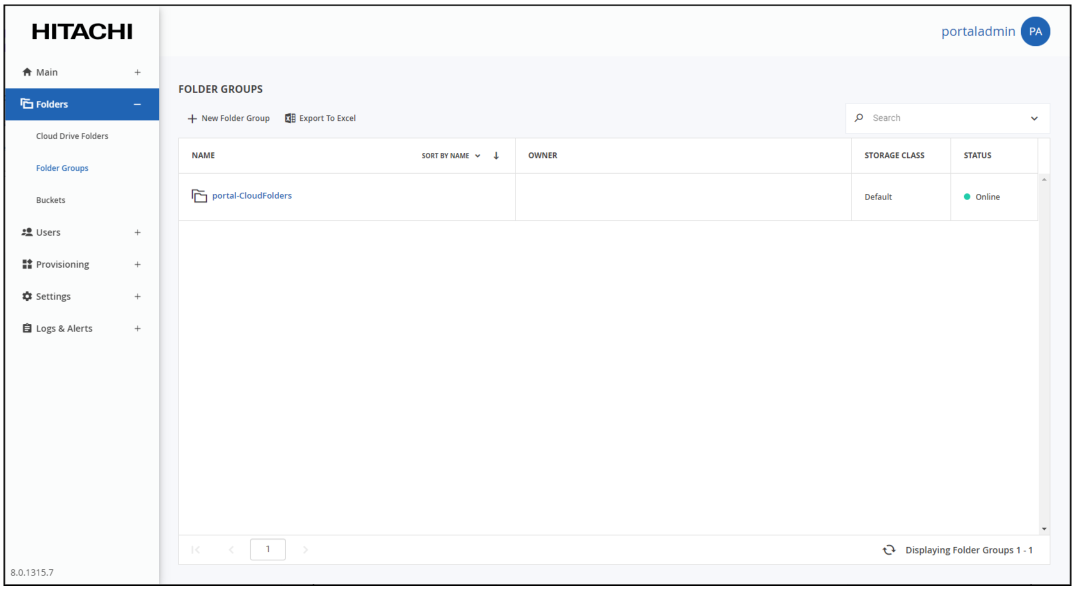
4. Click **SAVE**.

Editing a Folder Group

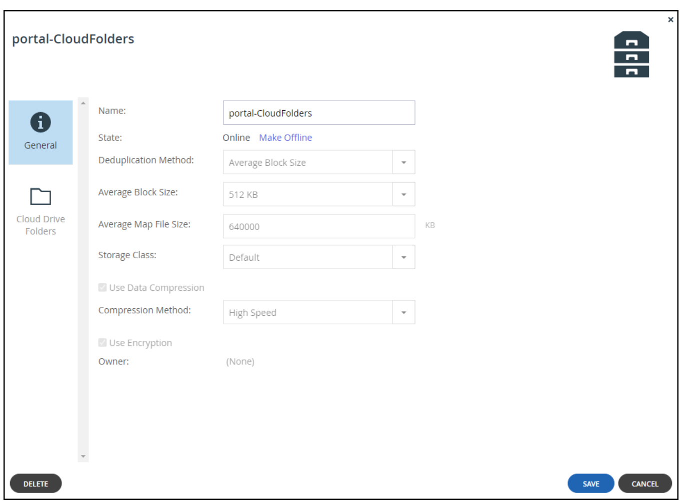
You can edit folder group properties.

To edit a folder group:

1. Select **Folders > Folder Groups** in the navigation pane.
   The **FOLDER GROUPS** page opens, displaying all folder groups.



2. Click the folder group's name**.**
   The folder group window is displayed with the folder group name as the window title and options for **Cloud Drive Folders**.

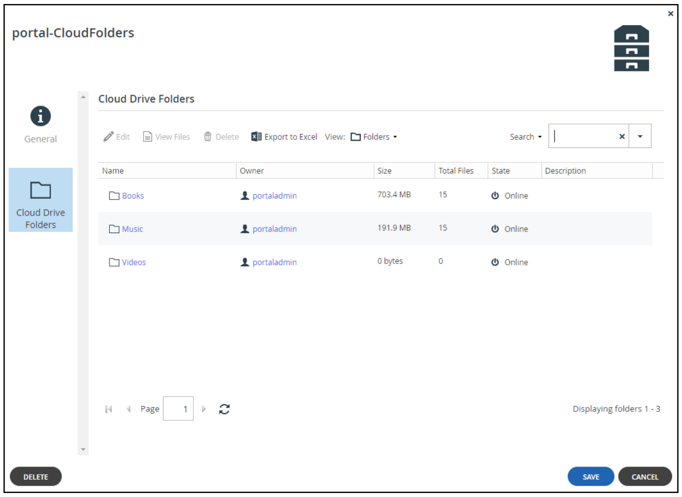


3. Edit enabled fields in the **General** option.
   Name – The name for the folder group.
   State – The folder group's state:
      Online – The folder group is online. Click **Make Offline** to change the state to offline.

Offline – The folder group is offline. Click **Make Online** to change the state to online. All member folders will inherit the folder group's state.

Owner – The owner for the folder group. When editing a folder group, you can click on the owner's name to open the User Account Manager and manage the owner's user account. For information on managing user accounts, see Managing Users.

4. To manage cloud folders in a folder group, click the **Cloud Drive Folders** option.

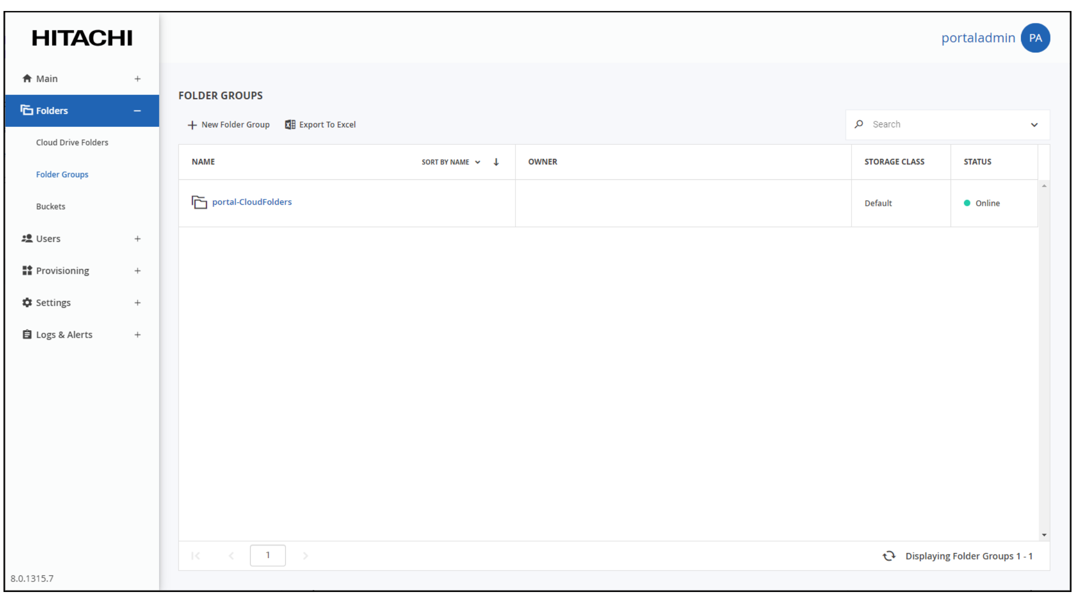


5. Perform any folder task.
6. Click **SAVE**.

Deleting Folder Groups

To delete a folder group:

1. Select **Folders > Folder Groups** in the navigation pane.
   The **FOLDER GROUPS** page is displayed.



2. Either,

   a) Select the folder group row to delete and click **Delete Folder Group**.
      A confirmation window is displayed.

   b) Click **DELETE FOLDER GROUP** to confirm.

   Or,

   a) Click the folder group.

   b) Click **DELETE**.
      A confirmation window is displayed.

   c) Click **YES** to confirm.

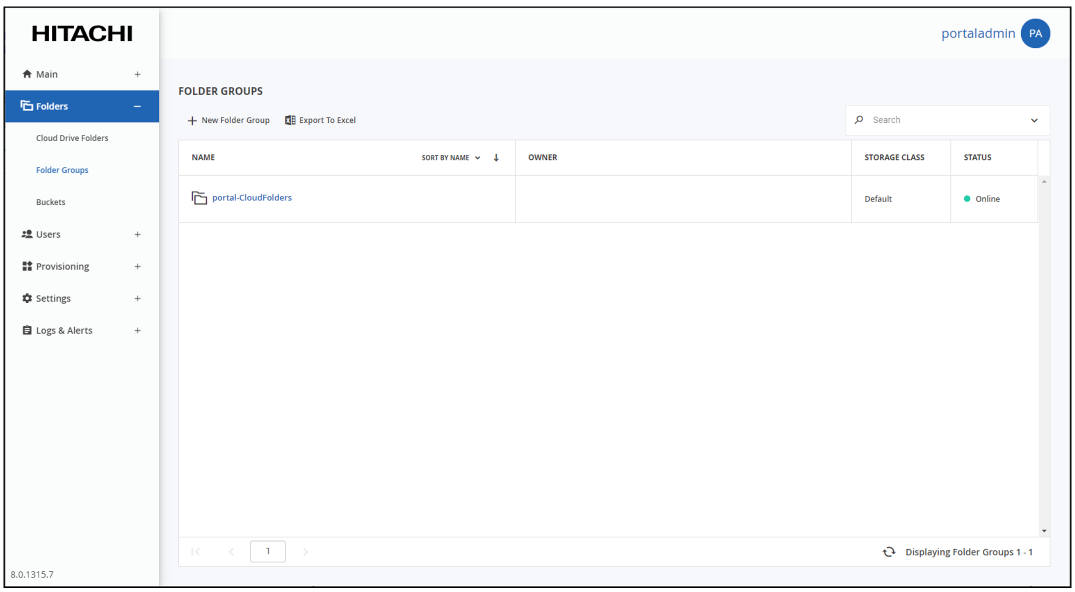
The folder group is deleted.

Exporting Folder Group Details to Excel

You can export a list of folder groups and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of folder groups to Microsoft Excel:

1. Select **Folders > Folder Groups** in the navigation pane.
   The **FOLDER GROUPS** page is displayed.



2. Click **Export to Excel**.

The folder group list is downloaded to your computer.

Setting Up Access to Portal Content Using the S3 API: HCP Anywhere Enterprise Fusion

HCP Anywhere Enterprise Fusion enables the content of cloud folders to be accessed using the S3 API, either using supported S3 operations in programs or using an S3 browser application like FileZilla, WinSCP, Cyberduck, CloudBerry, and S3 Browser.

The capabilities of HCP Anywhere Enterprise Fusion include:

- **In-Place Read/Write** – Enables reading and writing directly to a global file system using the S3 protocol eliminating expensive and time-consuming processes of copying data to external S3 buckets.
- **Single Namespace Across File and Object** – Interact with data generated at the edge using standard object storage S3 protocols, or access cloud-generated data from the edge using NAS protocols. Data is available where you need it, when you need it.
- **Support for Multipart Uploads and Presigned URLs** – Benefit from advanced data transfer capabilities like multipart uploads and pre-signed URLs, making ingestion and sharing of large files even more efficient.
- **Robust Security** – All data is secured in transit via TLS and encrypted at rest, providing an added layer of protection.

To set up access to a cloud folder using the S3 API, you need to do the following:

- Setting Up the HCP Anywhere Enterprise Portal Server
- Creating an S3 Bucket for the cloud folder
- Creating Access Key IDs and Secret Access Keys

After these steps, you can access the cloud folder content using the S3 API by providing the following:

- The endpoint for the bucket, defined when you create the bucket
- The Access Key ID
- The Secret Access Key
  For details, see Accessing Portal Content Using the S3 API,

Setting Up the HCP Anywhere Enterprise Portal Server

The global administrator must specify at least one portal server as an S3 endpoint. For details, see the description of the S3 Endpoint field in the server settings in the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*.

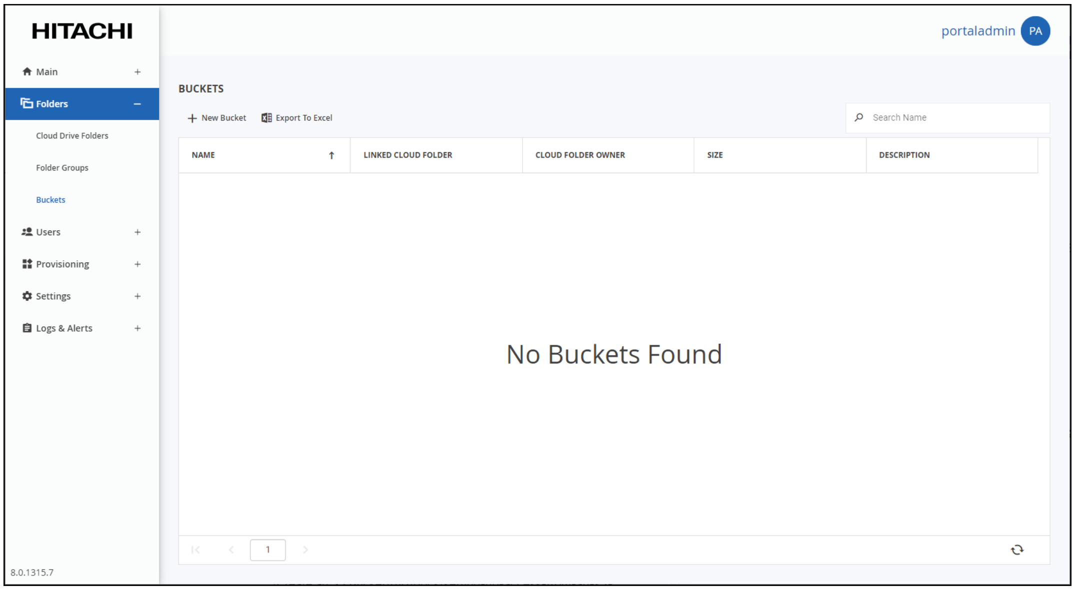
Note: Checking the **S3 Endpoint** is required on only one server. For high availability, the global administrator can set the **S3 Endpoint** on more than one server.

Creating an S3 Bucket

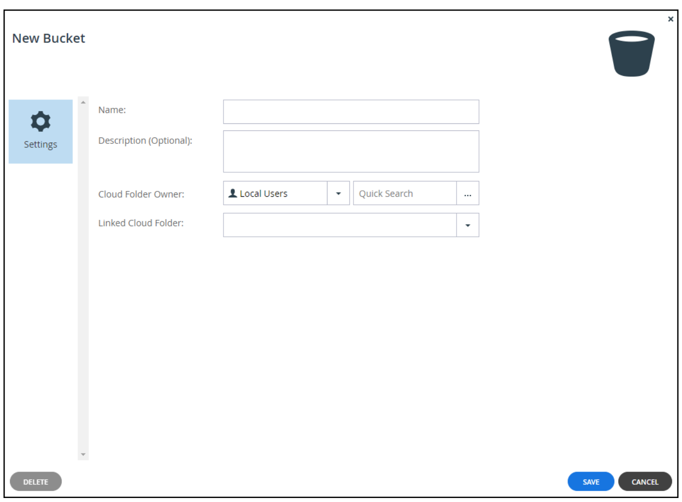
To access content you must set up the required cloud folders as buckets, one bucket for each cloud folder.

To create an S3 bucket:

1. Select **Folders > Buckets** in the navigation pane.
   The **BUCKETS** page opens, displaying all cloud folders linked as S3 buckets.



2. Click **New Bucket**.
   The **New Bucket** window is displayed.



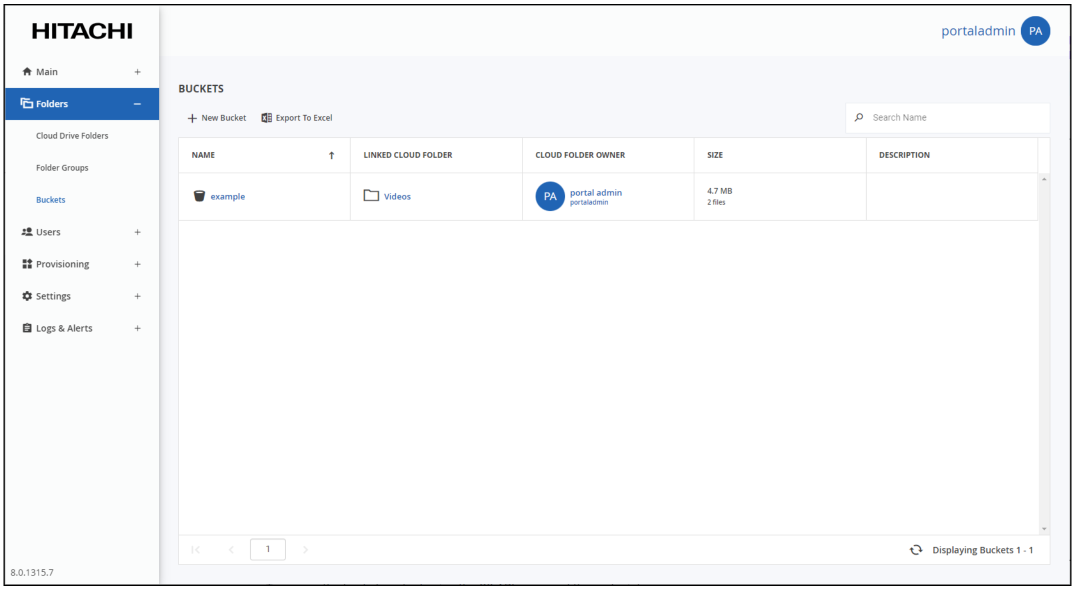
3. Complete the fields:
   Name – A name for the bucket. The name cannot include uppercase letters.
   Description (Optional) – A description for the bucket.
   Cloud Folder Owner – The user who owns the bucket. The owner controls access to the

bucket using the Access Key ID and Secret Access Key pair created for that user.

Linked Cloud Folder – A folder from the list of folders associated with the folder owner.

Note: You cannot specify a cloud folder that was defined with **Enable Windows ACLs** checked for the cloud folder.

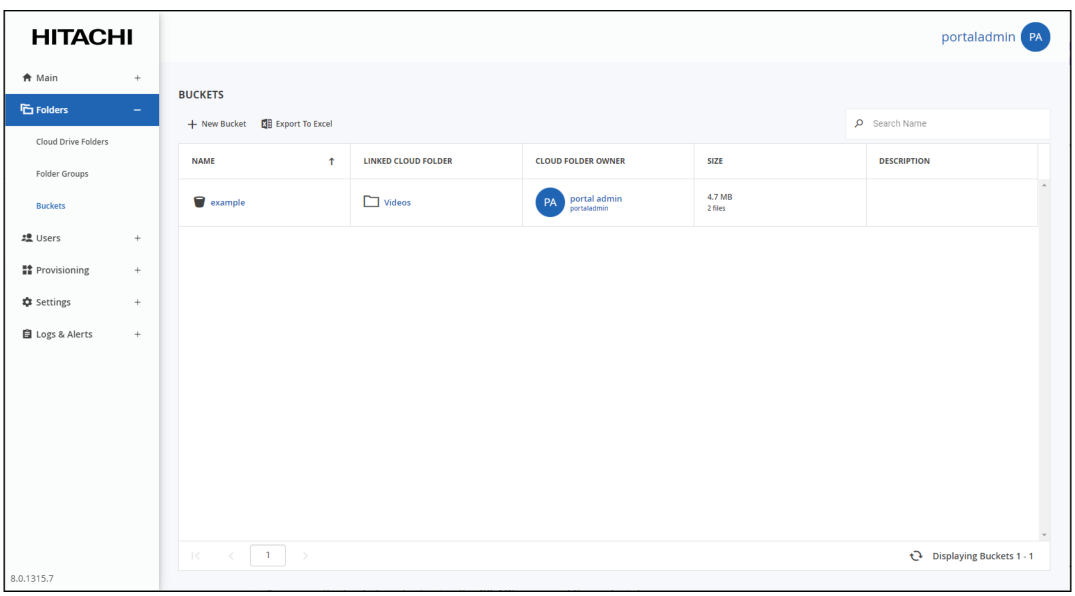
4. Click **SAVE**.



To access the bucket content using the S3 API, you need the endpoint.

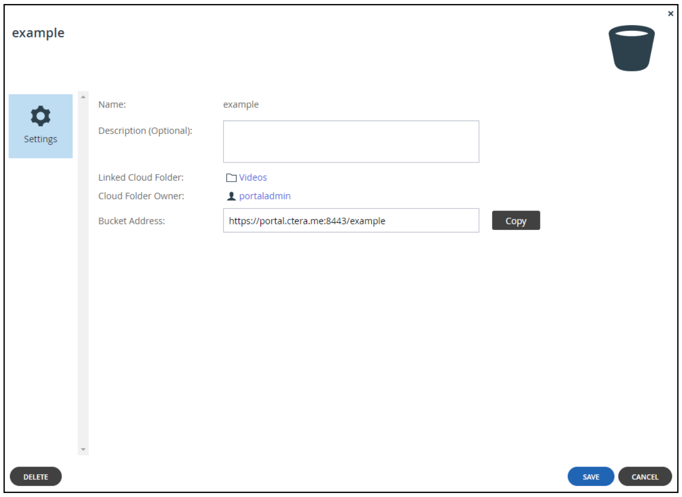
To get the bucket endpoint:

1. Select **Folders > Buckets** in the navigation pane.
   The **BUCKETS** page opens, displaying all cloud folders linked as S3 buckets.



2. Click the bucket.

The bucket window is displayed with the name of the bucket as the window title.

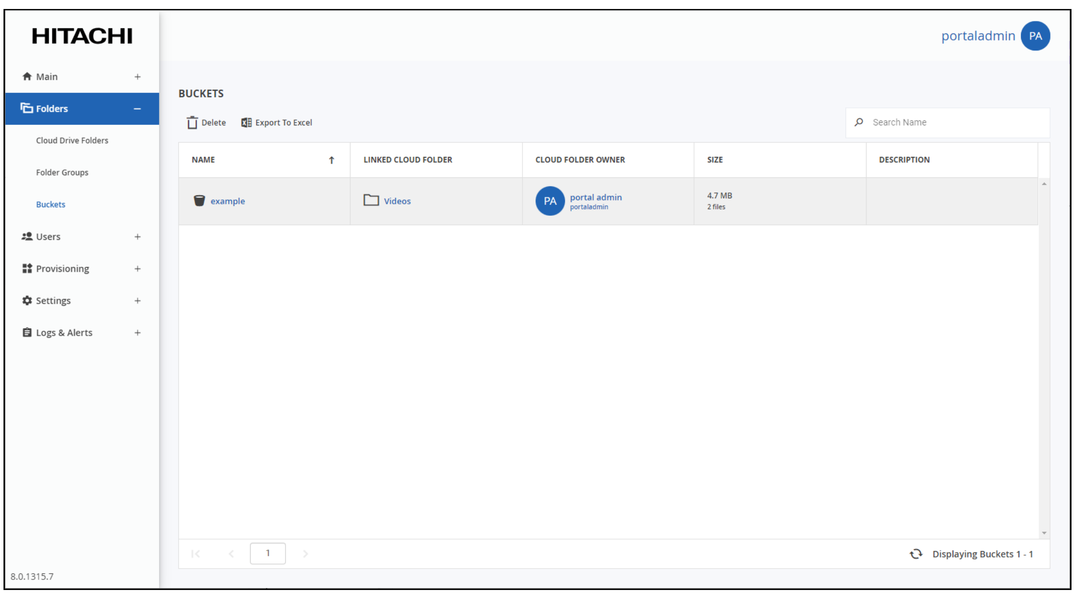


3. Copy the **Bucket Address** to use as the endpoint.

   Note: The endpoint includes the DNS name and not the IP address. You cannot access the bucket using an endpoint with an IP address.

4. Optionally, edit the **Description (Optional)** field.
5. Click **SAVE** or **CANCEL**.

You can delete a bucket by selecting the bucket row and clicking **Delete**.



Creating Access Key IDs and Secret Access Keys

A single Access Key ID and Secret Access Key pair can be used to access all the buckets assigned for a specific user. Each user can have more than one pair of Access Key IDs and Secret Access Keys, up to a maximum of 100.

Both the administrator can create the Access Key ID and Secret Access Key pair for a user as described in Setting Up API Keys to Access S3 Buckets, or the end user can create the Access Key ID and Secret Access Key pair in the end user portal, as described in the *Hitachi Content Platform Anywhere Enterprise Portal End User Guide*.

Accessing Portal Content Using the S3 API

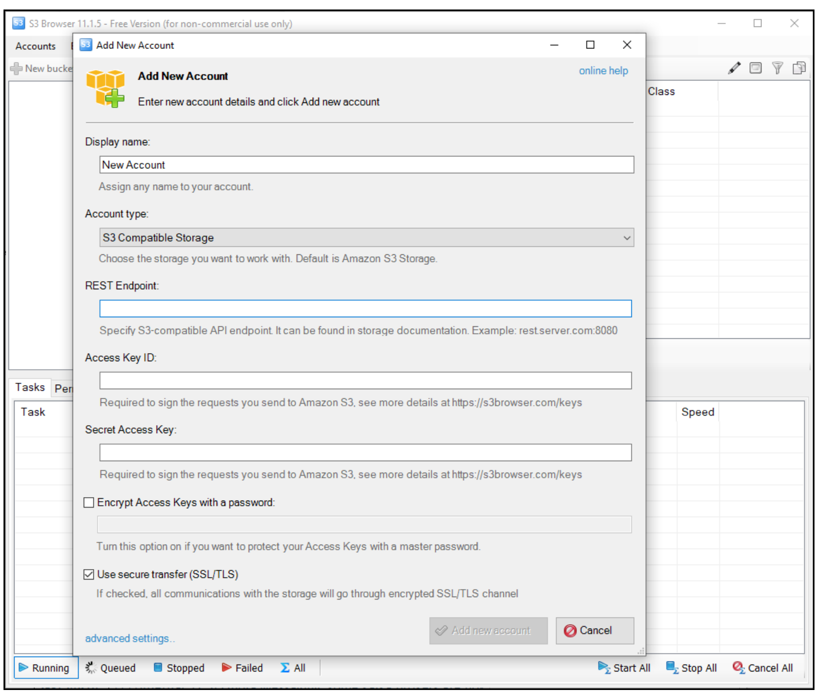
Access to portal content using the S3 API can be done using an S3 browser or in code.

Access via an S3 Browser

You require the following information:

- The endpoint for the bucket
- The Access Key ID
- The Secret Access Key

You enter this information in the S3 browser to access the content, for example using S3 Browser:



Access via Code Using the S3 Protocol

The following S3 operations are supported:

- GetObject
- HeadObject
- DeleteObject
- S3 PutObject
- S3 ListObject
- Copy
- Get Byte Range

Note: The following operations are **not** supported:

- Create a bucket
- Versioning
- SignedURLs

Chapter 6. HCP Anywhere Enterprise Portal Zones

Note: Zones are not enabled by default. The global administrator enables zones for all team portals, as described in *Configuring Global Settings* in the *Hitachi Content Platform Anywhere Enterprise Portal Global Administration Guide*.

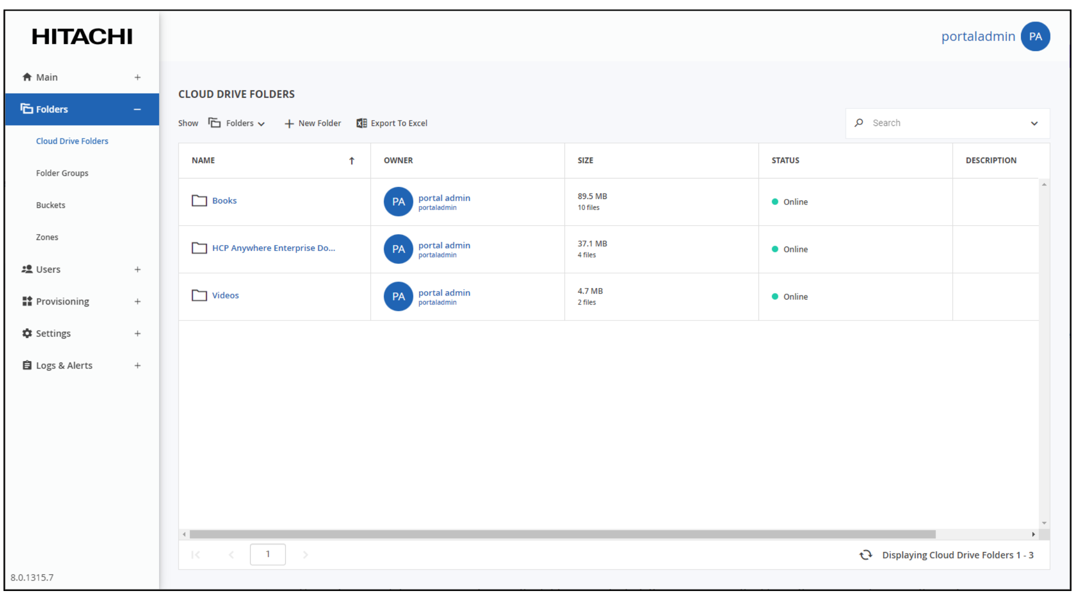
HCP Anywhere Enterprise Portal provides enterprises with a global file system, integrating branch office and cloud file services under a global namespace. The global namespace is the content of all folders and subfolders that are in a team portal.

HCP Anywhere Enterprise Portal zones enables the global file system to be segmented into logical units. Only the relevant subset of the namespace is accessible by each edge location. This means that each edge location is separated from every other edge location in the enterprise, enabling privacy and security between locations, preventing internal data leakage between groups and also ensuring data sovereignty compliance.

Zones are defined at the team portal level for edge filers connected to the portal. Once defined, the edge filer has no access to any folder in the portal that is not defined as belonging to that zone. When content is required by more than one location, the relevant folders can belong to more than one zone.

Any edge filer that is connected to a portal with zones defined for it, is automatically associated with the default zone. An edge filer can be associated with more than one zone. In this case the edge filer will sync folders from every zone it is associated with. More than one zone can be associated with a single edge filer. All the folders defined for all the zones are synced with the edge filer. Also, more than one edge filer can be associated with a zone.

After the global administrator has enabled zones, the **Zones** item is displayed under **Folders** in the navigation pane.



Defining a Zone

Zones are defined per team portal, after they are enabled, for every team portal in the HCP Anywhere Enterprise Portal.

Some countries have strict rules about where data is stored. In cases like this, a zone can be defined for that country so that all the data from the global namespace that has to be restricted to the country is accessible via edge filers in the country.

Different departments in a company do not need to be overloaded with files from other departments that they never need. With an edge filer used the content required by each department and zones defined for each department edge filer, users have access to their data and are not overloaded with unwanted content from other departments. In addition, there is the extra security consideration that users cannot access sensitive content belonging to another department, such as human resources. Even if all the edge location content is accessed from a single edge filer, by creating multiple zones associated with this edge filer, you can separate the content on the edge filer in to logical units.

All zone actions are logged in the audit log.

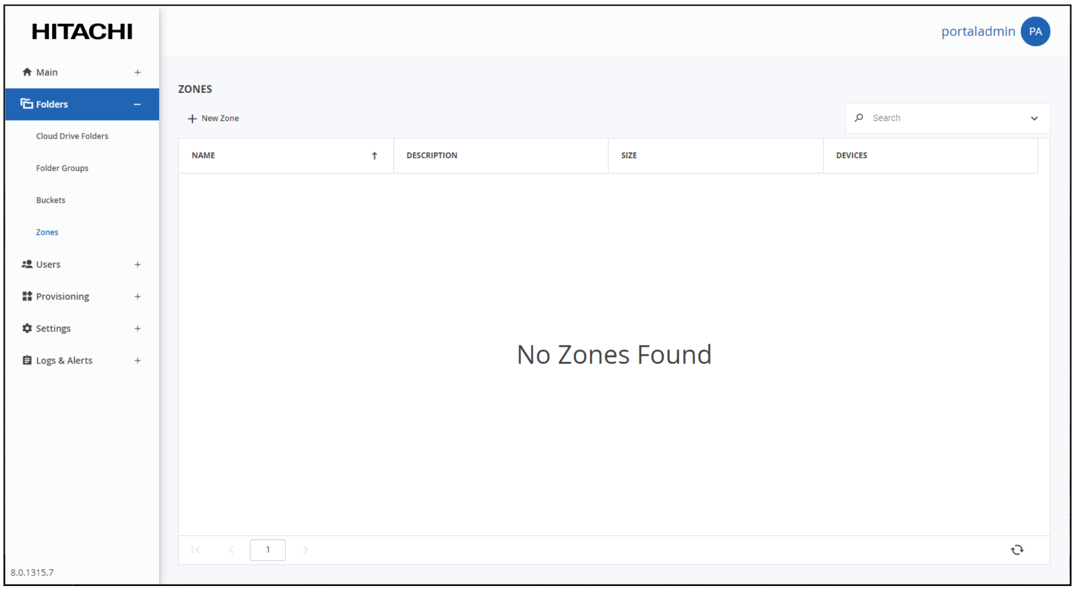
In this chapter

Creating, Editing, or Deleting Zones

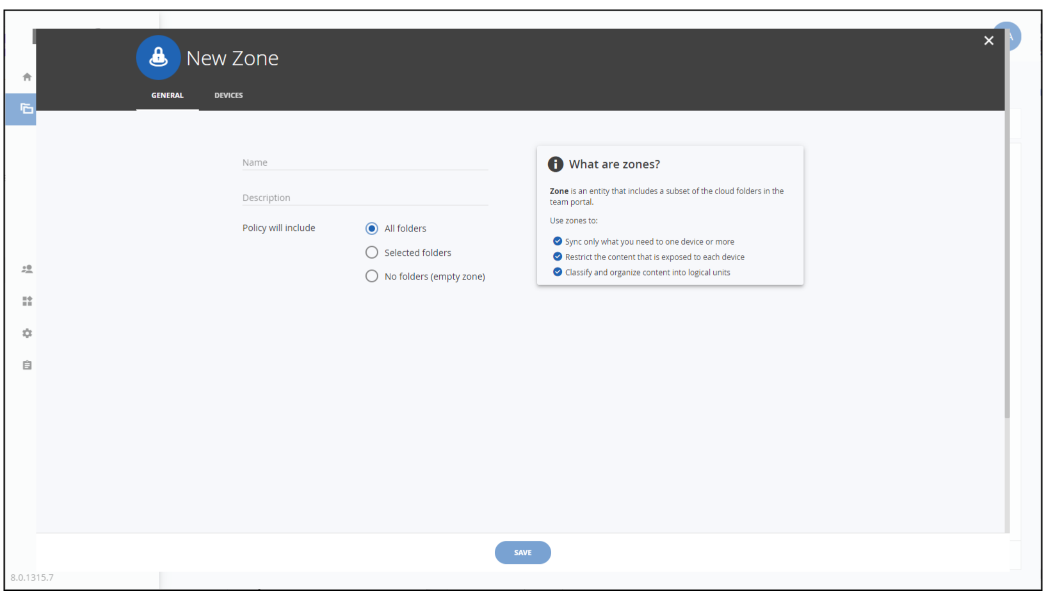
You can create a zone or edit an existing zone.

To create or edit a zone:

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.



2. Either,
   - Create a new zone, click **New Zone**.
     The **New Zone** window is displayed.

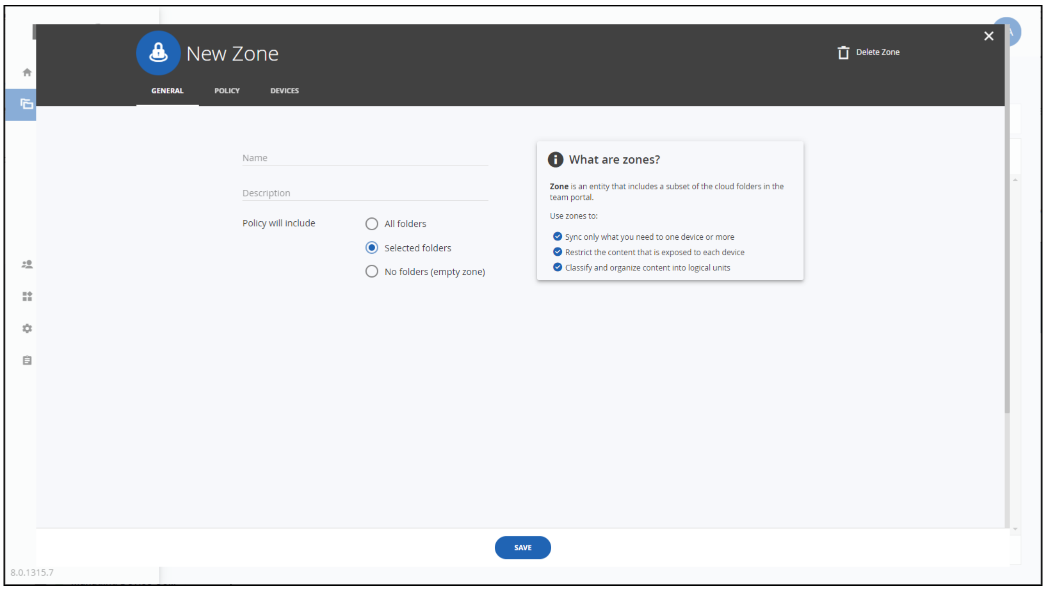


Or,

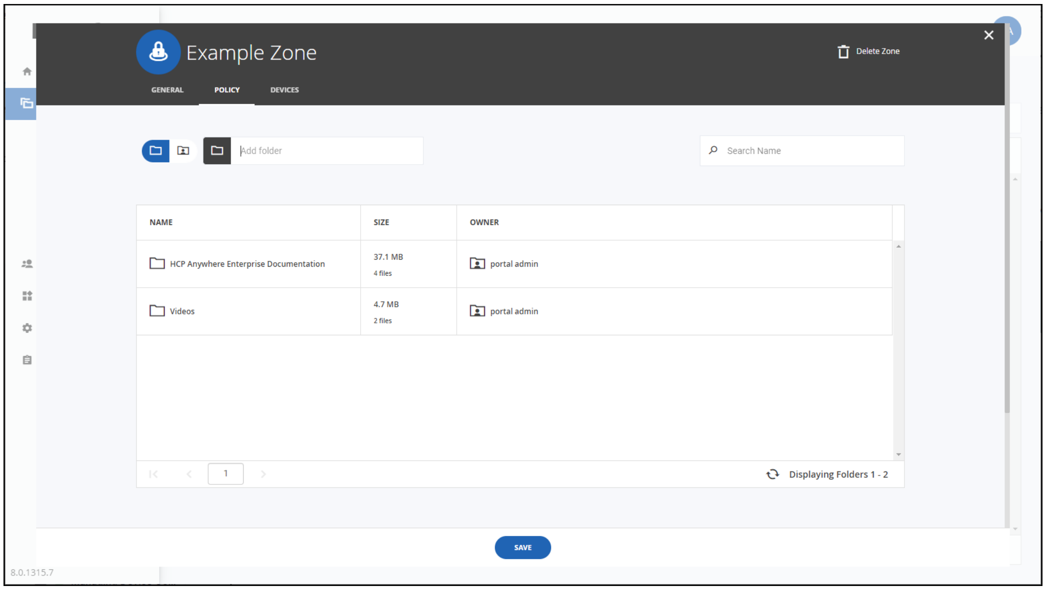
- Edit an existing zone, click the zone name**.**
  The zone window is displayed with the zone name as the window title.

3. Complete the fields in the **GENERAL** tab:

   Name – A name for the zone. The name must be unique. The name can contain alpha, numeric and space characters. You must enter a name to specify selected folders or edge filers.
   Description – A description for the zone.
   Policy will include – The folder policy to apply to the zone.
   - **All Folders** – All the folders in the global namespace are included in the zone.
   - **Selected Folders** – Only the specified folders are included in the zone. When this option is selected, the **POLICY** tab is displayed, enabling you to specify the folders to include in the zone.

     Select cloud folders or user folders and then start typing the name of a folder. The list of folders that match what you type is displayed, enabling you to select the folders to add to the zone.
     Folders are identified by the **OWNER** column in the **POLICY** tab.



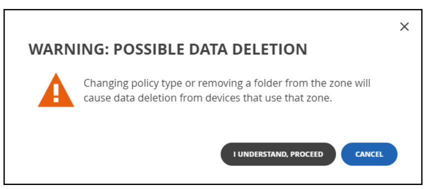
Note: Adding a cloud folder automatically includes all the cloud folder subfolders. Any folder added to the cloud folder at a later date is also included automatically in the zone.

- **No Folders** – The zone will not include any folders.

4. In the **DEVICES** tab, specify edge filers that can see the folders in the zone. When edge filers are specified, only those edge filers have access to the folder in the zone. When no edge filers are selected, every edge filer has access to the folders in the zone.

   Start typing the name of an edge filer. The list of edge filers that match what you type is displayed, enabling you to select the edge filers to add to the zone.

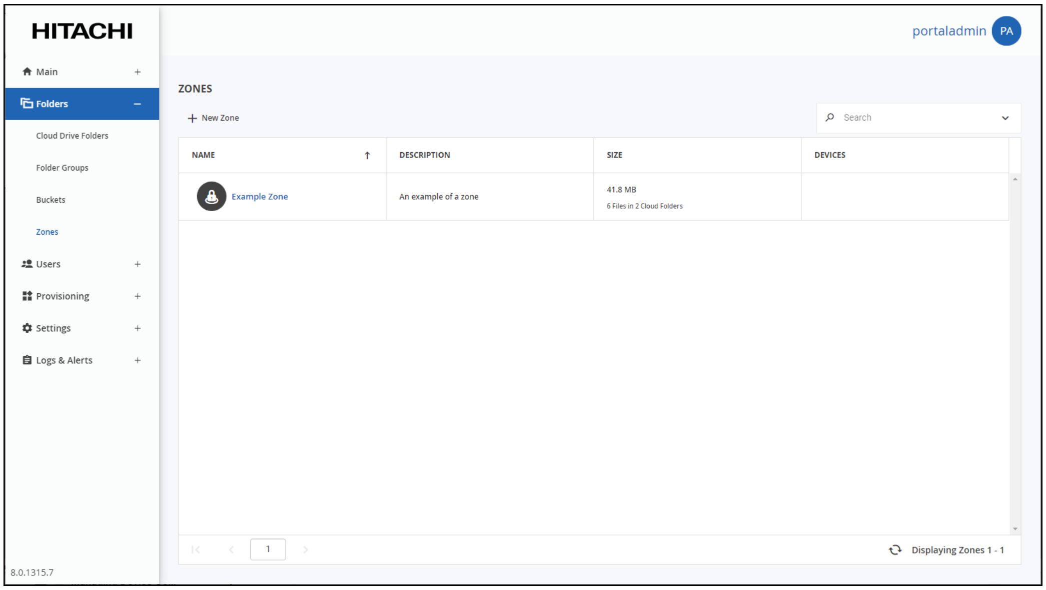
   Note: An edge filer that has already been added to a zone can still be added to another zone. If you change the policy for a zone from **All folders**, the following warning is displayed.



   To continue with the change, click **I UNDERSTAND, PROCEED**. Otherwise, click **CANCEL**.

5. Click **SAVE**.

The zone is created or updated.



Deleting a Zone

If only one zone is defined, it cannot be deleted. Also, if a zone is defined as the default zone, as described in Setting or Unsetting the Default Zone, it cannot be deleted. If the zone to delete is the default zone, first make another zone the default zone, in order to delete this zone.

To delete a zone:

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.
2. Select the zone's row.
3. Click **Delete.**

   A confirmation window is displayed.
4. Click **DELETE** to confirm.

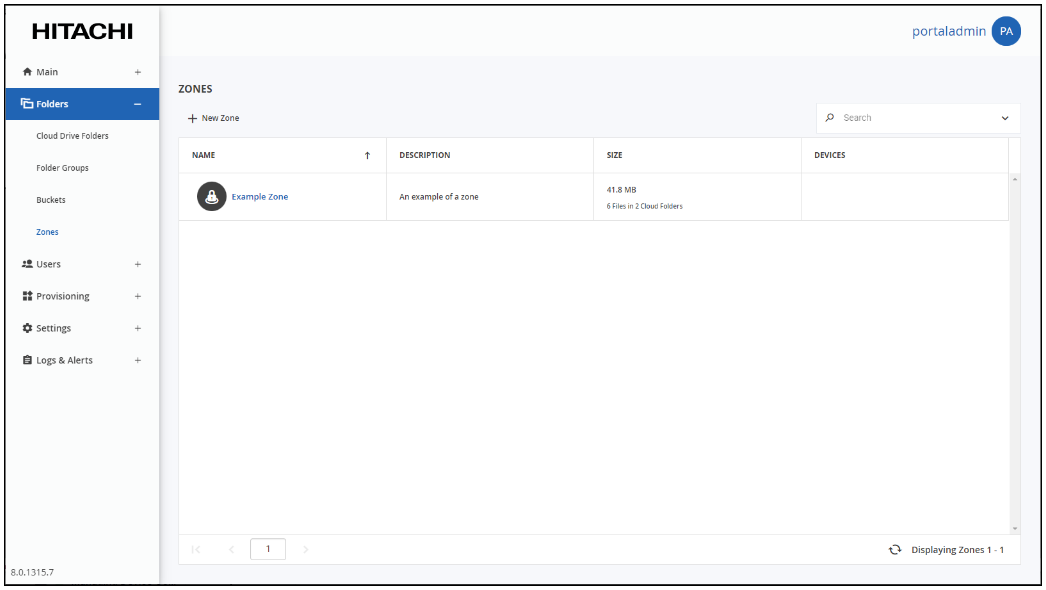
The zone is deleted.

Viewing Zones

Each team portal can define the zones for that specific team portal.

To view zones:

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.

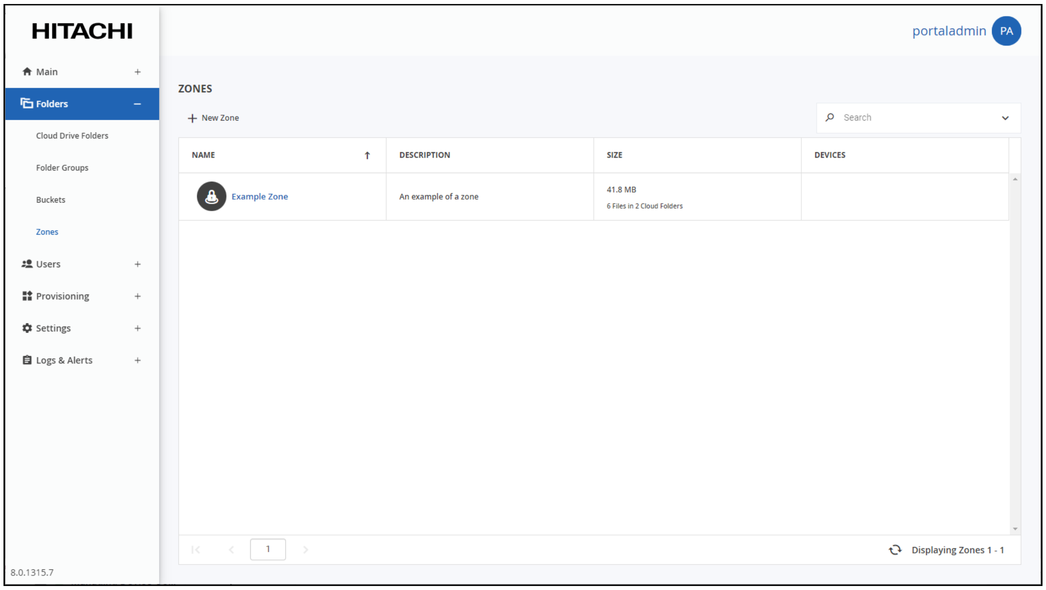


NAME – The zone's name.
DESCRIPTION – An optional description of the zone.
SIZE – The current size of the cloud folder in the zone. The total number of files and folders is displayed under the size.
DEVICES – The list of edge filers that are included in the zone. If no edge filers are listed, all edge filers are included.

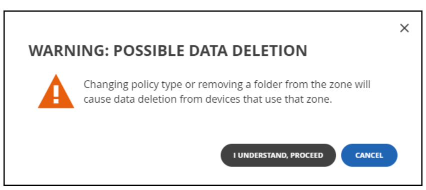
Removing a Folder from a Zone

To remove a folder from a zone:

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.



2. Click the zone with the folders to remove.
3. Click the **POLICY** tab.
4. Select the folder’s row.
5. Click **Remove from zone**.
   A confirmation window is displayed warning that the folder will be deleted from the edge filers using the zone. Click that you understand to delete the folder from the zone.

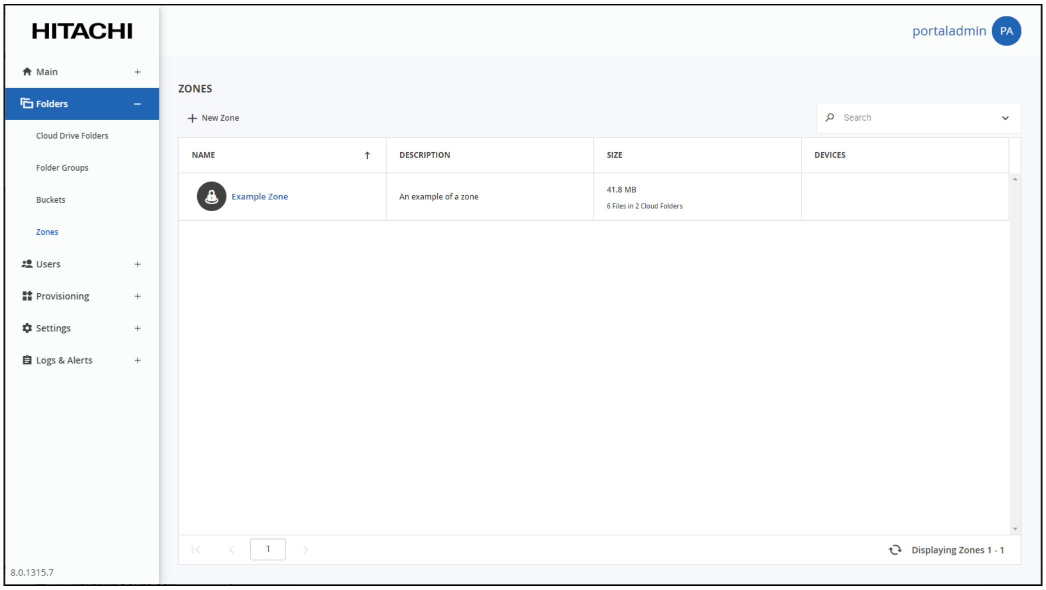


The selected folder is removed from the zone.

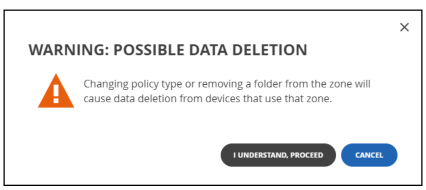
Removing a HCP Anywhere Enterprise Edge Filer from a Zone

To remove an edge filer from a zone:

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.



2. Click the zone with the edge filers to remove.
3. Click the **DEVICES** tab.
4. Select the edge filer's row.
5. Click **Remove from zone**.
   A confirmation window is displayed warning that all the content of the zone will be deleted from the HCP Anywhere Enterprise Edge Filer. Click that you understand to delete the HCP Anywhere Enterprise Edge Filer from the zone.

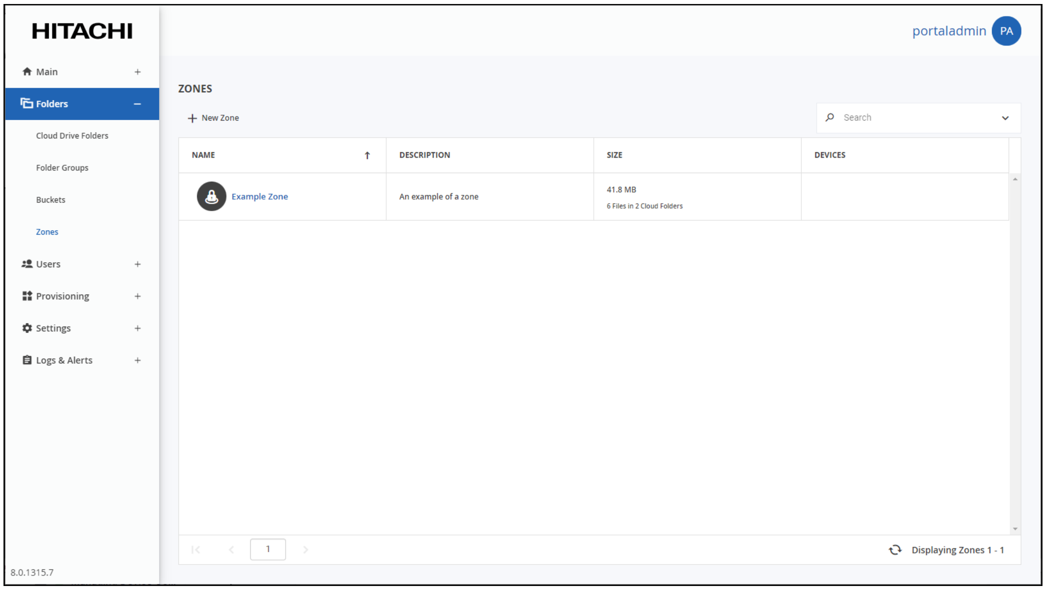


The selected HCP Anywhere Enterprise Edge Filer is removed from the zone. If a HCP Anywhere Enterprise Edge Filer is removed from all the zones, it is automatically added to the default zone.

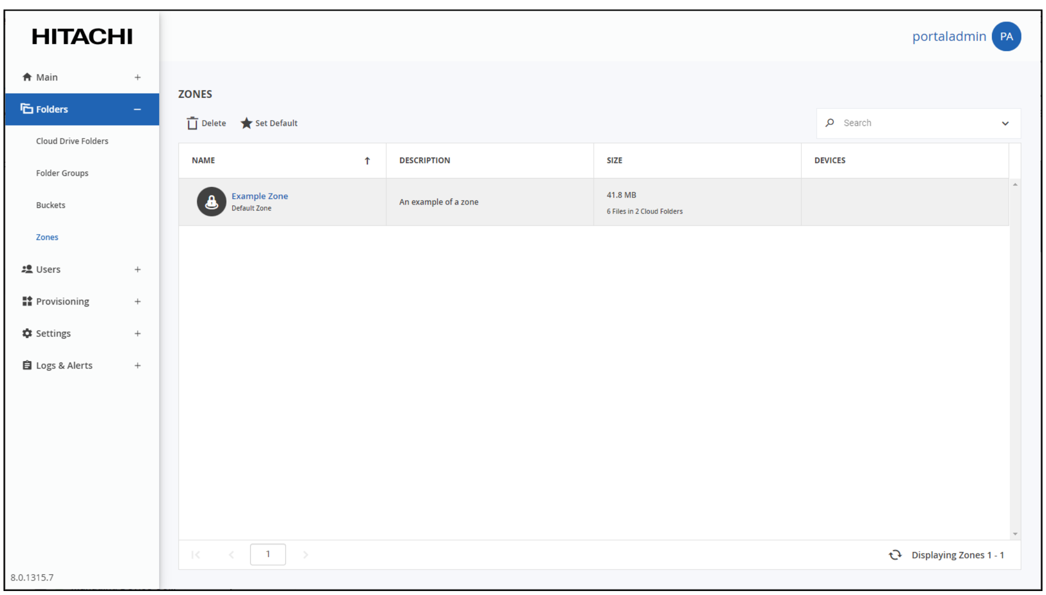
Setting or Unsetting the Default Zone

To set a zone as the default:

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.

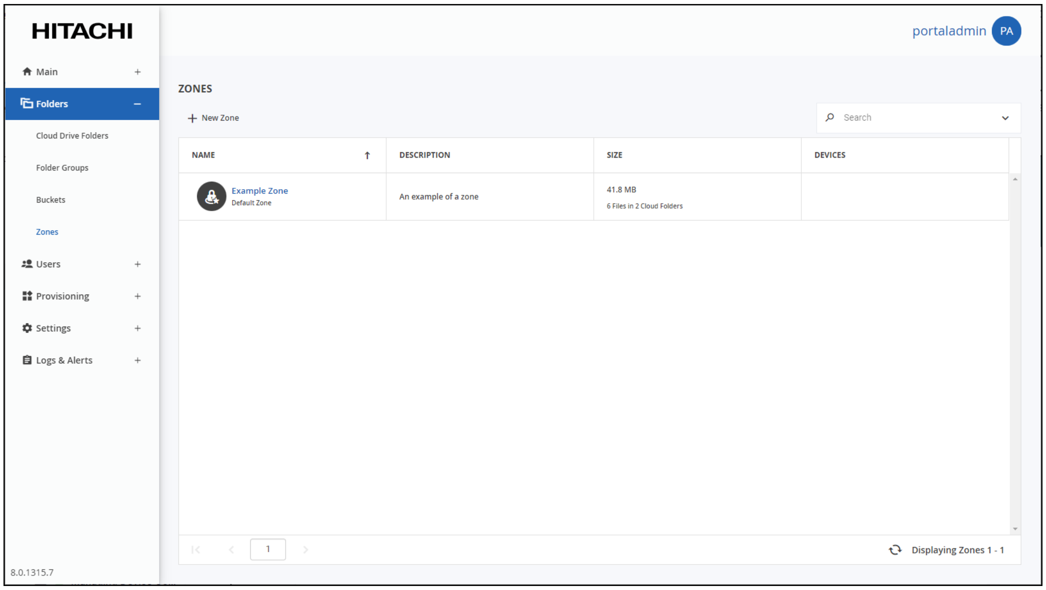


   The **ZONES** page opens, displaying all the zones.
2. Select the desired zone's row.



3. Click **Set Default**.

The selected zone becomes the default zone. `Default Zone` is displayed under the zone name.



To remove a zone from being the default:

Note: To remove the default setting from a zone requires specifying another zone as the default zone.

1. Select **Folders > Zones** in the navigation pane.
   The **ZONES** page opens, displaying all the zones.
2. Select the zone's row that will become the default zone instead of the current default zone.
3. Click **Set Default.**

   The selected zone replaces the old default zone as the default.

Chapter 7. Managing Snapshots

The HCP Anywhere Enterprise Portal retains previous file versions for each user, by using snapshots. Snapshots are read-only copies of files as they were at a particular point-in-time.

A new snapshot is created every 30 seconds.

In addition to the snapshots of previous versions, the HCP Anywhere Enterprise Portal manages a current snapshot, which is writable and includes every change made to data. After the snapshot is closed it becomes read-only, as a new current snapshot is created. In case of a failure, recovering any file from the current snapshot is immediate, so the RPO is almost zero (you only lose the last changes made locally that were not synced to the portal before the failure).

The HCP Anywhere Enterprise Portal creates snapshots automatically and retains them according to a configurable snapshot retention policy. So long as a snapshot is retained by HCP Anywhere Enterprise Portal, the relevant version of the user data can be retrieved.

HCP Anywhere Enterprise Portal supports snapshots of the HCP Anywhere Enterprise Portal Cloud Drive.

In this chapter

The Snapshot Retention Policy Options

A retention policy specifies the following:

- **The number of hours to retain all snapshots**
  Every snapshot is retained for this amount of time. After this time has passed for any given snapshot, the snapshot may be retained or deleted depending on the other settings.
- **The number of hourly snapshots to retain**
  For example, if hourly snapshots are set to 10, then the last 10 hourly snapshots are retained. If daily snapshots are set to 0, then the hourly snapshot are deleted when the next hour starts.
- **The number of daily snapshots to retain**
  For example, if daily snapshots are set to 10, then the last 10 daily snapshots are retained. If daily snapshots are set to 0, then the daily snapshot are deleted when the next day starts.
  Note: A day is defined as starting at 00:00:00 and ending at 23:59:59.
- **The number of weekly snapshots to retain**
  A weekly snapshot is the latest snapshot taken during the week.
  Note: A week is defined as starting on Monday and ending on Sunday.
  Example 1: Snapshots were successfully taken every day until the current day, which is Sunday. The weekly snapshot is the one taken on Sunday, as it is the latest snapshot taken this week.

Example 2: Snapshots were successfully taken every day until the current day, except the Saturday and Sunday snapshots, which were not taken because the device was turned off. The weekly snapshot is the one taken on Friday, as it is the latest snapshot taken this week.

- **The number of monthly snapshots to retain**
A monthly snapshot is the latest snapshot taken during the month.
Example 1: Snapshots were successfully taken every day until the current date, which is April 30th. The monthly snapshot is the one taken on the 30th, as it is the latest snapshot taken this month.
Example 2: Snapshots were successfully taken every day until the current date, except snapshots for the 25th through the 30th, which were not taken because the device was turned off. The monthly snapshot is the one taken on the 24th, as it is the latest snapshot taken this month.
- **The number of quarterly snapshots to retain**
A quarterly snapshot is the latest snapshot taken during the quarter.
Example 1: Snapshots were successfully taken every day until the current date, which is the March 31. The quarterly snapshot is the one taken on March 31st, as it is the latest snapshot taken this quarter.
Example 2: Snapshots were successfully taken every day until the current date, except snapshots for March 25 through 31 were not taken because the device was turned off. The quarterly snapshot is the one taken on March 24th, as it is the latest snapshot taken this quarter.
- **The number of yearly snapshots to retain**
A yearly snapshot is the latest snapshot taken during the year.
Example 1: Snapshots were successfully taken every day until the current date, which is the December 31st. The yearly snapshot is the one taken on the 31st, as it is the latest snapshot taken this year.
Example 2: Snapshots were successfully taken every day until the current date, except snapshots for the 25nd through the 31st were not taken because the device was turned off. The yearly snapshot is the one taken on the 24th, as it is the latest snapshot taken this year.
- **The numbers of days to keep deleted files**
The retention period for deleted files. This retention period applies only to the current snapshot. When portal users delete a file or a folder, either via the Web interface or via the local synchronization folder, the deleted data is moved to a trashcan. It is then retained in the trashcan for a number of days, defined in the retention policy of the user's assigned subscription plan. As long as files are retained, users can recover their deleted data.
The minimum value is 1 day.

Note: The snapshots retention policy does not apply to the current snapshot, which remains on the portal until it is replaced by a newer snapshot. The moment a snapshot is not current it follows the retention policy, based on the time the snapshot was taken.

Configuring a Snapshot Retention Policy

The snapshot retention policy is configured as part of the subscription plan described in Provisioning and specifically in steps **4** and **5** of the procedure To add or edit a subscription plan:, in the S**napshot Retention Policy** window.

Snapshot Retention for the Cloud Drive Service

Each user account using the Cloud Drive service is assigned a home folder in the HCP Anywhere Enterprise Portal, when the user account is created. This Cloud Drive home folder serves as the block destination for HCP Anywhere Enterprise Edge Filer sync operations. Snapshots of Cloud Drive folders are taken for each folder once every 30 seconds, if there were any changes in the folder during that 30 seconds.

For example, assume a file is synced to the portal at 09:10am. The portal opens a snapshot which will close after 30 seconds. At 09:24am a new file is synced to the portal and a new snapshot is opened. Between 09:10am and 09:24am no snapshot is open, since there are no changes between the user local files and the files synced to the portal. The first snapshot is registered as a previous version, with the opening time for the snapshot, 9:10am.

Applying a Snapshot Retention Policy

Snapshot retention policies can be applied as part of the subscription plan at the following levels:

At the portal level – The snapshot retention policy defined in the subscription plan applies to all users in the portal, as described in Provisioning.

At the user level – A subscription plan including the snapshot retention policy can be applied to individual users in the portal. See Provisioning User Accounts for details about assigning a subscription plan to an individual user account.

Applying a Snapshot Retention Policy at Both the Virtual Portal and User Levels

When a snapshot retention policy is assigned to a portal, the policy is globally enforced as a set of maximum values for all users in the portal. Individual users in that portal can be assigned user-level snapshot retention policies, so long as the values in the user-level policy do not exceed those of the portal-level policy.

For example, a portal called *example* is assigned a subscription plan, *example-plan*, which includes the following snapshot retention policy.

- Retain 7 daily snapshots
- Retain 4 weekly snapshots
- Retain 12 monthly snapshots

Users in the *example* portal cannot be assigned a snapshot retention policy that exceeds the values specified in *example-plan*. Therefore, users in this portal cannot be assigned the following snapshot retention policy:

- Retain 10 daily snapshots
- Retain 15 weekly snapshots
- Retain 17 monthly snapshots

However, they can be assigned the following snapshot retention policy:

- Retain 6 daily snapshots

- Retain 2 weekly snapshots
- Retain 9 monthly snapshots

Applying a Snapshot Retention Policy For a Shared Folder

When two users with different snapshot retention policies collaborate on the same file, snapshots are retained according to the project owner's retention policy.

Snapshot Consolidation

The *snapshot consolidator* is a scheduled job that runs every hour. It is responsible for deleting all the snapshots that should not be retained, according to the retention policy.

Chapter 8. Provisioning

Users in the team portal obtain services through subscription plans for an open-ended period of time.

A portal is subscribed to a global plan that determines the maximum licenses and snapshot retention policies for the whole portal. A default user subscription plan is created automatically and contains the licenses specified in the global plan. All user accounts are assigned to this default plan.

You can create alternate subscription plans and assign those to individual user accounts. You can change the default plan that is assigned to users. You can also define conditions for automatically assigning plans to users based on user attributes.See Provisioning User Accounts for details about assigning a subscription plan to an individual user account.

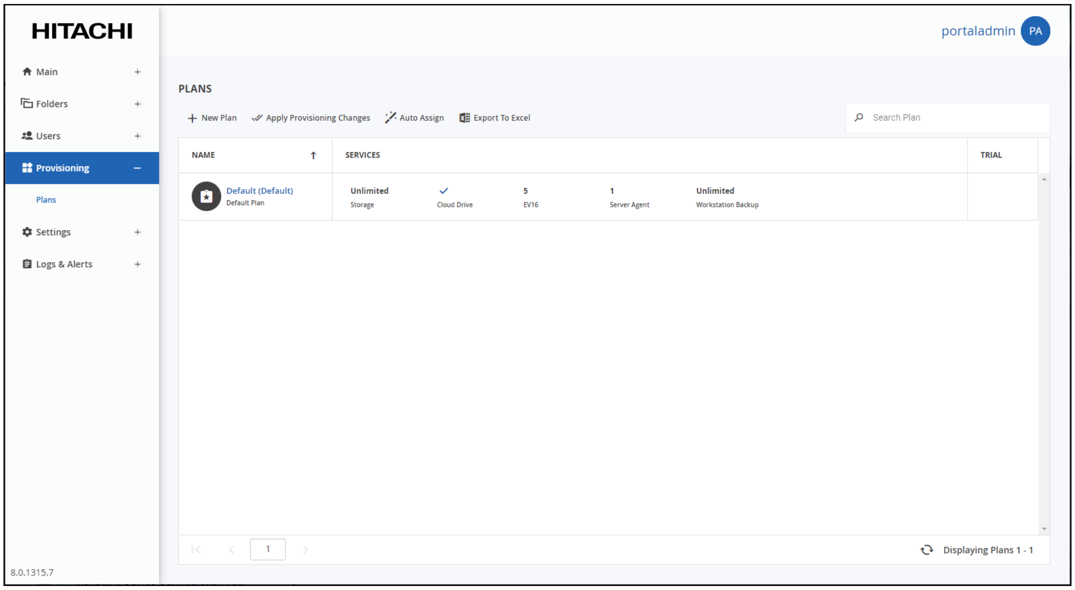
In this chapter

See Provisioning User Accounts for details about assigning a subscription plan to an individual user account.

Viewing Subscription Plans

To view all plans:

- Select **Provisioning > Plans** in the navigation pane.
  The **PLANS** page is displayed.



The page includes the following:
NAME – The subscription plan's name. Default Plan is displayed under the plan name for the default plan.
SERVICES – The services provisioned in the plan. The following list includes all the services. The services displayed in a specific plan are the services that are licensed.

Storage – The amount of storage allocated for the plan.
Cloud Drive or **Cloud Drive Connect** – The portal is provisioned either for full access to the portal, Cloud Drive, or for restricted access for example, when a HCP Anywhere Enterprise Edge Filer becomes unavailable and users need to be able to almost seamlessly continue working by connecting to the portal for their files, Cloud Drive Connect.
EV8 – The number of EV8 HCP Anywhere Enterprise Edge Filer licenses included in the plan.
EV16 – The number of EV16 HCP Anywhere Enterprise Edge Filer licenses included in the plan.
EV32 – The number of EV32 HCP Anywhere Enterprise Edge Filer licenses included in the plan.
EV64 – The number of EV64 HCP Anywhere Enterprise Edge Filer licenses included in the plan.
EV128 – The number of EV128 HCP Anywhere Enterprise Edge Filer licenses included in the plan.
EV256 – The number of EV256 HCP Anywhere Enterprise Edge Filer licenses included in the plan.
Server Agent – The number of HCP Anywhere Enterprise Agent licenses included in the plan.

TRIAL – If the plan includes a free trial period, this column displays the number of days included in the free trial period.

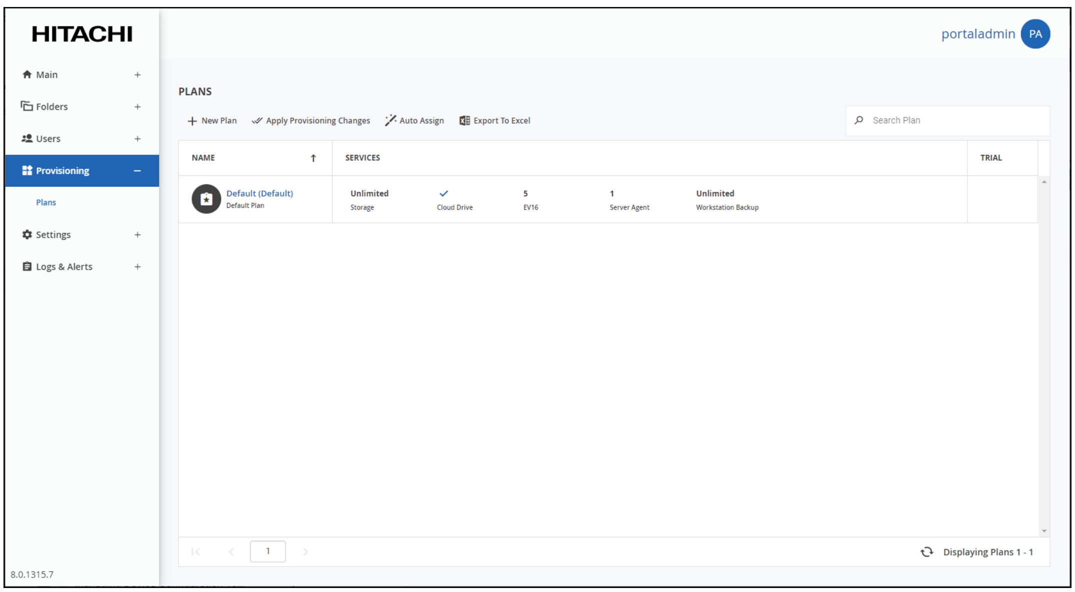
Adding, Editing, or Deleting a Subscription Plan

Adding or Editing a Subscription Plan

Note: Editing a plan that has already been assigned to users can change what the users can do. For example, if you change a plan by changing the cloud drive license from **Full** to **None**, all users with the plan will not be able to access their cloud drive. The cloud drive content is not deleted from the portal, so the team administrator can assign these users with a plan that includes the **Full** cloud drive license and this will re-enable the users to access their files.

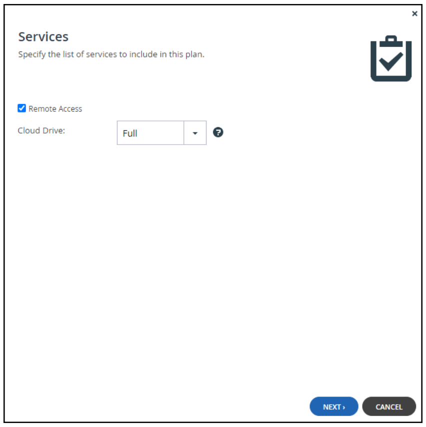
To add or edit a subscription plan:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.



2. To add a new plan, click **New Plan**.

   Or,
   To edit an existing plan, click the plan's name**.**
   The plan wizard opens, displaying the **Services** window.



3. Choose which services to include in the plan:

   Remote Access – Include remote access in the subscription plan. Remote access includes both access to the device's management interface via the HCP Anywhere Enterprise Portal and a dedicated URL, access to the user's files via the HCP Anywhere Enterprise Portal and a dedicated URL.

   Note: Device owners can disable remote access via the device's management interface.

   Cloud Drive – Select the license type you want.

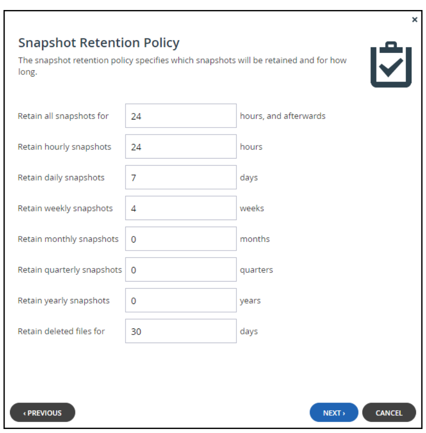
   Full – The HCP Anywhere Enterprise Portal can be accessed by users.

   Connect – Users can access their folders and files and add to them. Users cannot sync their files nor share them with other users.

   None – Cloud drive services are not included in the plan.

4. Click **NEXT**.

   The **Snapshot Retention Policy** window is displayed. This policy applies to Cloud Drive snapshots from HCP Anywhere Enterprise Edge Filers.



5. Set the snapshot retention policy.

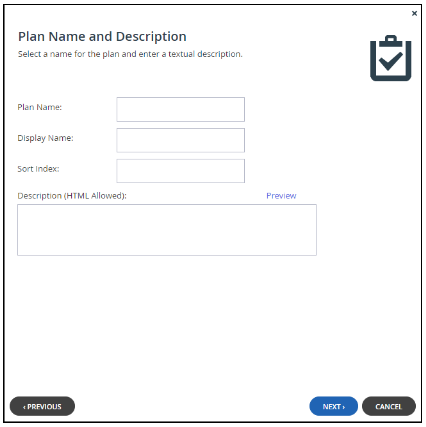
   Retain all snapshots for – The number of hours after creation that all snapshots are retained.
   Retain hourly snapshots – The number of hourly snapshots that are retained.
   Retain daily snapshots – The number of daily snapshots that are retained.
   Retain weekly snapshots – The number of weekly snapshots that are retained.
   Retain monthly snapshots – The number of monthly snapshots that are retained.
   Retain quarterly snapshots – The number of quarterly snapshots that are retained.
   Retain yearly snapshots – The number of yearly snapshots that are retained.

Retain deleted files for – The number of days to retain deleted files. The minimum is 1 day.

Note: For an explanation of each policy, see Managing Snapshots.

6. Click **NEXT**.

   The **Plan Name and Description** window is displayed.

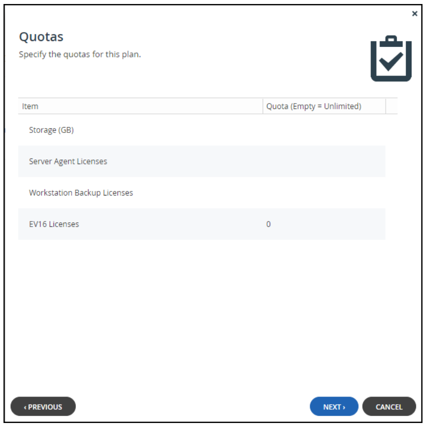


7. Specify the plan name and provide a description.

   Plan Name – A name for the plan. Only letters and numbers can be used for the name.
   Display Name – The name to use when displaying this plan in the end user portal and notifications.
   Sort Index – Optionally, an index number to assign the plan, to enable custom sorting of the plans displayed to end users in the Subscribe to Plan wizard.
   Description – A description of the plan. HTML tags can be used in the description.
   Click **Preview** to open a new page in the browser displaying the plan description.

8. Click **NEXT**.

   The **Quotas** window is displayed.



9. For each item, click in the quota field and enter the number to include in the plan.

   For example, to include 100GB of storage space, click in the Storage (GB) item's quota field and enter 100.

   Note: The quotas must not exceed the number specified in the license. An error message is displayed when you attempt to assign a user to a plan with a quota that exceeds the number specified in the license. The items shown are the items that are licensed.

10. Click **NEXT**.

The **Wizard Completed** screen is displayed.

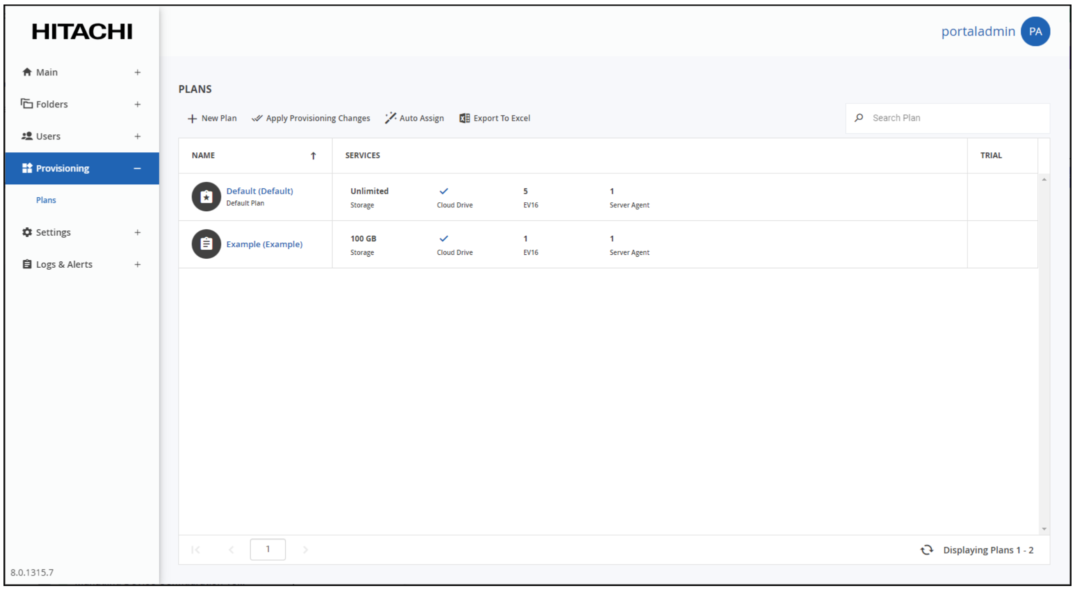
11. Click **FINISH**.

New plans are applied every day at midnight. Existing plans that are edited are immediately applied. You can use apply new plan changes immediately by clicking **Apply Provisioning Changes**. The **Apply Provisioning Changes** window is displayed and the changes are applied. Either click **CONTINUE IN BACKGROUND** or wait for the update to complete and click **CLOSE**.

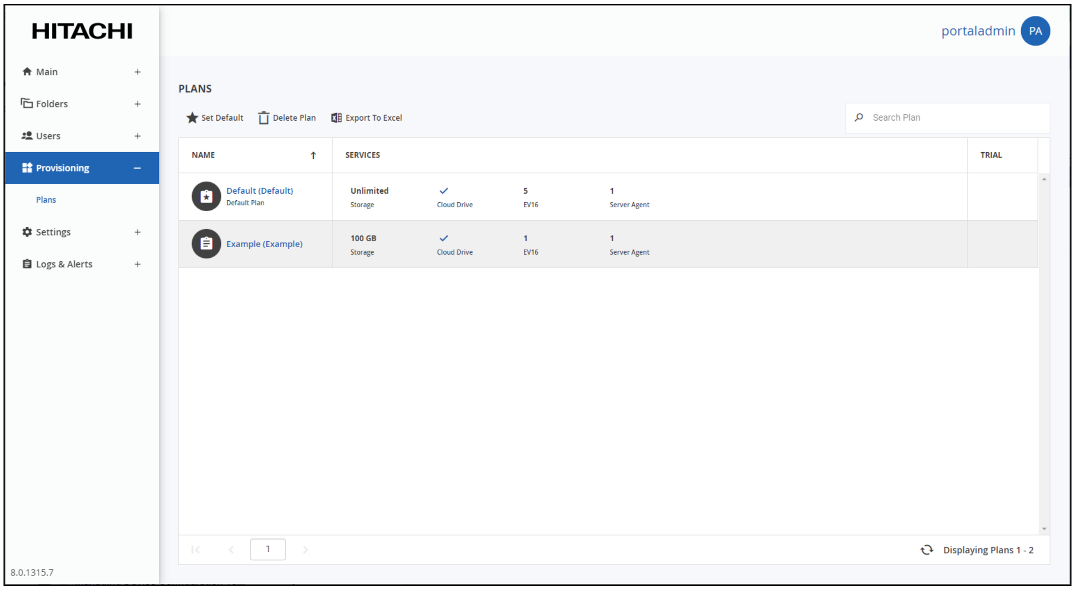
Deleting a Plan

To delete a plan:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.



2. Select the plan's row.



3. Click **Delete Plan.**

   A confirmation window is displayed.
4. Click **DELETE** to confirm.

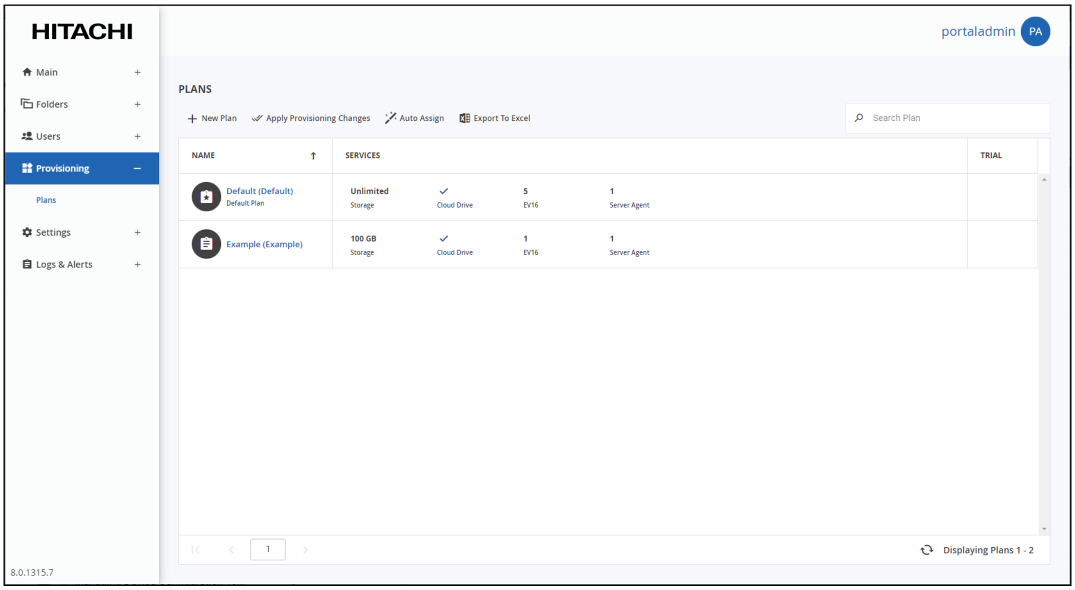
The subscription plan is deleted.

Setting or Unsetting the Default Plan

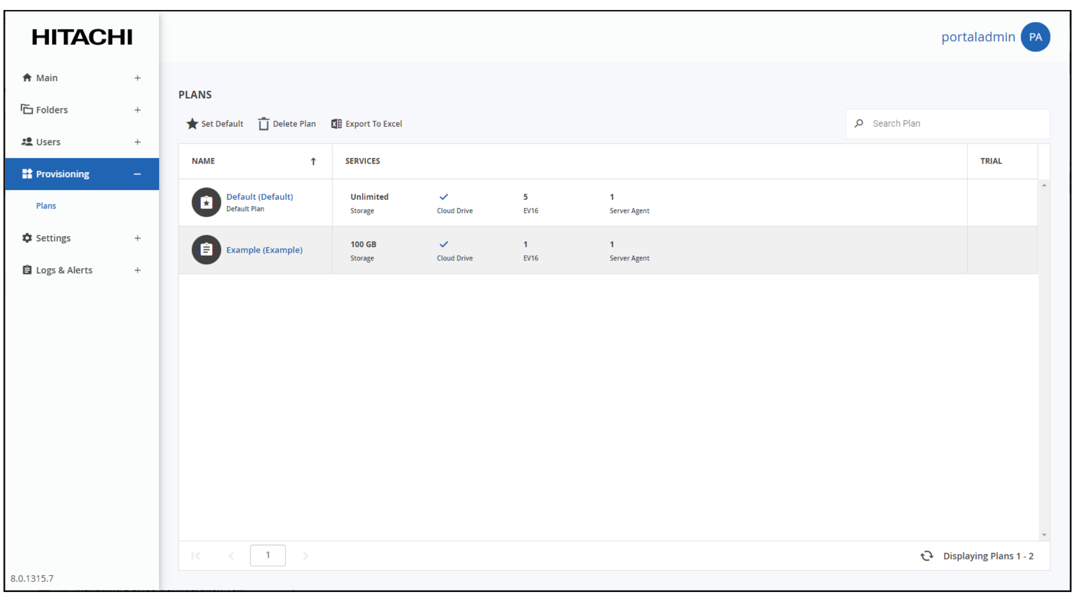
The default plan is automatically assigned to all new user accounts.

To set a plan as the default:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.



2. Select the desired plan's row.



3. Click **Set Default.**

The selected plan becomes the default subscription plan. The plan icon changes to reflect that the plan is the default and `Default Plan` is displayed under the plan name.

To remove a subscription plan from being the default:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.
2. Select the default subscription plan's row.
3. Click **Remove Default.**

The subscription plan is no longer the default.

Automatically Assigning Plans

Automatic plan assignment allows you to define a policy that determines which subscription plans will be assigned to which users.

You can automatically assign subscription plans based on the following user attributes:

- Username
- User Groups
- Role
- First Name
- Last Name
- Company
- Billing ID
- Comment

The policy rules are processed in ascending order. The first rule that matches applies. You can change the rules' order by using the Move Down/Move Up buttons. You can also choose to apply a default plan in the event that no rule applies.

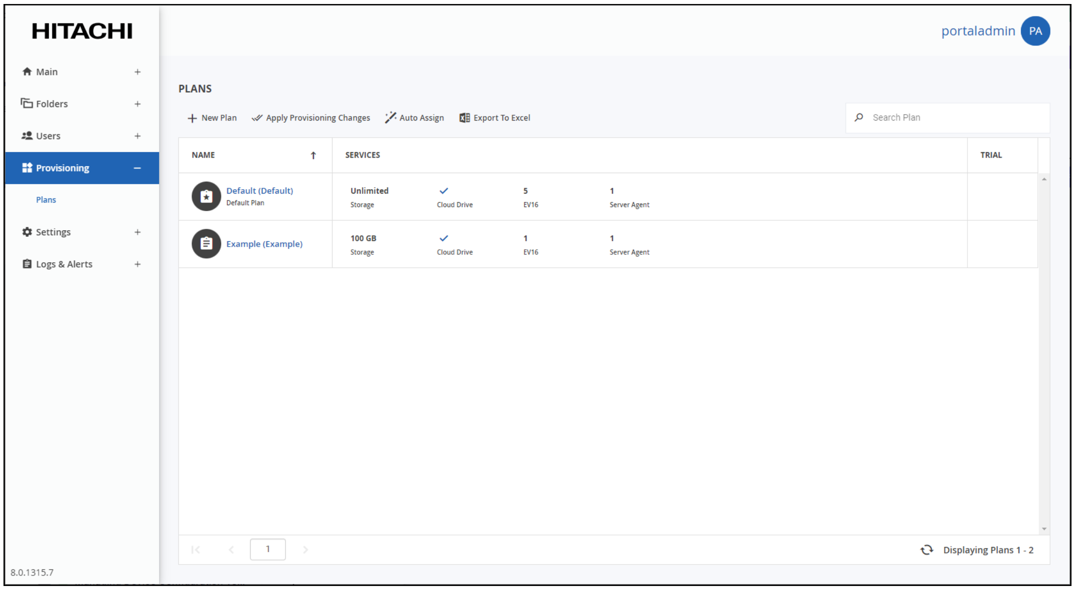
If the portal is integrated with a Directory Service, such as Active Directory you can define a policy even before users have joined the service, so that when users join, they are automatically assigned the appropriate plan to get the correct quota and licenses.

Note: In order that new users in an Active Directory group are automatically assigned to a plan, the Active Directory group must have been fetched or already in the Active Directory groups under the portal.

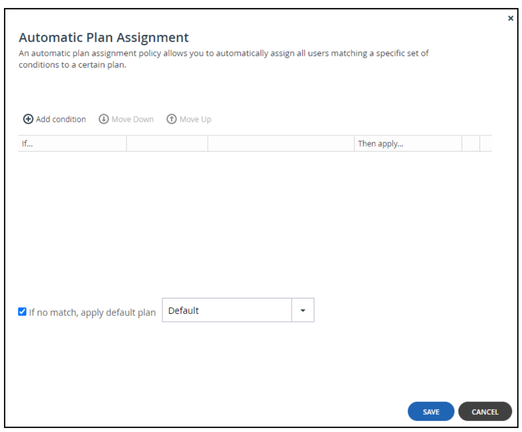
For details about using directory services, see Using Directory Services For the Users.

To configure automatic plan assignment:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.



2. Click **Auto Assign**.
   The **Automatic Plan Assignment** window is displayed.



3. Click **Add condition** to define a condition.
   a) In the **If** column select a user attribute.
   b) Select an operator, such as *is one of*.
   c) Enter a value to apply on the operator.
   When adding a condition for *User Groups*, the only operator is *includes one of*. You have to put the exact name of the group to apply the plan and not part of the name, even if that part is unique.
   d) In the **Then apply** column select a plan to apply if a user satisfies the condition.
   e) Order the conditions by selecting a condition and using the **Move Down** and **Move Up** options to move the condition to the required place in the list.
   The order of the conditions is critical to applying the correct plan. For example, if a user is

a member of two different groups in the auto plan assignment, whichever condition applies to the group the user is in first in the list of conditions is the plan that user gets. Therefore, order the list of conditions with the least restrictive conditions at the top of the list.

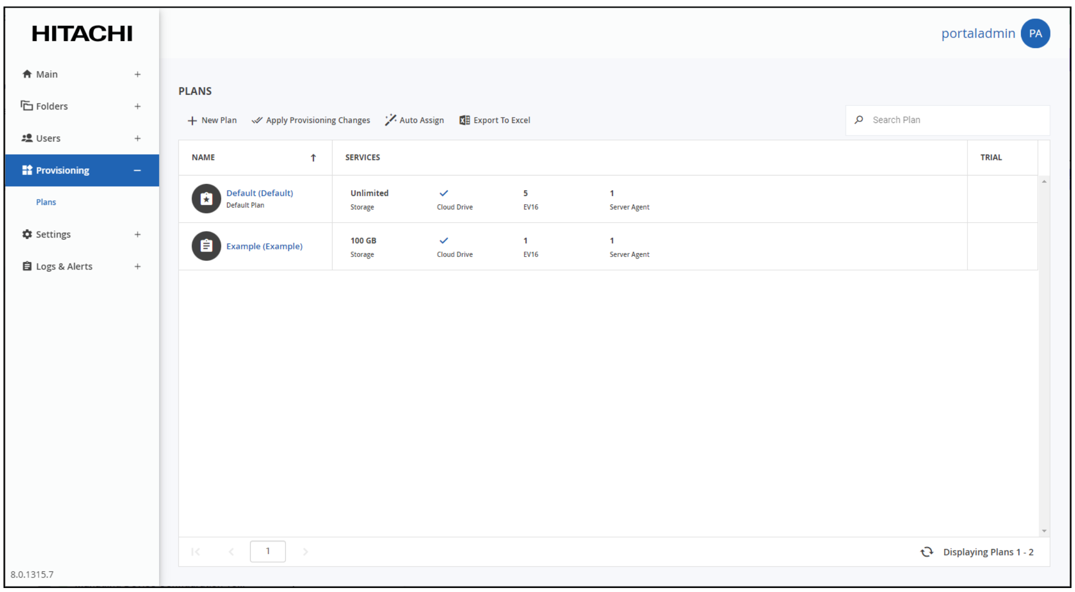
4. To delete a condition, click in its row.
5. Click **SAVE**.

Exporting Plan Details to Excel

You can export a list of plans and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of plans to Microsoft Excel:

1. Select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page opens, displaying all the plans.



2. Click **Export to Excel**.

The list of plans is exported to your computer. Each plan includes the HCP Anywhere Enterprise Agent, HCP Anywhere Enterprise Edge Filer, and cloud drive quotas.

Chapter 9. Using Directory Services For the Users

HCP Anywhere Enterprise Portal can be integrated with the following directory services:

- Microsoft Active Directory – If you are integrating the HCP Anywhere Enterprise Portal with Active Directory, make sure the ports described in the planning part of the portal installation guide are opened.
- LDAP directory services:
  - OpenDS
  - Oracle Unified Directory
- Apple Open Directory

User accounts are automatically fetched and refreshed from the directory, and user authentication is performed using the directory.

Portal administrators can define an access control list specifying which directory service groups and individual users are permitted to access the portal, and which user roles they are assigned in the portal.

Note: Users must have an email address, as well as a first and last name, defined in the directory service. Users without one of these attributes cannot log in to the portal and will cause synchronization to fail.
Nested groups are not supported by default since supporting nested groups has a performance impact. If you need support for nested groups, contact Hitachi Vantara support.

After users are fetched, they can be viewed in the portal. For details, see Managing Users.

In this chapter

How Directory Service Synchronization Works

When integrated with a directory service, the portal fetches user data from the directory upon the following events:

- An administrator can manually fetch specific users from the directory. See Manually Fetching User Data.
- If a user attempts to sign in, but does not yet have a local portal account, their user account is automatically fetched from the directory.
- The directory services settings are configured to automatically create a local portal account, without the user having to sign in to the portal.
- The portal automatically re-fetches all previously fetched directory users, every day at midnight, as part of the daily *Apply provisioning changes* task.
- An administrator can force a re-synchronization of all previously fetched directory users, by running the **Apply Provisioning Changes Wizard**. See Applying Provisioning Changes.

HCP Anywhere Enterprise Portal handles special cases as follows:

- If during the fetch it is determined that a user exists in the local user database but not in the directory, then the user is assumed to have been deleted, and HCP Anywhere Enterprise Portal deletes the user from the local user database. The user's folders are not deleted.
- If the access control list specifies that the user is no longer allowed to access HCP Anywhere Enterprise Portal, then HCP Anywhere Enterprise Portal changes the user account's role to "Disabled". The user account is not deleted.

Note: Each virtual portal can optionally be integrated with a different Active Directory or LDAP directory.

Integrating HCP Anywhere Enterprise Portal with a Directory Service

Before integrating the portal to an active directory, to set up integration with TLS:

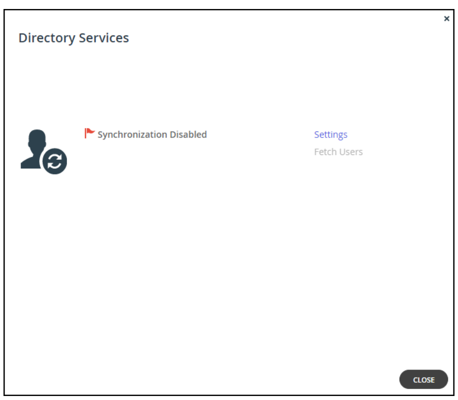
- LDAPS (TCP port 636) and Global Catalog SSL (TCP port 3269) ports must be opened.
- Domain controllers must have a domain controller certificate with the EKU (Enhanced Key Usage) Client Authentication/ServerAuthentication.
  - **a)** On the domain controller, open the Certificates MMC and export the domain controller certificate into **`.cer`** format.
  - **b)** Import the certificate on each HCP Anywhere Enterprise Portal application server: Log in to each HCP Anywhere Enterprise Portal application server using SSH and then run the command: `portal-cert.sh import -f` *`certificate`*`.cer` *`Alias Name`*

  Note: You only need to import the certificate and not the whole certificate chain.
  - **c)** After importing the certificate to each HCP Anywhere Enterprise Portal application server, run the command to start the portal: `portal-manage.sh restart`
  - **d)** Follow the instructions in Active Directory, checking **Use TLS**.
  - **e)** Remove access to ports TCP 389 and TCP 3268.

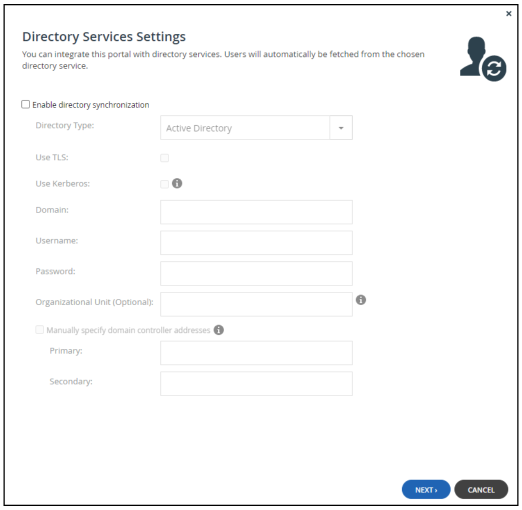
To integrate a virtual portal with a directory service:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **Directory Services** under **USERS** in the **Control Panel** page.
   The **Directory Services** window is displayed.



3. Click **Settings** to set directory settings, including enabling connecting to a directory service. If you have already connected to a directory service, you can fetch all the users from the domain by clicking **Fetch Users**, as described in Manually Fetching User Data.
   After clicking **Settings**, the **Directory Services Settings** window is displayed.

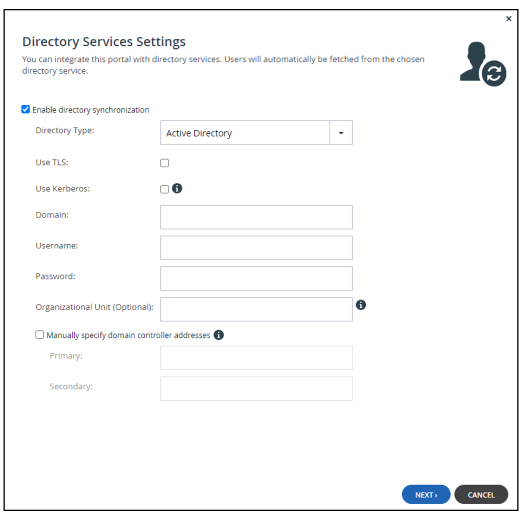


Enable Directory Synchronization – Enable integration with a directory domain.
Directory Type – The type of directory with which to integrate portal:

- Active Directory
- LDAP
- Apple Open Directory

After selecting the directory type the fields are enabled and match the type selected.

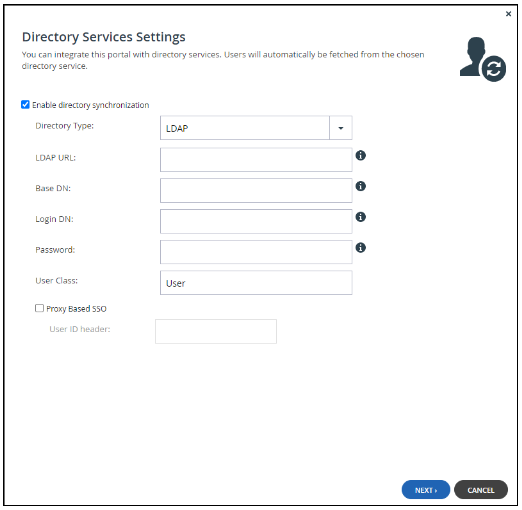
Active Directory



Use TLS – Connect to the Active Directory domain using SSL.
Use Kerberos – Use the Kerberos protocol for authentication when communicating with the Active Directory domain. This is useful for achieving Single Sign-on (SSO) with Windows computers. If unchecked, NTLM is used.
Note: Only one team portal, per system, can use Kerberos.
Domain – The name of Active Directory domain with which you want to synchronize users.
Username – The name to use for authenticating to Active Directory.
Password – The password for authenticating to Active Directory.
Organizational Unit (Optional) – The name of the organizational unit within the Active

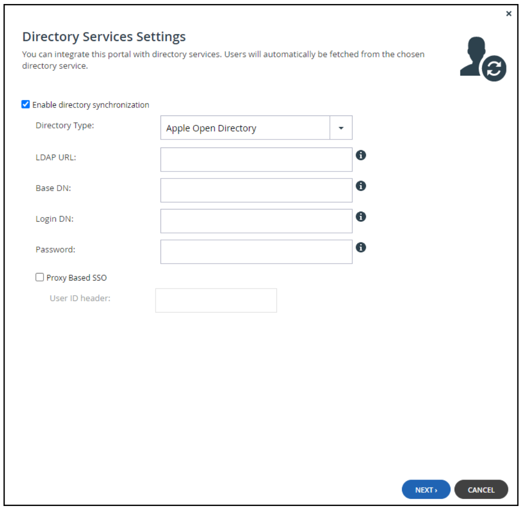
Directory domain.
Manually specify domain controller addresses – The IP address of the Active Directory domain controllers. If unchecked, DNS is used to automatically find the domain controllers.
 Primary – The address of the primary domain controller.
 Secondary – The address of the secondary domain controller.

LDAP Directory Server



LDAP URL – The URL to connect to the LDAP server. Both ldap and ldaps are supported. The default port is 389 for *ldap* and 636 for *ldaps*.
Base DN – Optional: The base DN of the LDAP server.
Login DN – The bind DN: The distinguished name of a user with full user read rights, used for binding to the directory. For example, `cn=Manager,dc=company,dc=com`
Password – The password to use for binding to the LDAP server.
User Class – The LDAP object class for user objects in the LDAP directory.
Proxy Based SSO – To configure an access manager that supports proxy-based SSO, also known as reverse proxy-based SSO:
 User ID Header – The attribute that your access manager adds to each incoming HTTP request.

Apple Open Directory Server



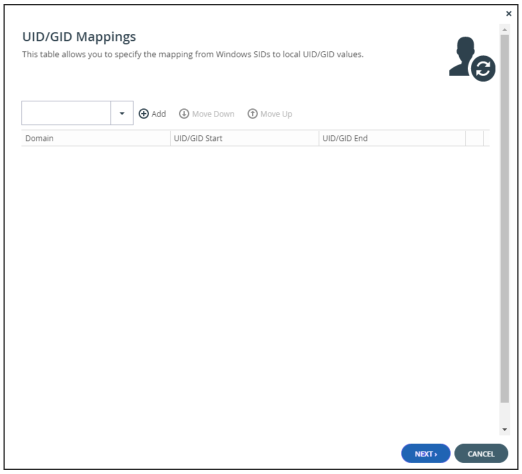
LDAP URL – The URL to connect to the Apple Open Directory server.
Base DN – Optional: The base DN of the Apple Open Directory server.
Login DN – The distinguished name of a user with full user read rights, used for binding, authenticating, to the LDAP server, also known as bind DN.
Password – The password to use for binding to the Apple Open Directory server.
Proxy Based SSO – To configure an access manager that supports proxy-based SSO, also known as reverse proxy-based SSO:

  User ID Header – The attribute that your access manager adds to each incoming HTTP request.

4. Click **NEXT**.

Active Directory

The portal connects to the domain and the **UID/GID Mappings** window is displayed.



a) To add the other Active Directory domains in the tree/forest, do the following for each one:

b) Select the user to add to the group and click **Add**.
In the **Add domain** field, enter the Active Directory domain name, or select it from the drop-down list.

Click **Add**.
The domain is added.
In the **UID/GID Start** field enter the starting number in the range of portal user and group IDs (UID/GID) to assign to users and user groups from this Active Directory domain.
In the **UID/GID End** field enter the ending number in the range of portal user and group IDs (UID/GID) to assign to users and user groups from this Active Directory domain.

c) You can re-order the list of added domains by selecting a domain and clicking **Move Up** or **Move Down**.
The order in which domains are displayed represents the order in which the domains are displayed in lists throughout the portal interface.

d) To remove an Active Directory domain, select the domain row and click .
The domain is removed.

e) Click **NEXT**.

The **Access Control** window is displayed.

LDAP

The portal connects to the LDAP server and the **Advanced LDAP Mappings** window is displayed. To configure the portal to match a custom LDAP schema:

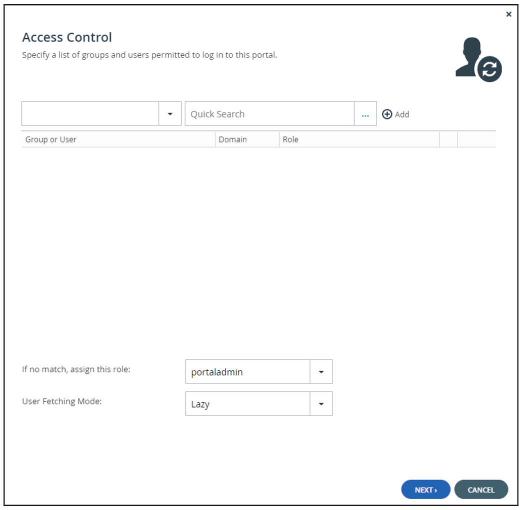
a) Edit the LDAP mappings: Click each attribute that maps to the corresponding user properties.
The following user properties must be mapped to LDAP attributes:
username – The user name in the portal to uniquely identify the user. This can map to any LDAP attribute that uniquely identifies the user, such as **userPrincipalName**.
password – The user password. The corresponding LDAP attribute is **userPassword**.
email – The user email. The corresponding LDAP attribute is **mail**.
firstName – The user first name. The corresponding LDAP attribute is **givenName**.
lastName – The user family name. The corresponding LDAP attribute is **sn**.
memberOf – The group the user is a member of. The corresponding LDAP attribute is **memberOf**.

b) Click **NEXT**.

The **Access Control** window is displayed.

Apple Open Directory

The portal connects to the Apple Open Directory server and the **Access Control** window is displayed.



5. Add each directory user and user group allowed to access the portal:

a) In the drop-down list, select one of the following:
Domain Users – Search the users defined in directory service.
Domain Groups – Search the user groups defined in directory service.

b) Select the user or user group from the drop-down list or in the **Quick Search** field, enter a string that is displayed anywhere within the name of the user or user group you want to add.

c) Select the user or group and click **Add**.
The user or user group is added to the list of users and user groups with access to the portal.

6. To remove a user or group, select the row and click .

The user or user group is removed.

7. In each user and user group's row, click in the **Role** column, then select the user role from the drop-down list.

Disabled – The user account is disabled. The user cannot access the end user portal view.
End User – The user can access the End User Portal.
Read/Write Administrator – The user can access the end user portal view as an administrator with read-write permissions.
Read Only Administrator – The user can access the end user portal view as an administrator with read-only permissions.
Support – The user can access the end user view portal as an administrator and has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the portal.

8. To assign a role for a directory user or user group with no match in the access control list, select the user role from the **If no match, assign this role** drop-down list: **Disabled**, **End User**, **Read/Write Administrator**, **Read Only Administrator**, **Support**.

9. To automatically fetch new users and create home folders for them, without the need to perform a manual fetch for them or to require them to sign in to the portal, select **Eager** from the **User Fetch Mode** drop-down list.

Lazy – Users are created and data associated with them after either the user signs in to

the portal or a manual fetch is performed for the users.
Eager – Users in groups in the access control list are immediately created and home folders created for them.

10. Click **NEXT**.

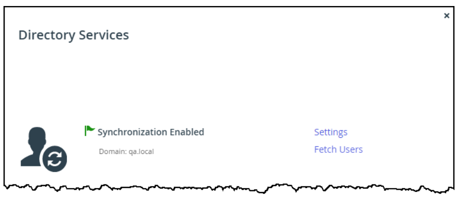
    The **Wizard Completed** window is displayed.

11. Click **FINISH**.

    The **Apply Changes** window is displayed.
    While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN BACKGROUND**.

12. Click **CLOSE**.

    Synchronization with the directory server is enabled.
    Click **Fetch Users** to retrieve the users from the directory, to use in the HCP Anywhere Enterprise Portal.

13. Click **CLOSE**.

The users in the HCP Anywhere Enterprise Portal are automatically updated at midnight of every night with the users in the directory. To immediately fetch the users, see Manually Fetching User Data.

Manually Fetching User Data

You can manually fetch user data from an integrated directory, after the connection with the directory service is established, as described in Integrating HCP Anywhere Enterprise Portal with a Directory Service:

- To immediately update data in the local user database, instead of waiting for HCP Anywhere Enterprise Portal to automatically fetch data at midnight.

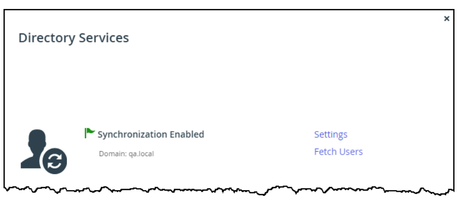
  Note: If a user in Active Directory is disabled, manually fetching the user data immediately updates the portal users, instead of waiting until the portal automatically re-fetches all previously fetched directory users, every day at midnight.

- To create an account for a user that does not yet exist in the local user database, before their first login.

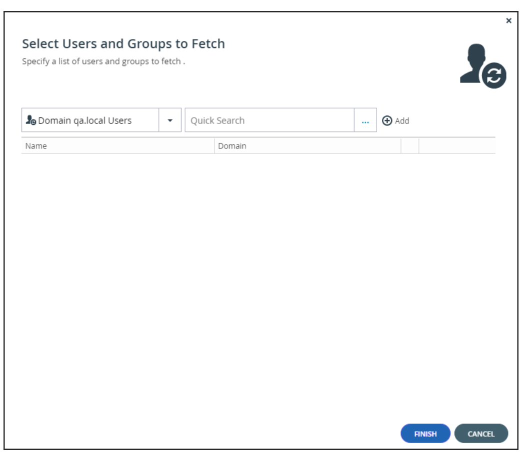
To manually fetch user data:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **Directory Services** under **USERS** in the **Control Panel** page.
   The **Directory Services** window is displayed.



3. Click **Fetch Users**.
   The **Select Users and Groups to Fetch** window is displayed.



4. Add each directory user and user group allowed to access the portal:

a) In the drop-down list, select one of the following:
   Domain Users – Search the users defined in directory service.
   Domain Groups – Search the user groups defined in directory service.

b) Select the user or user group from the drop-down list or in the **Quick Search** field, enter a string that is displayed anywhere within the name of the user or user group you want to add.

c) Select the user or group and click **Add**.
   The user or user group is added to the list of users and user groups to fetch.

5. To remove a user or group, select the row and click .

   The user or user group is removed from the list.

6. Click **FINISH**.

   The User data is fetched from the directory, and the **Apply Changes** window is displayed and the changes are applied.
   While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN BACKGROUND**.

7. Click **CLOSE**.

Chapter 10. Managing Users

End users and team administrators are registered with the HCP Anywhere Enterprise Portal and have access to the End User Portal. Each user is represented in the HCP Anywhere Enterprise Portal by a *user account*.

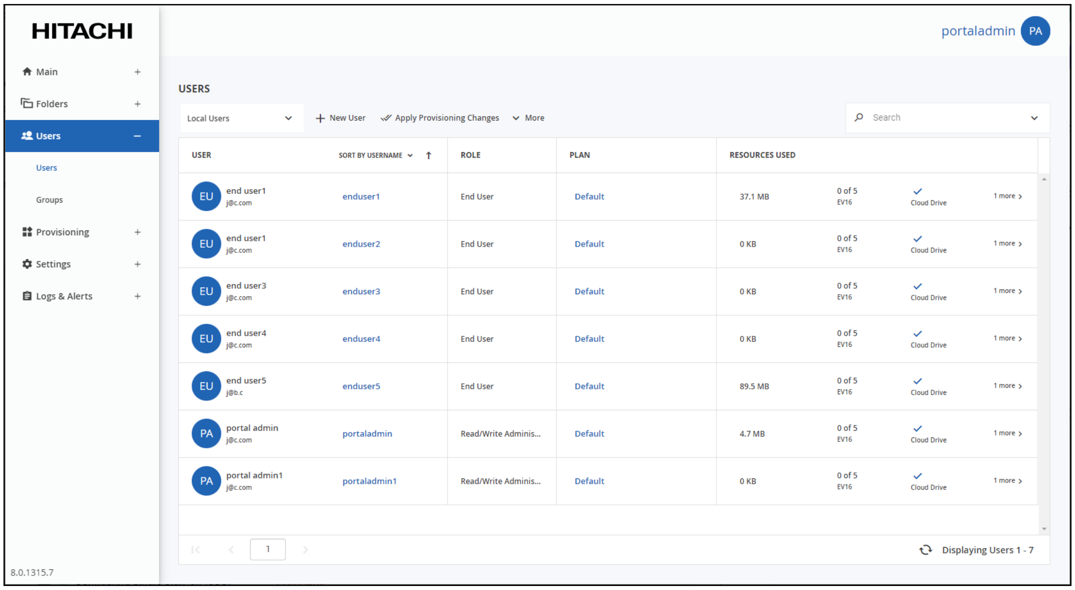
Users and groups of users should be added directly in the portal or by using directory services, such as Active Directory. You can attach a directory service and fetch users and groups from the directory service. For information about using a directory service, see Using Directory Services For the Users.

In this chapter

Viewing Users

To view all users in the portal:

- Select **Users > Users** in the navigation pane.
  The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



USER – The user’s first and last names.

 Email (under the user name) – The administrator's email address.
 Username – The username.
 Company (under the user name) – The name of the user's company.
 Disabled – Displayed if the user is defined as disabled and cannot access the portal.

ROLE – The user role: End User, Disabled, Read/Write Administrator, Read Only Administrator, Support.

PLAN – The plan assigned to the user. You can access the plan details directly by clicking the plan. For details, see Provisioning.

RESOURCES – The resources allocated to the user. The information can be different per user. Expanding the column or clicking **more >** displays more information:

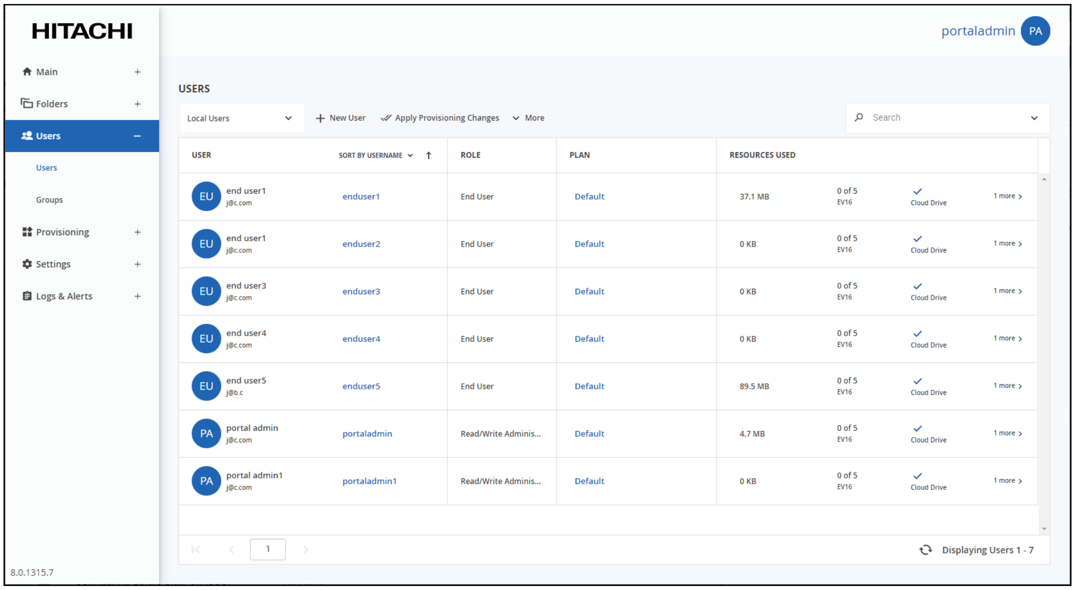
- The number and type of HCP Anywhere Enterprise Edge Filer licenses used.
- The amount of storage the user has consumed out of the total number provisioned.
- Whether or not the user has the Cloud Drive service.
- The number of HCP Anywhere Enterprise Agents installed out of the total number provisioned.

To view only a specific type of user:

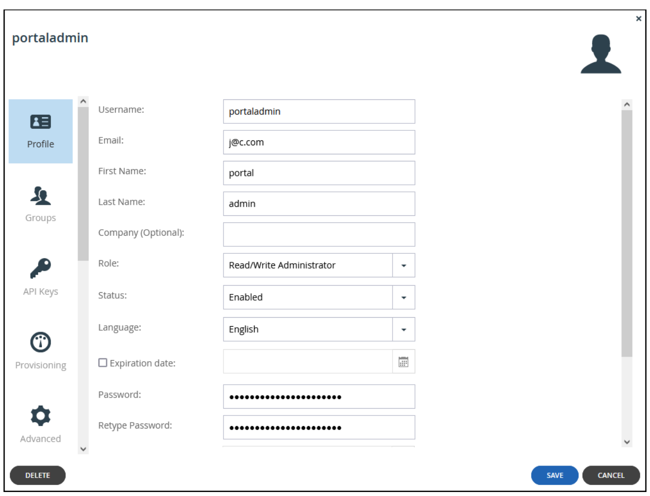
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the portal.
2. Click the filter drop-down to filter the users either by the default **Local Users** or by a domain.

Viewing Details of a User

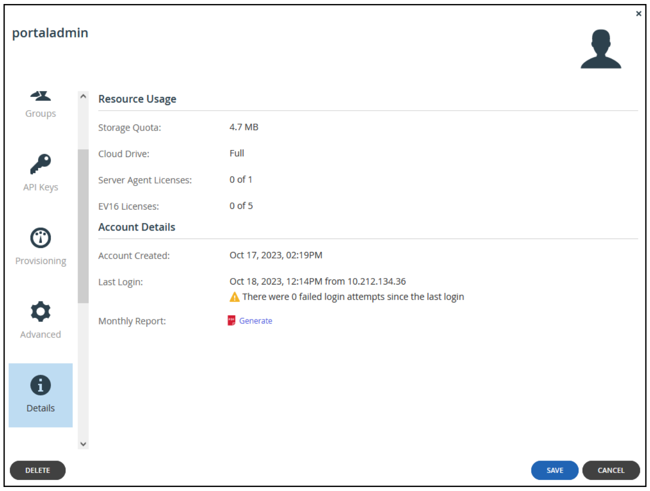
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.



3. Select the **Details** option.
   The user details that are displayed vary, dependent on the user.



Storage Quota – The amount of storage the user has consumed. If the global administrator set a storage quota for you, the current usage and the quota are displayed with the percentage used of the quota.

Cloud Drive – Whether the user is provisioned to have the Cloud Drive service.

Server Agent Licenses – The number of HCP Anywhere Enterprise Agents installed out of the total number available in the user account's subscription plan.

EV*nn* Licenses – The number of HCP Anywhere Enterprise Edge Filer licenses associated with the user account. If the user's subscription plan includes HCP Anywhere Enterprise Edge Filers, this number is expressed as the number of licenses used from the total number of HCP Anywhere Enterprise Edge Filer licenses of this type available in the subscription plan.

Account Created – The date and time when the user account was created.

Last Login – The date and time when the user last signed on to the HCP Anywhere Enterprise Portal as well as details about how many successful and failed times the user attempted to sign on and the IP addresses used to sign-on.

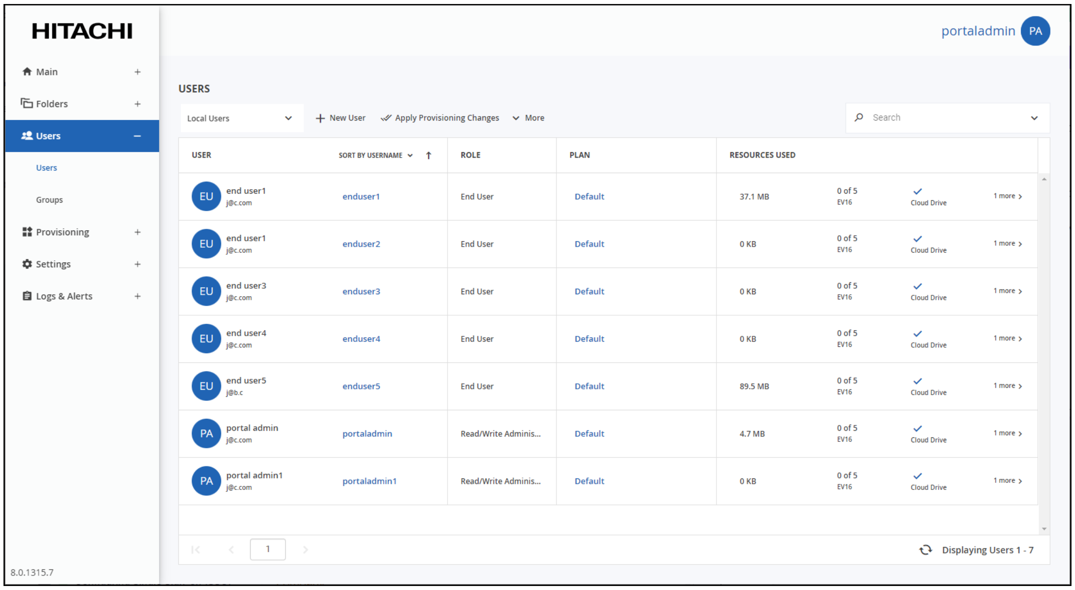
Monthly Report – A link for Manually Generating a Monthly Report for a User a monthly report of events in the user account in PDF format.

Manually Generating a Monthly Report for a User

You can trigger the immediate generation and sending of the monthly report for a specific user account.

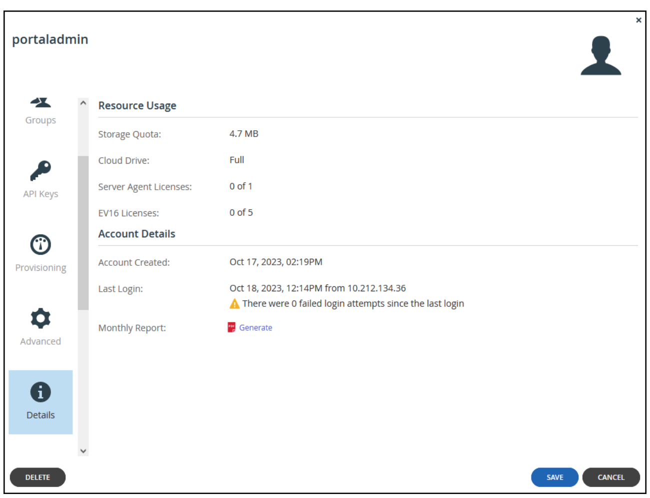
To generate a monthly report for the user:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



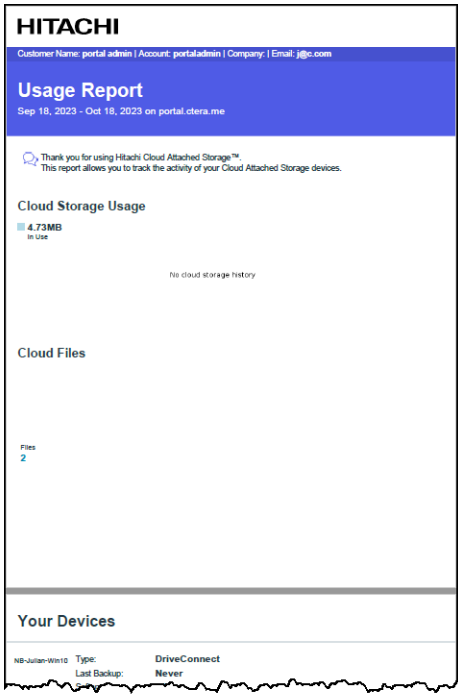
2. Click the user's name.

   The user window is displayed with the user name as the window title.
3. Select the **Details** option.



4. In the **Details** option, click **Generate**.

A report, by default *report.pdf*, is generated and downloaded to the computer, similar to the following example:



Adding User Accounts

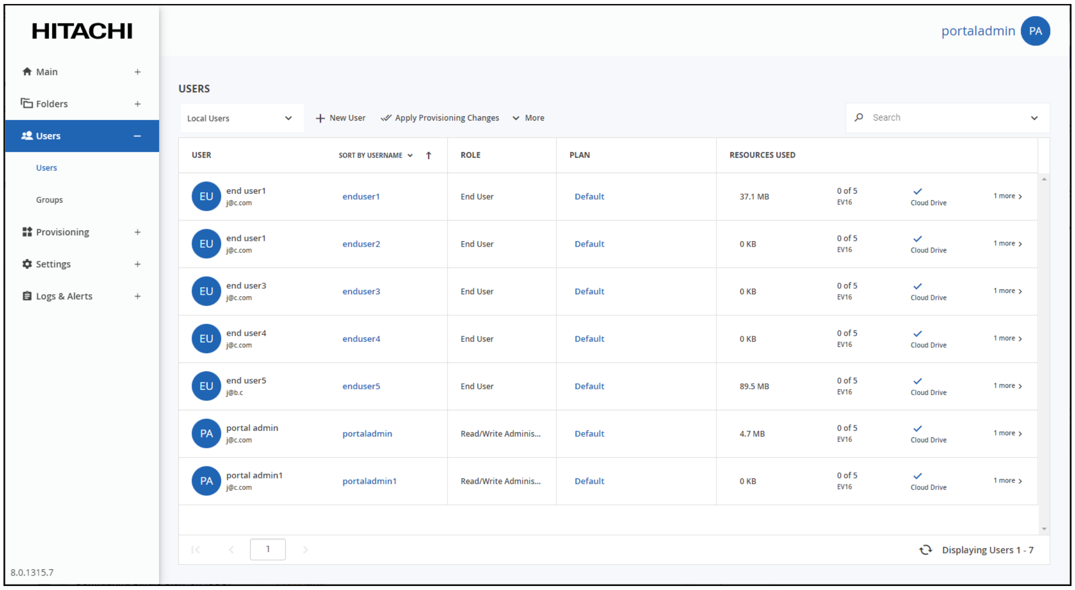
You can add users to the portal in the following ways:

- Using directory services, such as Active Directory. For information about using a directory service, see Using Directory Services For the Users.
- Adding the user directly in the HCP Anywhere Enterprise Portal.
- Inviting a user to register.
- Importing user details to the HCP Anywhere Enterprise Portal.

Adding Users In the HCP Anywhere Enterprise Portal User Interface

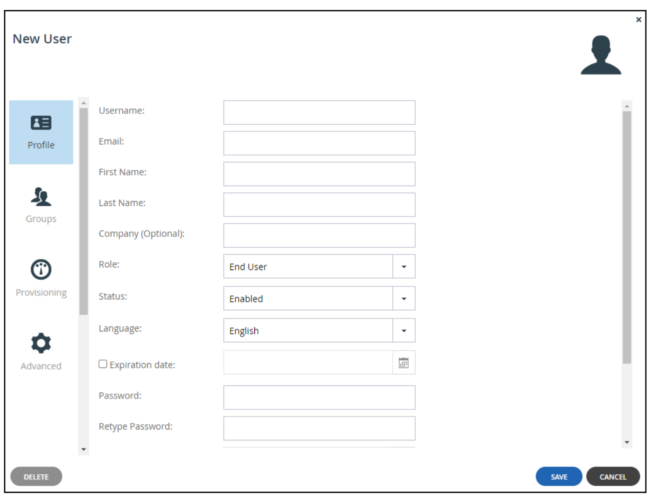
To add a user or edit an existing user in the HCP Anywhere Enterprise Portal:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click **New User**.

   The **New User** window is displayed.



3. Complete the fields in the **Profile** option.

   Username – A name for the user's HCP Anywhere Enterprise Portal account.
   Email – The user's email address.
   First Name – The user's first name.
   Last Name – The user's last name.
   Company (Optional) – The name of the user's company.
   Role – The user's role:

Disabled – The user account is disabled. The user cannot access the HCP Anywhere Enterprise Portal.
Compliance Officer – The user can access the end user portal view as an administrator with read-write permissions and manage compliance settings for cloud drive folders.
End User – The user can access the HCP Anywhere Enterprise Portal as an end user.
Read/Write Administrator – The user can access the end user HCP Anywhere Enterprise Portal view as an administrator with read-write permissions.
Read Only Administrator – The user can access the end user HCP Anywhere Enterprise Portal view as an administrator with read-only permissions.
Support – The user can access the end user HCP Anywhere Enterprise Portal view as an administrator and has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the HCP Anywhere Enterprise Portal.

Status. Select the account status:

Enabled – The account is enabled, and the user can access the HCP Anywhere Enterprise Portal.
Disabled – The account is disabled, and the user cannot access the HCP Anywhere Enterprise Portal.
The default value for new users is *Enabled*.
The default value for invited users is *Disabled*. The status changes to *Enabled* when the invited user activates the account.

Note: In order to access the end user portal view, the user must have a role other than **Disabled**, and the status must be enabled.

Language – The language used for the user interface.
Expiration date – The expiration date of the user account.
Password / Retype Password – A password for the user's account. Password requirements depend on the password policy, which can be overridden and modified in the **Virtual Portal Settings**, in Password Policy.
Force Password Change – An expiration date for the user account password. When the password has expired, the user must configure a new password on the next login.
Numeric UID (Optional) – A numeric user ID to assign the user's account.
Comment – A description of the user account.

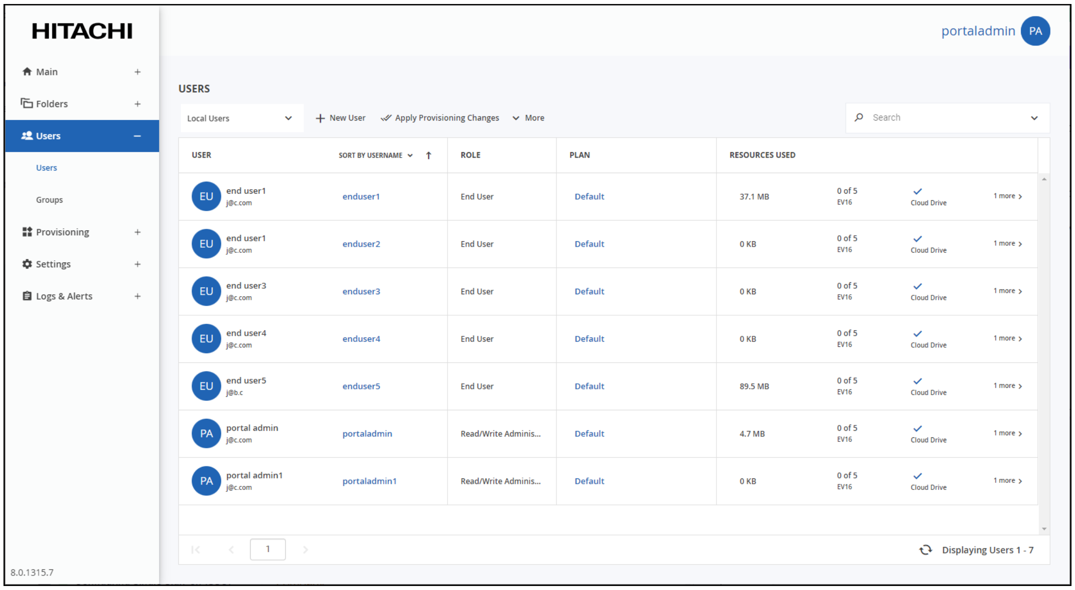
4. Click **SAVE**.

After a user is added, the options available to the administrator, such as the user devices and cloud drive folders. Some of these options, such as devices and folder groups are shortcuts to the relevant setting.

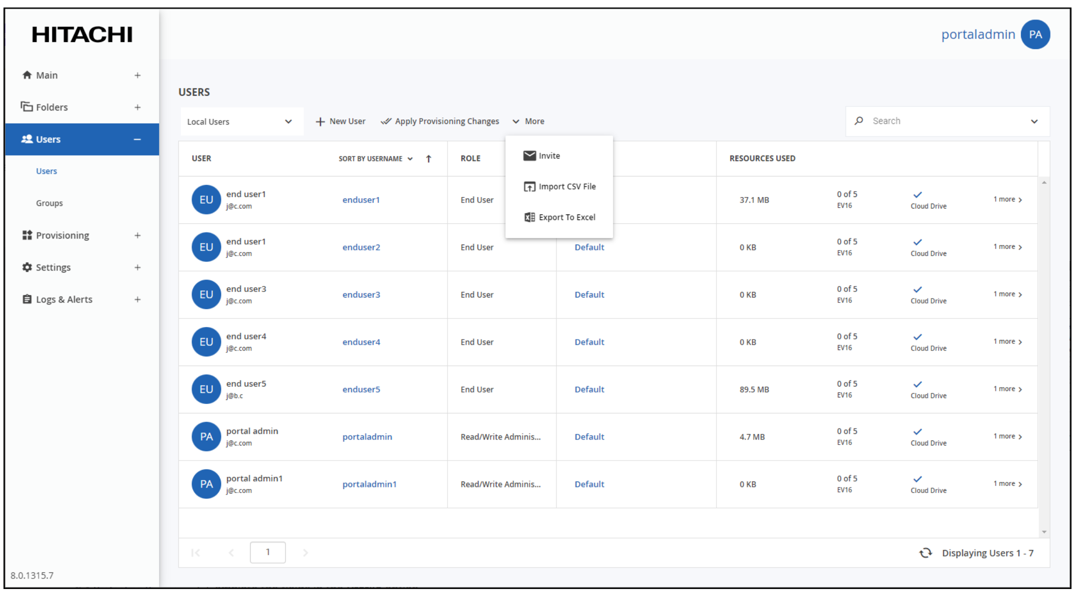
The user receives an email and can access the portal using the username and password from the administrator. By default, the email does not include the user password, for added security, and the user must contact the portal administrator for the password. Inviting users from the **USERS** page, with the **More > Invite** option, enables the user to choose a password on initial logon without needing to contact the administrator. For details, see Inviting Users to Register.

Inviting Users to Register

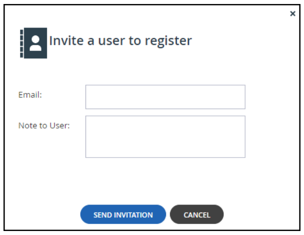
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click **More > Invite**.



The **Invite a user to register** window is displayed.



3. Enter the following:

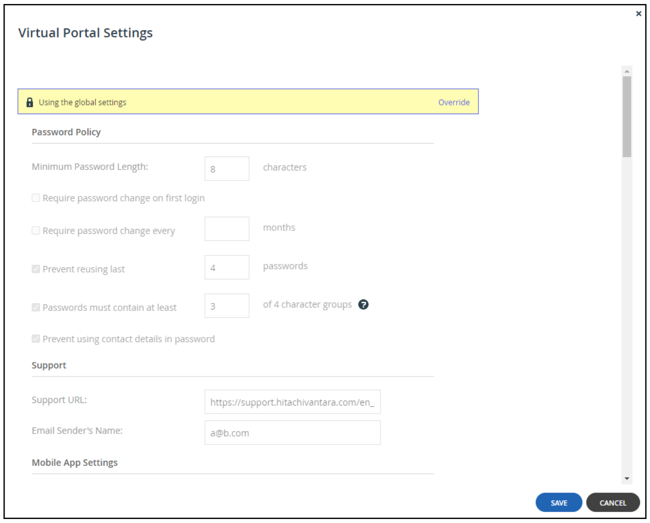
   Email – The email address of the user you want to invite to register.
   Note to User – A message you want to send to the user.
4. Click **SEND INVITATION**.

The invited user receives an invitation by email with a link to complete the registration. The user chooses a password on initial logon without needing to contact the administrator. Administrators receive email notifications that the user has registered.

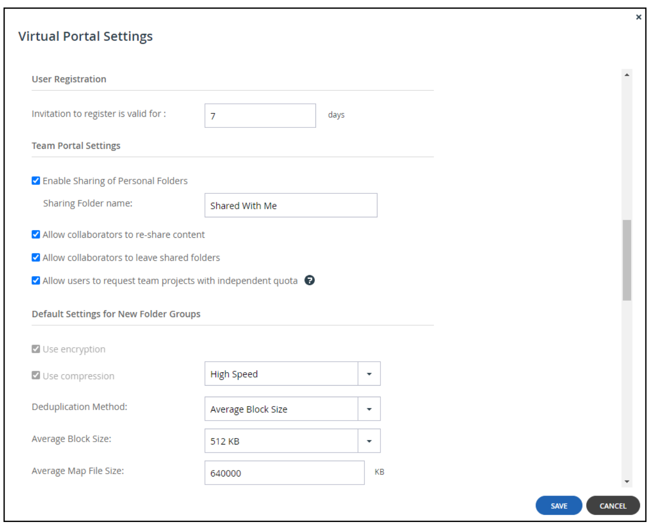
To control the expiration period of registration invitations:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **Virtual Portal**, under **SETTINGS** in the **Control Panel** page.



3. Override global settings if necessary.
4. Scroll down to **User Registration** and set the number of days the invitation is open.



5. Click **SAVE**.

Importing Users from a File

You can import users and their details from a comma separated values (*.csv) file.

The *.csv file's columns must be in the following order:

1. Username
2. First name
3. Last name
4. Email address
5. Company (Optional)
6. Password

7. Role – Valid values: ReadWriteAdmin, ReadOnlyAdmin, Support, EndUser
8. Plan (Optional)
9. Numeric UID (Optional)
10. External Account ID (Optional)
11. Comment (Optional)
12. Status (Optional) – Valid values: active, inactive

Optional fields can be left blank.

The following example csv file includes users rw-admin, support, and user1:

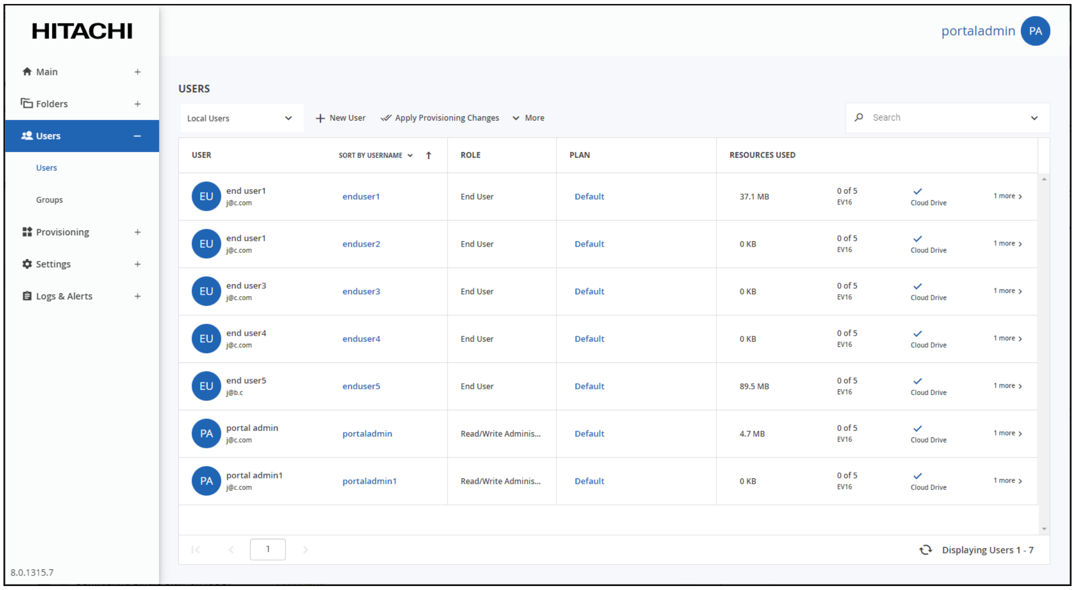
```
rw-admin,John,Doe,flast@example.com,,Chang3Me!,ReadWriteAdmin,,,,
Read/Write Admin Account,active
support,Jane,Doe,support@example.com,,Chang3Me!,Support,,,,Support
Account,inactive
user1,Fred,Blogs,fblogs@example.com,,Chang3Me!,EndUser,Default,1,,,ac
tive
```

where:

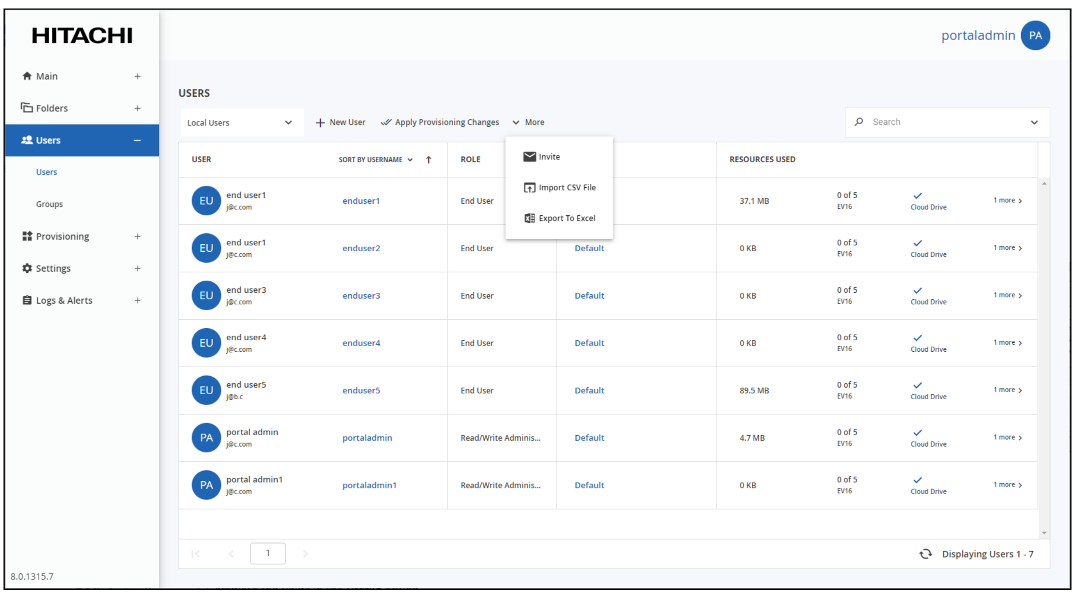
Field	First User	Second User	Third User
Username	rw-admin	support	user1
First name	John	Jane	Fred
Last name	Doe	Doe	Blogs
Email address	flast@example.com	support@example.com	fblogs@example.com
Company	—	—	—
Password	Chang3Me!	Chang3Me!	Chang3Me!
Role	ReadWriteAdmin	Support	Enduser
Plan	—	—	Default
Numeric UID	—	—	1
External Account ID	—	—	—
Comment	Read/Write Admin Account	Support Account	—
Status	active	inactive	active

To import users from a .csv file:

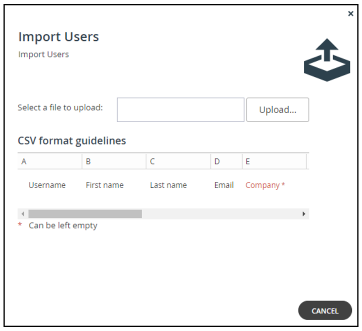
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click **More > Import CSV File**.



The **Import Users** window is displayed.



3. Click **Upload** and select the file with the users to upload.
4. Click **Open**.

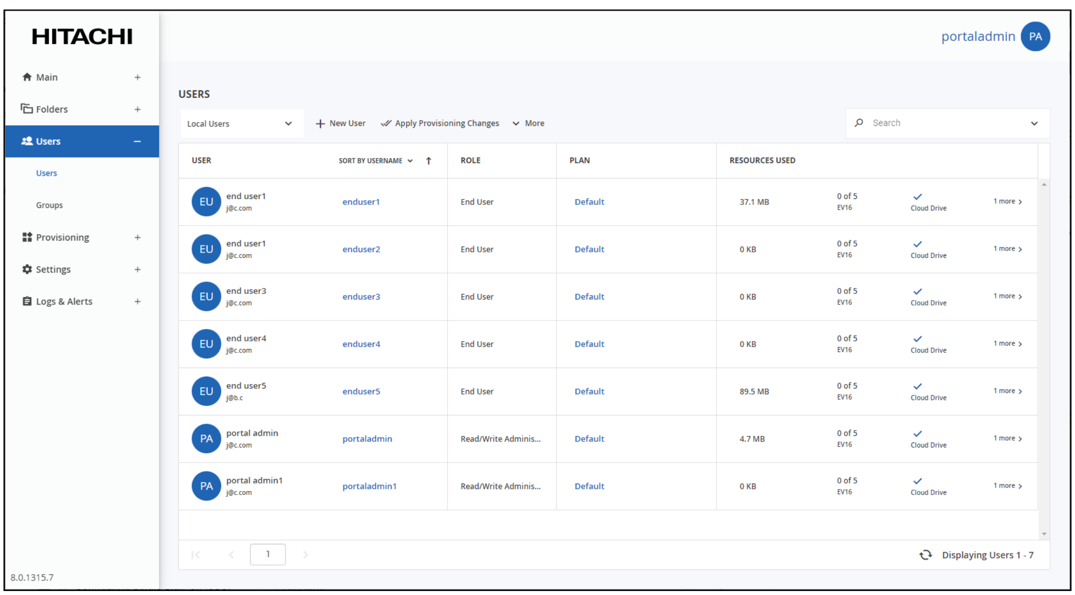
   The file is uploaded and the **Import Completed** window is displayed.
5. Click **FINISH**.

Editing Users

You can edit user details, including the devices with which the user has connected to the portal and the user's cloud drive.users to the portal in the following ways:

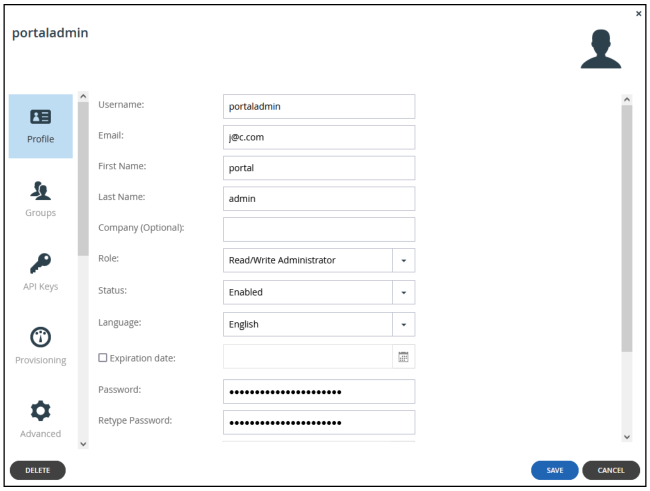
To edit an existing user:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.

   The user window is displayed with the user name as the window title.



3. Edit the fields in the **Profile** option:

Username – A name for the user's HCP Anywhere Enterprise Portal account.
Email – The user's email address.
First Name – The user's first name.
Last Name – The user's last name.
Company (Optional) – The name of the user's company.
Role – The user's role:

- **Disabled** – The user account is disabled. The user cannot access the HCP Anywhere Enterprise Portal.
- **Compliance Officer** – The user can access the end user portal view as an administrator with read-write permissions and manage compliance settings for cloud drive folders.
- **End User** – The user can access the HCP Anywhere Enterprise Portal as an end user.
- **Read/Write Administrator** – The user can access the end user HCP Anywhere Enterprise Portal view as an administrator with read-write permissions.
- **Read Only Administrator** – The user can access the end user HCP Anywhere Enterprise Portal view as an administrator with read-only permissions.
- **Support** – The user can access the end user HCP Anywhere Enterprise Portal view as an administrator and has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the HCP Anywhere Enterprise Portal.

Status. Select the account status:

- **Enabled** – The account is enabled, and the user can access the HCP Anywhere Enterprise Portal.
- **Disabled** – The account is disabled, and the user cannot access the HCP Anywhere Enterprise Portal.

The default value for new users is *Enabled*.
The default value for invited users is *Disabled*. The status changes to *Enabled* when the invited user activates the account.

Note: In order to access the HCP Anywhere Enterprise Portal, the user must have a role other than **Disabled**, and the status must be enabled.

Language – The language used for the user interface.
Expiration date – The expiration date of the user account.
Password / Retype Password – A password for the user's account. Password requirements depend on the password policy, which can be overridden and modified in the **Virtual Portal Settings**, in Password Policy.
Force Password Change – An expiration date for the user account password. When the

password has expired, the user must configure a new password on the next login.
Numeric UID (Optional) – A numeric user ID to assign the user's account.
Comment – A description of the user account.

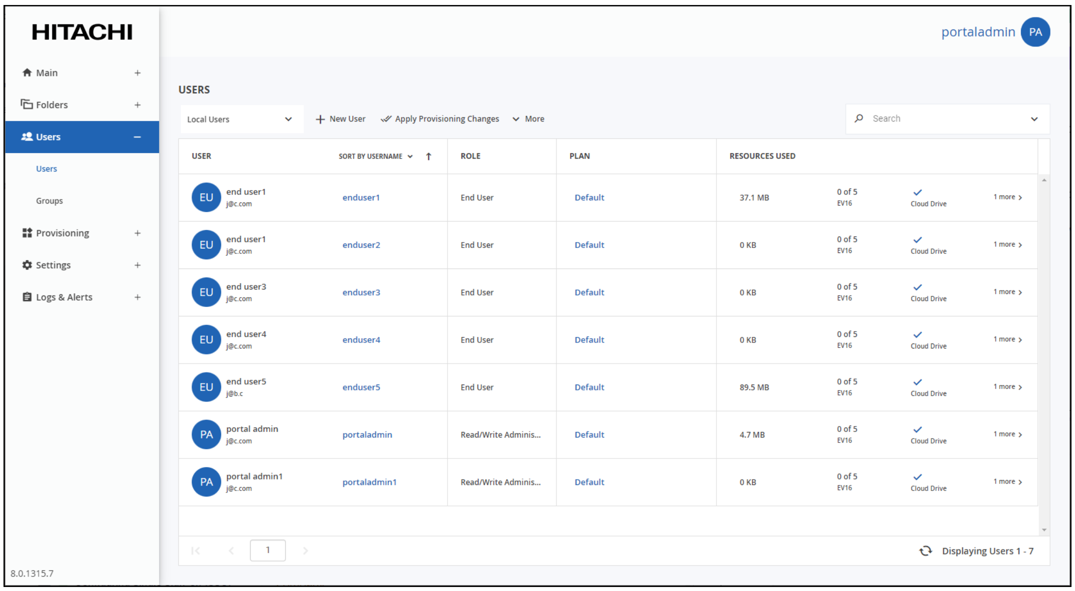
4. Click **SAVE**.

Deleting User Accounts

Deleting a user account from the HCP Anywhere Enterprise Portal cancels the user's subscriptions to plans, and deletes all of the user's folders and folder groups.

To delete a user account:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Either,
   a) Select the user's row to delete and click **Delete**.
   A confirmation window is displayed.
   b) Click **DELETE USER INCLUDING ASSOCIATED FOLDERS** to confirm.
   Or,
   a) Click the user.
   b) Click **DELETE**.
   A confirmation window is displayed.
   c) Click **DELETE USER INCLUDING ASSOCIATED FOLDERS** to confirm.

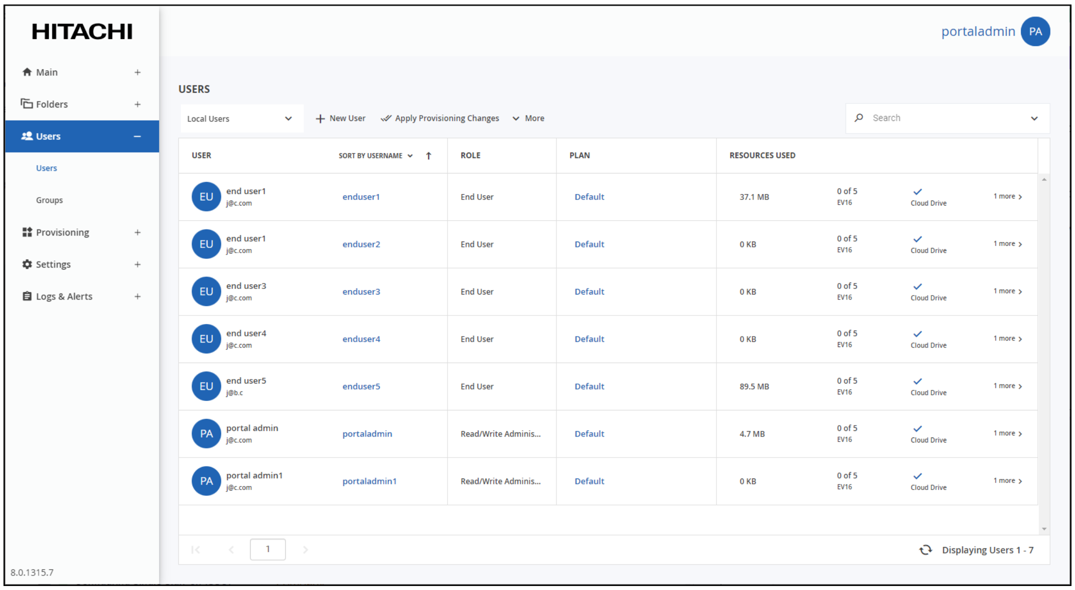
The user is deleted.

Enabling or Disabling User Accounts

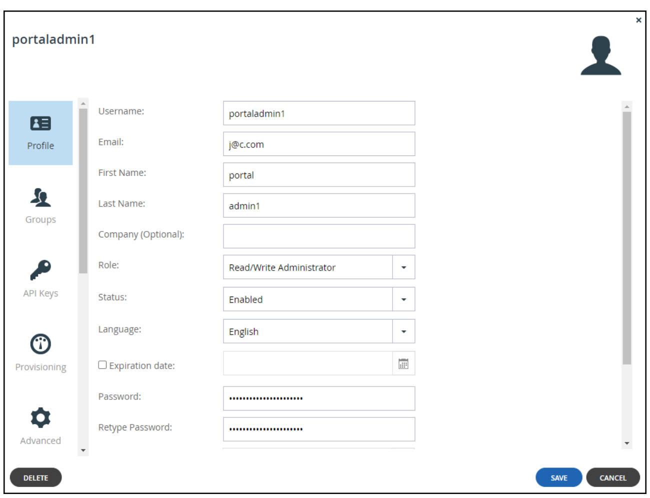
You can disable or enable a user account. Disabling the account prevents the user from accessing the HCP Anywhere Enterprise Portal, without removing the user or associated folders and files from the portal.

To enable or disable a user account:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user to disable or enable.
   The user window is displayed with the user name as the window title.



3. In the **Status** field, select **Enabled** or **Disabled** as required.
4. Click **SAVE**.

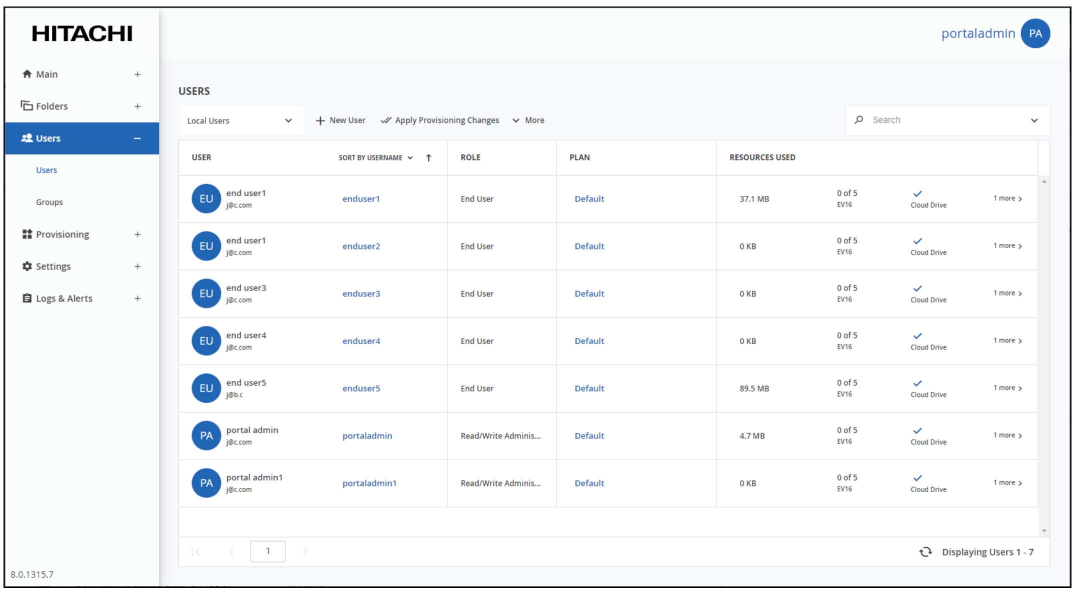
Setting Up API Keys to Access S3 Buckets

Users may be assigned to a default subscription plan or assigned automatically to another plan based on automatic template assignment settings. For details, see Provisioning. If desired, you can subscribe an individual user to a different subscription plan. You can also unsubscribe the user account, which deletes all files stored in the account and terminates the account.

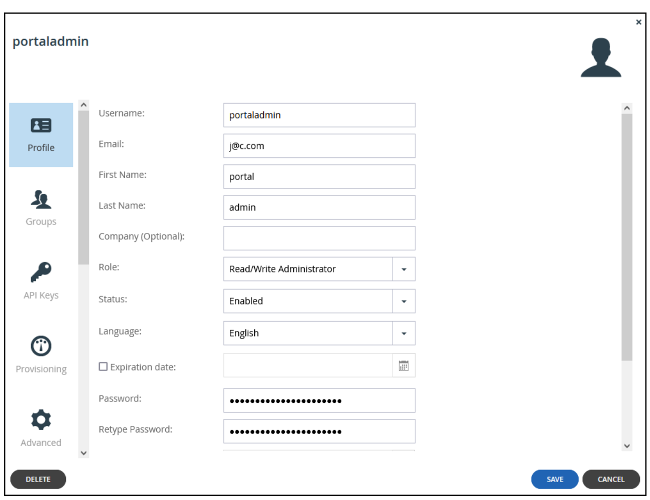
You can create your Access Key ID and Secret Access Key in the portal.

To create an Access Key ID and Secret Access Key pair:

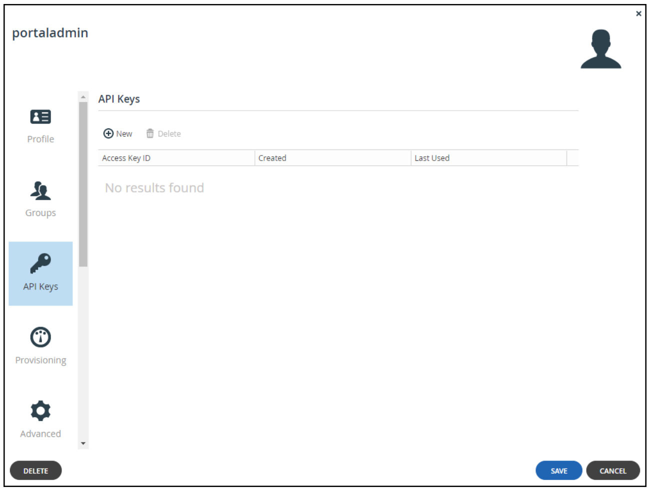
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.

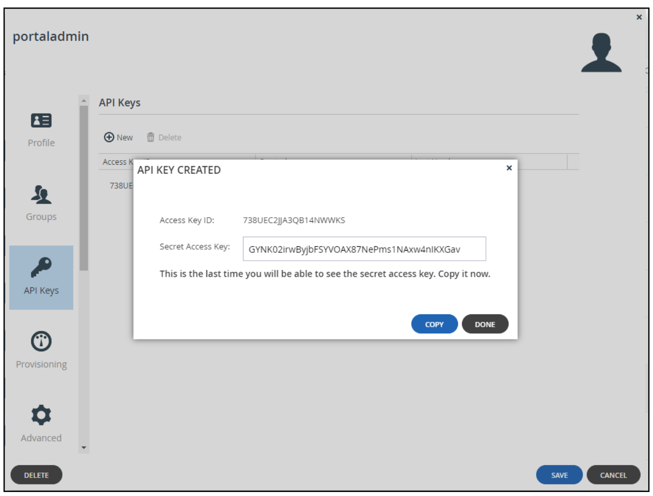


3. Select the **API Keys** option.



4. Click **New**.

The **API KEY CREATED** window is displayed with the Access Key ID and the Secret Access Key.



5. Click **Copy** to copy the **Secret Access Key** to the clipboard.

6. Save the **Secret Access Key** to give to the end user.

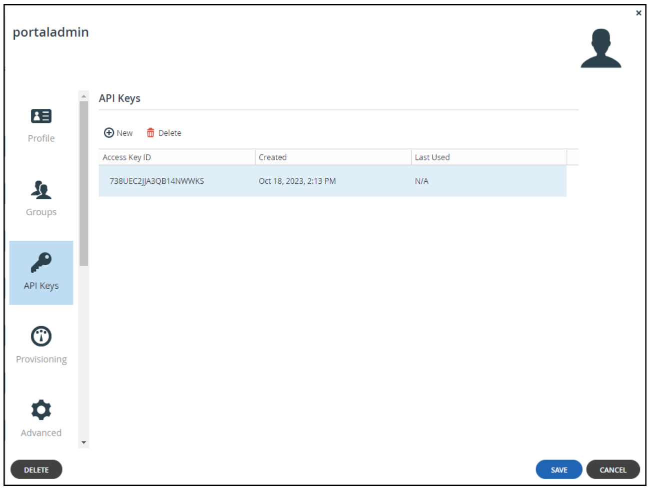
Note: The HCP Anywhere Enterprise Portal does not save the **Secret Access Key**, so if you do not save it you will not be able to pass it to the end user.

7. Click **Done**.

8. Click **SAVE**.

You can create up to 100 key pairs.

If you lose the Secret Access Key you can select the user and in the **API Keys** option select the row for that key and click **Delete** to remove it.



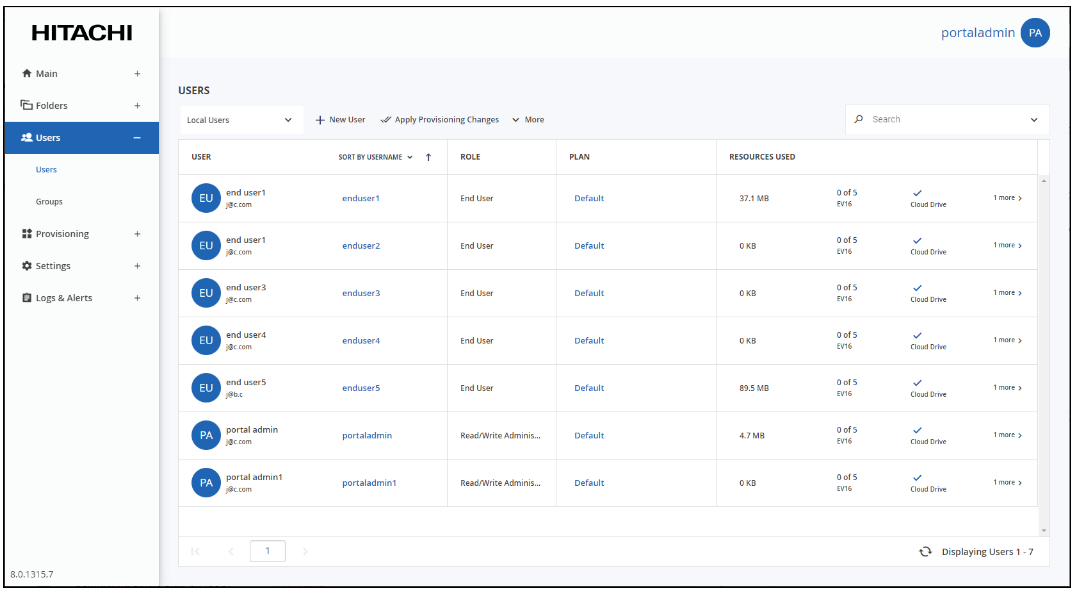
Provisioning User Accounts

Users may be assigned to a default subscription plan or assigned automatically to another plan based on automatic template assignment settings. For details, see Provisioning. If desired, you can subscribe an individual user to a different subscription plan. You can also unsubscribe the user account, which deletes all files stored in the account and terminates the account.

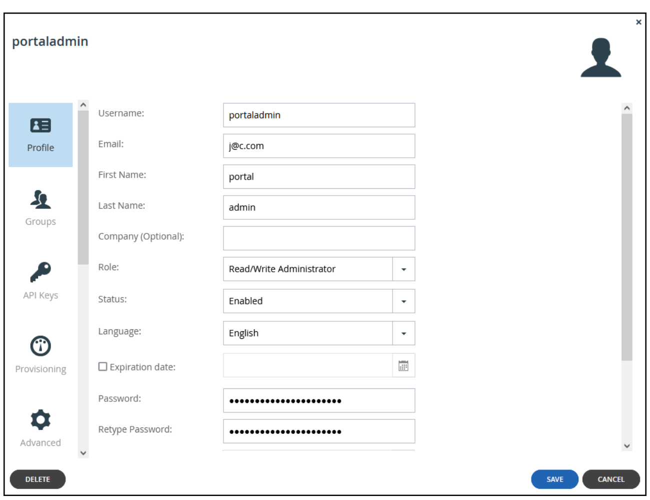
Assigning a User to a Plan

To assign a user to a plan:

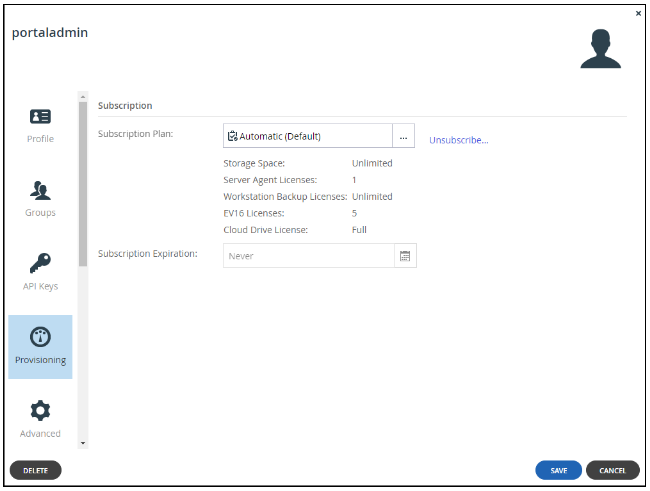
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.

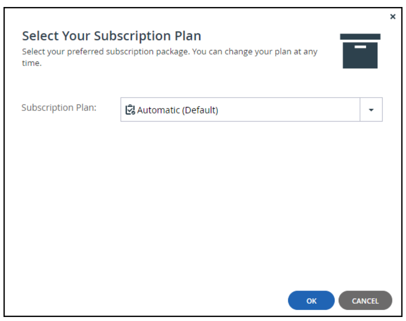


3. Select the **Provisioning** option.



4. Click the **Subscription Plan.**

   The **Select Your Subscription Plan** window is displayed.



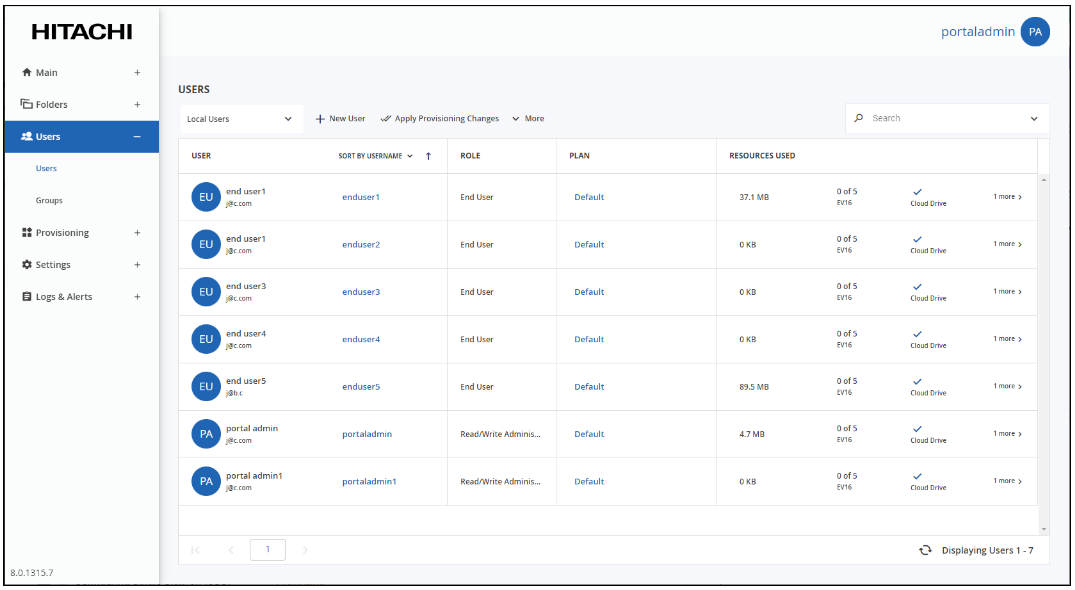
5. In the **Subscription Plan** drop-down list, select the subscription plan to assign the user.
6. Click **OK**.
7. Click **SAVE**.

Unsubscribing (Terminating) a User Account

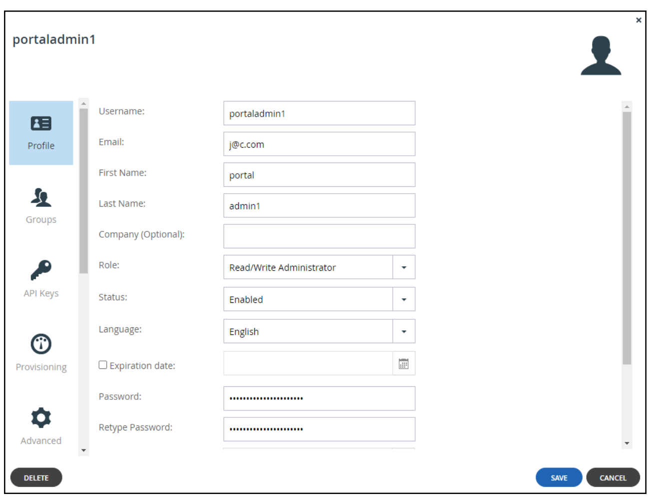
Unsubscribing a user from a plan terminates the account and removes all the files stored in the account.

To terminate a user account:

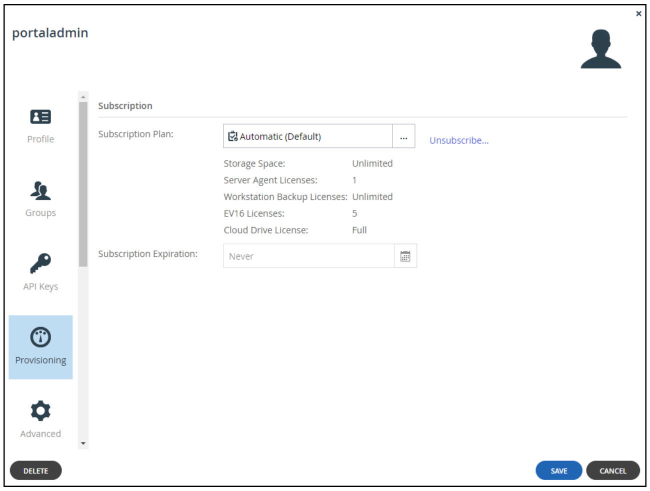
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.

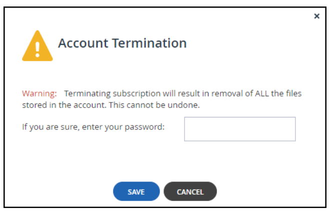


3. Select the **Provisioning** option.



4. Click **Unsubscribe**.

   The **Account Termination** window is displayed.



5. If you are sure you want to proceed, enter your password.
6. Click **SAVE**.

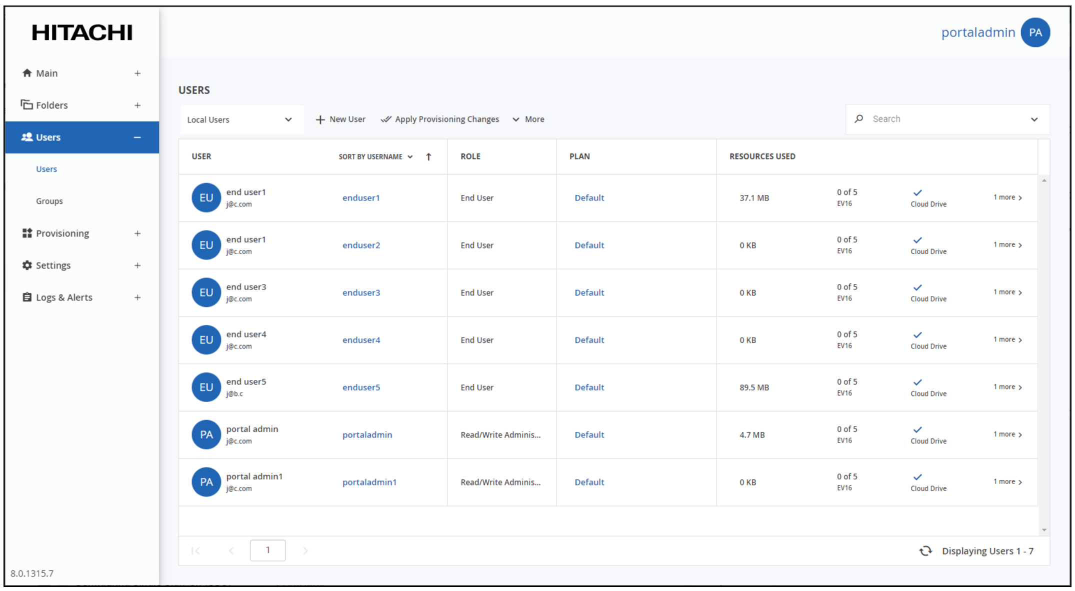
Applying Provisioning Changes

HCP Anywhere Enterprise Portal applies changed plan settings to all users every day at midnight. You can also apply all changes immediately.

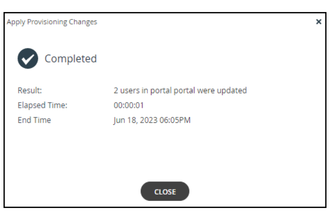
Note: If the HCP Anywhere Enterprise Portal is integrated with a directory service, applying provisioning changes will also cause the HCP Anywhere Enterprise Portal to synchronize all the users with the directory.

To apply provisioning changes:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click **Apply Provisioning Changes**.
   The **Apply Provisioning Changes** window is displayed and the changes are applied.
   Note: While the changes are being applied you can either stop the process, by clicking **STOP** or close the window while the process continues to run in the background by clicking **CONTINUE IN BACKGROUND**.



3. Click **CLOSE**.

Managing User Groups

User groups are groups of users that you can define and then use to simplify assigning user permissions. Groups are useful when setting several types of policies and permissions, such as:

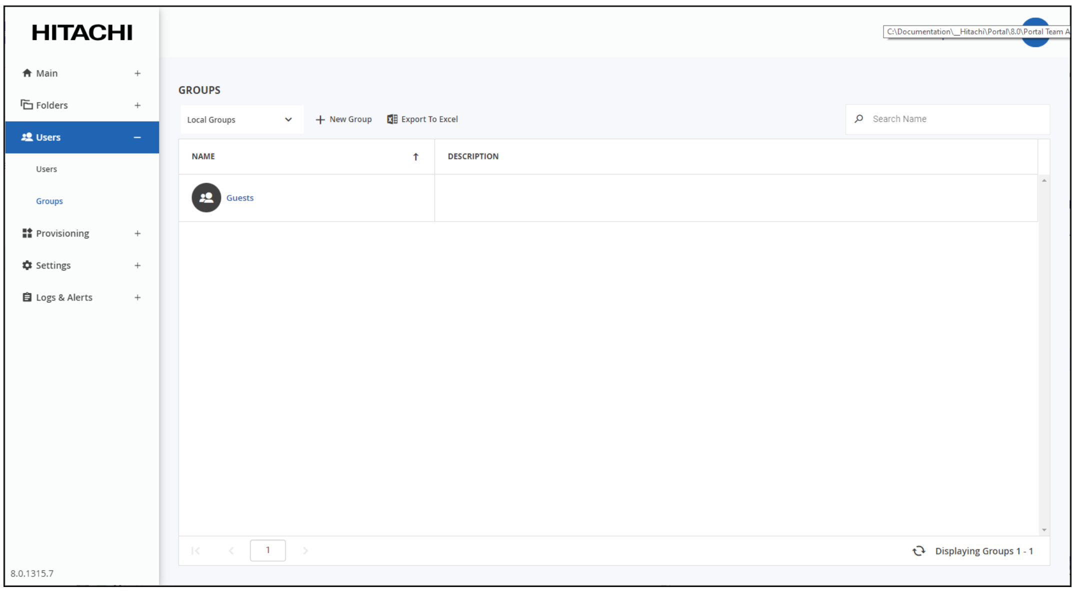
- Automatic template assignment policy. See Configuring the Automatic Template Assignment Policy.
- Setting permissions for accessing folders. See Managing Folders and Folder Groups.
- Setting Managing Collaboration.

Note: You can create groups manually, as described below, or you can fetch groups from a directory service, as described in Using Directory Services For the Users.

Viewing Groups

To view all user groups:

- Select **Users > Groups** in the navigation pane.
  The **GROUPS** page opens, displaying the user groups for the HCP Anywhere Enterprise Portal.



NAME – The user group's name.
DESCRIPTION – A description of the user group.

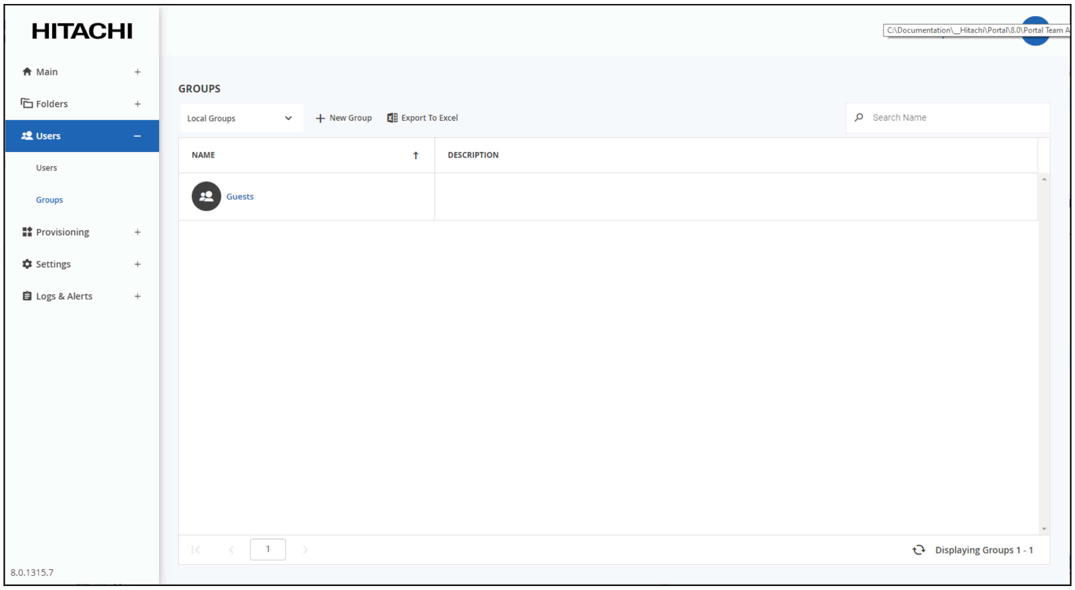
To view only local groups or only groups from directory services:

1. Select **Users > Groups** in the navigation pane.
   The **GROUPS** page opens, displaying the user groups for the HCP Anywhere Enterprise Portal.
2. Click the filter drop-down to filter the users either by the default **Local Users** or by an Active Directory or LDAP directory name.

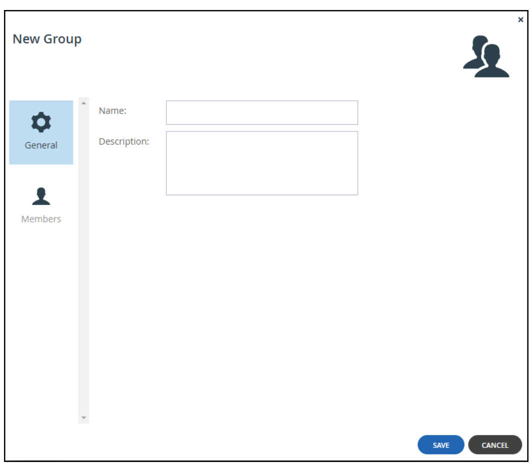
Adding or Editing Groups

To add or edit a user group:

1. Select **Users > Groups** in the navigation pane.
   The **GROUPS** page opens, displaying the user groups for the HCP Anywhere Enterprise Portal.

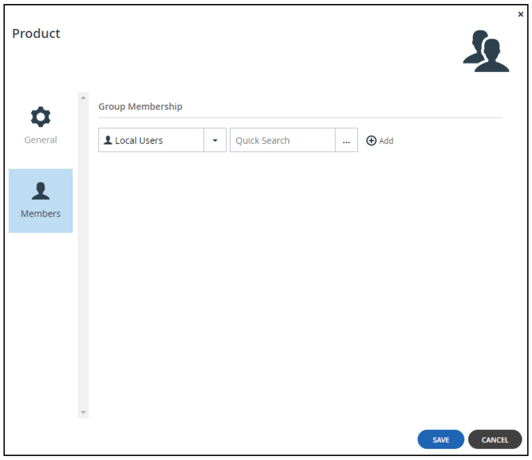


2. Either,
   - Add a group, click **New Group**.
     The **New Group** window is displayed.



   Or,
   - Edit an existing group, click the group's name**.** The group window is displayed with the username of the group as the window title.
3. Complete the fields in the **Profile** option:

   Name – A name for the group.
   Description – Optionally, a description of the group.
4. Select the **Members** option.



5. Select either **Local Users** or the Active Directory or LDAP directory name.
6. In the **Quick Search** field, enter a string that is displayed anywhere within the name of the user.

   A list of users matching the search string is displayed.
7. Select the user to add to the group and click **Add**.

   Note: Users can belong to multiple user groups.
   A user can be added to an existing group from the **Users > Users** option, described in Adding a User to an Existing Group.
8. To remove a user from the group, select the user row and click .

   The user is removed from the group.
9. Click **SAVE**.

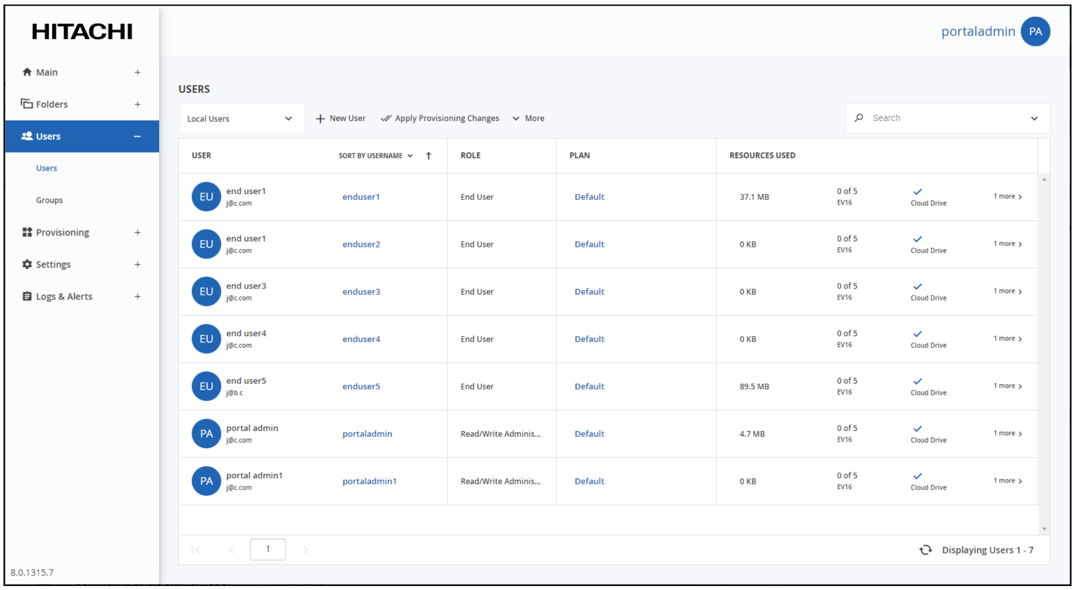
The user is added to the list of group members.

Adding a User to an Existing Group

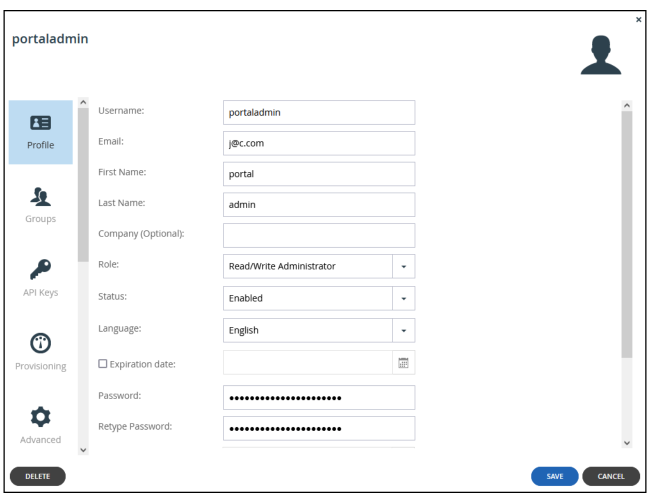
A User can be added to an existing group from the **Users > Users** option.

To add a user to an existing group:

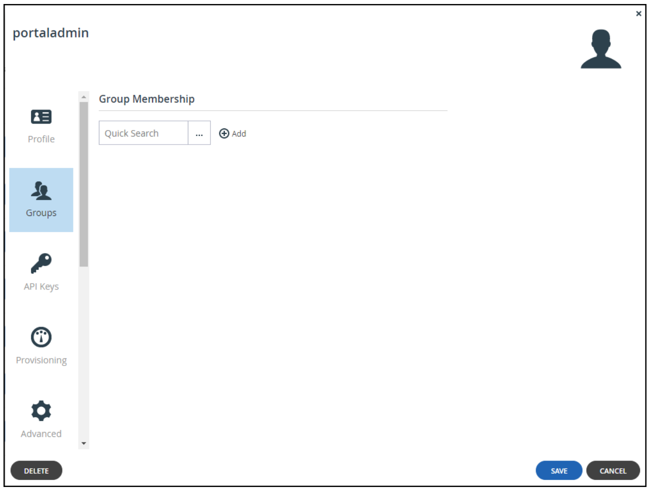
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.



3. Select the **Groups** option.



4. In the **Quick Search** field, enter a string that is displayed anywhere within the name of the group.

   A list of groups matching the search string is displayed.
5. Select the group and click **Add**.

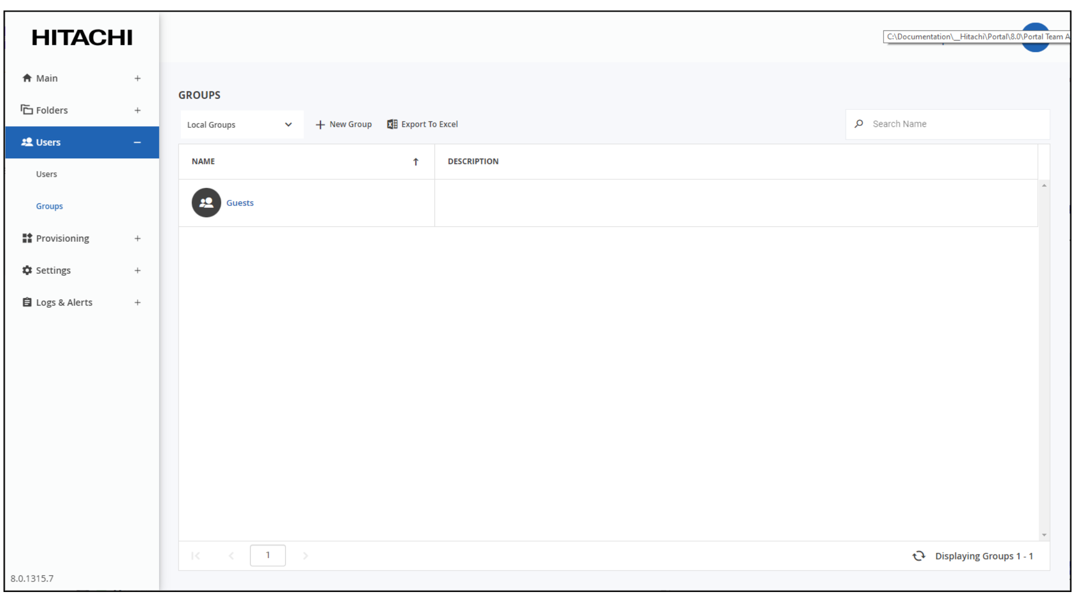
   Note: Users can belong to more than one user group.
6. Click **SAVE**.

Exporting Group Information to Excel

You can export a list of groups and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of groups to Microsoft Excel:

1. Select **Users > Groups** in the navigation pane.
   The **GROUPS** page opens, displaying the user groups for the HCP Anywhere Enterprise Portal.



2. Click **Export to Excel**.

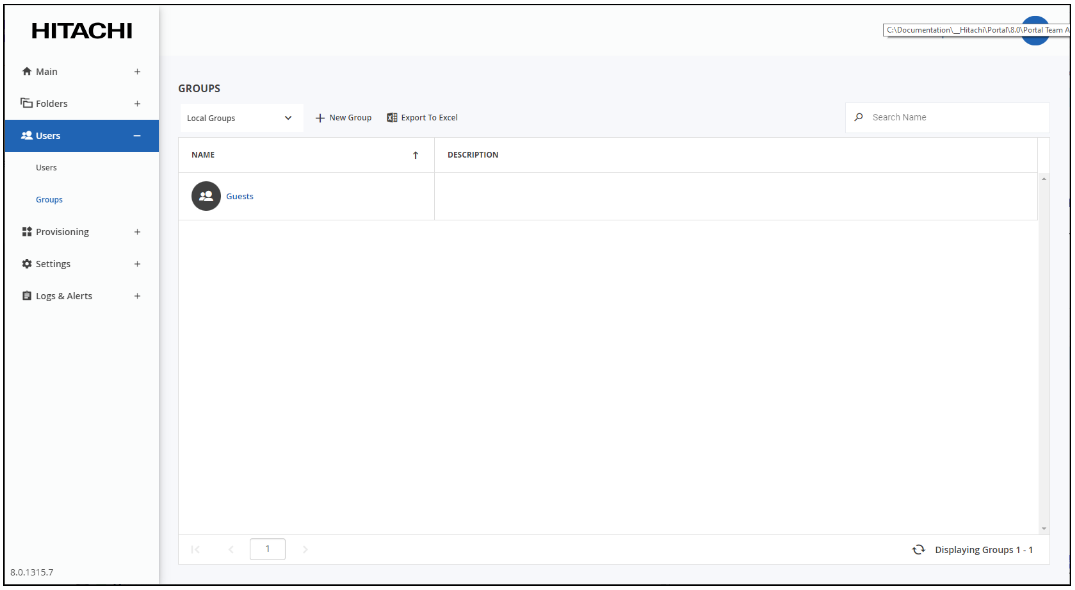
The group list is downloaded to your computer.

Deleting Groups

To delete a user group:

Note: Deleting a user group does not delete the users.

1. Select **Users > Groups** in the navigation pane.
   The **GROUPS** page opens, displaying the user groups for the HCP Anywhere Enterprise Portal.



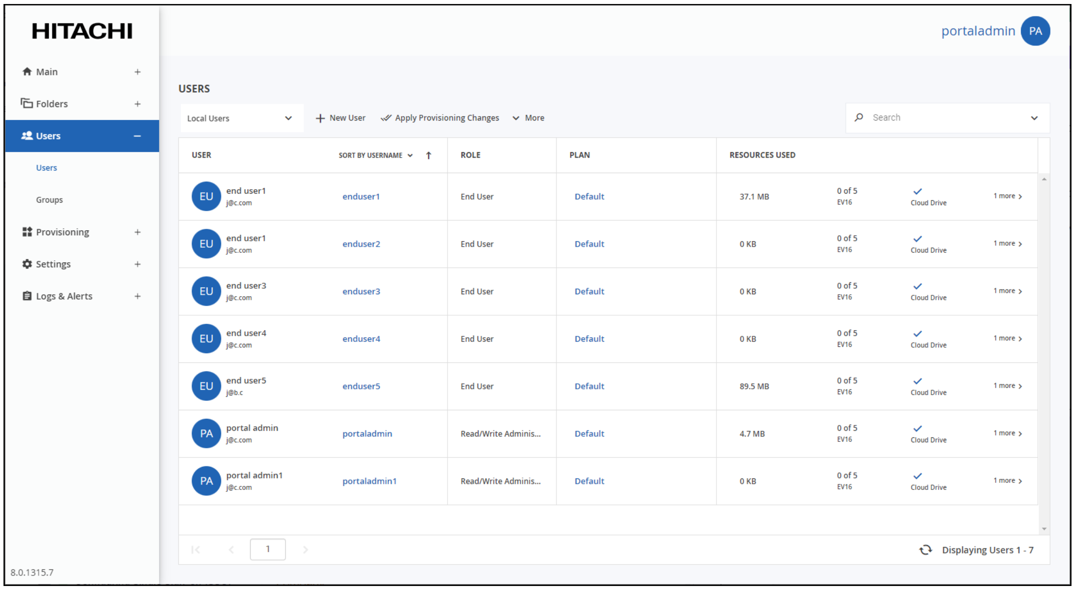
2. Select the group's row to delete and click **Delete Group**.
   A confirmation window is displayed.
3. Click **DELETE GROUP** to confirm.

The group is deleted.

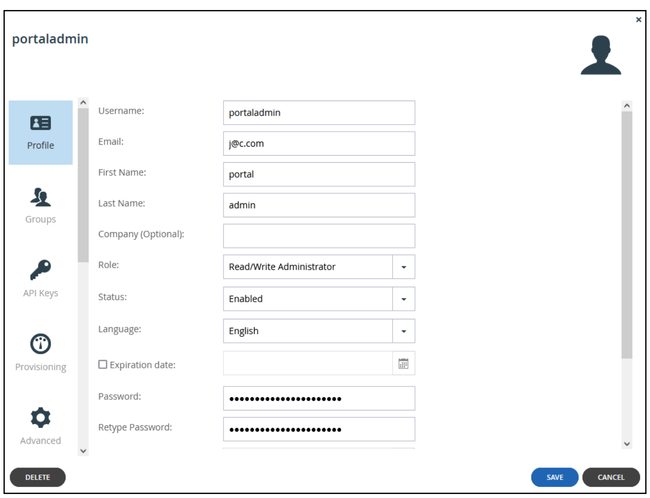
Configuring Deduplication for a User Account

To configure user account deduplication:

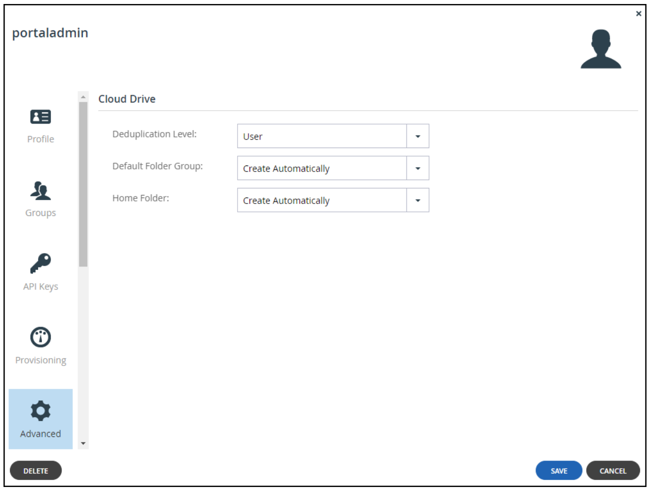
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.



3. Select the **Advanced** option.



Deduplication Level – The default deduplication level to use for new cloud folders. Deduplication is performed on the device before the data is uploaded to the portal:

- **User** – Create a single folder group for the user account, containing all of the user account's cloud folders. Deduplication is performed for the user account's folder group.
- **Portal** – Use a single folder group that is shared by the entire virtual portal, containing all of the cloud folders in the portal.
- **Folder** – Create a folder group for each of the user account's devices, containing all of the device's cloud folders. Deduplication is performed separately for each of the user account's folder groups.

  When the HCP Anywhere Enterprise Edge Filer is configured as a Caching Gateway, use **Folder**.

Default Folder Group – Displayed only if **User** is selected as the *Deduplication Level*. Select the default folder group to use for all of the user account's cloud folder:

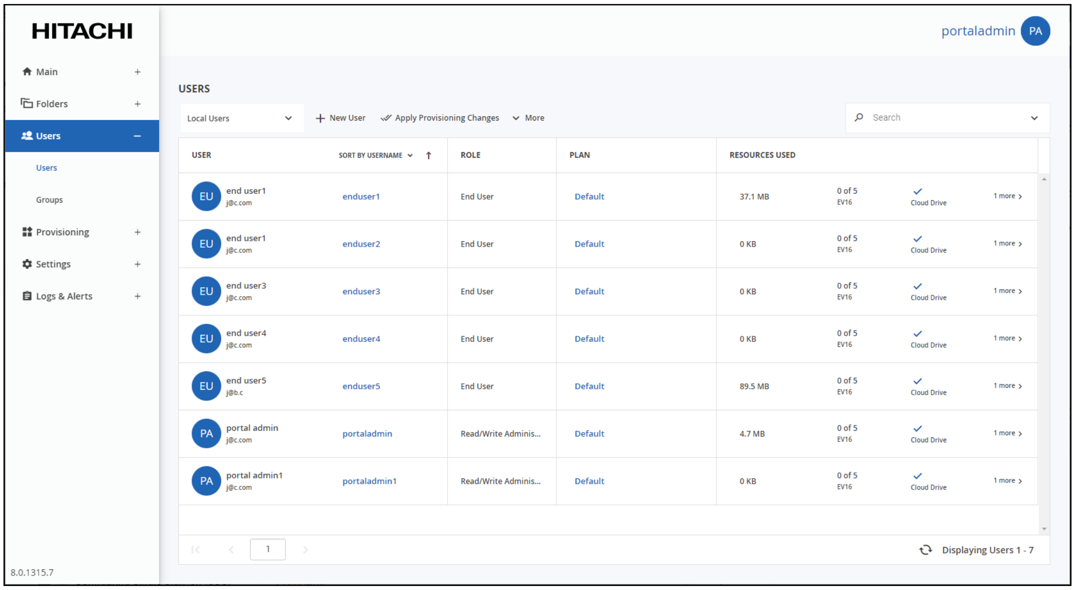
- An existing folder group.
- **Create Automatically** – Automatically create a new folder group.

Home Folder – When configured, one of the user's personal folders to act as the user's home folder. The home folder is a personal folder that is linked to the user account and cannot be deleted.

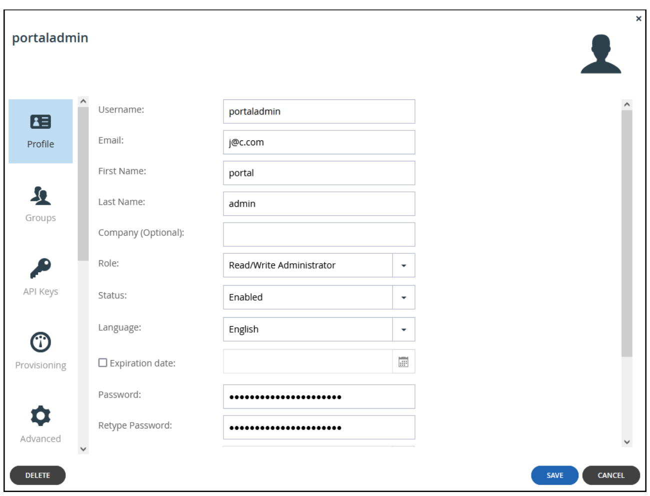
4. Click **SAVE**.

Managing a User's Devices

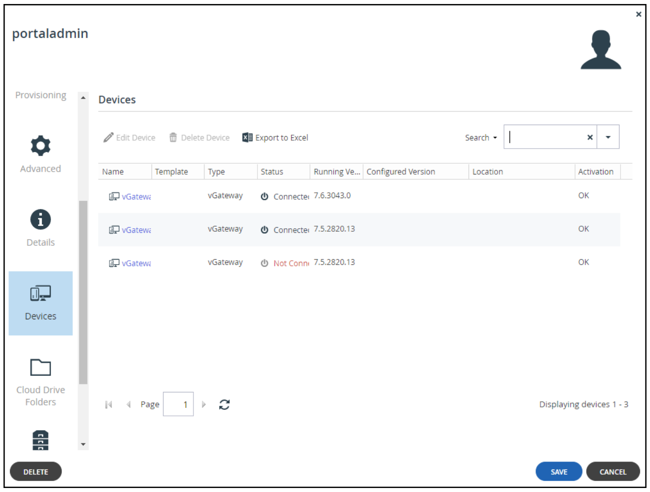
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name.
   The user window is displayed with the user name as the window title.



3. Select the **Devices** option.



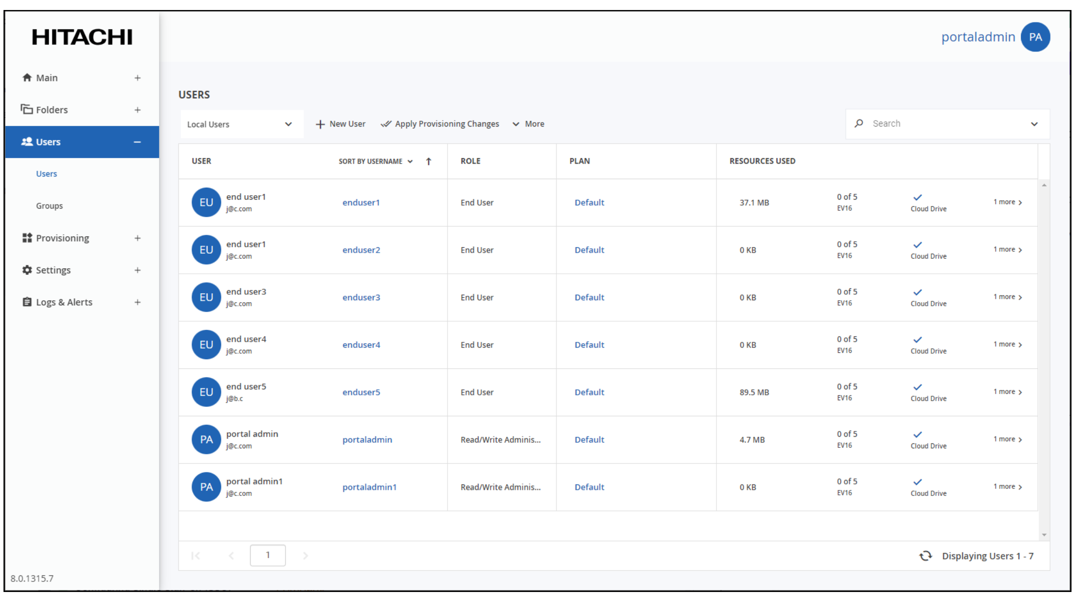
You can perform any of the device management tasks described in Managing Devices.

Managing Cloud Drive Folders and Folder Groups for a User Account

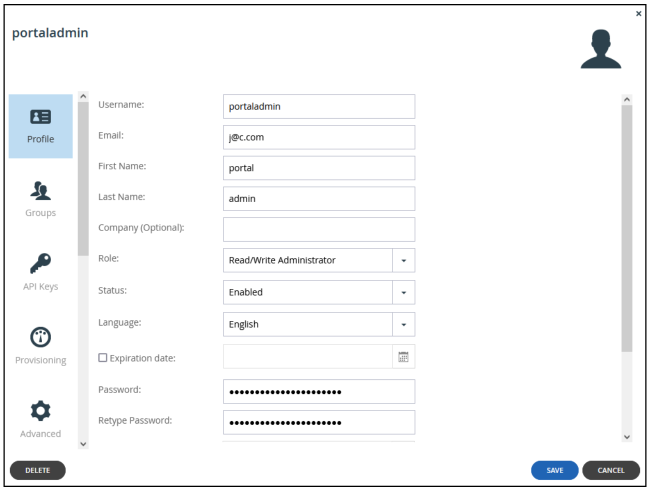
Managing Cloud Drive Folders

To manage cloud folders:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.

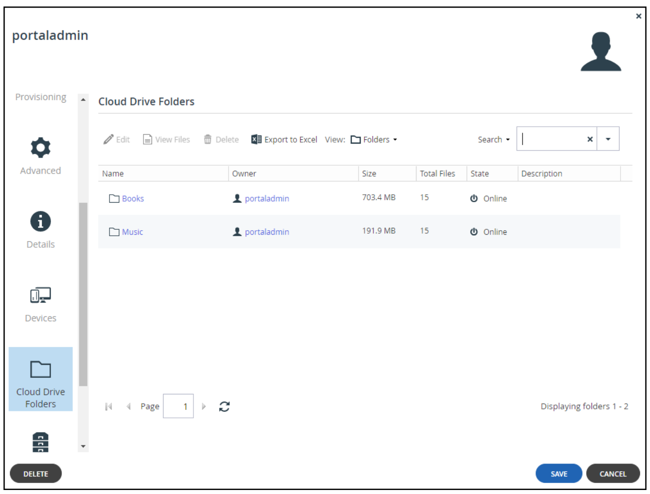


2. Click the user's name.
   The user window is displayed with the user name as the window title.

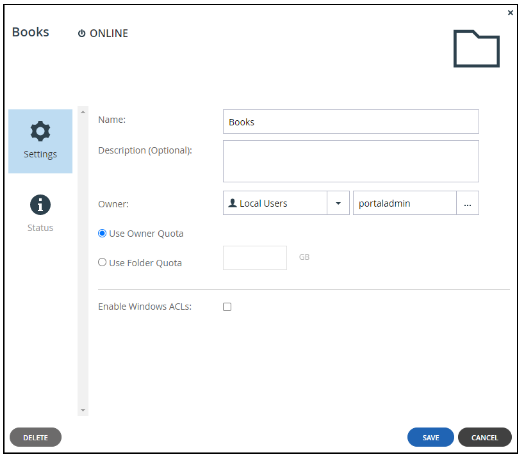


3. Select the **Cloud Drive Folders** option.

   The **Cloud Drive Folders** option displays all cloud drive folders owned by the user.



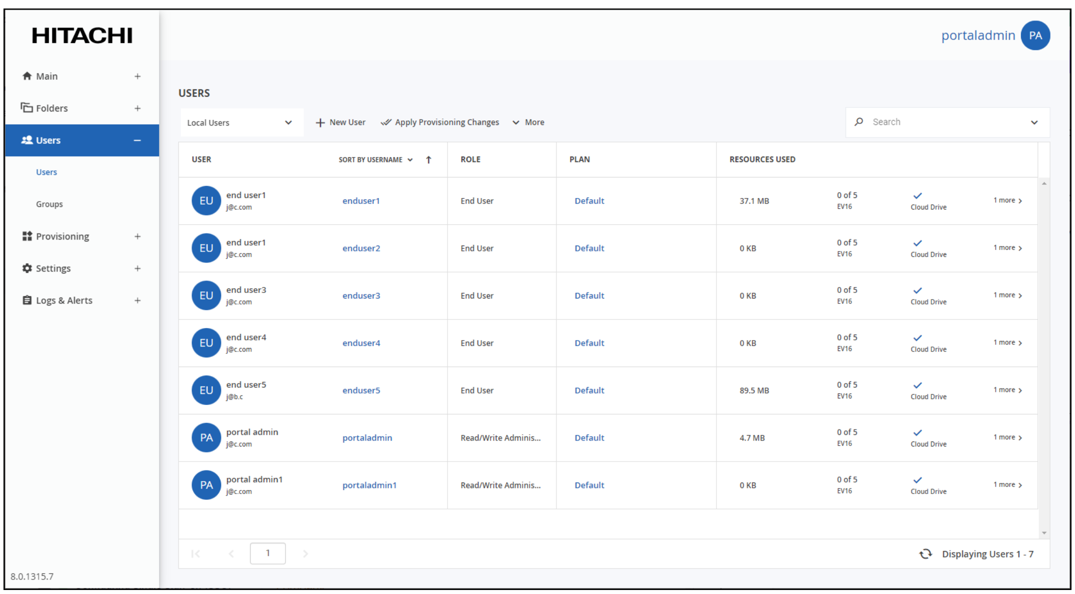
4. Click **Export to Excel** to export the folder details of all the cloud drive folders to a comma separated values (*.csv) Microsoft Excel file on your computer.
5. Select a row and click **View Files** to open the end user portal view with the files from the folder displayed.
6. Select a row and click **Delete** to delete the folder from the cloud drive after confirming this is what is wanted.
7. Click a folder to configure its settings and review its status: The number of files and the storage used by these files.



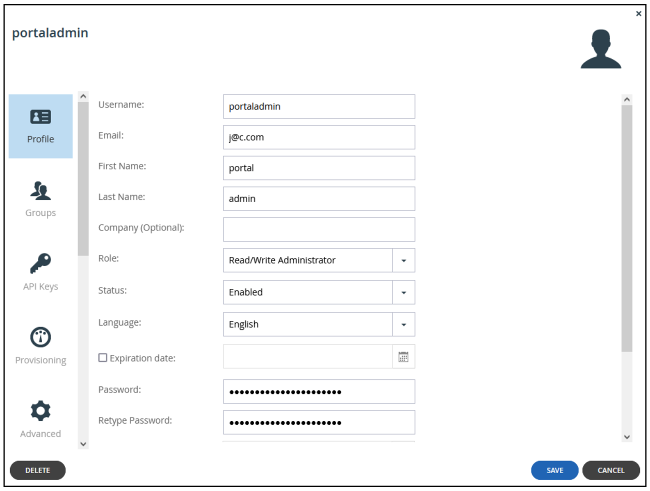
- You can add a description for the folder as well as changing the folder and owners names. You can also set the folder to inherit the Windows ACLs from the local PC settings.

Managing Folder Groups

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.

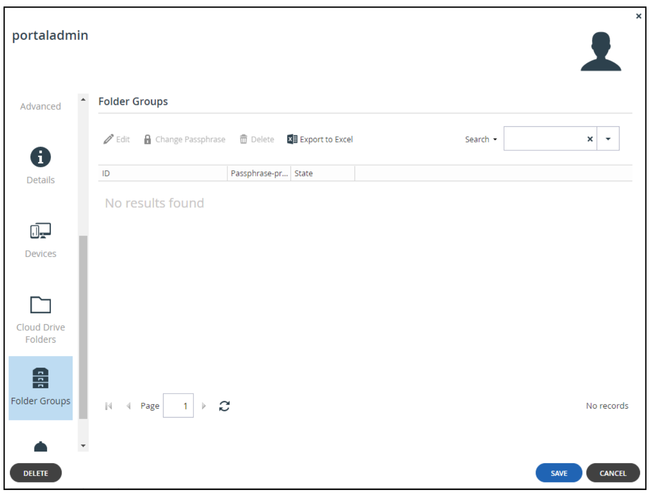


2. Click the user's name.
   The user window is displayed with the user name as the window title.



3. Select the **Folder Groups** option.

   The **Folder Groups** option displays all folder groups associated with the user.



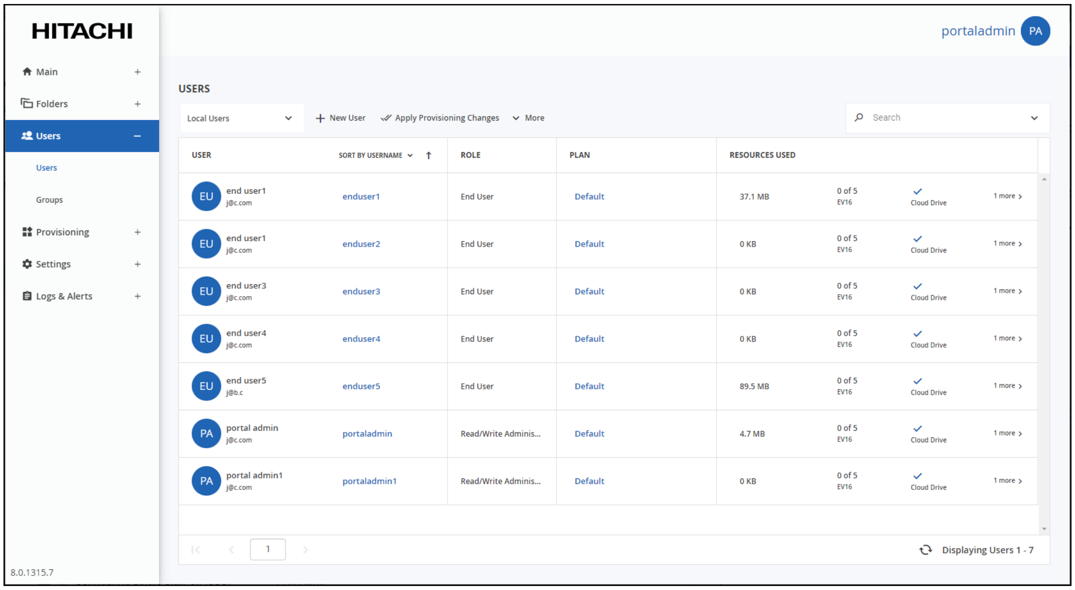
You can perform any of the folder group management tasks described in [Managing Folders and Folder Groups](#).

Exporting User Details to Excel

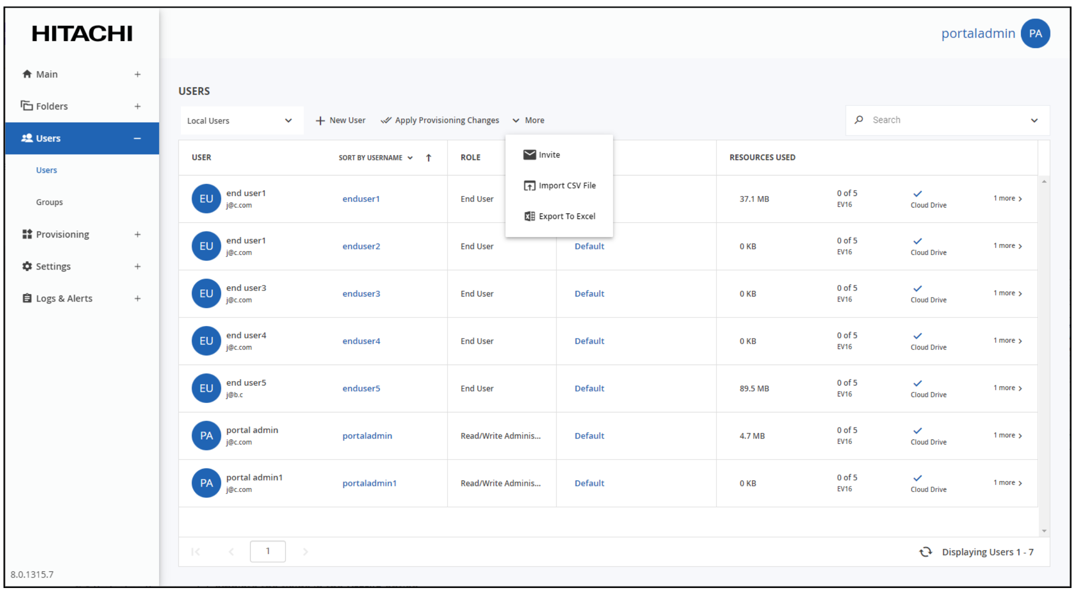
You can export a list of user accounts and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a user details to Microsoft Excel:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click **More > Export to Excel**.



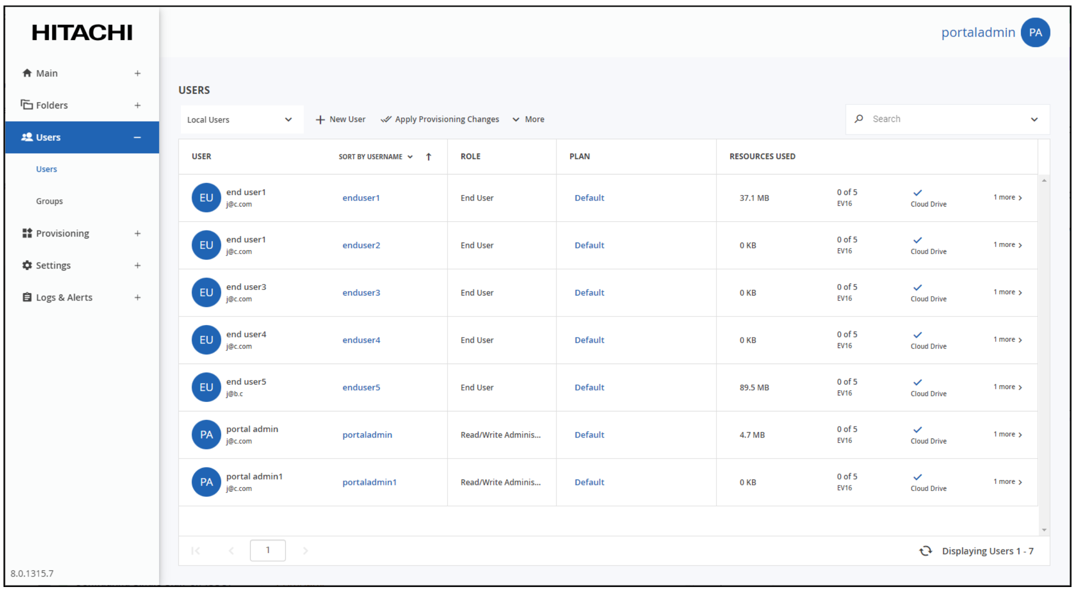
The user list is downloaded to your computer. For each user, the report includes user details such as names and email address, role, subscription plan for the user, and the available licenses.

Managing Administrator Users

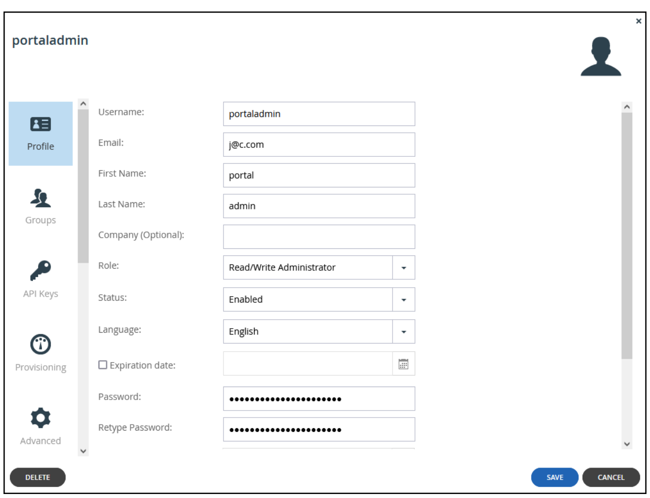
Configuring Alerts For Team Administrators

You can specify alerts that team administrators receive.

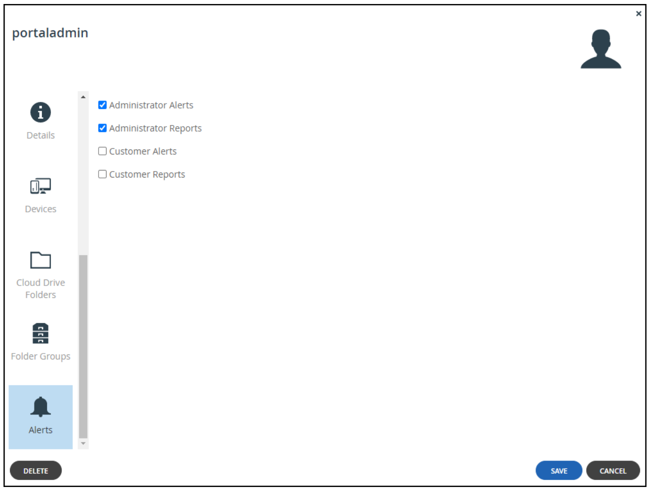
1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. Click the user's name for an administrator user.
   The user window is displayed with the user name as the window title.



3. Select the **Alerts** option.



4. Check the types of alerts to receive:

   Administrator Alerts – Notifications about portal-level problems.
   Administrator Reports – Notifications reporting portal-level activity.
   Customer Alerts – Notifications about device-level problems.
   Customer Reports – Notifications about customer activity.
5. Click **SAVE**.

Customizing Administrator Roles

By default, HCP Anywhere Enterprise Portal includes built-in administrator roles for administrators:

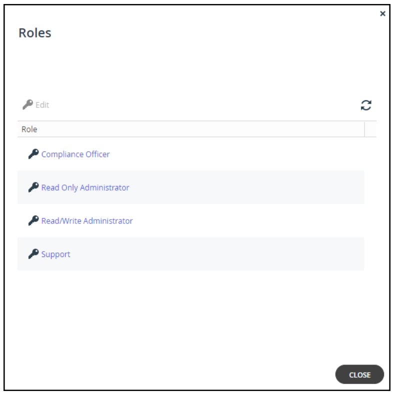
- **Compliance Officer** – The administrator can manage HCP Anywhere Enterprise Vault on folders. For details, see Folder (WORM) Compliance: HCP Anywhere Enterprise VAULT.
- **Read/Write Administrator** – The administrator has read/write permissions throughout the portal.
- **Read Only Administrator** – The administrator has read-only permissions throughout the portal.
- **Support** – The administrator has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the portal.

You can customize these roles, adding or removing permissions.

To customize an administrator role:

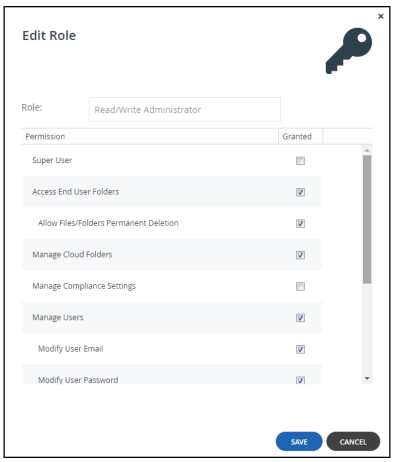
1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **User Roles**, under **USERS** in the **Control Panel** page.
   The **Roles** window is displayed.



3. Either click a role or select a role's row and click **Edit**.

   The **Edit Role** window is displayed.



4. Check the permissions you want to include in the role, and uncheck those that you don't want to include.

   Note: The permissions that can be included are role dependent.

   Super User – Allow all the permissions.

   Access End User Folders – Allow administrators to access end users' folders. If this option is not selected, and an administrator with this role attempts to access an end user's folder, the administrator will be prompted to enter the folder owner's password.

   Allow Files/Folders Permanent Deletion – Allow administrators to permanently delete end user files, folders and backups. Permanent deletion means that the file is not saved for the amount of time specified for the The numbers of days to keep deleted files value in the snapshot retention policy, but it and all versions saved in previous snapshots are deleted as well as the version on all devices.

   Manage Cloud Folders – Allow administrators to manage cloud folders. Without this permission, an administrator only has read/write access to:

   - Folders to which he is the owner.
   - Folders that are owned by someone in a user group the administrator belongs to.
   - Folders to which the administrator has collaboration permissions.

   For all other projects and personal folder objects, the administrator has read-only access. Also, without this permission, the administrator cannot approve or reject a team project folder request, as described in Approving Or Rejecting a Team Project Folder.

Note: A Read/Write Administrator with both **Access End User Folders** and **Manage Cloud Folders** roles can also share the end user cloud folders.

Manage Compliance Settings – Allow administrators to manage compliance settings for cloud folders. For details, see Folder (WORM) Compliance: HCP Anywhere Enterprise VAULT.

Note: The **Compliance Officer** role has this value set by default.

Manage Users – Allow administrators to edit user emails and passwords and add, edit, and delete users.

Modify User Email – Allow administrators to modify the email addresses associated with user accounts.

Modify User Password – Allow administrators to modify the passwords associated with user accounts.

Manage Plans – Allow administrators to add, edit, delete, assign, set defaults, and remove default plans.

Modify Virtual Portal Settings – Allow administrators to modify virtual portal settings. This option is selected by default and cannot be modified.

Modify Roles – Allow administrators to modify administrator roles.

Allow Single Sign On to Devices – Allow administrators to remotely manage devices for which Remote Access with single sign on (SSO) is enabled, without entering the username and password for accessing the device.

Allow Remote Wipe for Devices – This feature is currently not supported.

5. Click **SAVE**.

Permissions Per Administrator Role

The different administrator roles have different permissions.

Permission	Compliance Officer	Read/Write Administrator	Read Only Administrator	Support
Super User	No	Yes (Default is No)	No	No
Access End User Folders	Yes	Yes	Yes	Yes (Default is No)
Allow Files/Folders Permanent Deletion	Yes	Yes (Default is No)	No	No
Manage Cloud Folders	Yes	Yes	No	Yes
Manage Compliance Settings	Yes	Yes (Default is No)	No	No
Manage Users	Yes	Yes	No	Yes
Modify User Email	Yes	Yes	No	Yes
Modify User Password	Yes	Yes	No	Yes
Manage Plans	Yes	Yes	No	Yes
Modify Virtual Portal Settings	Yes	Yes	No	Yes (Default is No)

Permission	Compliance Officer	Read/Write Administrator	Read Only Administrator	Support
Modify Roles	Yes	Yes	No	Yes (Default is No)
Allow Single Sign On to Devices	Yes (Default is No)	Yes	Yes (Default is No)	Yes (Default is No)
Allow remote wipe for devices	Yes	Yes	Yes (Default is No)	Yes (Default is No)

Chapter 11. Configuring Single Sign-On (SSO) to the HCP Anywhere Enterprise Portal

You can define Single Sign-On, SSO, to a HCP Anywhere Enterprise Portal either in Active Directory using the Kerberos protocol or using an external identity provider providing support for Security Assertion Markup Language, SAML 2.0.

When SSO is enabled on the HCP Anywhere Enterprise Portal, users' passwords are not stored on HCP Anywhere Enterprise Portal.

In this chapter

Using Active Directory for Single Sign-On

You can configure single sign-on for one team HCP Anywhere Enterprise Portal, for users defined in Microsoft Active Directory, using the Kerberos protocol. When single sign on is configured, HCP Anywhere Enterprise Agents automatically and transparently authenticate to the HCP Anywhere Enterprise Portal using their Active Directory credentials, upon first login to the PC on which they are installed.

Note: Users logging on to a PC running a HCP Anywhere Enterprise Agent, with CAC, Common Access Card, are automatically and transparently authenticated to the HCP Anywhere Enterprise Portal. Single sign-on (SSO) to the HCP Anywhere Enterprise Portal must be defined in Microsoft Active Directory, using the Kerberos protocol.
Only one virtual portal can be defined with single sign-on using Kerberos.

A service principal name (SPN) account on Active Directory uniquely identifies an instance of a service. Before the HCP Anywhere Enterprise Portal can use Kerberos authentication, you must register the SPN on the account object that the HCP Anywhere Enterprise Portal uses to log on and then create a keytab file.

To configure Kerberos for single sign-on with HCP Anywhere Enterprise Portal:

- Kerberos requires the clocks of the relevant hosts to be synchronized. Ensure that the HCP Anywhere Enterprise Portal server's clock is synchronized with the Active Directory clock, preferably by synchronizing the HCP Anywhere Enterprise Portal server's underlying clock, for example, via VMware Tools for a portal running on ESXi, with an NTP server.
- In order to authenticate with aes256-cts-hmac-sha1-96, make sure that the Active Directory domain controller policy supports this authentication. If this is not the case, change the **ssouser** configuration in the Active Directory server, so that the account supports AES 128 bit and AES 256 bit encryption.
- Generate a new keytab with AES256 encryption, copy it to the HCP Anywhere Enterprise Portal and then run `portal-keytab.sh` with the new keytab on the portal and `klist purge` in the HCP Anywhere Enterprise Agent workstation.

- Verify the following in the *libdefaults* section of the **krb5.conf**:
  `default_tkt_enctypes = aes256-cts-hmac-sha1-96`
  `default_tgs_enctypes = aes256-cts-hmac-sha1-96`
- Connect the HCP Anywhere Enterprise Portal to Active Directory.

Note: Only one virtual portal can be defined with single sign-on using Kerberos. If the global administrator has set up SSO using Kerebos on another virtual portal, you cannot set SSO using Kerebos on this HCP Anywhere Enterprise Portal.

To configure SSO on the portal:

Note: Part of this procedure includes stopping the HCP Anywhere Enterprise Portal, which will result in some downtime.

1. Enable the keytab file on the HCP Anywhere Enterprise Portal:

a) Log in to the HCP Anywhere Enterprise Portal as root, using SSH.

b) Run the following command to stop the portal: `portal-manage.sh stop`

c) Copy the keytab file from the Active Directory server to `/usr/local/ctera/apache_tomcat` on the HCP Anywhere Enterprise Portal server.

d) Run the following command: `portal-keytab.sh` *`keytabfile`* where *keytabfile* is the full name and path of the keytab file.

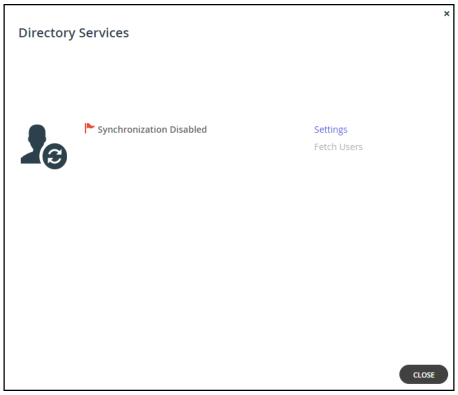
e) Run the following command to start the portal: `portal-manage.sh start`

2. Add the Active Directory server to the HCP Anywhere Enterprise Portal:

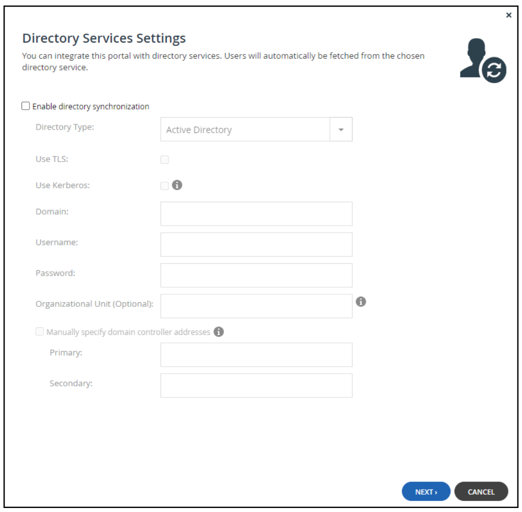
a) Log in to the portal.

b) Select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

c) Select **Directory Settings**, under **USERS** in the **Control Panel** page.
The **Directory Services** page is displayed.



d) Click **Settings**.
The **Directory Services Settings** window is displayed.



e) Specify the following:
Check **Enable directory synchronization**.
In **Directory Type**, select Active Directory.
Check **Use Kerberos**.
In **Domain**, enter the Active Directory domain.
In **Username**, enter the username for the Active Directory URL.
In **Password**, enter the password for the Active Directory URL.

f) Click **NEXT** to the end of the wizard.

g) Click **FINISH**.

SSO is now configured on the HCP Anywhere Enterprise Portal.

Note: A single virtual HCP Anywhere Enterprise Portal can be configured to enable simultaneous SSO access via both Kerberos SSO and WebDAV SPNEGO, described in Enabling WebDAV Access Without Additional Authentication (Using SPNEGO). For details, see Using Kerberos and SPNEGO Together.

Enabling WebDAV Access Without Additional Authentication (Using SPNEGO)

When using WebDAV to access files from the HCP Anywhere Enterprise Portal global file system, the files must be accessible without requiring additional authentication. This functionality is enabled using SPNEGO. SPNEGO is a standard specification defined in the Simple and Protected GSS-API Negotiation Mechanism (IETF RFC 2478).

Note: Access to the HCP Anywhere Enterprise Portal using HCP Anywhere Enterprise Drive Connect also uses WebDAV to display the content in a file manager.

HCP Anywhere Enterprise Portal Support For SPEGNO Authentication

The following configuration is required to enable using WebDAV to access files from the HCP Anywhere Enterprise Portal global file system without requiring additional authentication, using SPNEGO:

1. On all Windows clients that connect to the portal, as the Active Directory user:
   - **a)** Change the *`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains`* registry entry:
     Add a new key: *portalSuffix*, for example `myportal.com`.
     In the new key add a new `DWORD (32-bit) Value` entry, called `https` and set the value to `1`.
   - **b)** Change the *`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1`* registry entry:
     Add a new `DWORD (32-bit) Value` entry, called `1A00` and set the value to `0`.
   - **c)** Save the registry.
2. On all Windows clients that connect to the portal, as a Windows administrator user:
   - **a)** Change the *`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`* registry entry:
     Add a new entry of type `Multi-String Value`.
     Change the name of the entry to `AuthForwardServerList`.
     Modify the entry by adding the URL for the portal, specifying just the DNS suffix, for example, `https://*.myportal.com`.
   - **b)** Save the registry.
3. On Windows 7 clients that connect to the portal, apply the update described in https://support.microsoft.com/en-us/topic/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-winhttp-in-windows-c4bd73d2-31d7-761e-0178-11268bb10392.
4. On Mac clients that connect to the portal, configure Kerberos for authentication in the /etc/krb5.conf file.

   For example:

```
[domain_realm]
   .DOMAIN.COM = DOMAIN.COM
   DOMAIN.COM = DOMAIN.COM
[libdefaults]
   default_realm = DOMAIN.COM
   dns_lookup.kdc = true
```

```
   forwardable = true
   noaddresses = true
[realms]
DOMAIN.COM = {
   kdc = domain.com:88
}
```

5. Restart all clients.
6. Configure the ADFS/Kerberos server as described in https://gusto77.wordpress.com/2015/09/02/apache-tomcat-spnego-authentication-configuration

   Register the SPN using the portal DNS: `setspn -A HTTP/`*`portalname.myportal.com user`*

   Create a keytab file: `ktpass /out c:\tomcat.keytab /mapuser `*`user@DOMAIN.COM`*` /princ HTTP/`*`portalname.myportal.com@DOMAIN.COM`*` /pass `*`user_password`*` /kvno 0 /pType KRB5_NT_PRINCIPAL`

   Move the keytab file to the tomcat server: `/usr/local/ctera/apache-tomcat/`*`SPNEGO_KEYTAB`*
7. Configure the portal application servers.
   a) Edit `/usr/local/ctera/apache-tomcat/jaas.config` to match the SPN configured in the Kerberos server, in step **6**.

   ```
   ...
   com.sun.security.jgss.accept {
      com.sun.security.auth.module.Krb5LoginModule required
      useKeyTab=true
      keyTab="/usr/local/ctera/apache-tomcat/SPNEGO_KEYTAB"
      principal="HTTP/portalname.myportal.com@DOMAIN.COM"
      storeKey=true doNotPrompt=true;
   };
   ...
   ```

   b) Set the portal to support SPNEGO: `set /settings/supportSPNEGO true`
   c) If there are Windows 7 clients, on every portal application server, edit `/usr/local/ctera/apache-tomcat/conf/server.xml`:

   ```
   sslProtocol="TLS"
   sslEnabledProtocols="TLSv1.2"
   ```

   d) Restart the servers.

Using Kerberos and SPNEGO Together

In an environment where single sign-on for a HCP Anywhere Enterprise Portal is configured for users defined in Microsoft Active Directory, using the Kerberos protocol, you can also configure access to the HCP Anywhere Enterprise Portal via WebDAV using SPNEGO.

Note: Only one virtual HCP Anywhere Enterprise Portal can be defined with single sign-on using Kerberos. If the global administrator has set up SSO using Kerebos on another virtual HCP Anywhere Enterprise Portal, you cannot set SSO using Kerebos on this HCP Anywhere Enterprise Portal.

To use both Kerberos and SPNEGO to enable SSO to a HCP Anywhere Enterprise Portal:

1. Create a new Active Directory Principal and create a new keytab file for this service principal. Run the following command on the domain controller:
   `ktpass -princ` *SPN* `-out` *path_to_keytab*
   `-mapuser` *account_name@DOMAIN* `-mapOp set -pass` *account_password*
2. Import the keytab file into the HCP Anywhere Enterprise Portal next to the existing keytab files.
3. Manually add using the keytab file to the */usr/local/ctera/apache-tomcat/jaas.config* file.

   Note: You cannot use portal-keytab.sh to add the keytab, as it will overwrite the existing keytab and not add the second keytab, as required.

Using SAML 2.0 For Single Sign-On

HCP Anywhere Enterprise Portal supports user identity federation over SAML 2.0. SAML enables you to centralize your corporate user identities and provide Single Sign-On (SSO) capabilities to all of your enterprise applications. When SSO is enabled on the HCP Anywhere Enterprise Portal, users' passwords are not stored on HCP Anywhere Enterprise Portal, instead, user authentication is performed through the identity provider's login page.

To configure SAML SSO, you need an SAML identity provider. HCP Anywhere Enterprise Portal SAML single sign-on has been certified with the following identity providers:

- Microsoft Active Directory Federation Services (ADFS):Configuring Microsoft ADFS to Work with HCP Anywhere Enterprise Portal
- Microsoft Entra ID (Azure Active Directory): Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal
- Okta: Configuring Okta to Work with HCP Anywhere Enterprise Portal
- OneLogin: Configuring OneLogin to Work with HCP Anywhere Enterprise Portal
- Swivel AuthControl Sentry: Configuring Swivel AuthControl Sentry to Work with HCP Anywhere Enterprise Portal

Before setting up SAML in the HCP Anywhere Enterprise Portal:

- The users must be defined. For details, see Using Directory Services For the Users.
- You have to define access to the HCP Anywhere Enterprise Portal on the identity provider side. Although each identity provider can have a different procedure for setting this up, the SAML protocol requires the following information:
  Entity ID – A globally unique name for a SAML entity. This entity is defined at the identity provider, IdP, side.
  Sign-in page URL – The location where the SAML assertion is sent with HTTP POST. This is often referred to as the SAML Assertion Consumer Service (ACS) URL for the SAML endpoint at the IdP side.
  Log-out page URL – The location where the logout response will be sent.
  Identity Provider Certificate – The authentication used by the identity provider.
  The terms used for this information can vary between the different identity providers.

  Note: If you want to use a different identity provider, contact Hitachi Vantara to validate the provider.

  You need to enable SSO on the HCP Anywhere Enterprise Portal and specify the identity provider's parameters. Once configured, the provider handles the sign-in process for all HCP Anywhere Enterprise Portal users. The provider is also responsible for authentication credentials for the users.

You need to set up the HCP Anywhere Enterprise Portal as a SAML application in the identity provider before Defining SAML Single Sign-on in a HCP Anywhere Enterprise Portal.

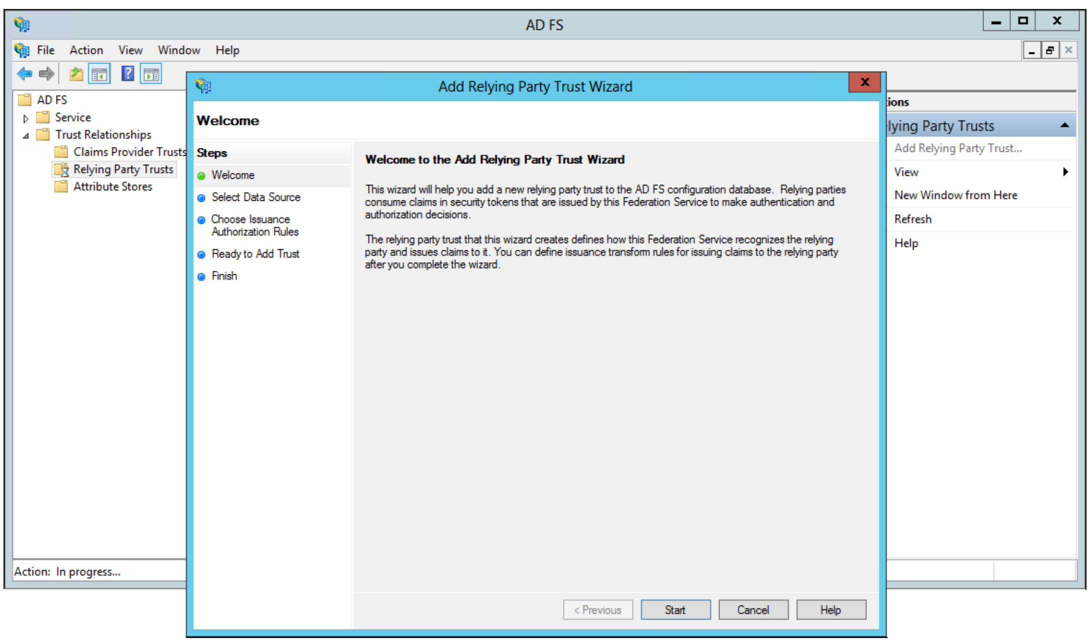
Configuring Microsoft ADFS to Work with HCP Anywhere Enterprise Portal

You set up SAML single sign-on support in ADFS and gather the information you need to connect the HCP Anywhere Enterprise Portal to ADFS.

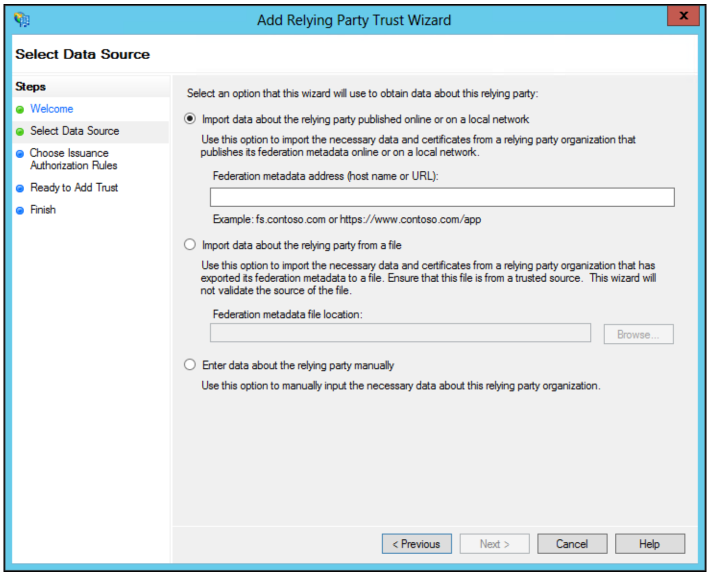
To get the SAML single sign-on information:

1. Login to the Windows Server ADFS machine as the administrator.
2. Open **AD FS Management**.

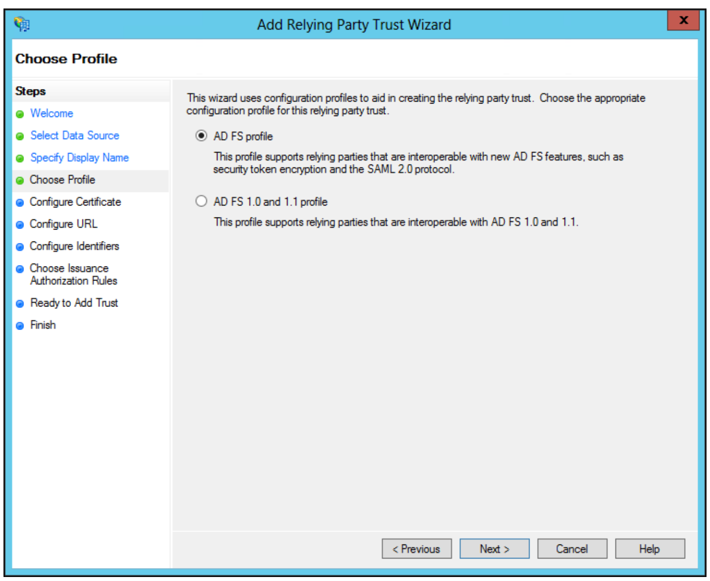
   Note: The procedure and screens are based on AD FS running on Windows 2012 server. This might be different on other versions of Windows server.
3. In the left pane navigation tree, select **Trust Relationships** and right-click **Relying Party Trusts**.
4. Click **Add Relying Party Trust**.



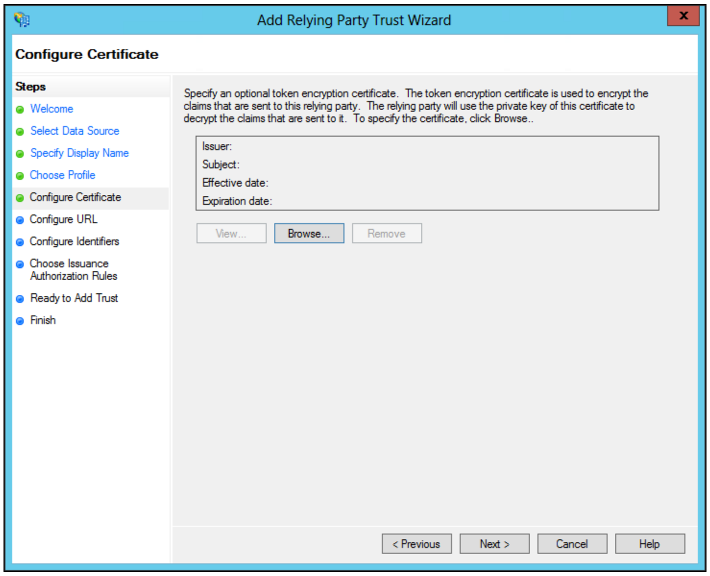
5. Click **Start**.



6. Choose the **Enter data about the relying party manually** option and click **Next**.
7. Enter a display name for the relying party and optionally add notes about the party and click **Next**.

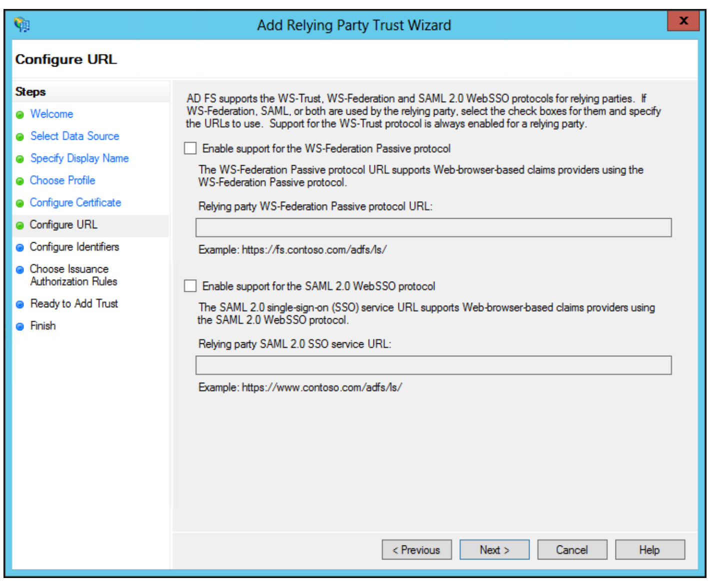


8. Choose the **AD FS Profile** option and click **Next**.

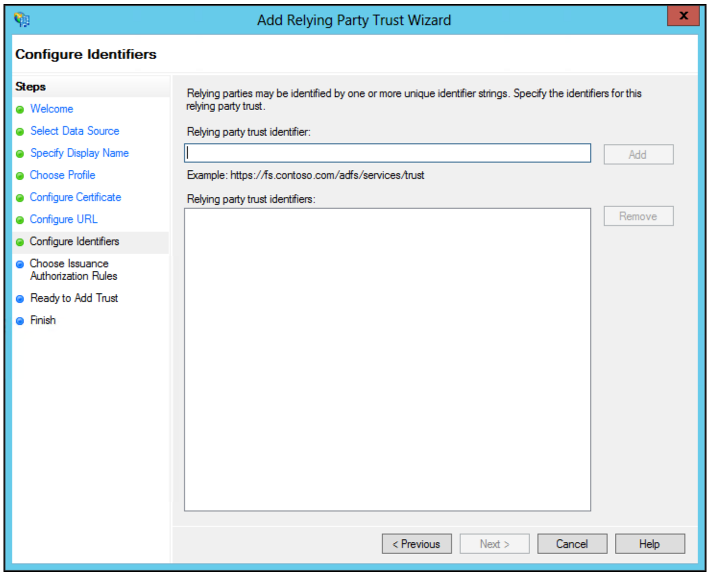


9. Optionally, if you want to encrypt claims sent to the relying party, browse to the HCP Anywhere Enterprise Portal certificate and select it and click **Open**.

   The issuer, subject, effective date and expiry date information for the certificate is displayed.
10. Click **Next**.

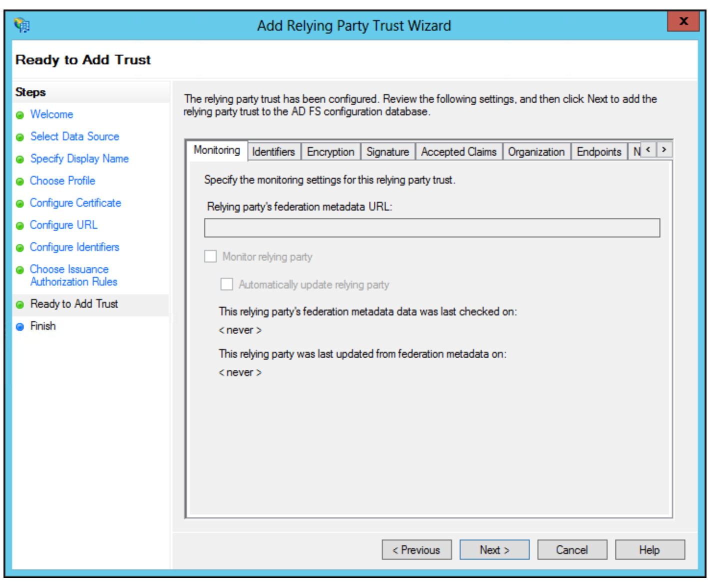


11. Check **Enable support for the SAML 2.0 WebSSO protocol** and enter the HCP Anywhere Enterprise Portal URL followed by **/SAML**, as in the following example:
    `https://exampleportal.hcp.me/ServicesPortal/saml`
12. Click **Next**.



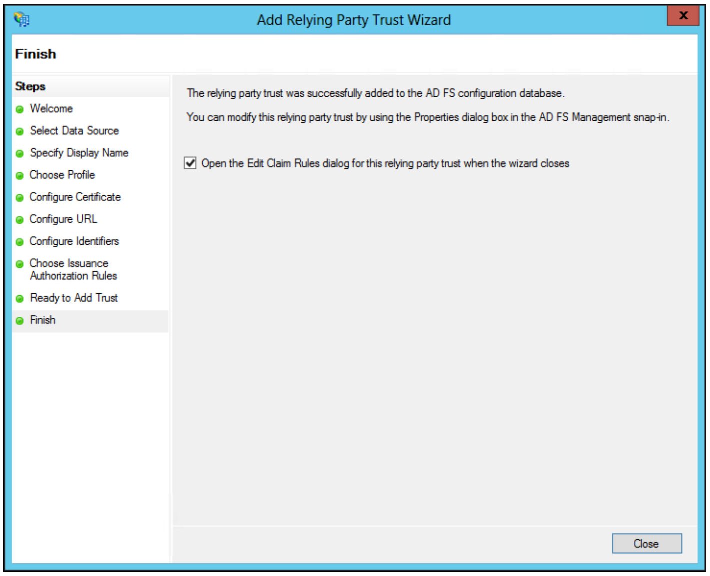
13. Set the **Relying party trust identifier** and click **Add**. For example, `hcp-adfs`

    You use the **Relying party trust identifier** in the HCP Anywhere Enterprise Portal **Entity ID/Issuer ID** field, in the procedure To configure SAML single sign-on: in step **4**, when setting up SAML in the HCP Anywhere Enterprise Portal.
14. Click **Next**.
15. Leave the default to allow all users access, unless you want to restrict the users with access to the HCP Anywhere Enterprise Portal to users for whom you add issuance authorization rules, as described in the ADFS documentation.
16. Click **Next**.



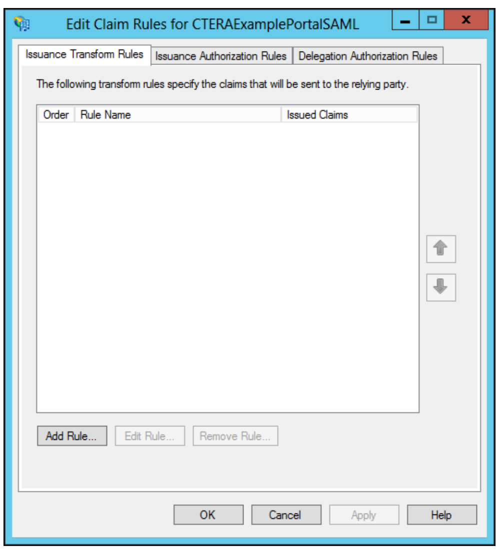
A summary of the wizard steps is displayed in the tabs.

17. Select the **Signature** tab and import the HCP Anywhere Enterprise Portal Certificate.
18. Click **Next**.

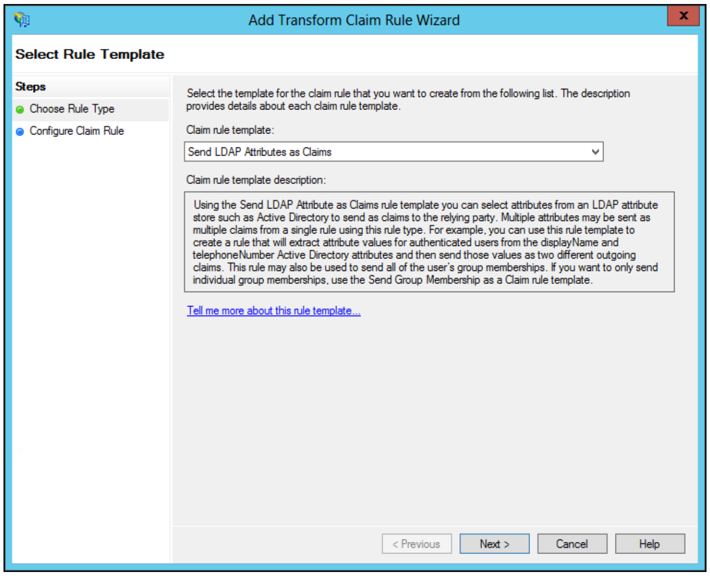


19. Check the **Open Edit Claim Rules dialog for this relying trust when the wizard closes** and click **Close**.

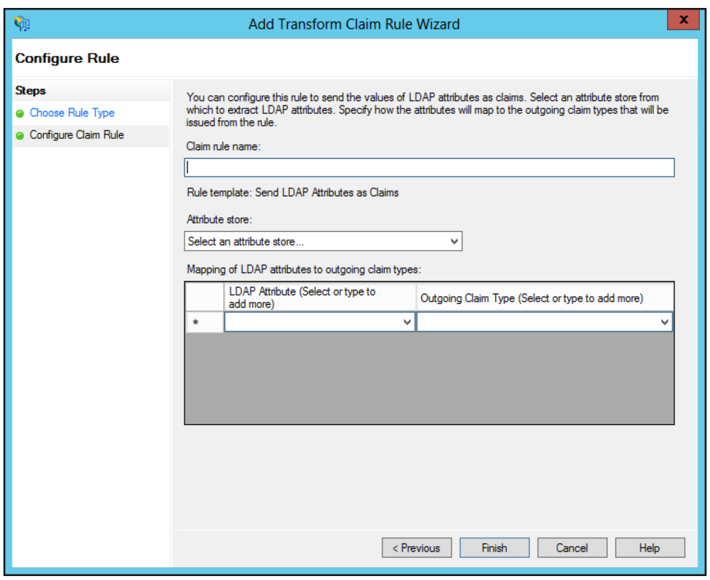
    The Edit Claim Rules dialog for the relying party is displayed.



20. Click **Add Rule**.



21. Select **Send LDAP Attributes as Claims** for the **Claim rule template** and click **Next**.



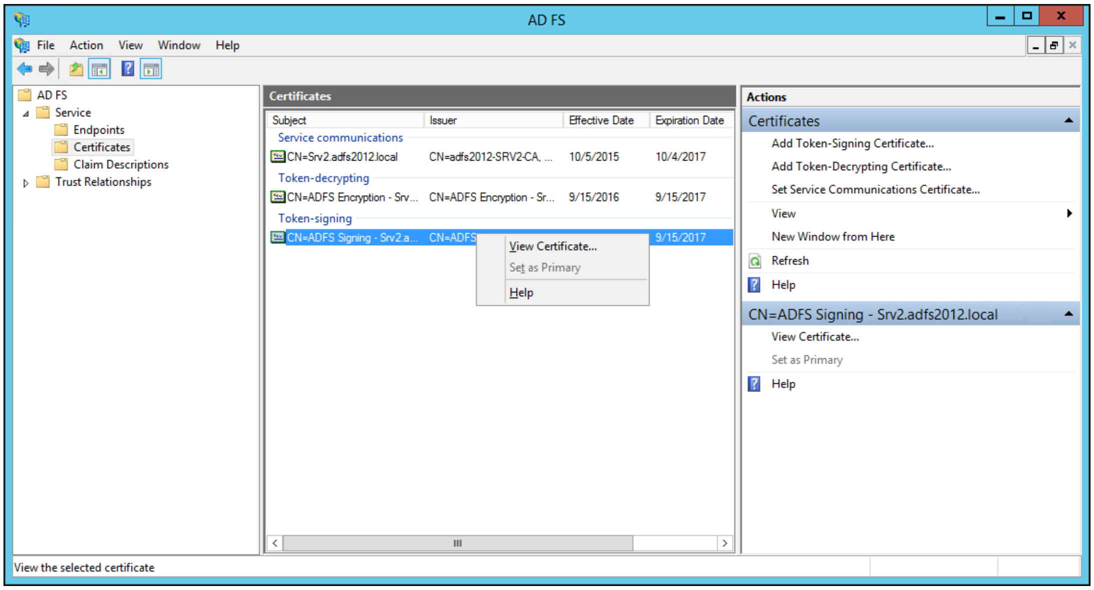
22. Enter the following:

Claim rule name – A name for the rule.
Attribute store – Select the store from the list, for example, Active Directory.
LDAP Attribute – Use **User-Principal-Name**.
Outgoing Claim Type – Select **Name ID**.

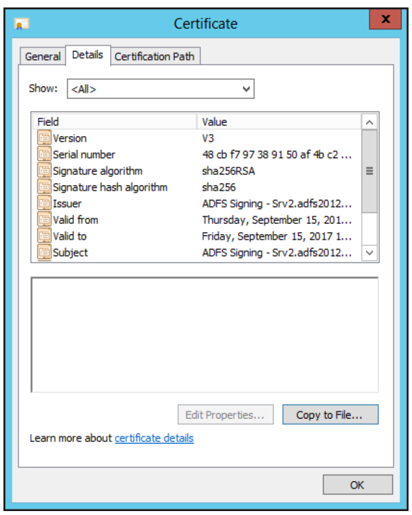
23. Click **Finish**.

24. Click **OK**.

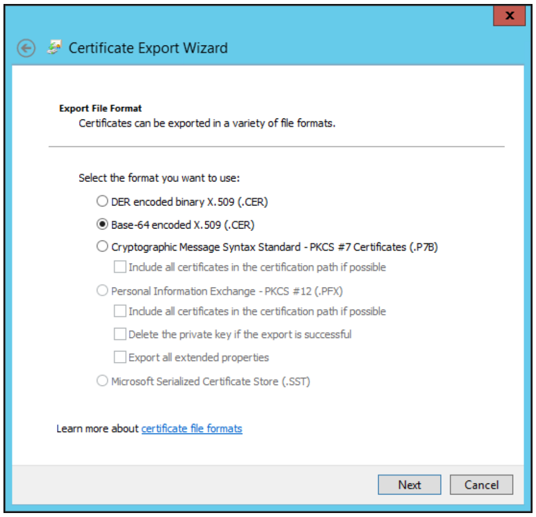
25. In the left pane navigation tree, select **Service > Certificates**, right-click the certificate under **Token-signing** and click **View Certificate**.



26. Select the **Details** tab and click **Copy to File**.



27. Click **Next** in the **Certificate Export** wizard and select the **Base-64 encoded X.509** option.



28. Click **Next** and enter a file name.
29. Click **Next** and then **Finish**.

You upload this certificate when setting up SAML in the HCP Anywhere Enterprise Portal.

Encrypting the SAML Response

When using ADFS for SAML to sign in to the HCP Anywhere Enterprise Portal, the SAML response can be encrypted, as follows:

1. Add the HCP Anywhere Enterprise Portal certificate to the relaying party in ADFS.
2. Using SSH, log in as root to your HCP Anywhere Enterprise Portal server.
3. Run the following command in ADFS PowerShell: set-ADFSRelyingPartyTrust –TargetName “<relaying party name>” -EncryptClaims $True

   For example,
   set-ADFSRelyingPartyTrust –TargetName “HCP Anywhere Enterprise Portal” -EncryptClaims $True
   To turn the encryption off, run the command but set to $False.

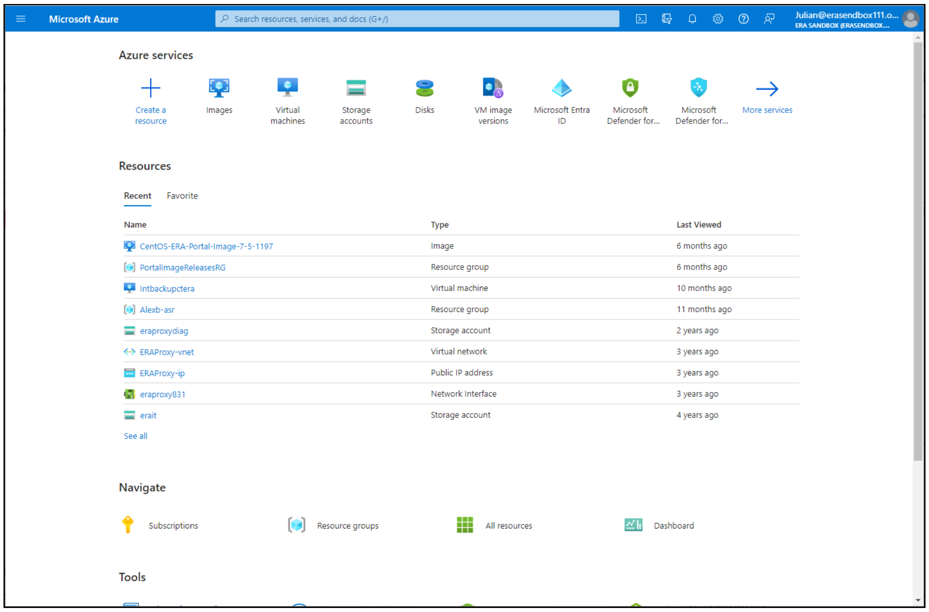
Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal

You set up SAML single sign-on support in Azure and gather the information you need to connect the HCP Anywhere Enterprise Portal to Entra ID (Azure Active Directory).

Note: Microsoft changes the look and feel of Azure from time to time. The following procedure and screens might have changed but the basic procedure will be the same.

To get the SAML single sign-on information:

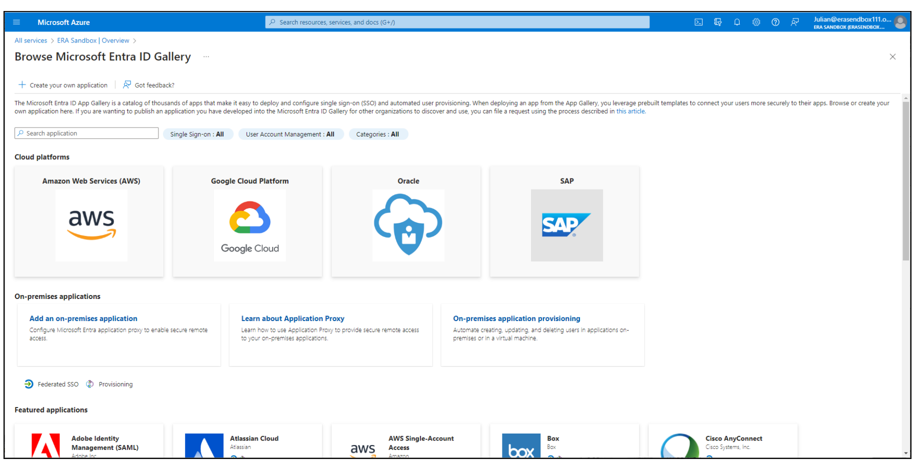
1. Login to Azure as the administrator.
   The home page is displayed.



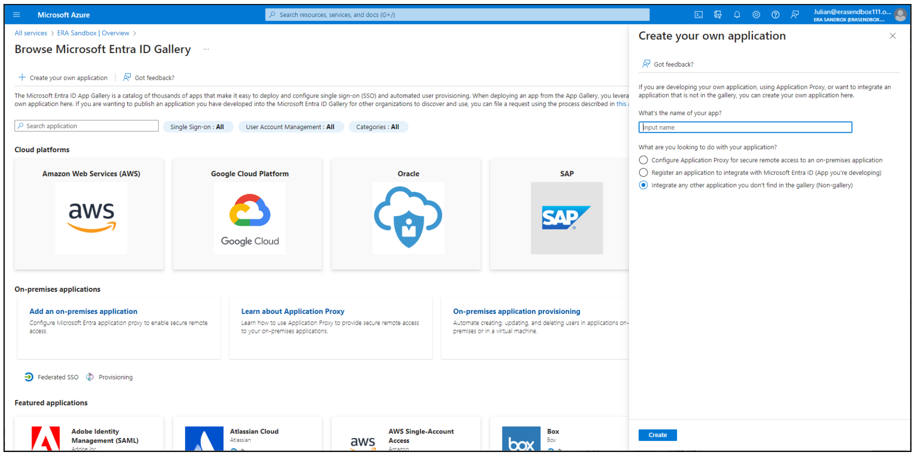
2. Access the **Microsoft Entra ID** service.

   The **Overview** page is displayed.
3. Scroll down and under **Quick Actions** click **Add enterprise applications**.

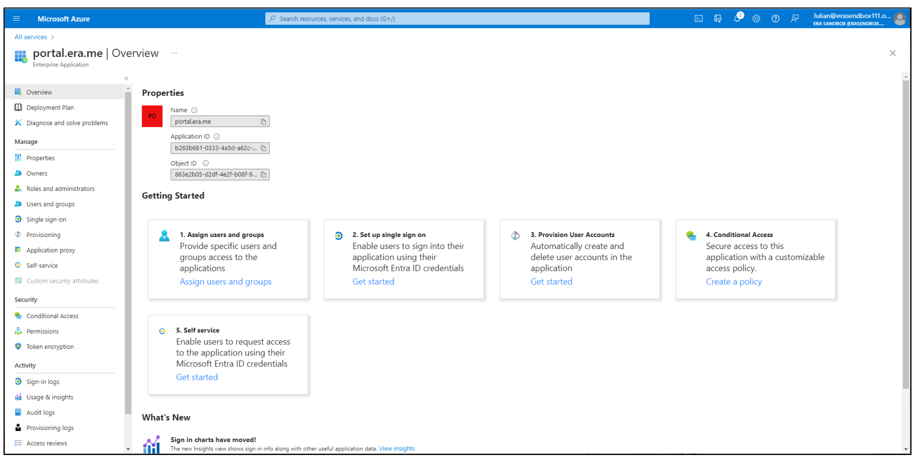
   The **Browse Microsoft Entra ID Gallery** page is displayed.



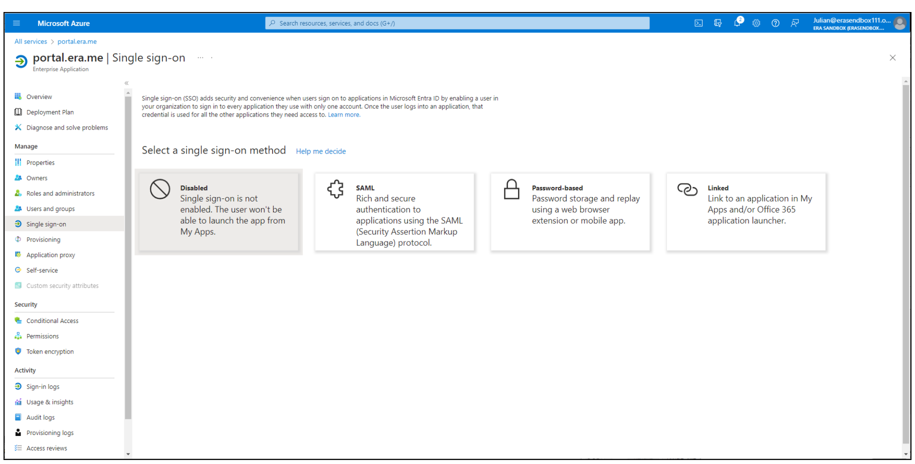
4. Click the **Create your own application** tab.
   The **Create your own application** blade is displayed.



5. Enter the DNS name for the portal in the **What's the name of your app** box and click **Create**.

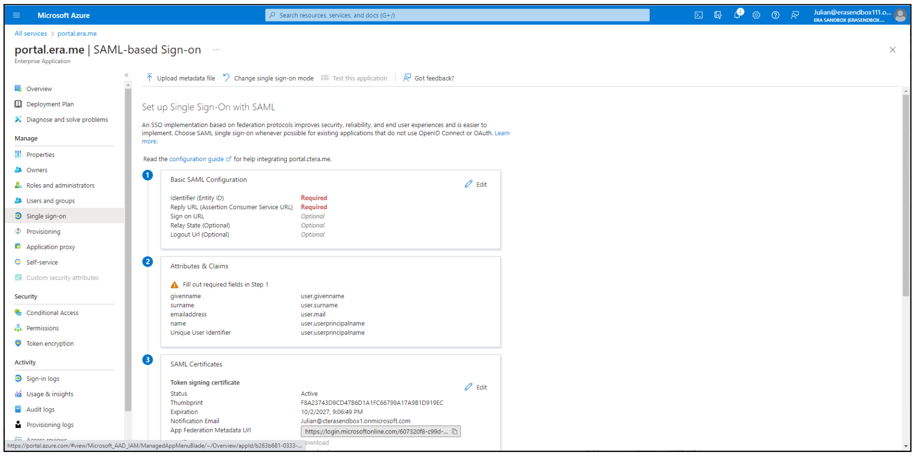


6. In the navigation pane, click **Single sign-on** or click **2. Set up single sign on**.



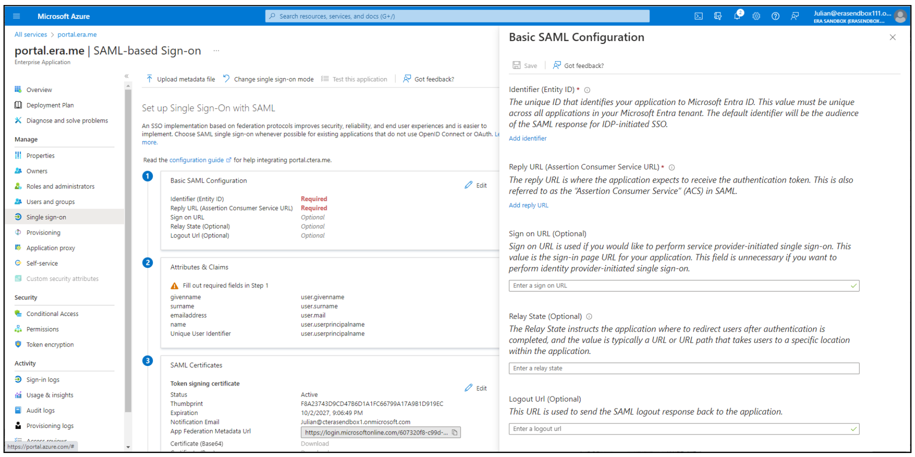
7. Click **SAML**.

The **SAML-based Sign-on** page is displayed.



8. Click the pen icon to edit the **Basic SAML Configuration**.

   The **Basic SAML Configuration** blade is displayed.



9. Set the **Identifier (Entity ID)** to something that uniquely identify the set up. For example, `hcp-azureAD`.

   You use this value in the HCP Anywhere Enterprise Portal **Entity ID/Issuer ID** field, in the procedure *To configure SAML single sign-on*, described in Defining SAML Single Sign-on in a HCP Anywhere Enterprise Portal, when setting up SAML in the HCP Anywhere Enterprise Portal.
10. Enter the URL to access the HCP Anywhere Enterprise Portal login in the **Reply URL (Assertion Consumer Service URL)** box:

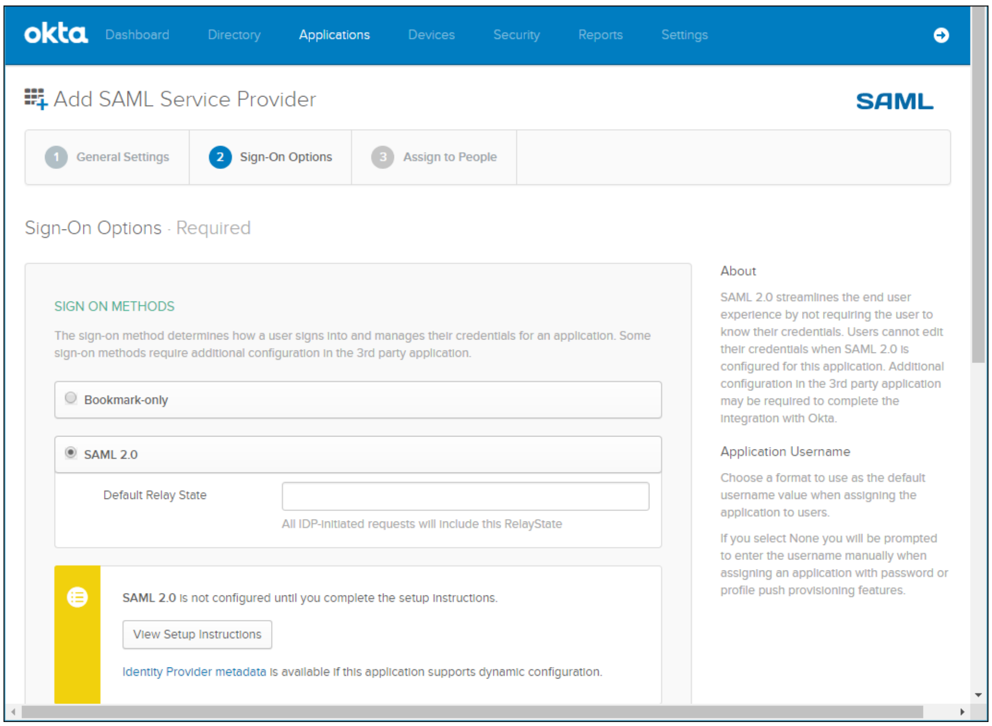
    `http://<teamportal>.<DNS_Suffix>/ServicesPortal/saml` where `<teamportal>` is the name of the HCP Anywhere Enterprise Portal, and `<DNS_Suffix>` is the DNS suffix for the HCP Anywhere Enterprise Portal installation.
11. Click **Save**.
12. Click **Download** for the **Certificate (Base64)**.
13. Optionally, edit **Attributes & Claims**.

Configuring Okta to Work with HCP Anywhere Enterprise Portal

You set up SAML single sign-on support in Okta using the *SAML Service Provider* application. You then gather the information you need to connect the HCP Anywhere Enterprise Portal to Okta.

To get the SAML single sign-on information:

1. Login to Okta as the account administrator.
2. Select **Applications** from the top menu and then click **Add Application**.
3. Select **SAML Service Provider** from the list of applications.
4. Change the **Application label** to the name you want to be displayed, for example *HCP Anywhere Enterprise*, and click **Next**.



5. In **Sign-On Options**, click **Identity Provider metadata** and download the certificate.

   You upload this certificate after converting it to a .pem format, when setting up SAML in the HCP Anywhere Enterprise Portal.
6. Set the **Assertion Consumer Service URL** and the **Service Provider Entity Id**.

   The **Assertion Consumer Service URL** is the URL where SAML responses are posted, as follows: *https://fully_qualified_domain_name/ServicesPortal/saml*.
   For example, `https://myportal.example.com/ServicesPortal/saml`.
   You use the **Service Provider Entity Id** in the HCP Anywhere Enterprise Portal **Entity ID/Issuer ID** field when setting up SAML in the HCP Anywhere Enterprise Portal.
7. Continue to set up the application, as described in Okta documentation.
8. Select the application and click the **General** tab.
9. Scroll down to the **App Embed Link** section. You use the **EMBED LINK** value in the HCP Anywhere Enterprise Portal **Sign-in page URL** field when setting up SAML in the HCP Anywhere Enterprise Portal.

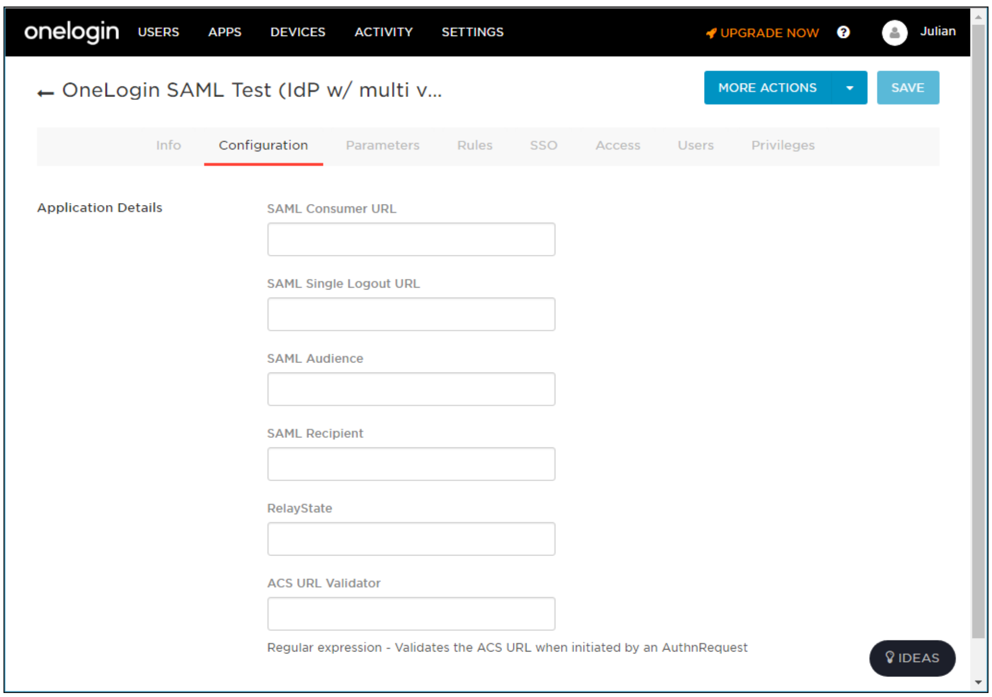
10. By default, Okta has a sign-out page. You can specify your own sign-out page in Okta, under **Settings > Customization**. which you can use as the **Log-out page URL** when setting up SAML in the HCP Anywhere Enterprise Portal.

Configuring OneLogin to Work with HCP Anywhere Enterprise Portal

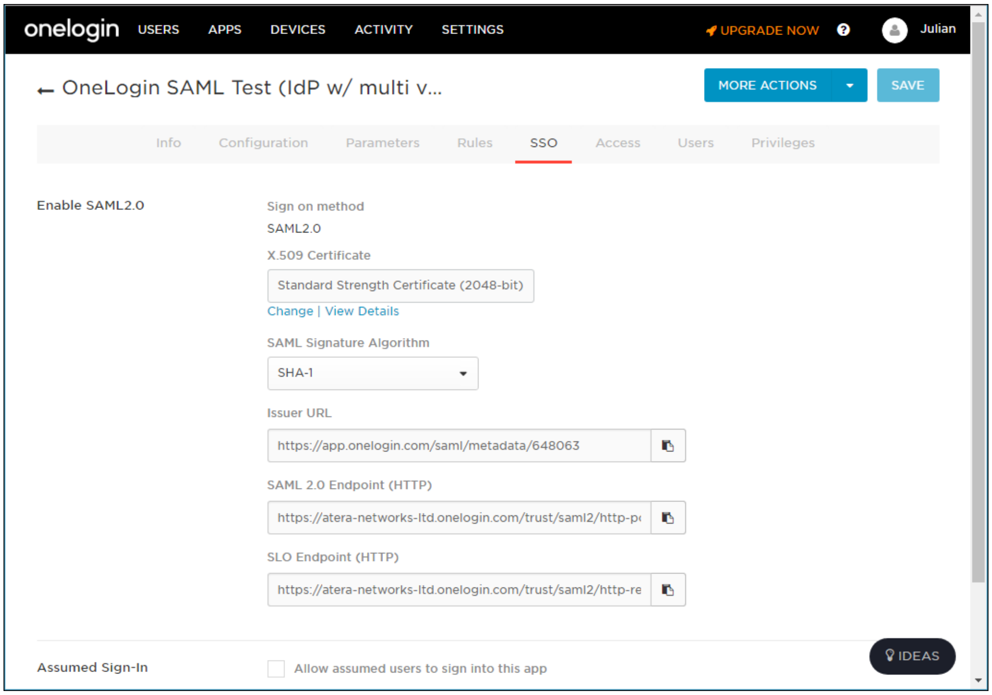
You set up SAML single sign-on support in OneLogin using a SAML application. You then gather the information you need to connect the HCP Anywhere Enterprise Portal to OneLogin.

To get the SAML single sign-on information:

1. Login to OneLogin as the administrator.
2. Select **APPS > Company Apps** from the top menu and click **ADD APP**.
3. Select the relevant **SAML** service provider from the list of applications.
4. Change the **Display Name** to the name you want to be displayed, for example *HCP Anywhere Enterprise*, and click **SAVE**.
5. Select the **Configuration** tab.



6. Enter values.
   You use the **SAML Audience** value in the HCP Anywhere Enterprise Portal **Entity ID/Issuer ID** field when setting up SAML in the HCP Anywhere Enterprise Portal.
   You use the **SAML Single Logout URL** value in the HCP Anywhere Enterprise Portal **Log-out page URL** field when setting up SAML in the HCP Anywhere Enterprise Portal.
7. Select the **SSO** tab.



You use the **SAML 2.0 Endpoint (HTTP)** value in the HCP Anywhere Enterprise Portal **Sign-in page URL** field when setting up SAML in the HCP Anywhere Enterprise Portal.

8. Click **View Details** under the **X.509 Certificate** field and click **DOWNLOAD** to download the X.509 PEM certificate.

   You upload this certificate when setting up SAML in the HCP Anywhere Enterprise Portal.

Configuring Swivel AuthControl Sentry to Work with HCP Anywhere Enterprise Portal

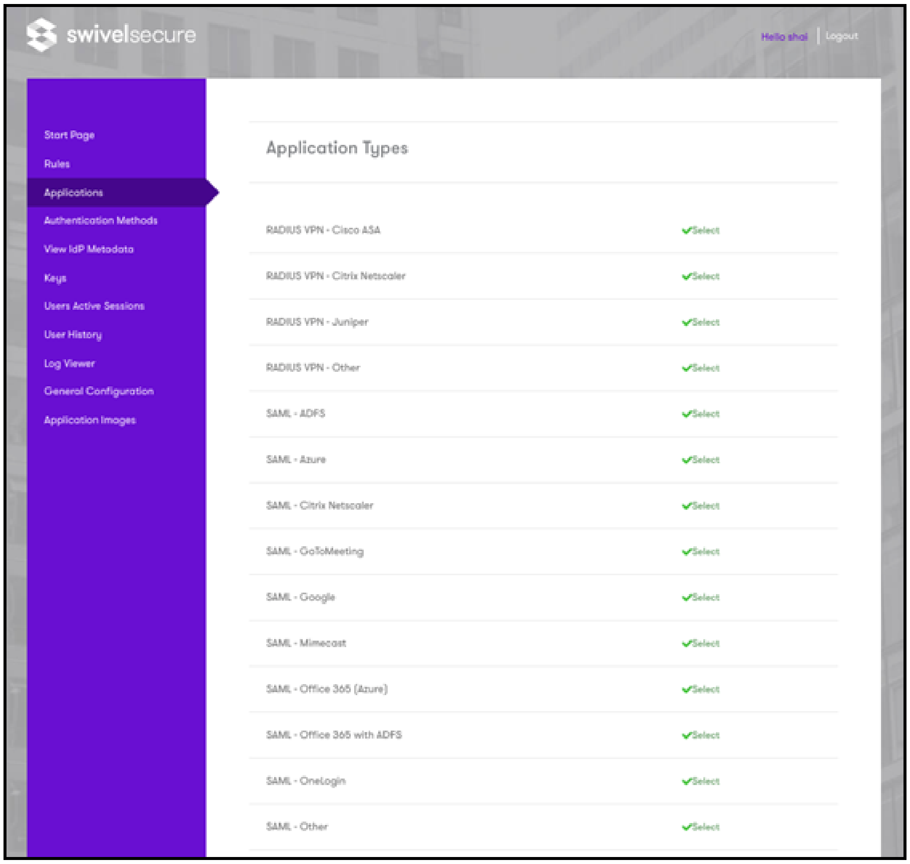
You set up SAML single sign-on support in Swivel AuthControl Sentry and gather the information you need to connect the HCP Anywhere Enterprise Portal to Swivel AuthControl Sentry.

Note: Before You Start, get a HCP Anywhere Enterprise logo image from Hitachi Vantara, to identify the HCP Anywhere Enterprise Portal SSO application.

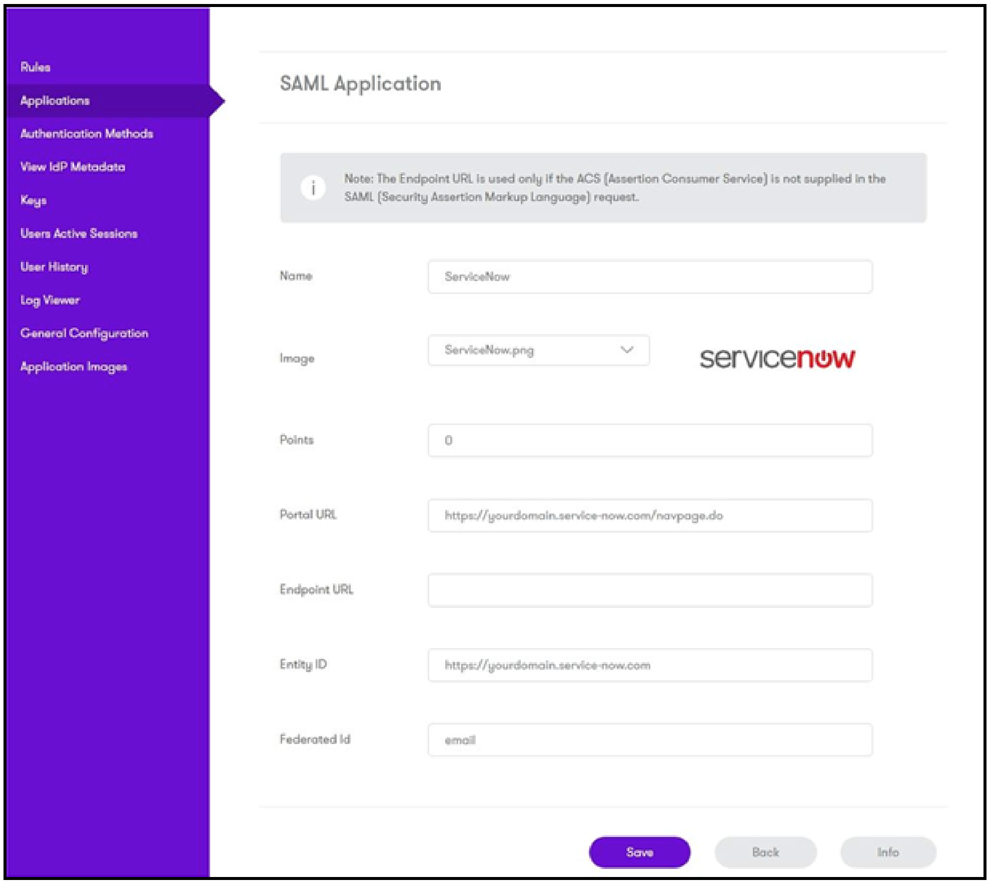
To get the SAML single sign-on information:

1. Login to Swivel AuthControl Sentry as the account administrator.
2. Select **Keys** from the navigation menu.

   The **Keys** screen is displayed.

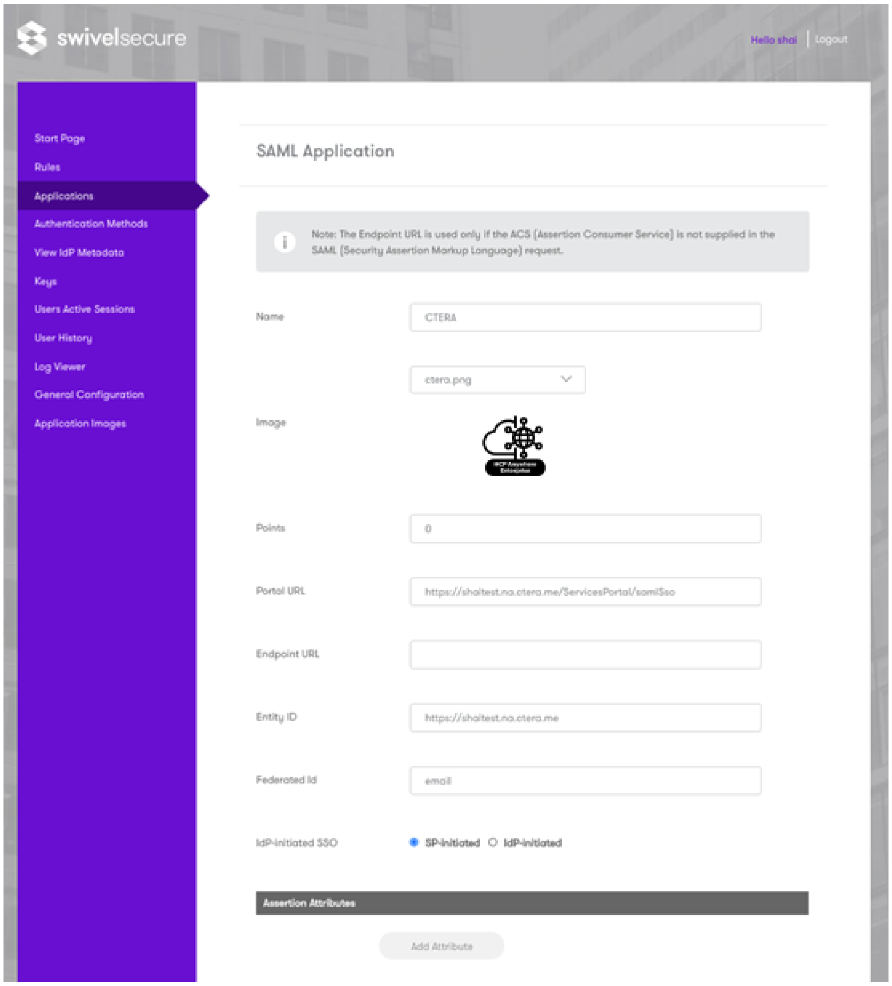


3. Click **Download** next to the **Cert** type.
4. Save the certificate as you will need to upload it to HCP Anywhere Enterprise Portal in step 4, in Defining SAML Single Sign-on in a HCP Anywhere Enterprise Portal.
5. Select **Application Images** from the navigation menu.

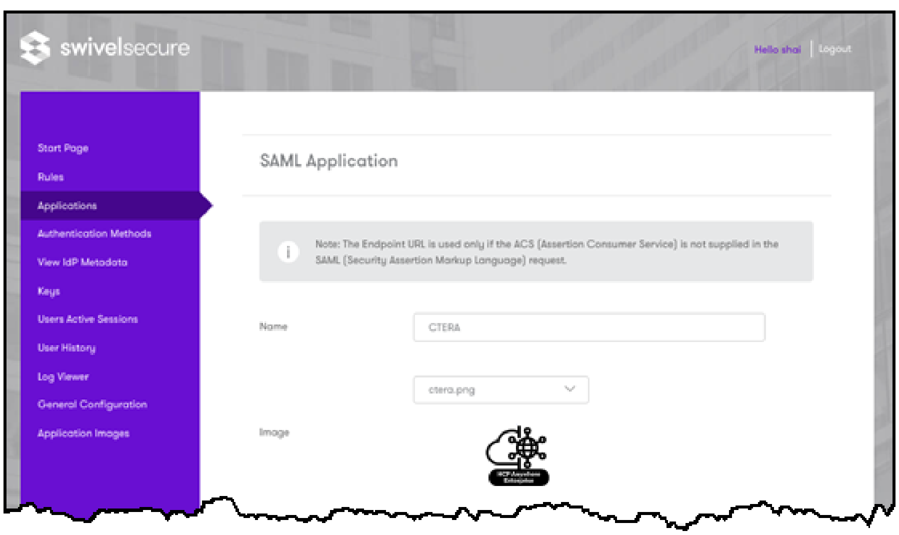


6. Click **Upload New Image**.
7. Upload the HCP Anywhere Enterprise logo image, that you received from Hitachi Vantara.
8. Select **Applications** from the navigation menu and then click **Add Application**.

   The **Application Types** screen is displayed.



9. Select **SAML - other**.
   The **SAML Application** screen is displayed.



10. Enter the following:

Name – An name to identify the application. Hitachi Vantara recommends a name such as HCP Anywhere Enterprise.
Image – A graphic to identify the application. Hitachi Vantara recommends using the Hitachi Vantara logo, uploaded in step **6**, above:
Points – The score the user needs from the authentication method in order to successfully authenticate to this application. The default is zero. If you set a value, you have to specify how the authentication methods that ill be applied. For details, refer to Swivel AuthControl Sentry documentation.
Portal URL – The URL to access the HCP Anywhere Enterprise Portal:
`http://<portal_name>.<DNS_Suffix>/ServicesPortal/samlSso` where `<portal_name>` is the name of the portal, and `<DNS_Suffix>` is the DNS suffix for the HCP Anywhere Enterprise Portal installation.
Endpoint URL – Leave this field empty.
Entity ID – Free text string that uniquely identifies your SAML identity provider. This must match the **Entity ID/Issuer ID** value you use when setting up SAML in the HCP Anywhere Enterprise Portal, described in step **4** in Defining SAML Single Sign-on in a HCP Anywhere Enterprise Portal. The format is similar to the following example:
`https://172.23.9.35:8443/sentry/saml20endpoint`
Federated Id – The field used to identify the user attempting to log on to the HCP Anywhere Enterprise Portal. Enter `email`.
Idp-Initiated SSO – Choose the SP-initiated option.

11. Click **Save**.

To verify that SSO has been set up in Swivel AuthControl Sentry:

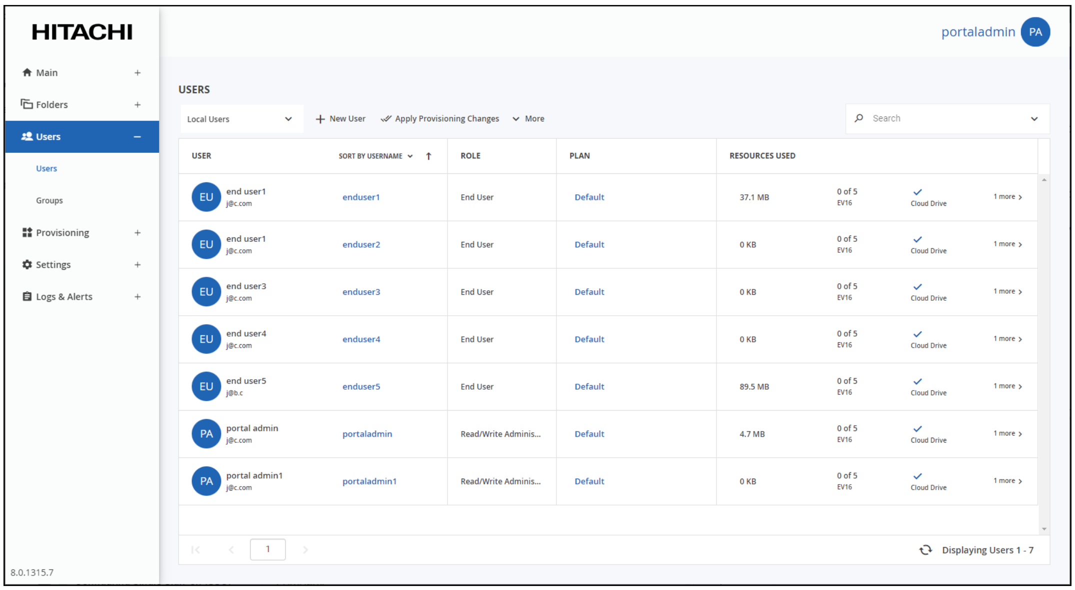
- As an administrator, access the AuthControl Sentry start page.
  The HCP Anywhere Enterprise Portal should be displayed.

Defining SAML Single Sign-on in a HCP Anywhere Enterprise Portal

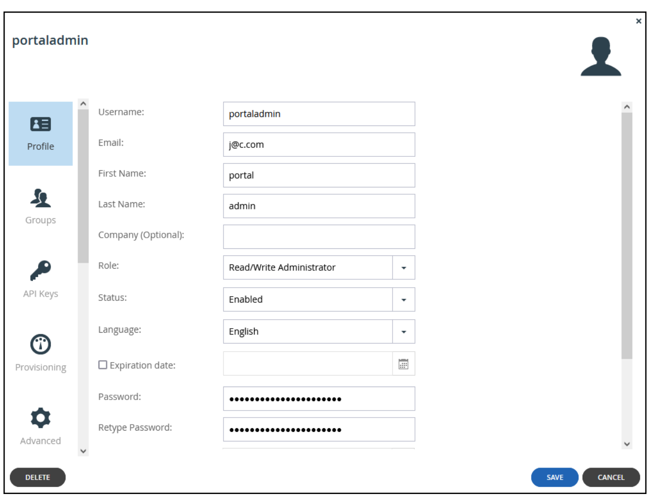
Before setting up SAML in the HCP Anywhere Enterprise Portal you must make sure that the username for every user in the HCP Anywhere Enterprise Portal is that user's email.

To check a username:

1. Select **Users > Users** in the navigation pane.
   The **USERS** page opens, displaying the users for the HCP Anywhere Enterprise Portal.



2. For each user, click the user's name.
   The user window is displayed with the user name as the window title and more options.

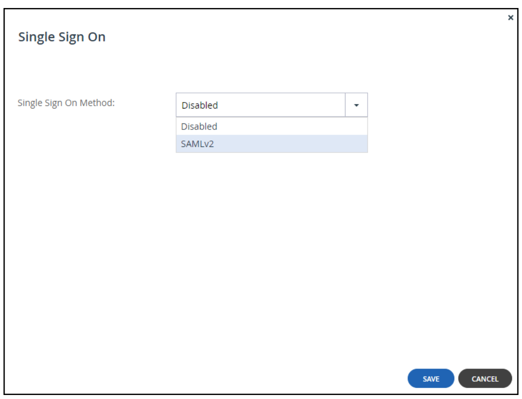


3. Verify that the **Username** field in the **Profile** option, is the same as **Email** for that user.

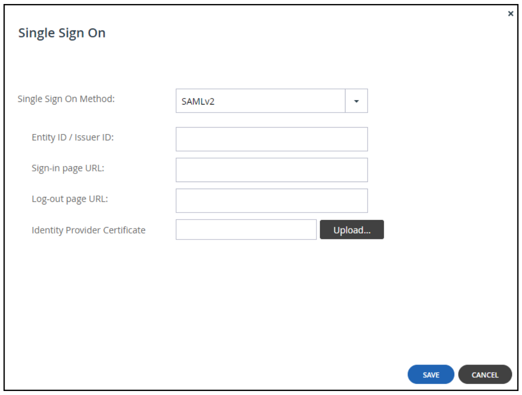
To configure SAML single sign-on:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **SSO** under **USERS** in the **Control Panel** page.
   The **Single Sign On** window is displayed.



3. Select **SAMLv2** from the drop-down box.
   Additional fields are displayed.



4. Enter the details of the SAML identity provider:

Entity ID/Issuer ID – The identity provider that issues the SAML assertion. This is a free text string that uniquely identifies your SAML identity provider and must match the entity ID that you choose when signing up for the identity provider's SSO service.

ADFS – The **Relying party trust identifier** value (see step **13**, in the procedure under Configuring Microsoft ADFS to Work with HCP Anywhere Enterprise Portal). For example, `hcp-adfs`. The value must be exactly the same as the **Relying party trust identifier** value, and is case sensitive.

Entra ID (Azure Active Directory) – The **Identifier (Entity ID)** value (step **7**, in the procedure under Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal). For example, `hcp-azureAD`. The value must be exactly the same as the **Identifier (Entity ID)** value, and is case sensitive.

Okta – The **Service Provider Entity Id** value.

OneLogin – The **SAML Audience** value.

Swivel AuthControl Sentry – The Identity ID, (step **10** in the procedure under Configuring Swivel AuthControl Sentry to Work with HCP Anywhere Enterprise Portal).

Sign-in page URL – The URL that HCP Anywhere Enterprise Portal redirects to when signing in. You need to get this from the provider.

ADFS – The ADFS server URL. For example, `https://exampleAD.adfs.local/adfs/ls`

Entra ID (Azure Active Directory) – The **Login URL** (step **7**, in the procedure under Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal).

Okta –The **EMBED LINK** value.

OneLogin – The **SAML 2.0 Endpoint (HTTP)** value.

Swivel AuthControl Sentry – The AuthControl Sentry start page.

Log-out page URL – The URL that HCP Anywhere Enterprise Portal redirects to when logging out of the HCP Anywhere Enterprise Portal. Without this URL configured, a logout will redirect to the sign-in page URL and log the user back into the HCP Anywhere Enterprise Portal.

ADFS – The logout URL. This is the same as the **Sign-in Page URL**.

Entra ID (Azure Active Directory) – The **Logout URL** from the fourth part of the **SAML-based Sign-on** blade (step **7**, in the procedure under Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal).

Okta – Either the default Okta sign-out page is used or a customized sign-out page defined in Okta.

OneLogin – The **SAML Single Logout URL** value. This is optional.

Swivel AuthControl Sentry – The logout page.

Identity Provider Certificate – The authentication certificate issued by the provider. You need to get this from the provider, usually by download from the provider's site. .pem and .cer certificates are valid. Click **Upload** to upload your provider's certificate to the HCP Anywhere Enterprise Portal.

ADFS – The Token-signin certificate from the ADFS .cer certificates saved to a file. This certificate must be a known root CA and not a self-signed certificate.

Entra ID (Azure Active Directory) – The **Certificate (Base64)** that you downloaded from the third part of the **SAML-based Sign-on** blade (step **12**, in the procedure under Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal).

Okta – The certificate downloaded from Okta and converted to .pem.

OneLogin – The X.509 PEM certificate downloaded from OneLogin.

Swivel AuthControl Sentry – The Identity ID (step **4** in the procedure under Configuring Swivel AuthControl Sentry to Work with HCP Anywhere Enterprise Portal).

5. Click **SAVE**.

Note: When the SAML identity provider is also connected to Active Directory, the user name to log in to the HCP Anywhere Enterprise Portal must be defined in the HCP Anywhere Enterprise Portal. The SAML response can be the user name or a unique customized filed, such as the user email and UPN (user principal name).

Chapter 12. Managing HCP Anywhere Enterprise Portal Data Policies and Permissions

In this chapter

Configuring Cloud Drive Policy

Cloud Drive policy determines the type of data that can be synchronized through HCP Anywhere Enterprise Agents and HCP Anywhere Enterprise Edge Filers, or uploaded to the portal.

To set Cloud Drive policy, you create *Allow* and *Deny* rules based on the following attributes:

- File Name
- File Size
- File Type

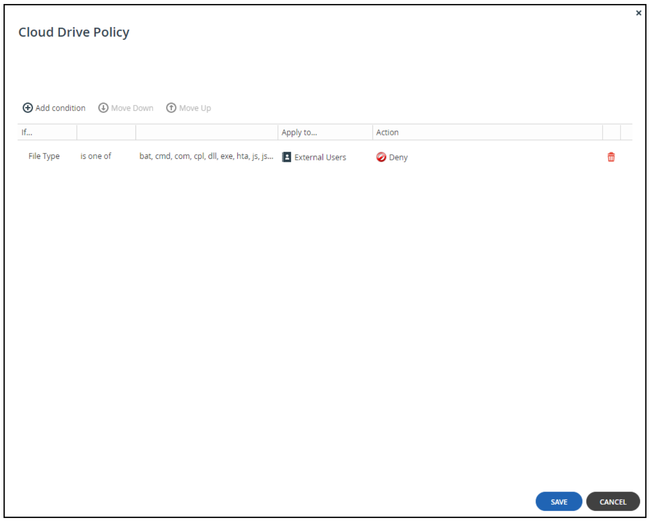
Each rule can be applied to everyone or to a specific user or group, whether they are users and groups from an integrated directory service or local users and groups defined in the portal.

You can also apply Cloud Drive policies to external users who were invited to collaborate by email address or by means of a public link, by using a special group called *External Users*.

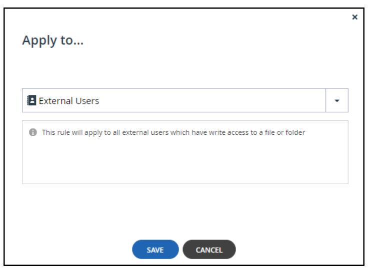
To configure Cloud Drive policy:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

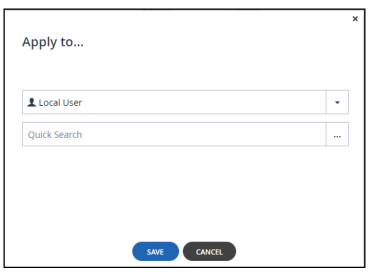
2. Select **Cloud Drive Policy** under **CLOUD DRIVE** in the **Control Panel** page.
   The **Cloud Drive Policy** window is displayed.



3. Click **Add condition** to define a condition.
   a) In the **If** column select a file attribute.
   b) Select an operator, such as *is one of*.
   c) Enter a value to apply on the operator.
   d) In the **Then apply** column select a plan to apply if a user satisfies the condition.
   e) In the **Apply to** column select to whom the policy applies.
   Click the user in the **Apply to** field.



   Select the type of user or group.
   For **Local User** and **Local Group** a **Quick Search** field is displayed.



   In the **Quick Search** field, enter a string that occurs anywhere within the name of the user. A list of users and groups matching the search string is displayed.Select the user or group and click **SAVE**.

f) In the **Action** column select **Allow** or **Deny** to allow or deny the specified condition.

4. To delete a condition, click 🗑 in the row with the condition to delete.
5. Click **SAVE**.

Managing Collaboration

Managing Collaboration Permissions

Users and groups can:

- Share files and folders through the end user portal.
- Create public links for access to files and folders
- Create team projects: shared folders without individual owners.

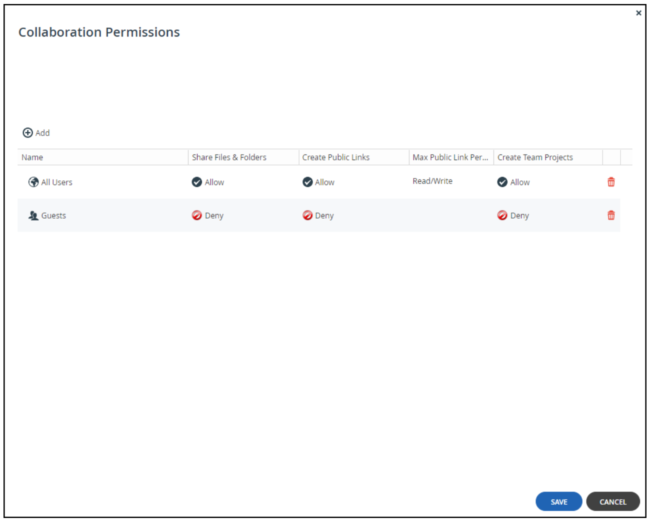
To set collaboration permissions, you define rules that give the required permissions to specified users or user groups:

- User rules get precedence over group rules.
- *Deny* rules have higher priority than *Allow* rules.

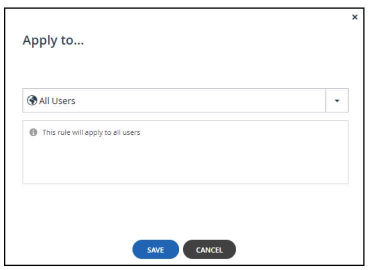
To add a collaboration permissions rule:

1. Select **Settings** in the navigation pane.
The **Control Panel** page is displayed.

2. Select **Collaboration Permissions** under **CLOUD DRIVE** in the **Control Panel** page.
The **Collaboration Permissions** window is displayed.



3. Click **Add** to define a permission.
   a) Click the user in the **Name** field to select to whom the permission applies.



   Unless the user is **All Users**, select the type of user or group.
   In the **Quick Search** field, enter a string that is displayed anywhere within the name of the user.
      A list of users and groups matching the search string is displayed.
   Select the user or group and click **SAVE**.
   b) In the **Share Files & Folders** column select **Allow** or **Deny** to allow or deny sharing files and folders with specified users, groups, or external email addresses.
   c) In the **Create Public Links** column select **Allow** or **Deny** to allow or deny creating a public link to any folder or file and then sending the link to anyone else they choose.
   d) In the **Max Public Link Permission** column select the link permission: Read/write, Read Only, or Preview Only.
   e) In the **Create Team Projects** column select **Allow** or **Deny** to allow or deny creating shared folders that are not displayed as shared by an owner because they are intended for team collaboration.
4. To delete a permission, click in the row with the permission to delete.
5. Click **SAVE**.

Setting Collaboration Policy

You can implement a corporate data sharing policy for collaboration with external users. You can define a policy to restrict external collaboration by specific users or groups and define the sanctioned collaboration domains.

Note: Actions performed on data shared with users outside of your corporate domain are logged in the access log and visible to the content owner, collaborators, and HCP Anywhere Enterprise Portal administrators.

Collaboration policy rules control:

- Which HCP Anywhere Enterprise Portal members can enable which external users to collaborate on data stored on the portal.
- What minimum type of authentication external users need if HCP Anywhere Enterprise Portal users share data with them.
- The highest level of access permission the external users are allowed by the specified HCP Anywhere Enterprise Portal members.

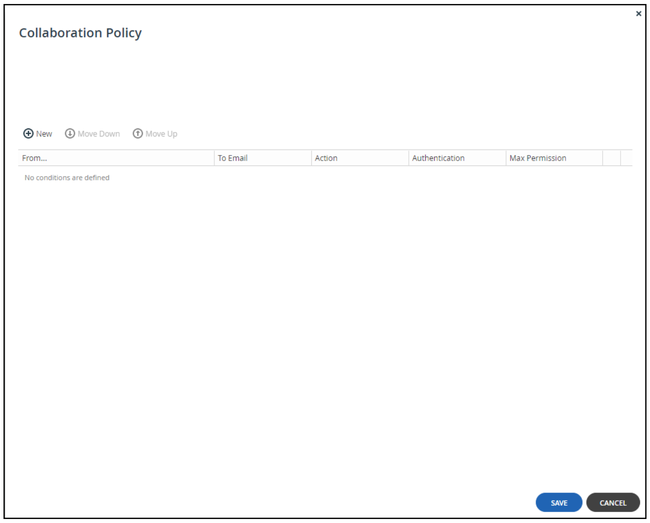
Optionally, each policy rule can apply to a subset of your HCP Anywhere Enterprise Portal members, allowing different collaboration rules for different portal users.

Note: Any external user email address which is not specifically denied by any collaboration policy rule will be allowed to collaborate.
The policy is not applicable to files and folders shared via public links or collaboration with internal users. Collaboration limits for internal users can be set as described in Managing Collaboration Permissions page.

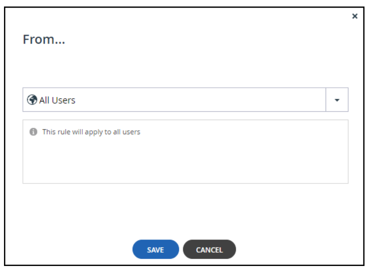
To add a collaboration policy rule:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **Collaboration Policy** under **CLOUD DRIVE** in the **Control Panel** page.
   The **Collaboration Policy** window is displayed.



3. Click **New** to define a policy.
   a) Click the user in the **From** field to select to whom the policy applies.



   b) Unless the user is **All Users**, select the type of user or group.
   c) In the **Quick Search** field, enter a string that exists anywhere in the name of the user. A list of users and groups matching the search string is displayed.
   d) Select the user or group and click **SAVE**.
4. In the **To Email** column, specify which external recipient email addresses the policy will apply to. You can enter an email address or you can specify an entire domain, by using wildcards. For example, to specify all gmail addresses, enter `*@gmail.com` or `@gmail.com`.
5. In the **Action** column select **Allow** or **Deny** to allow or deny the specified user or user group to collaborate on files and folders with external users at the specified email addresses.
6. In the **Authentication** column, set which authentication methods the external users will have to use in order to access the shared files or folders:

   Let User Choose – The end user chooses which authentication method to use to authenticate the external user for access to the shared file or folder.
   Email – The invitation recipient receives a time limited authenticated link to the file or folder. On every access, a new 6 digit passcode challenge is sent to the recipient by email which must be entered to access the file or folder.
7. In the **Max permission** column, set the highest permission level that the user can grant the external collaborator on any shared files:
   - **Read/Write**
   - **Read Only**
   - **Preview Only**

Note: *Preview Only* share recipients are able to view the file which is protected with a watermark that includes the recipient's email or IP address. Users with *Preview Only* permission are unable to download or copy the file. The file can also not be printed as a file. In addition, content shared in *Preview Only* mode cannot be synchronized for offline access by HCP Anywhere Enterprise Edge Filers.

8. You can move rules up and down the list on the policy page. When a user invites an external user to collaborate, the first rule on the list, from the top downwards, that matches the external users' email address applies.
9. Click **SAVE**.

Managing Policy for Team Projects

End users can request to use storage from the team HCP Anywhere Enterprise Portal quota, from the HCP Anywhere Enterprise Portal administrator, instead of from their own quota.

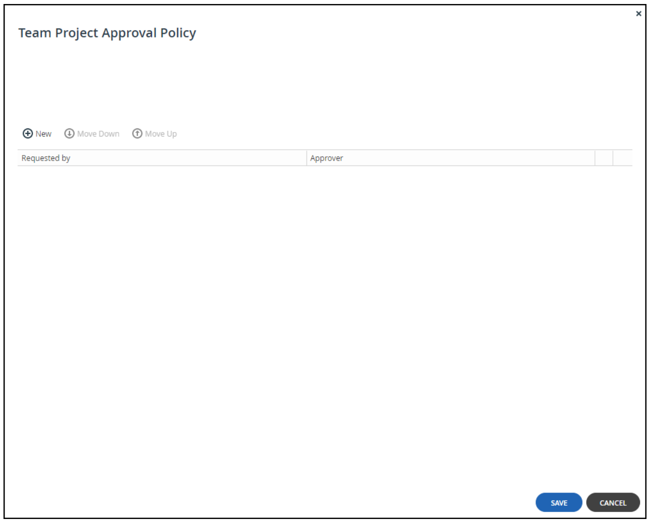
You can specify that requests from specific groups, or even from all users, can only be handled by specific administrators.

Note: The user can only request a team project if **Allow users to request team projects with independent quota** is enabled in the virtual portal settings for the team portal, described in Team Portal Settings.
By default, portal administrators defined as **Read/Write Administrators** with the **Manage Cloud Folders** role checked and can accept or reject the request, as described in Customizing Administrator Roles.

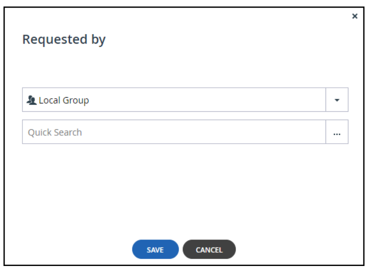
To limit which administrators can approve requests for specific users:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

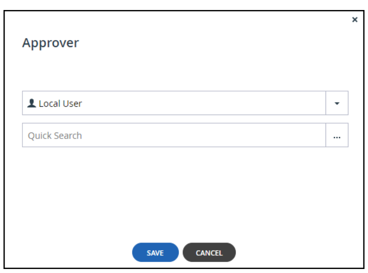
2. Select **Team Project Approval Policy** under **CLOUD DRIVE** in the **Control Panel** page.
   The **Team Project Approval Policy** window is displayed.



3. Click **New** to add a new policy.
   a) Click in the select box in the **Requested by** column.



   b) Select the group that can make this specific request from the drop-down list.
   Unless the user is **All Users**, select the type of user or group.
   In the **Quick Search** field, enter a string that is displayed anywhere within the name of the user.
   A list of users and groups matching the search string is displayed.
   Select the user or group and click **SAVE**.
   c) Click in the select box in the **Approver** column.



   d) Select the approver that can make this specific request from the drop-down list. The approver can be a local administrator or an Active Directory administrator or group of administrators. The approver must have a valid email and if it is an Active Directory group, the group must be mail-enabled.
   Unless the user is **Local User**, select the type of group.
   In the **Quick Search** field, enter a string that is displayed anywhere within the name of the

user or group.

A list of users and groups matching the search string is displayed.

Select the user or group and click **SAVE**.

Note: Only local users defined as administrators can be specified as approvers.

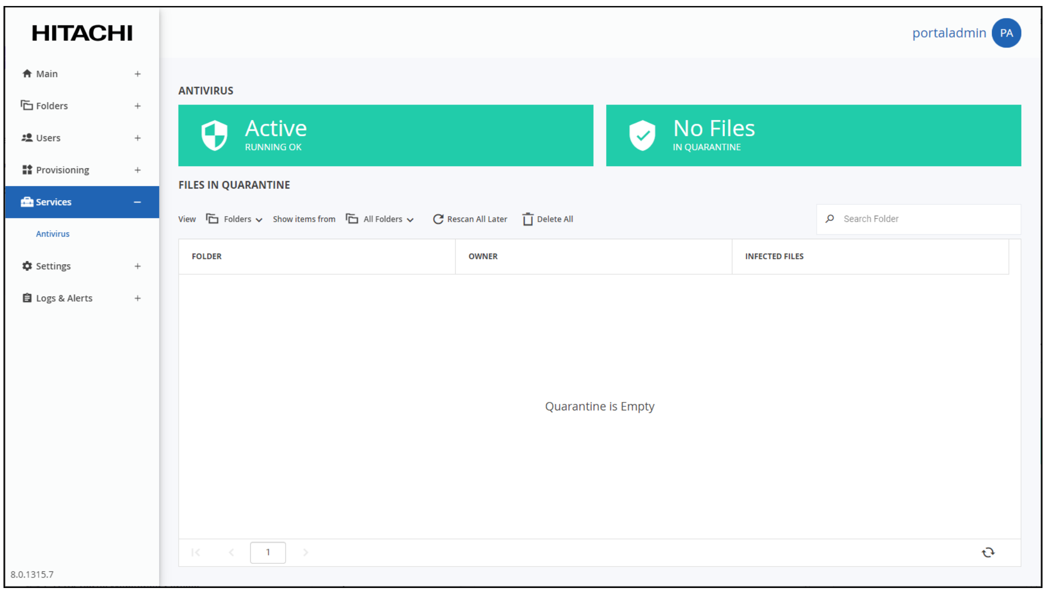
4. To delete a condition, click 🗑 in the row with the condition to delete.
5. Select a row and use the **Move Down** and **Move Up** buttons to change the order of the rows.
6. Click **SAVE**.

Chapter 13. Protecting the Data

Antivirus protection is only available in a virtual portal if:

- HCP Anywhere Enterprise Portal is licensed for antivirus.
- Antivirus functionality is enabled in the global administration.
- A subscription plan in global administration includes the antivirus option.
- The subscription plan that includes the antivirus option is provisioned for the portal in global administration.

When the antivirus service is available, the navigation pane includes a **Services** option.



In this chapter

- Managing Virus Protection
- Data Loss Prevention (DLP)

Managing Virus Protection

When antivirus scanning is implemented, files are scanned for malware automatically and transparently, before they are downloaded from the portal. When the browser used is Google Chrome, you are notified that a download failed. With other browsers, the download is unsuccessful without a notification. Background scanning checks for files that were not previously scanned, for example, when the antivirus was disabled or not running on a server. Background scanning scans the following:

- Files that were not previously scanned.
- Cloud drive folders.

If an infected file is found, the infected file is quarantined so that an administrator can determine if any action is necessary. The file is replaced by a text file with the name `file_name-infected.txt`, where *file_name* is the original name of the file.

Note: If a file called `file_name-infected.txt` already exists, the new infected file is call `file_name-infectedn.txt`, where n is a 1, 2, 3, etc, denoting the additional number of times an infected file with this name has been quarantined.

The text file contains information, including how the infected file was uploaded to the portal:

```
A file was moved to quarantine
File name: file_name
Uploaded from device: device_name
Detected threat: detected_threat
```

Or:

```
A file was moved to quarantine
File name: file_name
Uploaded via portal's UI
Detected threat: detected_threat
```

For example, *detected_threat* could be `File is infected with Trojan32`

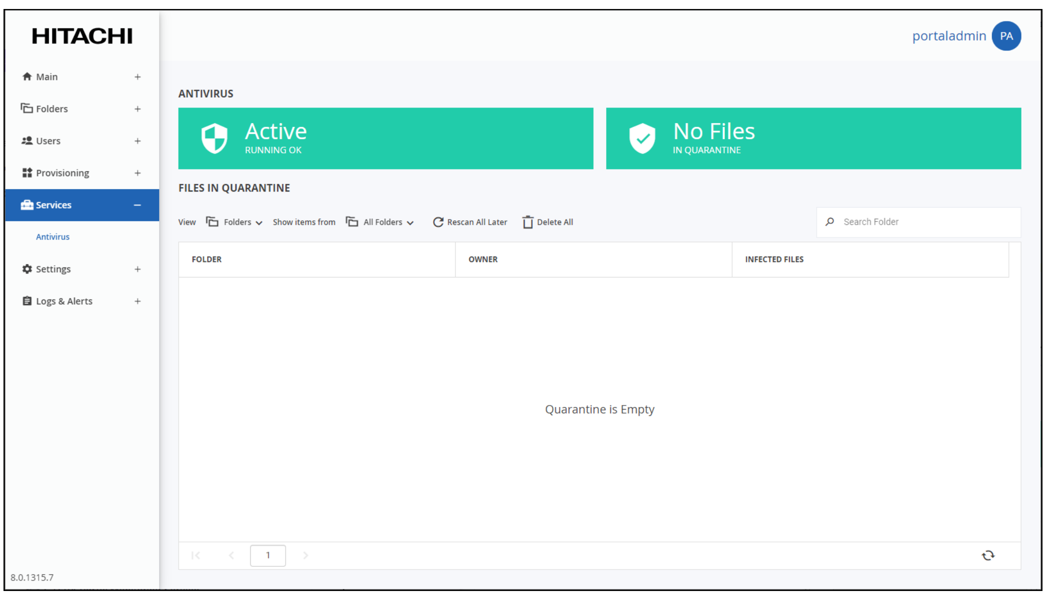
Administrators can view files that are quarantined by the antivirus servers, the Cloud Drive location and the user who owns the files.

To manage quarantined files:

1. Select **Services > Antivirus** in the navigation pane.

   Note: The **Services** menu item is only displayed if the portal is licensed for antivirus functionality, provisioned and enabled in the global administration view.

   The **ANTIVIRUS** page is displayed.



   If quarantined files were scanned, the quarantine block is displayed.

   The number of quarantined files is displayed with the number of folders that contained at least

one quarantined file.
You can also change the infected files view:

- Choose either **Folders** or **Files** from the **View** drop-down options.
  In the **Folders** view, you can select what type of folder to inspect, **All Folders** or **Cloud Folders**. The number of infected files displayed is for all the folders. In the **Files** view the list of infected files displayed is only from cloud folders. However, in the **Files** view you can search the list by file name.

2. Click on an owner to see details of the user who owns the infected file.
3. Select the **Files** view, or, in the **Folders** view, click on a link in the **INFECTED FILES** column to drill-down to the details of the infected files in that folder.

   The infected files in the folder are displayed as well as the owner of the folder.
   When clicking on the link in the **INFECTED FILES** column to display the details of the infected files in that folder, you can save all the files in an encrypted zip file.

You can download the infected files to a zip file by clicking **Save All as Zip**.

You can remove all the files from the list by clicking **Rescan All Later** in the **ANTIVIRUS > FILES IN QUARANTINE** view. These files will be rescanned and access blocked the next time an external user attempts to view or download them.

You can delete all the files from the list by clicking **Delete All** in the **ANTIVIRUS > FILES IN QUARANTINE** view or select an individual row and click **Delete** to delete just that file.

Data Loss Prevention (DLP)

This feature is currently not supported.

Chapter 14. Managing Devices

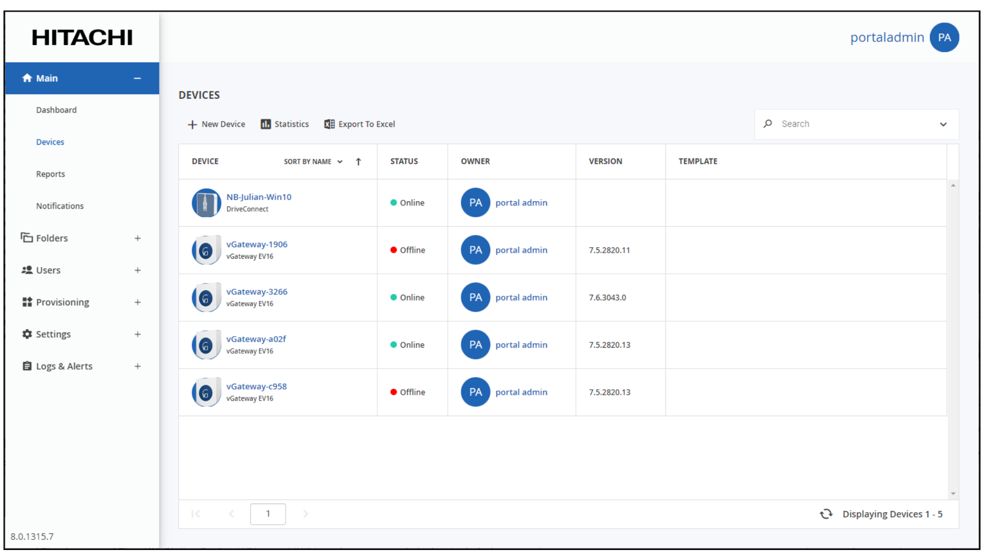
A *device* refers to a HCP Anywhere Enterprise Edge Filer connected to the HCP Anywhere Enterprise Portal. Devices are automatically added to the HCP Anywhere Enterprise Portal, when their owners connect the device to the HCP Anywhere Enterprise Portal.

In this chapter

Viewing All Devices

To view all devices connected to the virtual portal:

- Select **Main > Devices** in the navigation pane.
  The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.



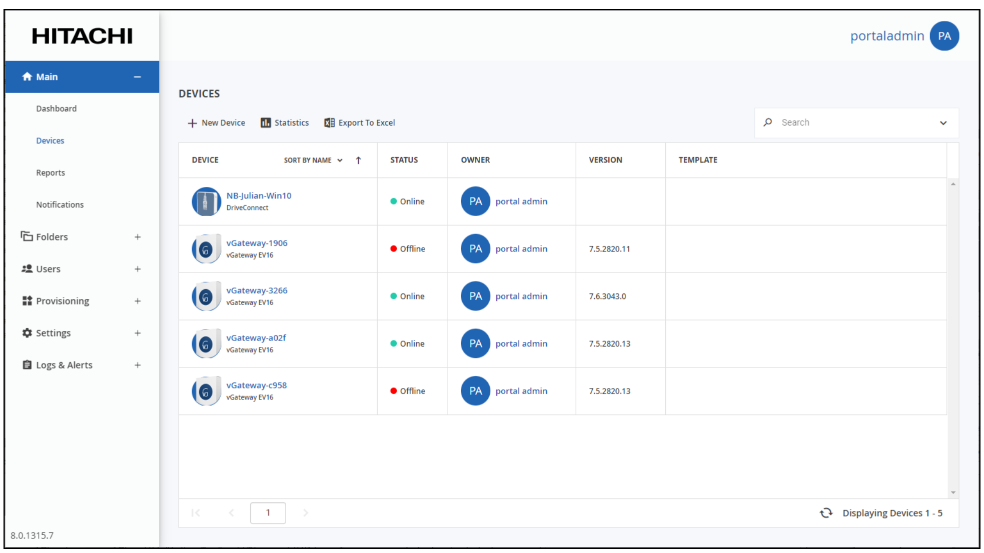
The page includes the following columns:

Column	Display
DEVICE	The device's name. To edit the device, click the device name. The type of device is displayed under the name.
STATUS	The device's connection status: **Online** or **Offline**.
OWNER	The user account name of the device's owner. To edit the user account, click the user account name.
VERSION	The firmware version currently installed on the device.
TEMPLATE	The template assigned to the device.
ZONES	The zone the device belongs to when Zones are enabled.

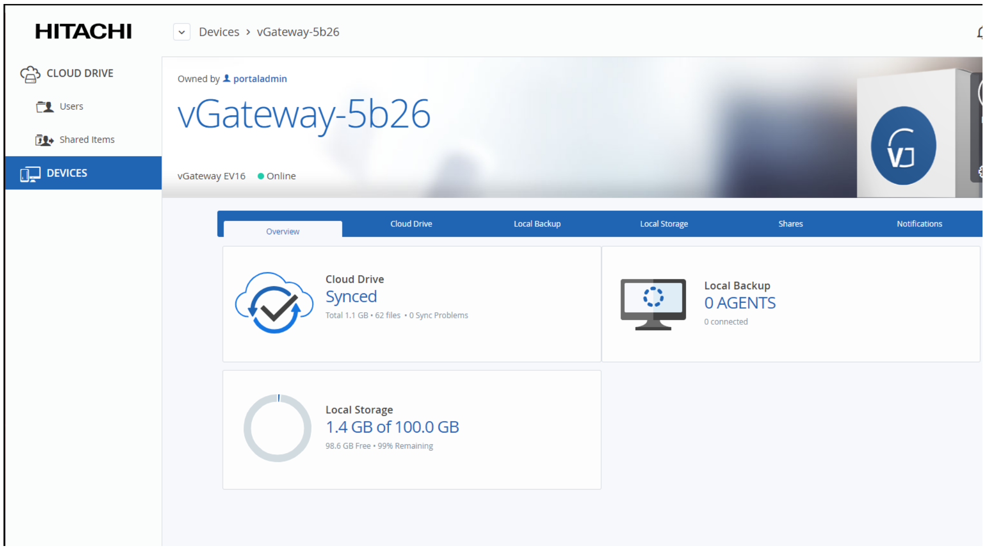
Viewing Individual Device Details

To view individual device details:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.



2. Click the device name.
   The device details are displayed in a new browser window.



The navigation pane can be different for each device as well as the details for each type of device and whether the device is connected to the HCP Anywhere Enterprise Portal or not.
From this window:

- Click **Remote Access** to access the device over the Internet for administration or to access files. The HCP Anywhere Enterprise Portal administrator must enable **Remote Access**.

Note: For a HCP Anywhere Enterprise Edge Filer, the device must be connected to the HCP Anywhere Enterprise Portal. For a PC, the HCP Anywhere Enterprise Agent must be installed on the PC and connected to the HCP Anywhere Enterprise Portal. Access to the device configuration with the HCP Anywhere Enterprise Portal is then available.

- Click the icon to edit the device settings, rename or delete the device and add text to describe a device.
- Click the icon to view information about the device: The IP address, software version, serial number, MAC address, firmware version and physical location. For a HCP Anywhere Enterprise Edge Filer, the license is also displayed and if required and enabled, can be changed.

The HCP Anywhere Enterprise Edge Filer details include the following tabs:

Overview – Details of the device, including an overview of the following:

The cloud drive status

Local storage

Cloud Drive – File sync details. You can also sync a folder, as described in Syncing Content to the HCP Anywhere Enterprise Portal Global File System and view HCP Anywhere Enterprise Edge Filer statistics, by clicking **Statistics**.

Local Backup – This feature is currently not supported.

Local Storage – Details about the HCP Anywhere Enterprise Edge Filer volumes and arrays storage utilization.

Shares – Manage the HCP Anywhere Enterprise Edge Filer shares from the portal.

Notifications – A list of notifications for this device.

The color of the exclamation mark to the left of each notification indicates the severity.

Managing Individual Device Details

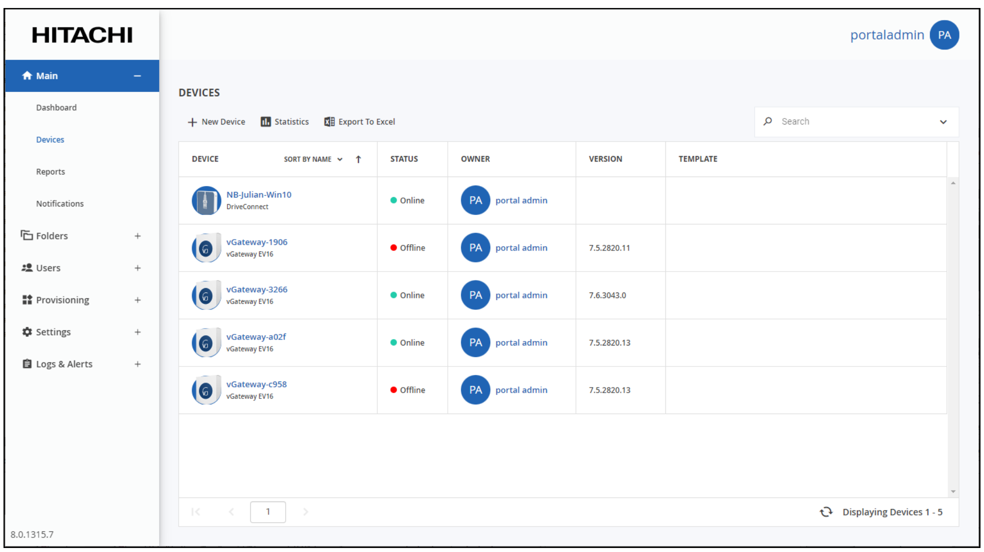
You can manage the following details for a device:

- The device name.
- A description of the device. You can use this to add comments about the device.
- Advanced settings, including:
  - The MAC address
  - The software version.
  - The configuration template, either the default template or another templates defined in the HCP Anywhere Enterprise Portal.

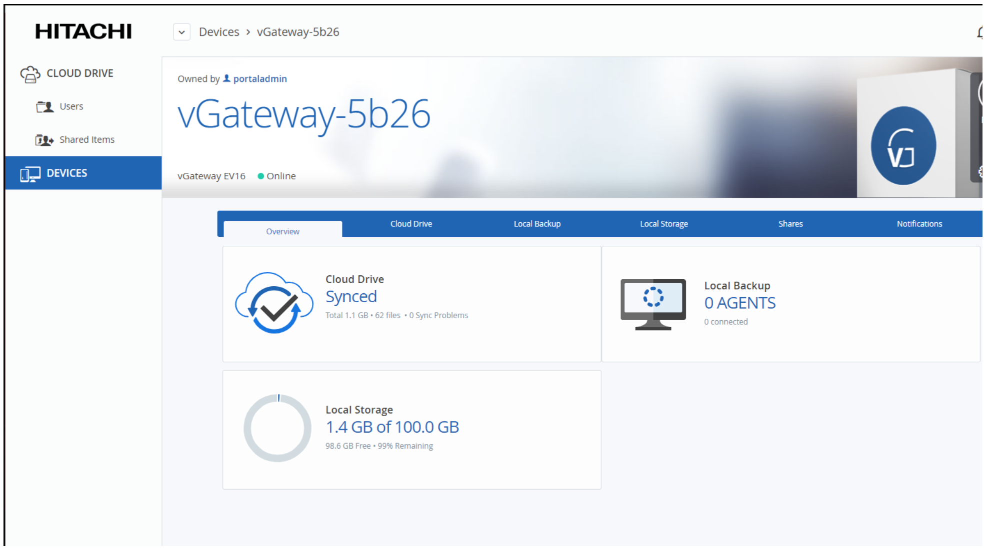
In addition, administrators can restart devices and delete devices from the HCP Anywhere Enterprise Portal, for example inactive devices that are using a license can be deleted to free up a license.

To manage individual device details:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.

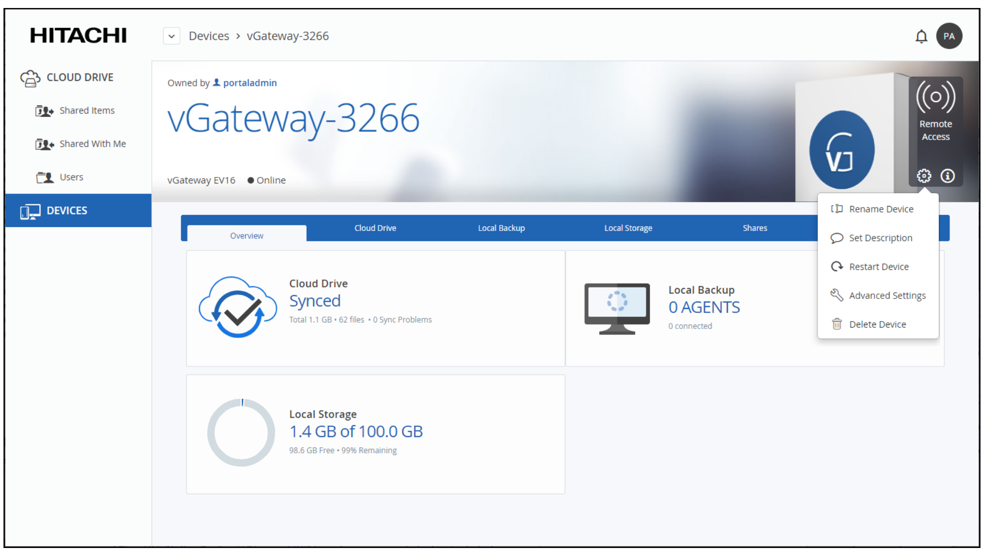


2. Click the device name.
   The device details are displayed in a new browser window.



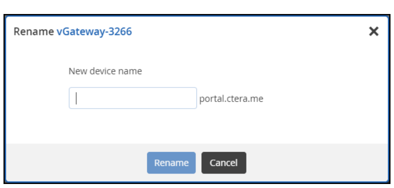
The details are different for each type of device and whether the device is currently connected to the HCP Anywhere Enterprise Portal.

3. Click the  icon and select the option required for the device.



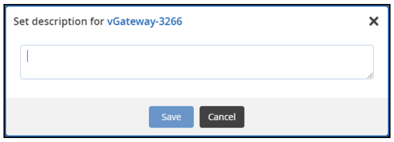
Note: The list of available options is dependent on the device. For example, only connected devices have a **Restart Device** option.

When **Rename Device** is selected, the **Rename** window is displayed.

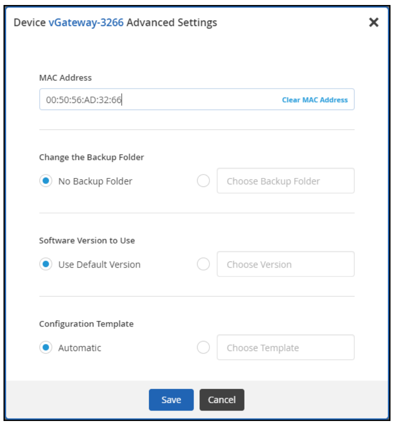


Enter the new device name and click **Rename**. The device is offline for a few seconds as the

name change is applied.
When **Set Description** is selected, the **Set Description** window is displayed.

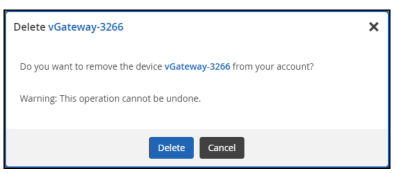


Enter any information you want to describe the device and click **Save**.
When **Restart Device** is selected, the **Restart Device** window is displayed prompting the restart. Only connected devices display the **Restart Device** option. Click **Restart** to restart the device.
When **Advanced Settings** is selected, the **Device Advanced Settings** window is displayed.



Enter the configuration you want for the device and click **Save**.

When **Delete Device** is selected, the **Delete *deviceName*** window is displayed.



Also see Deleting Devices.

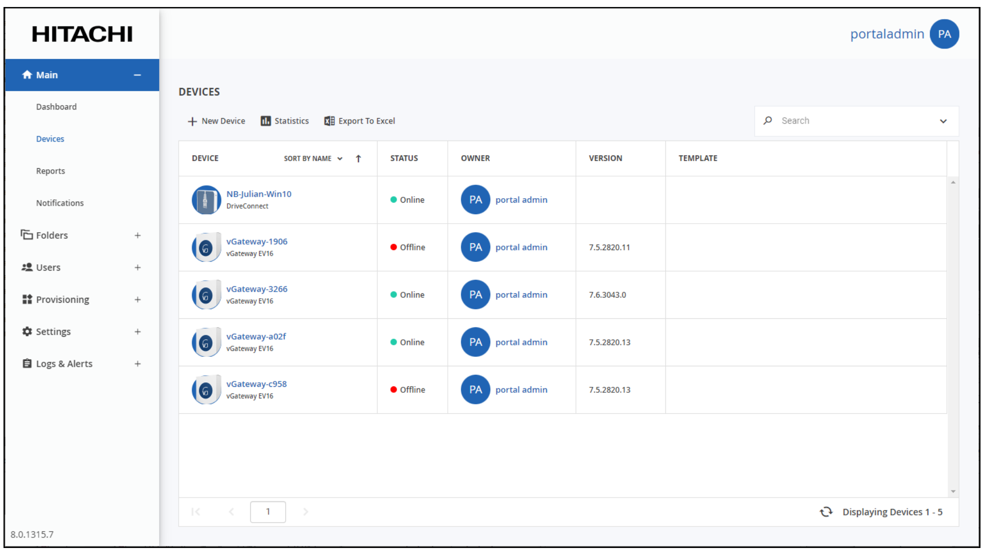
Syncing Content to the HCP Anywhere Enterprise Portal Global File System

When a HCP Anywhere Enterprise Edge Filer Agent or HCP Anywhere Enterprise Edge Filer is connected to the HCP Anywhere Enterprise Portal, files are synced between the device and the HCP Anywhere Enterprise Portal global file system. You sync content with the HCP Anywhere Enterprise Portal global file system from the device and configure what content should be synced. You can also throttle the sync data from the device, for example, to free up bandwidth from other tasks at certain times of the day.

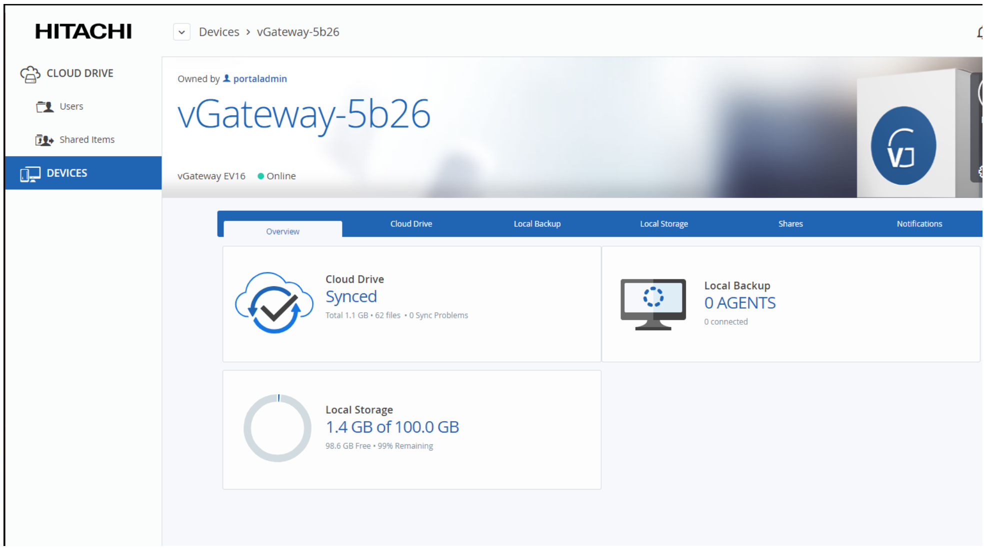
You can also sync content from the HCP Anywhere Enterprise Portal global file system.

To sync content from the HCP Anywhere Enterprise Portal global file system:

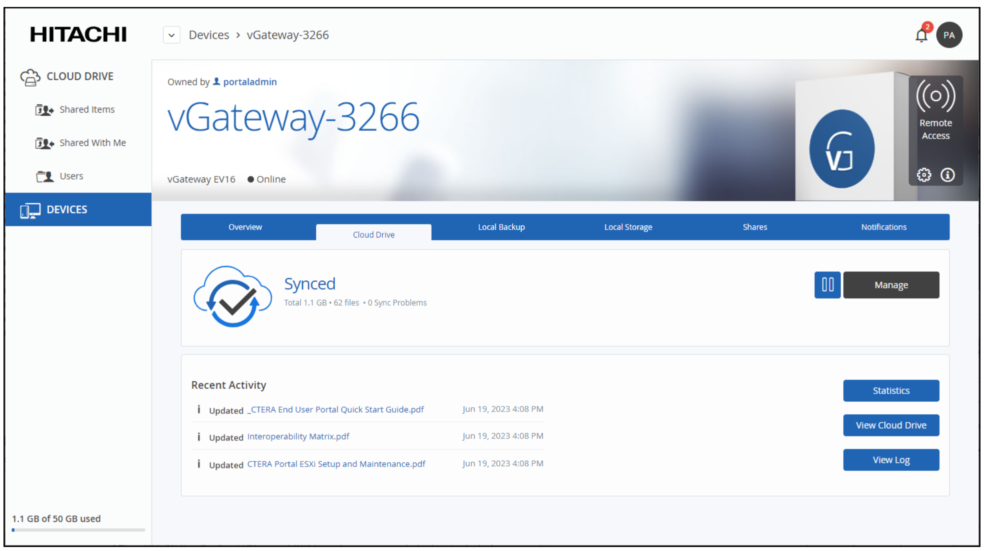
1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the team portal.



2. Click the device name.
   The device details are displayed in a new browser window.

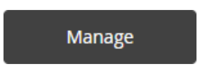


3. Click the **Cloud Drive** tab.
   The cloud drive details for the device are displayed.

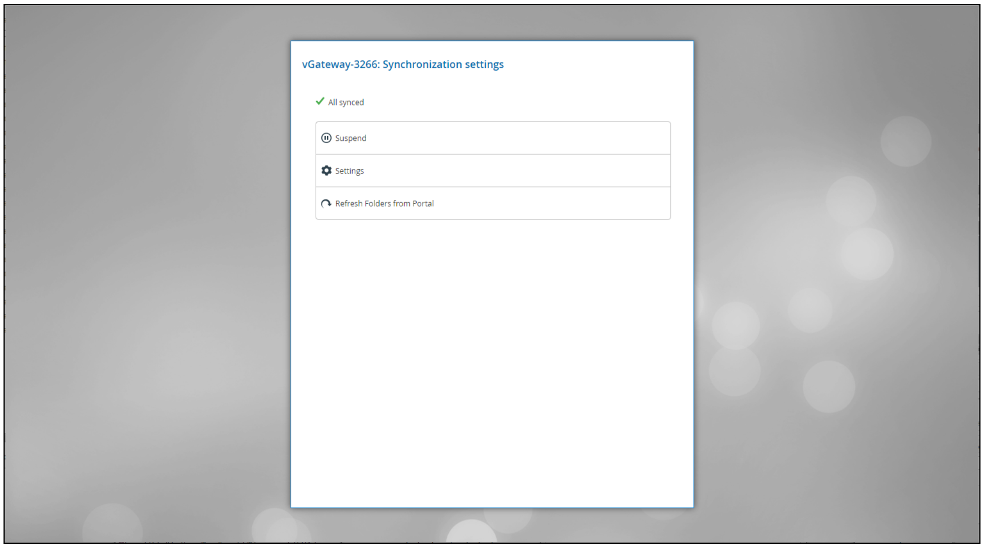


4. To suspend syncing, click .

   To resume syncing after it was suspended, click .

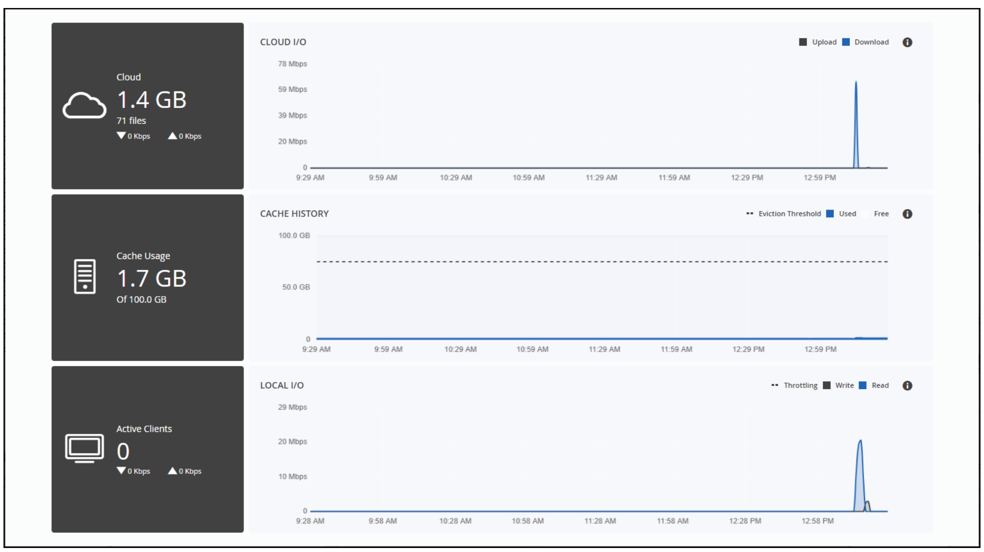
5. Click 

 to manage the sync settings.
   The settings window is displayed in a new browser window.



You can suspend or unsuspend syncing between the device and the portal global file system and refresh the device content from the portal global file system.
For details of the **Settings** option, see the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.

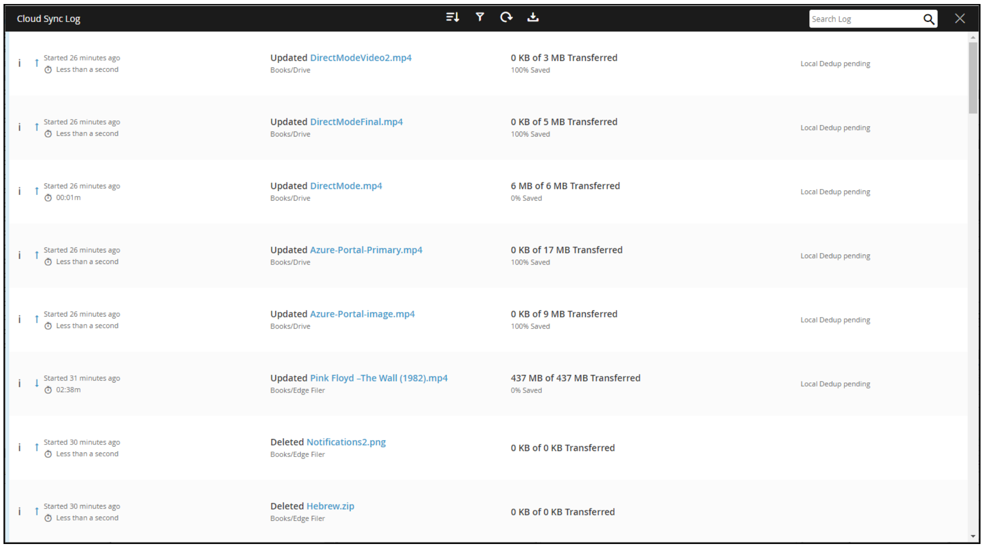
You can view device statistics by clicking Statistics.
The statistics window is displayed in a new browser window.



The graphs show the following:
Cloud I/O – Rate of transfer of data over time from the HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal (Upload) and the HCP Anywhere Enterprise Portal to the HCP Anywhere Enterprise Edge Filer (Download).
Cache History – The amount of data in the cache over time.
Local I/O – The write rate from the client to the HCP Anywhere Enterprise Edge Filer and the read rate from the HCP Anywhere Enterprise Edge Filer to the client, over time.

You can view the cloud drive in the end user view by clicking View Cloud Drive.

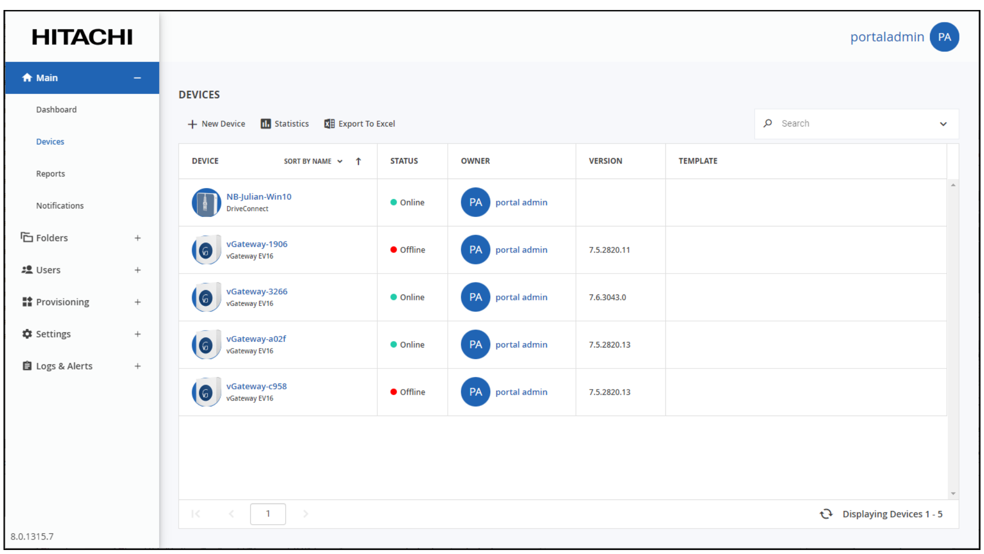
You can view a log of all file activity on the cloud drive by clicking View Log.



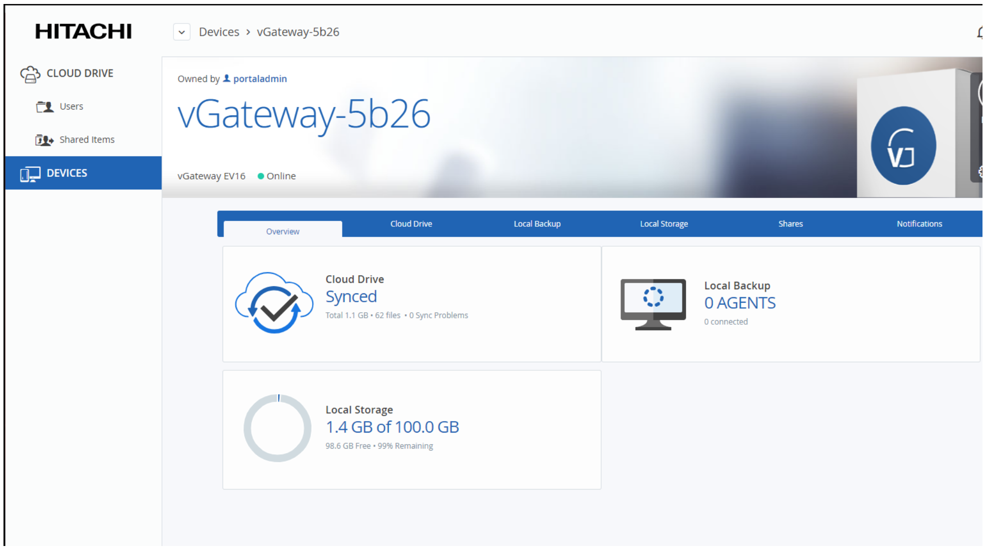
Note: The information is the same as when choosing **Cloud Sync Log** under **Logs & Alerts** in the navigation pane, but the presentation is different.

View the HCP Anywhere Enterprise Edge Filer Storage

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.

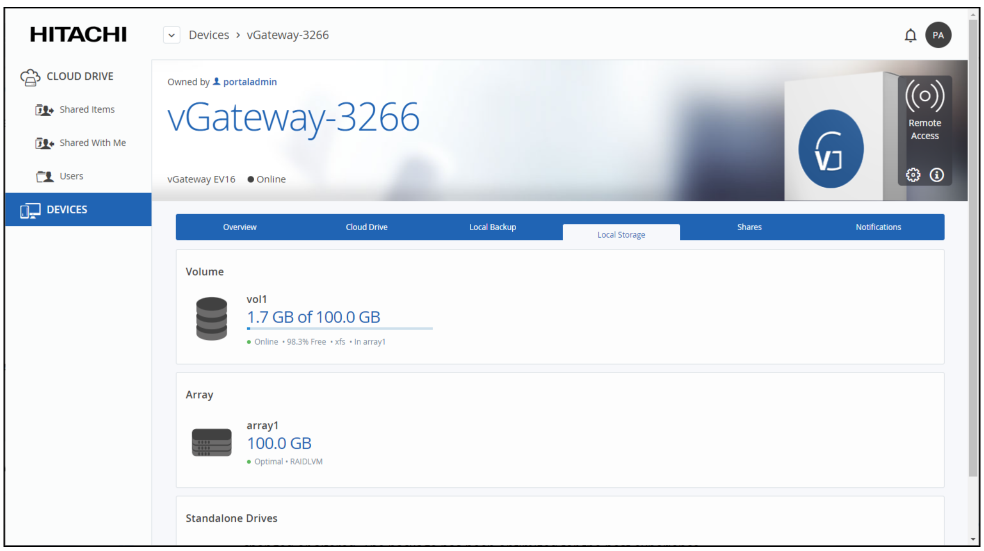


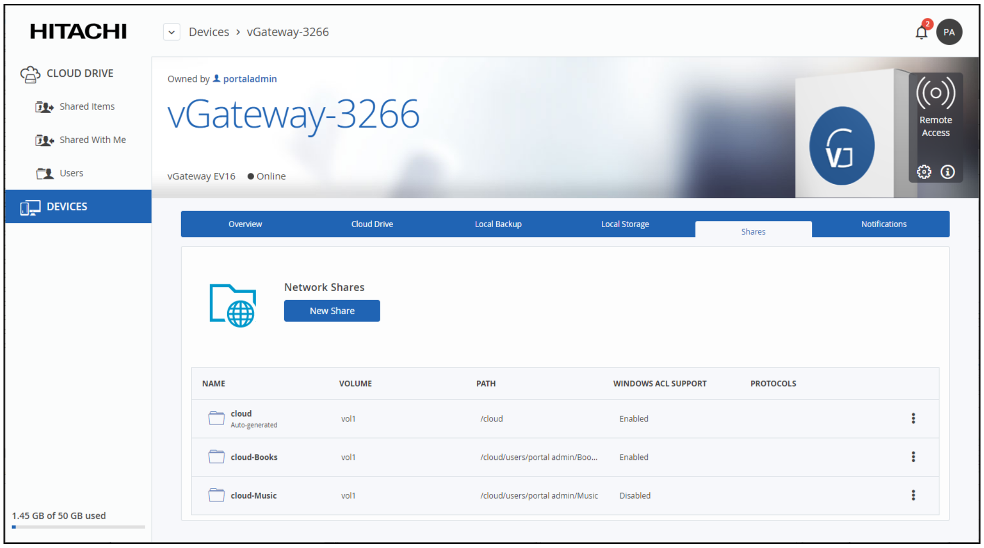
2. Click the HCP Anywhere Enterprise Edge Filer name.
   The HCP Anywhere Enterprise Edge Filer details are displayed in a new browser window.



3. Click the **Local Storage** tab.

   The HCP Anywhere Enterprise Edge Filer storage details are displayed.



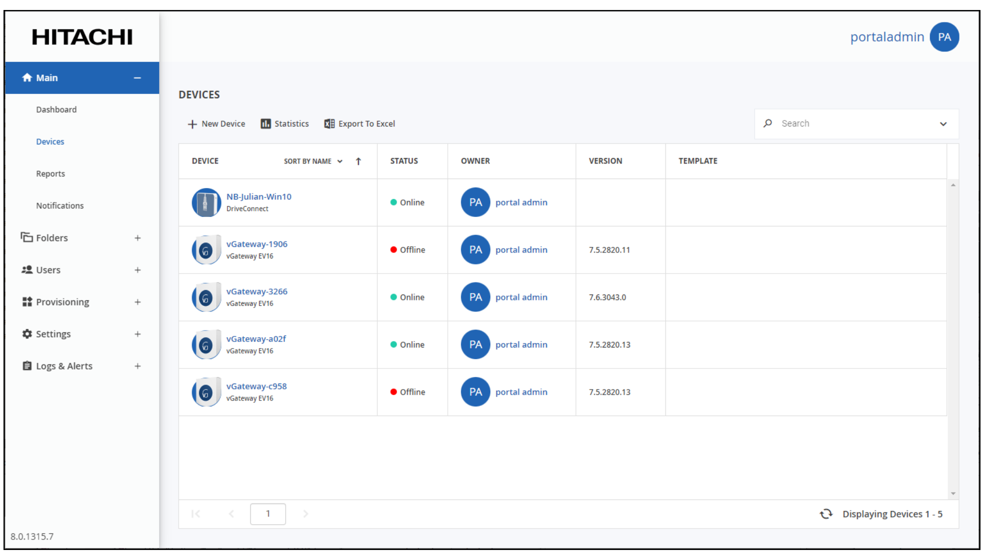


Managing the HCP Anywhere Enterprise Edge Filer Shares

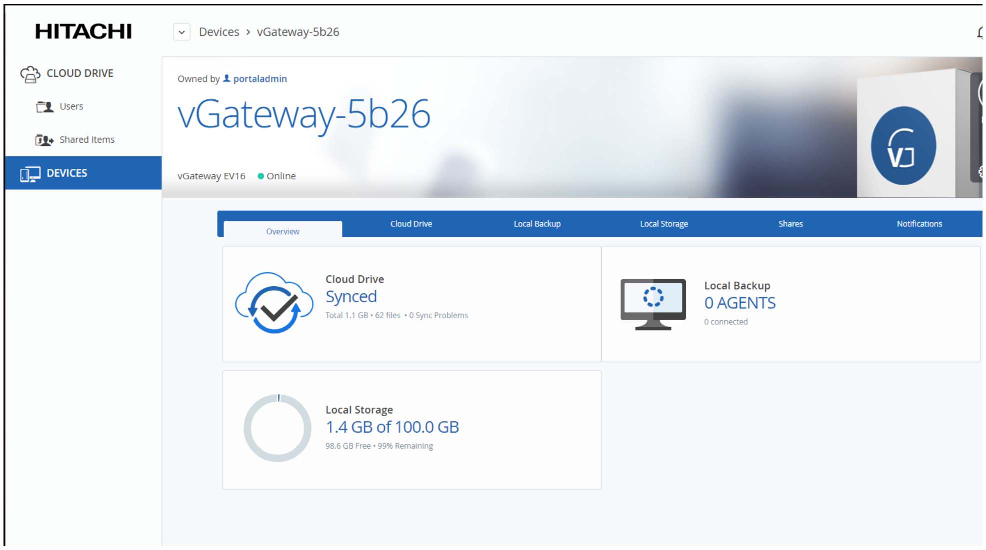
Manage the HCP Anywhere Enterprise Edge Filer shares from the portal.

To manage the HCP Anywhere Enterprise Edge Filer from the HCP Anywhere Enterprise Portal:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.

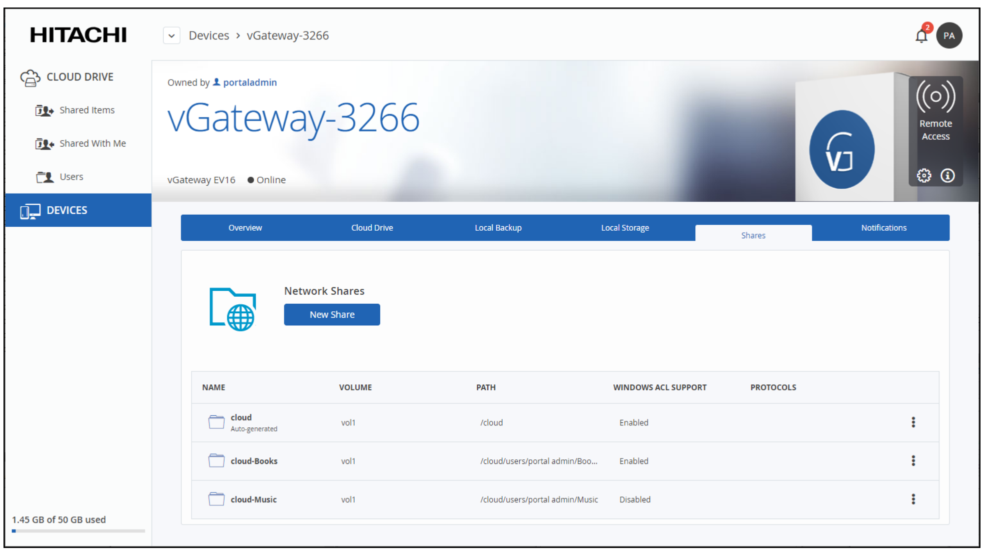


2. Click the HCP Anywhere Enterprise Edge Filer name.
   The HCP Anywhere Enterprise Edge Filer details are displayed in a new browser window.



3. Click the **Shares** tab.

   The share details for the device are displayed.



4. Click **New Share**.

   The **Select a Folder to Share** wizard opens, displaying the volumes and folders on the HCP Anywhere Enterprise Edge Filer.F or details of the **Select a Folder to Share** wizard, see the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.

5. Select the volume, folder, or subfolder on which you want to define the share.
   - To create a new subfolder to select as a nested share, select the parent folder, click **New Folder**, and then assign the subfolder a name.
   - You can define nested shares based on subfolders within your own cloud drive, which are available to users based on the permissions defined when creating the share. If the share has NT ACL settings, these settings are applied to the nested share and to every share below this share. For example, if the administrator has a personal cloud drive named *MyGateway*, to which he migrated a full old Windows File Server with the following

structure:

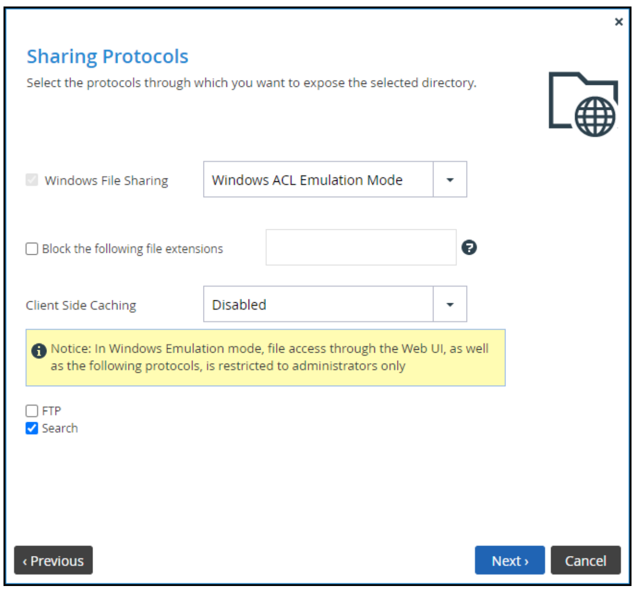
```
/Cloud
   /WIN-File-Server
     /Share1
     /Share2
   /My Files
   /Shared with me
```

If, before the Windows File Server migration, `\\Win-File-Server\Share1` and `\\Win-File-Server\Share2` shares were exposed in the old file server, users logged in to MyGateway can access the content of the shares: `\\MyGateway\Share1` and `\\MyGateway\Share2` after they are defined:

```
Share1 = \\MyGateway\Cloud\WIN-File-Server\Share1
Share2 = \\MyGateway\Cloud\WIN-File-Server\Share2
```

6. Click **Next** and then assign the network share a name.
7. Click **Next** to choose through which sharing protocols to expose this share.

   The **Sharing Protocols** window is displayed.



Windows File Sharing is checked by default and cannot be deselected. From the drop-down, select one of these access levels for the share:

- **Only Authenticated Users**. Users will be required to authenticate using their HCP Anywhere Enterprise Edge Filer user name and password, in order to access the network share.
- **Windows ACL Emulation Mode**. The share will be a Windows ACL emulation mode share.
  Users access the shared files and folders through standard Windows client computers; for example, using Windows Explorer through the SMB/CIFS access provided by the HCP Anywhere Enterprise Edge Filer.
  Windows ACL Emulation Mode also allows you to block users from writing specific file types into the HCP Anywhere Enterprise Edge Filer share or gaining control of the content located on it.

Block the following file extensions – The listed file extensions are blocked. Separate file extensions with a comma (,).

Client Side Caching. Server files are designated for off-line work so that a copy of the files is cached on the client computer and can be accessed when the client is off line in exactly the same way as if they were stored on the Windows file server.

Manual caching for documents – Users must cache files manually.

Automatic caching for documents – A copy of the files is cached automatically.

Disabled – The client computer cannot cache files locally and the updated copy must be retrieved from the file server.

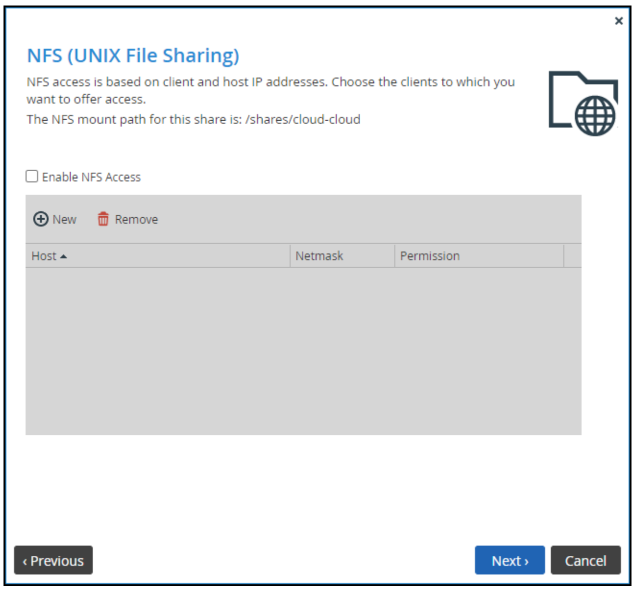
8. Specify how you want to share the files.

   FTP – Users will be able to access and download files on this share from the FTP site. The shares must not be ACL shares, or if they are ACL shares, the user must be an administrator. To configure the FTP server, go to **Shares > FTP Server**.

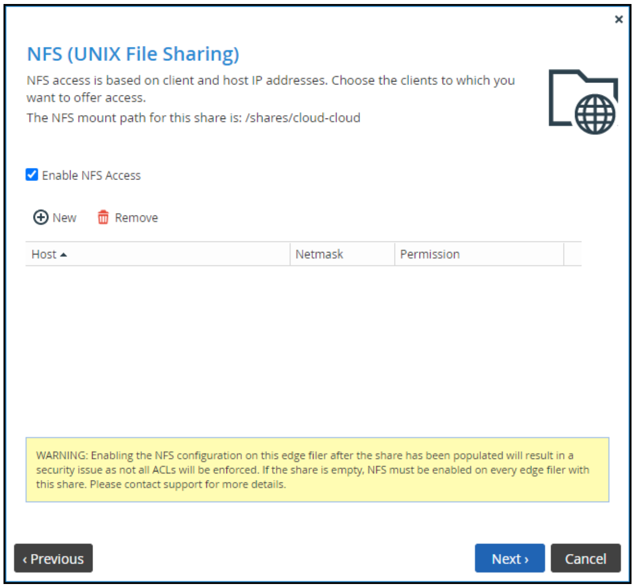
   Search – Users will be able to search for files in this share.

9. Click **Next**.

   The **NFS (UNIX File Sharing)** window is displayed.



10. Check the **Enable NFS Access** option to enable NFS clients to access the share.



Note: For a windows ACL emulated share, permissions are written differently when NFS access is enabled and when it is not enabled. If you have a standard windows ACL share with permissions and then turn on NFS, the NTACL permission are no longer readable and need to be reapplied. This applies for any device the data is shared on. Because the permissions synced, if a share doesn't match NFS enablement across devices, the permissions will be unreadable across devices as data is synced.: Either have **every** device referencing the share be NFS access enabled or not.

Either, click **New** to configure each client to which you want to grant access. A row is displayed in the table:

a) Enter the client's IP address and netmask in the appropriate fields.

b) Select the permitted level of access to the network share via NFS. Options are **None**, **PreviewOnly**, **Read Only**, or **Read/Write**.

Note: Preview Only permission prevents downloading, copying, or printing the file and content cannot be synchronized for offline access.

Or,

Click **Remove** and then select the client's IP address to remove the client from the list.

Note: The NFS mount path for the network share is specified at the top of the window.

11. Click **Next** and set which users can access this network share.

a) In the **Local Users** drop-down list, select one of the following:
Local Users – Search the users defined locally on the HCP Anywhere Enterprise Edge Filer.
Domain *domain* Users – Search the users belonging to the domain called *domain*.
Local Groups – Search the user groups defined locally on the HCP Anywhere Enterprise Edge Filer.
Domain *domain* Groups – Search the user groups belonging to the domain called *domain*.

b) In the **Quick Search** field, type a string that is displayed anywhere within the name of the user or user group you want to add, or click `. . .` to list the users.
A table of users or user groups matching the search string is displayed.

c) Select the user or user group in the table.
The user or user group is added to the list of users and user groups who should have access to the network share.

d) For each user and user group, click in the **Permission** field, and then select the access level from the drop-down list.

12. Click **Next** and then **Finish** to complete the wizard.

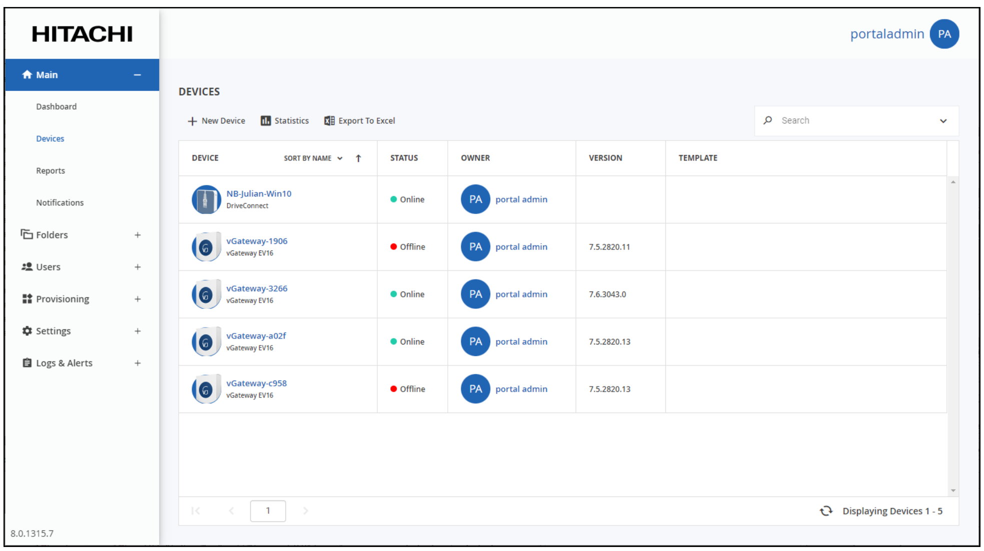
Click ⋮ next to the share to edit it or remove it.

Generating a Device Statistics Report

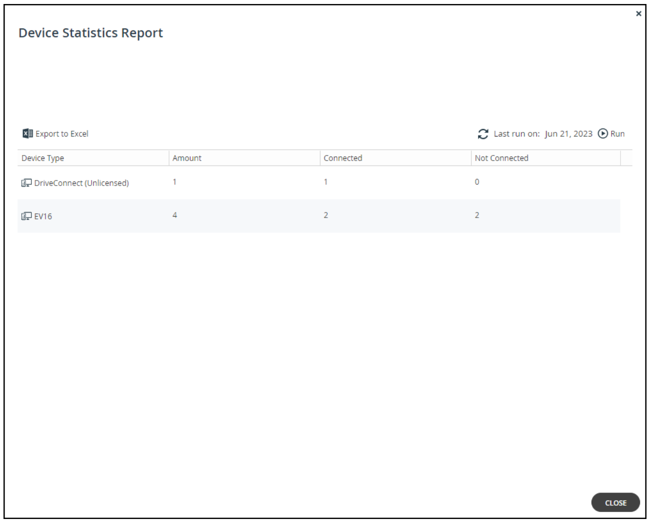
Administrators can generate a statistics report about all the devices registered to the HCP Anywhere Enterprise Portal.

To generate a statistics report:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.



2. Click **Statistics**.
   The **Device Statistics Report** window is displayed.



Note: The first time the **Device Statistics Report** window is displayed, it is empty. After generating a report, the window displays the last report generated.

3. Click **Run**.

   The report is generated, showing the list of devices types with the total number of registered devices and then the number of these devices currently connected or not connected to the portal.

You can export the list of devices and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export the Device Statistics Report to Microsoft Excel:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.
2. Click **Statistics**.

   The **Device Statistics Report** window is displayed.
3. Click **Export to Excel**.

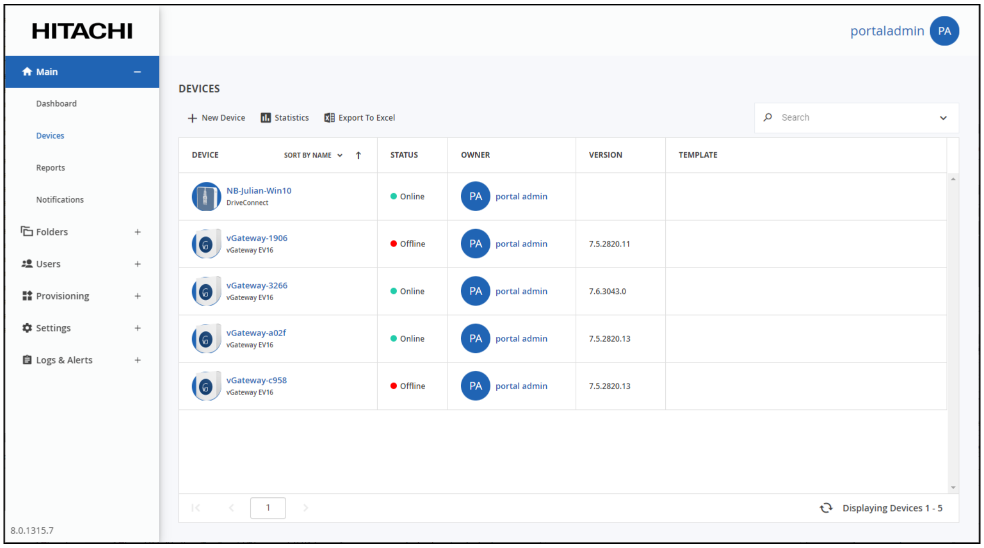
The report is exported to your computer.

Exporting a List of Devices to Excel

You can export the list of devices and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a list of devices to Microsoft Excel:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.



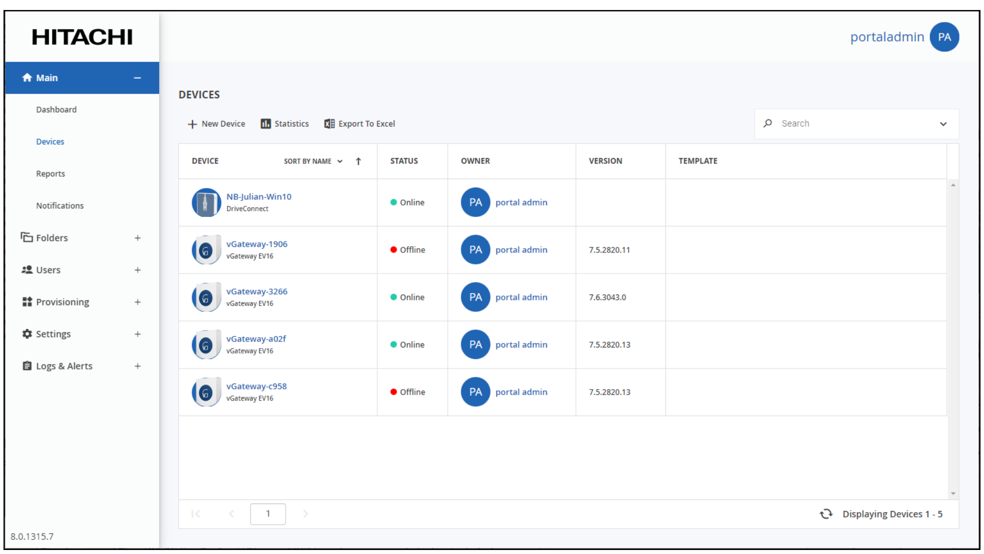
2. Click **Export to Excel**.

   The list of devices is exported to your computer. The report includes the type of device, version and any description set for the device.

Deleting Devices

To delete a device:

1. Select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to the HCP Anywhere Enterprise Portal.



2. Select the row of the device to delete and click **Delete**.

   A confirmation window is displayed.

3. Confirm the deletion.

The device is disconnected and is deleted from the HCP Anywhere Enterprise Portal.

Remotely Wiping Mobile Devices

This feature is currently not supported.

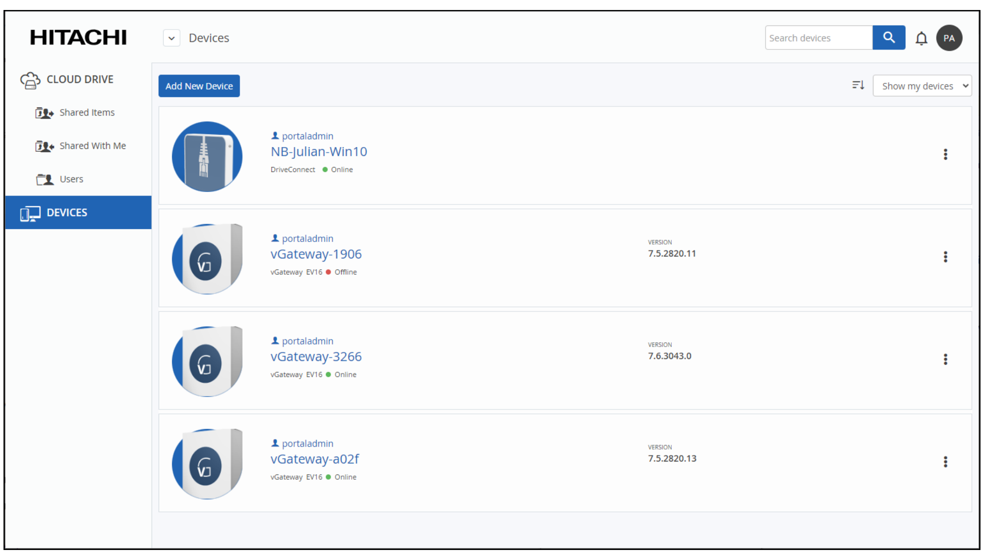
Managing Devices From the End User Portal View

An administrator can also remotely manage devices from the end user view. The **DEVICES** option displays all devices connected to the HCP Anywhere Enterprise Portal that you are managing.

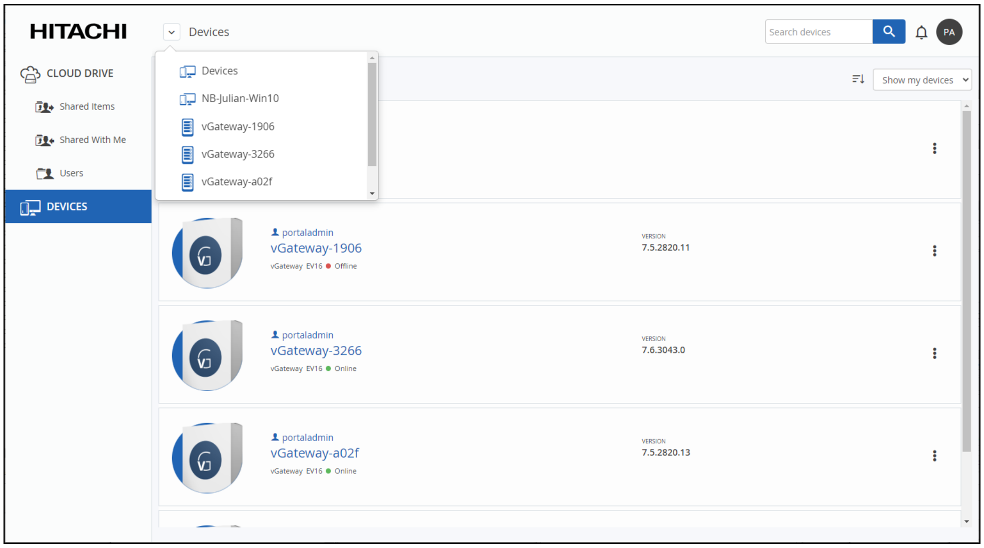
In addition, a read/write administrator can also edit device settings, such as the configuration template to apply to the device.

To edit device settings or restart a device:

1. In the end user view, click **DEVICES** in the navigation pane.
   The **Devices** page opens, displaying all the devices registered to the portal.



Note: When a device is displayed, you can also click the down arrow in the heading to list all the devices.



2. Click a device from the list to display device details and click the icon to the right of the device you want to manage and the following options are displayed in a popup menu.

Rename Device – Rename the device.
Set Description – Provide a description of the device.
Restart Device – If, the device is running, this option is displayed enabling the administrator to remotely restart the device.
Delete Device – Remove the device from the HCP Anywhere Enterprise Portal. If requested, you confirm the removal by entering your user name.

Note: You can also click a device to display details of the device and then click the icon in the device details screen. The addition option, **Advanced Settings**, is then available to enable Administrators to change the following:

The MAC address
The software version.
The configuration template, either the default template or to one of the other templates defined in the HCP Anywhere Enterprise Portal.

Chapter 15. Managing Notifications and Email Templates

As an administrator, you can receive and view notifications about portal and users as follows:

- In the end user view, by clicking the notifications  icon when it shows notifications.
- In the **NOTIFICATIONS** section of the main dashboard (**Main > Dashboard**). This section displays the highest priority notifications.
- In the **NOTIFICATIONS** page (**Main > Notifications**). Here, you receive all types of notifications that are enabled on the Notification Settings page (**Settings > Notification Settings**).
- By email. Notifications are sent to the administrator.

Notifications enable you to track error and warning conditions.

The notification dashboard displays error and warning conditions that are currently in effect, including alerts related to the system, storage nodes, specific virtual portals, users and devices.

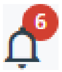
It is possible to mark specific notifications as hidden, if you do not feel that they require immediate attention. Those notifications can always be unhidden later if desired.

In this chapter

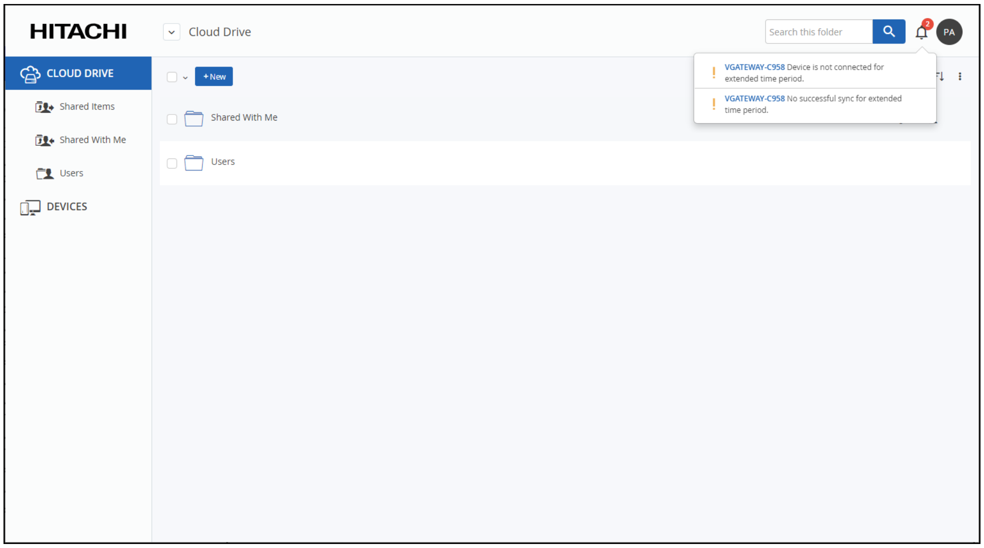
Viewing Notifications

You can view a summary of the highest priority notifications in the dashboard and all the notifications in the **NOTIFICATIONS** page.

Viewing Notifications in the End User View

When there are notifications, the number is displayed on the notifications icon. Clicking the notifications 

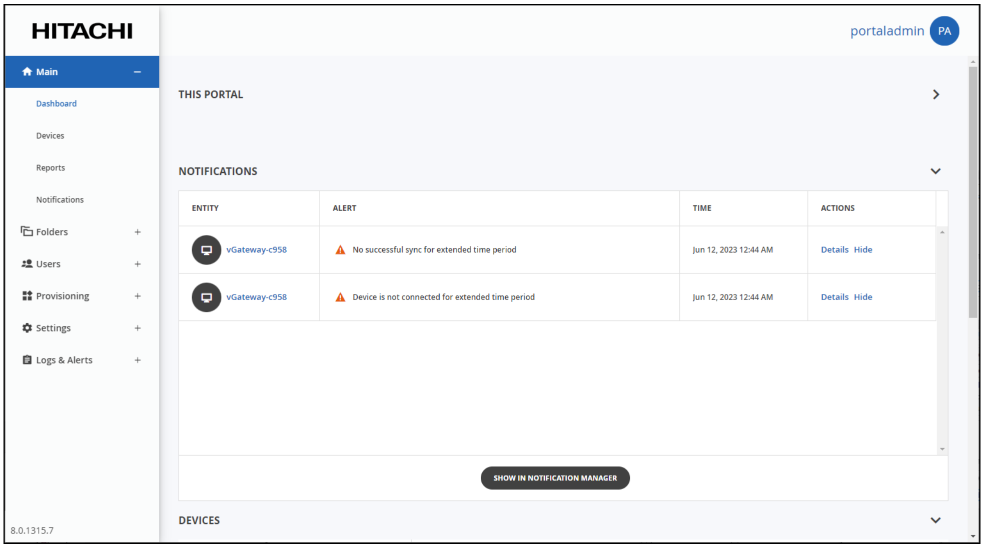
icon displays a list of notifications.



Clicking a notification in the list opens the device details to investigate the cause of the notification. Clicking **See all** displays the **NOTIFICATIONS** page in the administrator view in a new tab.

Viewing Notifications in the Main Dashboard

The dashboard displays a summary of the ten highest priority active notifications.

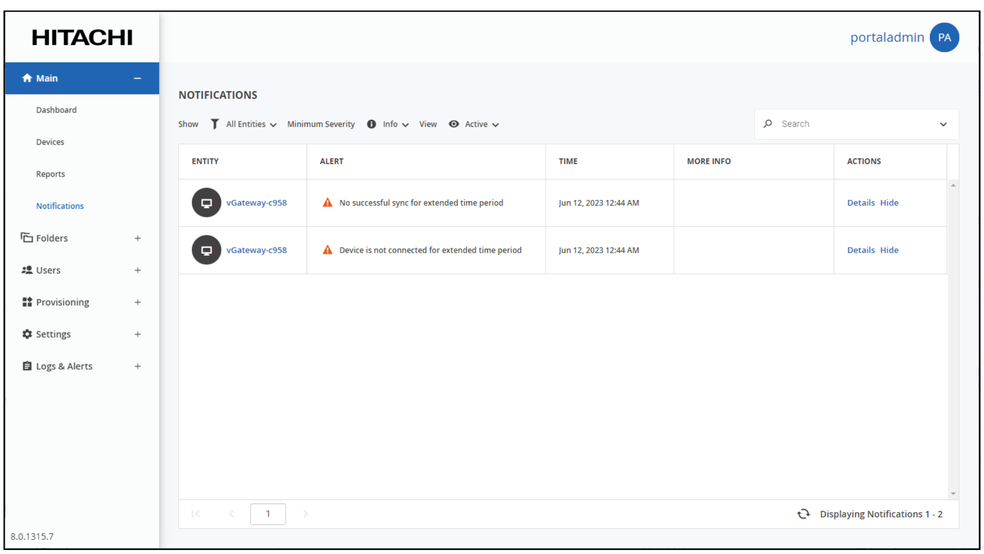


If there are notifications, you can go directly to the **NOTIFICATIONS** page by clicking **SHOW IN NOTIFICATION MANAGER**. Clicking the **ENTITY** in the list opens the device details in a new browser window to investigate the cause of the notification.

Viewing Notifications in the NOTIFICATIONS Page

To view notifications via the NOTIFICATIONS page:

1. Select **Main > Notifications** in the navigation pane.
   The **NOTIFICATIONS** page is displayed.



ENTITY – The entity for which the notification applies.

ALERT – The alert message.
TIME – The time at which the alert was triggered.
MORE INFO – Additional information about the notification.
ACTIONS – Actions you can perform on an alert, for example hiding the alert.

2. You can filter the display.

   Show – Filter notifications dependent on the notification source.
   - **All Entities** – Notifications from the portal, users, and devices.
   - **Portal** – Notifications from the portal.
   - **Users** – User notifications.
   - **Devices** – Device Notifications.

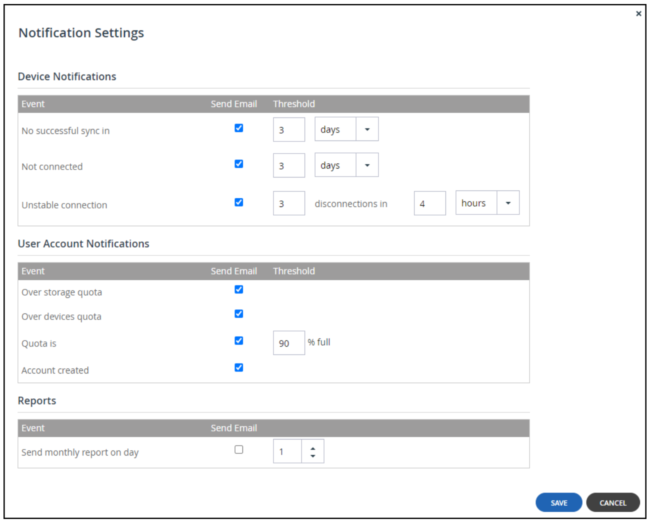
   Minimum Severity – Filter notifications dependent on the notification severity: **Info**, **Warning**, or **Error**.
   View – Filter notifications by whether they are active or hidden (not displayed).
3. You can search the list of alerts, searching everything or by entity or by the **MORE INFO** or **ALERT** columns.
4. You can unhide an notification that you marked as hidden by filtering the display to show hidden notifications and then clicking the **Unhide** link in the **ACTIONS** column for a hidden alert or selecting the notification row and clicking **Unhide**.

Configuring Notification Settings

To configure notifications for which emails are sent:

1. Select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.

2. Select **Notification Settings**, under **NOTIFICATIONS** in the **Control Panel** page.
   The **Notification Settings** window is displayed.



3. Select the notifications which you want to be informed about via email.

   The following notifications can be set:

   Device Notifications

   - A device has not synced with the portal for a specified number of hours or days.
   - A device has not been connected with the portal for a specified number of hours or days.
   - A device connection to the portal is unstable, having disconnected a specified number of times in a specified number of hours or days.

   User Account Notifications

   - The amount of storage used exceeds the quota.
   - The number of devices used exceeds the quota.
   - The amount of storage used is over a specified percentage of the quota.
   - An account was created.

   Reports

   - A monthly report is sent on a specified day of the month.

4. Click **SAVE**.

Email Notification Templates

Email notification templates are sent to portal administrators and end users.

The email notifications are in HTML format.

In this section

- Available Email Notification Templates
- Customizing Email Notification Templates

Available Email Notification Templates

The following email templates are provided.

The following email templates are provided by Hitachi Vantara.

Template Name	Description
Alert Notification	An alert is sent to portal administrators when a log is generated, if an applicable email alert is configured.
Audit Log Failure	A notification to system administrators to inform them that there is a problem with the audit log for a specific server.
Backup Completed Successfully	This feature is currently not supported.
Backup Completed With Errors Or Warnings	This feature is currently not supported.
Backup Did Not Complete On Schedule	This feature is currently not supported.
Change Email Notification	A notification to portal administrators that the portal is unlicensed and explaining how to get a license for the portal.
CloudSync Upload is Currently Back To Normal	A notification to portal administrators that syncing with the specified device is back to normal.
CloudSync Upload is Currently Stalled	A notification to portal administrators that the syncing with a specified device has stalled.
Device Activated	A notification to end users when their device has been activated.
Device Login Information Notification	A notification with device login information.
Device Never Backed Up	A notification to end users that their device has never backed up.
Device Not Connected	A notification to end users when their device has not connected to the HCP Anywhere Enterprise Portal for a certain number of days. The number of days is configured locally. See Configuring Notification Settings.
Device Wipe Completed	This feature is currently not supported.
Email Verification Code	A notification to guest invitation recipients of a pass code. The recipient must enter the passcode before accessing the file or folder that they are invited to share.
Expired Invitation To Register	A notification to an external user informing them that an invitation for the user to register has expired.
Folder Is Over Quota Limitation	A notification to end users with a folder which has used its full storage allocation.
Footer	The HTML footer that is displayed at the bottom of all notifications.
Header	The HTML header that is displayed at the top of all notifications.

Template Name	Description
Invitation To Collaborate	A guest invitation to access shared files or folders.
Invitation To Register	An invitation to an external user to register.
Malware Blocked	A notification to end users to tell them that malware was detected and blocked in a file they recently uploaded.
New User Notification	A notification to end users when an account has been created for them by an administrator, inviting them to use the portal. The email message contains log on information. By default, the email does not include the user password, for added security, and the user must contact the portal administrator for the password. Inviting users from the **USERS** page, with the **More > Invite** option, enables the user to choose a password on initial logon without needing to contact the administrator.
No Cloud Sync For Extended Time Period	A notification to end users if no cloud sync has occurred between their cloud drive and their workstation or server for a specified time period.
Password Recovery Notification	A notification to end users when a request is made to reset their password.
Reshare As Public Link	A notification to end users telling them that another user with whom they shared a folder has just created a public link to reshare that folder.
Reshare By Adding Collaborators	A notification to end users telling them that another user with whom they shared a folder has reshared your folder with other people, listing the new collaborators.
Sensitive File Blocked	A notification to end users telling them that a file with sensitive material has been blocked.
SMS Verification Code	A notification of a pass code to guest invitation recipients sent by SMS. The recipient must enter the passcode before accessing the file or folder that they are invited to share.
Successful User Registration	A notification to a end users informing them that a user they invited has successfully completed the registration process to.
Unstable Connection	A notification to a user when a device belonging to the user has repeatedly lost its connection to the portal, warning of unstable connectivity between the device and the portal.
User Account Activated	A notification to end users that the user's account is now active.
User Is Near Quota Limitation	A notification to end users when the amount of cloud storage space used reaches or exceeds a certain percentage. The percentage is configured locally.
User Is Over Agents Limitation	A notification to end users when the licensed number of HCP Anywhere Enterprise Agents has been exceeded.

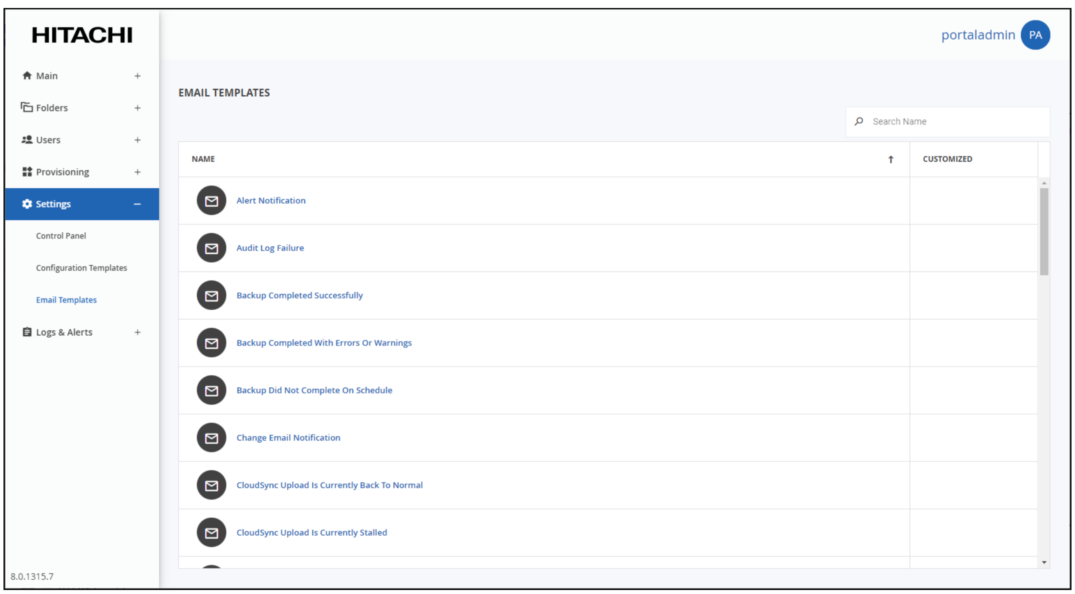
Template Name	Description
User Is Over Quota Limitation	A notification to end users when their cloud storage space is full.
User Report	A monthly report sent to end users, which includes the following information: • Account information • Storage statistics • Usage report • Details of all the user's devices

Customizing Email Notification Templates

Each email template includes variables, with the format *param.variableName*. When customizing a template, only variables in that template, and not from other templates, can be used. You can rearrange where the parameters will be displayed in the email message and add or change the text.

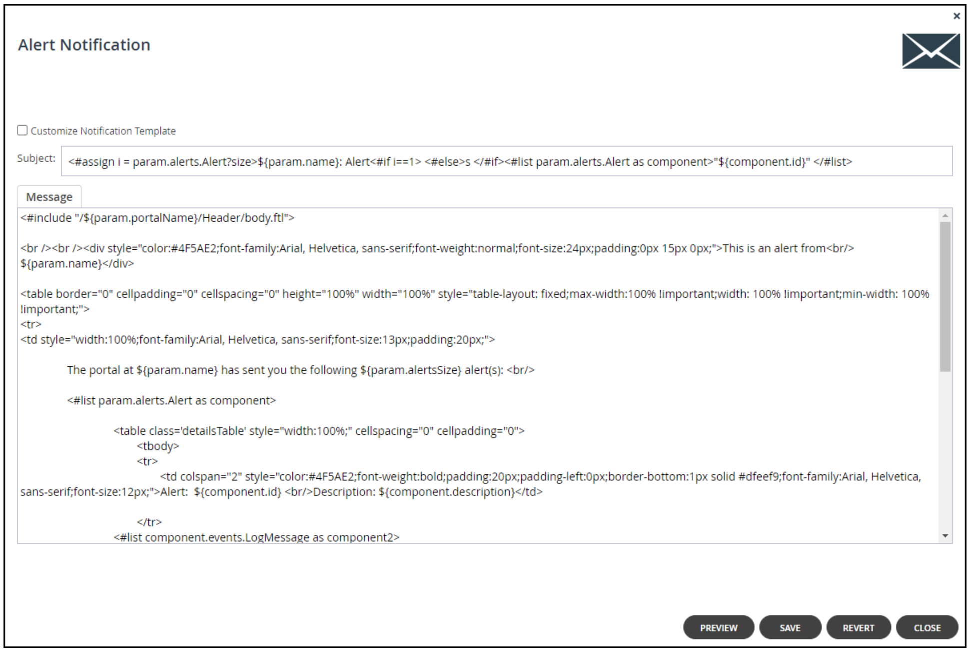
To customize email notification templates:

1. Select **Settings > Email Templates** in the navigation pane.
   The **EMAIL TEMPLATES** page is displayed with a list of email templates.



   For a description of each template, see Available Email Notification Templates.
2. Click the email template to edit.

   The template editor is displayed, with the email template content. For example, the **Alert Notification** template.



The template editor is displayed, with the email template content.

If the notification includes a PDF attachment, the editor includes a **PDF** tab.

3. Click **PREVIEW** to preview the current format of the email message and understand how each parameter is displayed in the output.

   Note: You can delete parameters from the email message or rearrange where the parameters will be displayed. You can also add or change the email message text. You cannot use parameters that are not already included in the template.

4. Select the **Customize Notification Template** check box to enable editing the template.
5. In the **Subject** field, type the text that should appear in the notification email's Subject line.

   Note: Some templates, such as the Header template, do not have a **Subject** field.

6. To edit the email message, In the **Message** tab, modify the template.
7. To preview changes to the email message, click **PREVIEW**.

   A window is displayed with the email content as it will be displayed to the recipient.

   Note: Some templates, such as the Header template, do not have a **PREVIEW** button.

8. To edit a PDF attachment, In the **PDF File** tab, modify the template.
9. To preview changes to the PDF, click **PREVIEW**.

   The PDF is downloaded to your computer. where you can open an review the content.

10. To undo unsaved changes, click **REVERT**.
11. Click **SAVE**.
12. Click **CLOSE**.

Chapter 16. Managing Device Configuration Templates

HCP Anywhere Enterprise Portal enables you to centrally manage device settings, by assigning devices to *device configuration templates*: When a device is assigned to a template, it inherits the following settings from that template:

- Installed software and firmware versions
- Automatic firmware updates

Devices can be assigned to templates in the following ways:

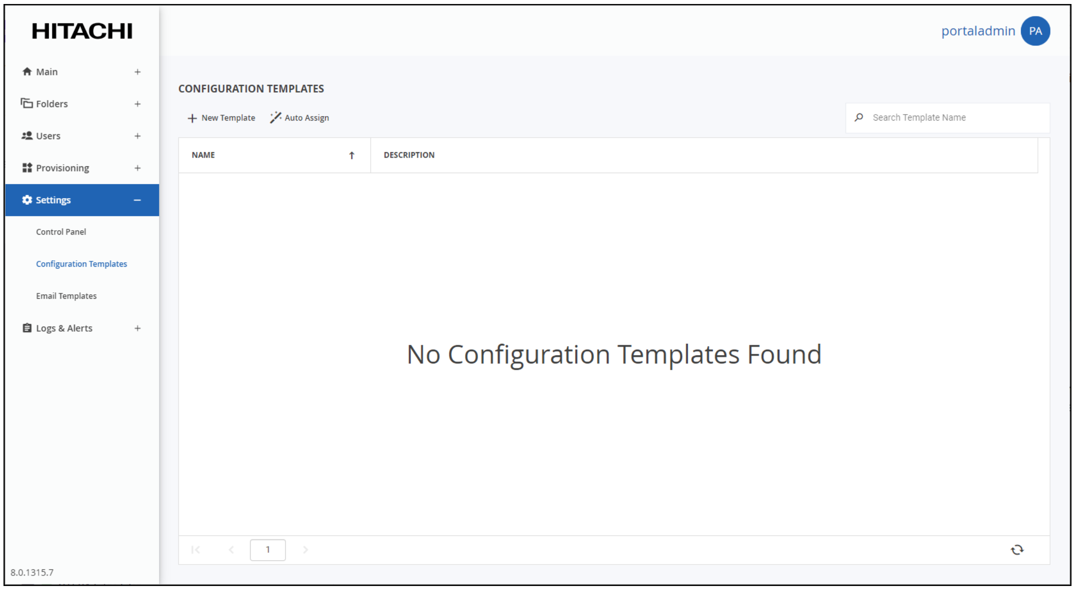
- Automatic template assignment.
  Devices can be assigned to templates based on the *automatic template assignment policy*, which specifies a set of criteria for assigning a template such as device type and operating system, as well as an optional default template that is assigned when none of the criteria are met.
  See Configuring the Automatic Template Assignment Policy.
- Manually, by editing the advanced device settings.
  See Managing Devices From the End User Portal View.

In this chapter

Viewing Device Configuration Templates

To view all device configuration templates in the portal:

- Select **Settings > Configuration Template** in the navigation pane.
  The **CONFIGURATION TEMPLATES** page is displayed.

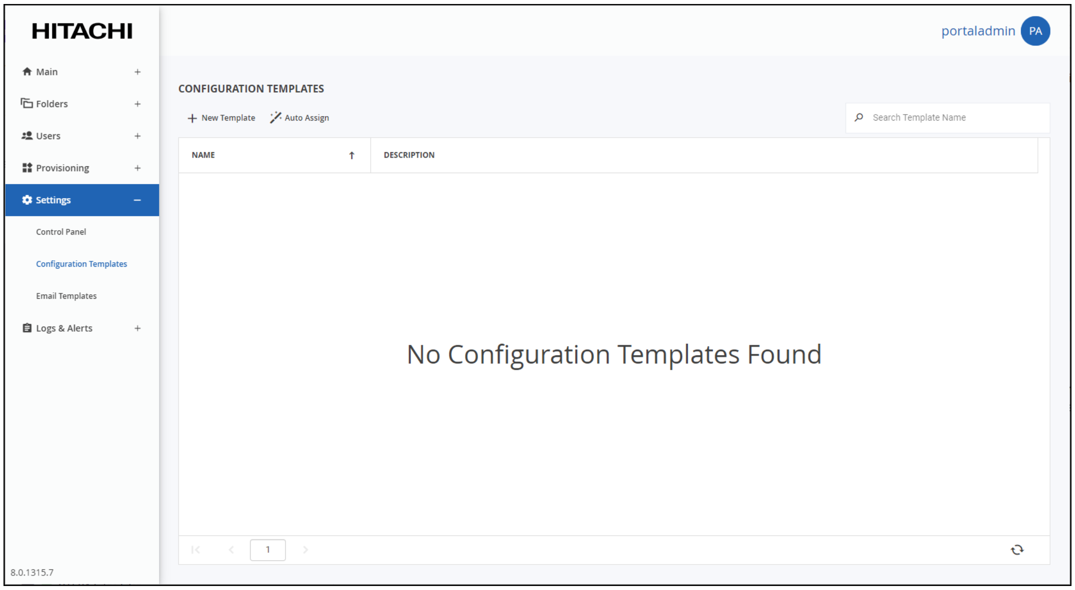


The portal does not have any predefined configuration templates.

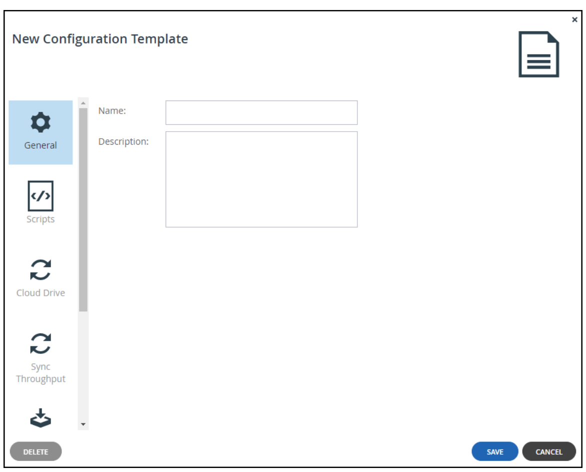
Adding and Editing Device Configuration Templates

To add or edit a device configuration template:

1. Select **Settings > Configuration Template** in the navigation pane.
   The **CONFIGURATION TEMPLATES** page is displayed.



2. Either,
   - Add a new template, click **New Template**.
     The **New Configuration Template** window is displayed.



   Or,
   - Edit an existing configuration template, click the template's name**.**
     The configuration template window is displayed with the configuration template name as the window title.
3. Enter the general details for the template:

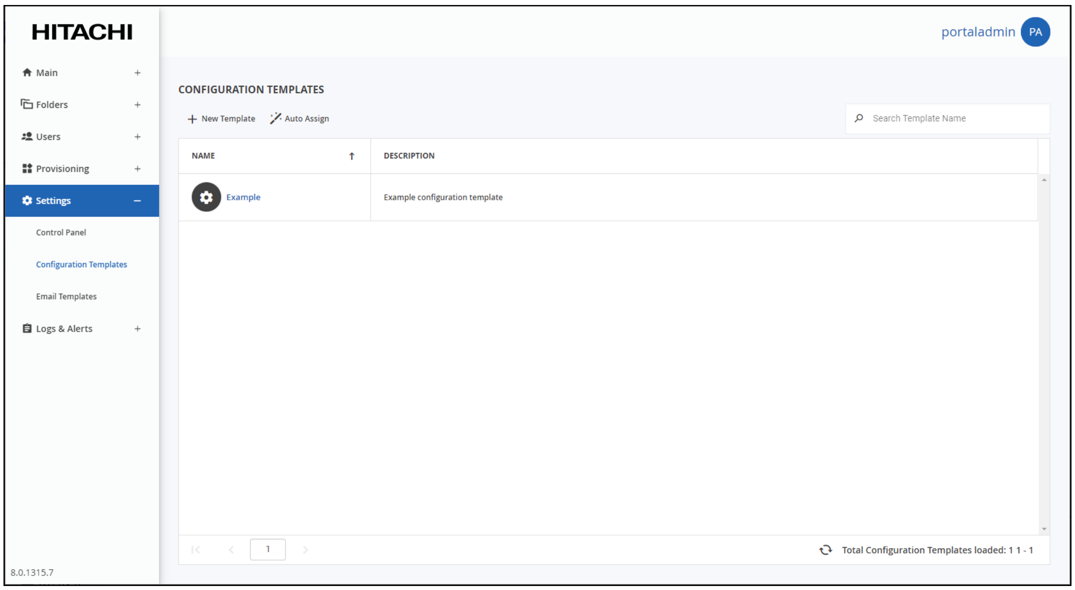
   Name – A unique name for the template. Spaces and special characters cannot be used in the name.

Description – A description of the template.

4. Access the following options to complete configuring the template:

   Scripts – This feature is currently not supported.
   Cloud Drive – Which HCP Anywhere Enterprise Portal cloud folders are be synchronized with the device, and with which folder each cloud drive folder is synced.
   Sync Throughput – Restrict bandwidth for specific hours in a day or on specific days.
   Software Updates – A firmware image for all relevant devices.
   Update schedule – Configure how and when to install updates.
   Consent Page – Configure a consent page that has to be accepted before a user can log in to a device, such as an edge filer, that is connected to the portal.

5. Click **SAVE**.



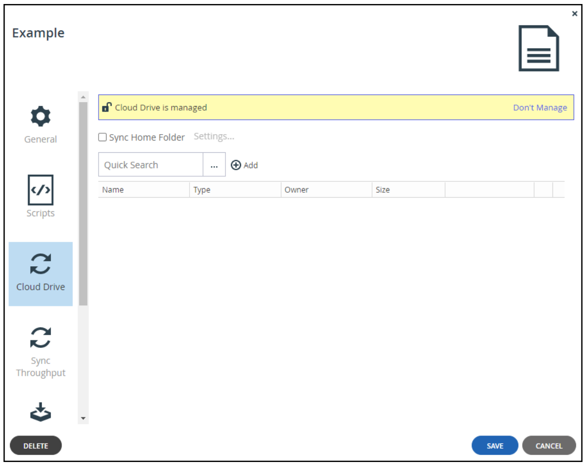
The configuration is saved and, after a few minutes, applied to devices to which the template is assigned, as described in Configuring the Automatic Template Assignment Policy or per device, in the **Advanced** settings for the device, as described in Managing Devices From the End User Portal View.

Cloud Drive

Specify which portal cloud folders are be synchronized with the device, and with which folder each cloud drive folder is synced.

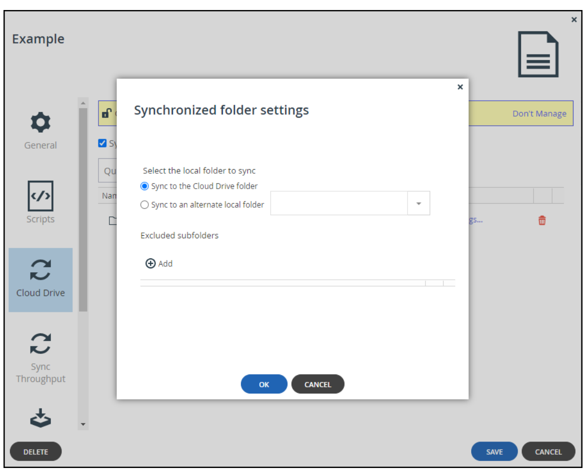
To manage cloud drive sync in the device template:

1. In the configuration template window, select the **Cloud Drive** option.



The device template will manage the cloud drive folders sync for devices using this template.

2. If you do not want managed cloud drive folder syncs, click **Don't Manage**. Click **Manage**, if the cloud drive is unmanaged.
3. To sync the home folder, select **Sync Home Folder** and click **Settings**.



4. Set which local folder on the device the cloud drive home folder should be synced:
   - Sync the folder to cloud drive folder on the HCP Anywhere Enterprise Edge Filer.
   - Sync the folder to an alternative local folder on the HCP Anywhere Enterprise Edge Filer, using one of the following environment variables.

     $USERS – The home directories folder on the HCP Anywhere Enterprise Edge Filer. For example, /Shares/Home Folder

     $PROJECTS – The projects folder on the HCP Anywhere Enterprise Edge Filer. For example, /Shares/Projects

When you specify a folder name, all of the files and subfolders in it are automatically included. You do not need to add "*" at the end of the folder name.

5. Exclude sub-folders: Click **Add** in the **Excluded sub-folders** section.

A row is added to the table.

6. Click in the row and enter the name of a subfolder to exclude from syncing.

7. Click **OK**.

8. To add more cloud drive folders to sync with the device:

a) Click in the **Quick Search** field and type a search string to search for the name of a cloud drive folder you want to add.
All the folders that include the search string in their names are displayed.

b) Select the folder you want to add.

c) Click **Add**.
The folder is added to the list.

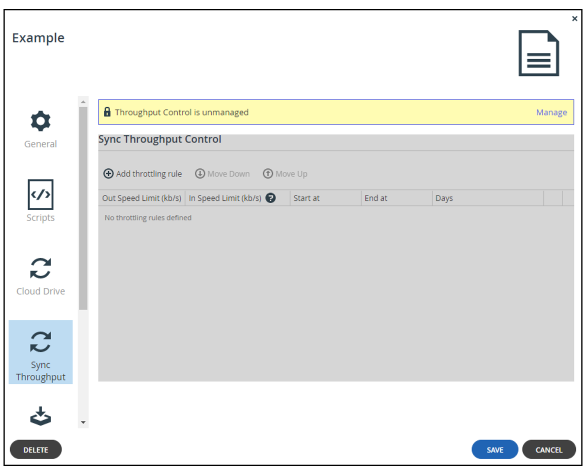
d) To set which folder on the device the folder should sync with, click the **Settings** button in the row.

e) Set the folder as described in steps 4 to 7.

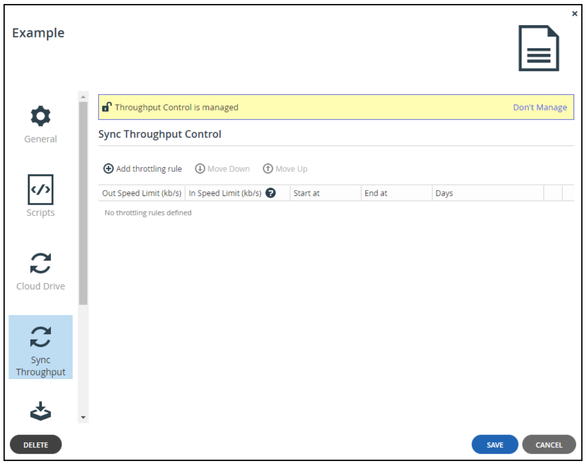
Sync Throughput

To control the cloud sync upload and download speeds:

1. In the configuration template window, select the **Sync Throughput** option.



2. Click **Manage**, if the sync throughput is unmanaged. The device template will manage the cloud drive sync throughput for devices using this template.



If you do not want managed cloud drive sync throughput, click **Don't Manage**.

3. Click **Add throttling rule** to set the throttling for sync throughput.

Note: When no throttling rules are defined, there is no speed restriction for uploading or downloading files to the Cloud Drive for syncing. A maximum of 50 rules can be defined.

a) Define the following for the throttling rule:

Out Speed Limit (kb/s) – The maximum speed to use for cloud drive sync upload in Kbits per second. The minimum value for the speed is 8kb/s. If there is no value, then there are no speed limits.

In Speed Limit (kb/s) – The maximum speed to use for cloud drive sync download in Kbits per second. The minimum value for the speed is 8kb/s. If there is no value, then there are no speed limits.

Start at – Specify the time when the bandwidth limit used for cloud drive sync upload starts.

End at – Specify the time when the bandwidth limit used for cloud drive sync upload ends. When the end time is before the start time, the end time is the next day.

Days – Specify that the bandwidth used for cloud drive sync upload should be restricted every day (the default) or only on specified days.

Note: When the start and end times for more than one rule overlap, the order of the rules in the list determines how they are implemented with the rule ate the top of the list implemented first. Use **Move Down** and **Move Up** to change the order the rules are listed.

b) To remove a rule, select the rule row and click .
The rule is removed.

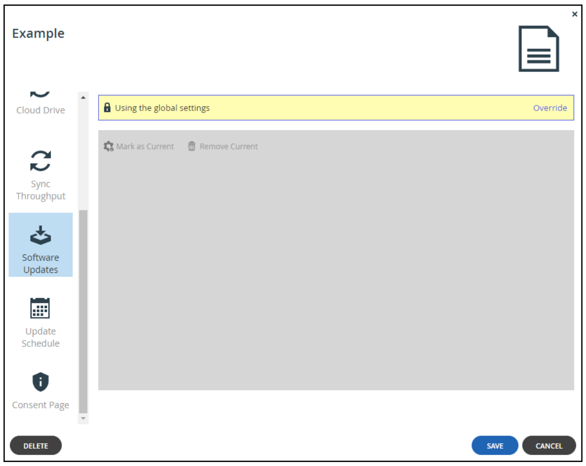
Software Updates

When you mark a firmware image as the current firmware image, all devices that are of the relevant device platform, assigned to this template, and set to automatically download firmware images will download this firmware image.

There can only be one current firmware image per device platform.

To mark a firmware image as the current firmware image:

1. In the configuration template window, select the **Software Updates** option**.**



2. Click **Override** if you want to override global settings.

   When global settings are overridden, you can revert to global settings, by clicking **Use global settings**.
3. If firmware has been added to the HCP Anywhere Enterprise Portal firmware repository, select the desired firmware image's row.
4. Click **Mark as Current**.

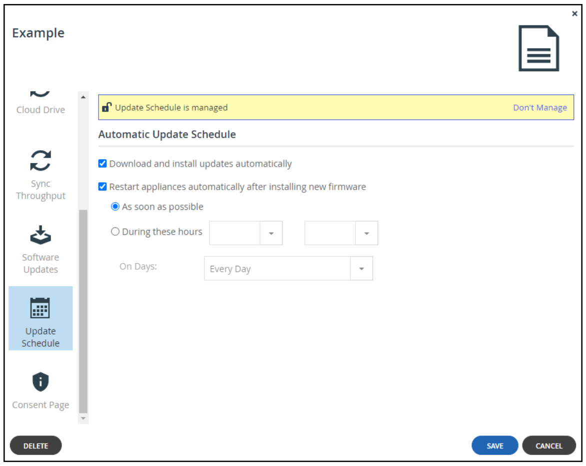
The selected firmware image becomes the current firmware image and is marked with .

Update schedule

You can configure your devices to automatically download and install firmware updates.

To configure automatic firmware updates:

1. In the configuration template window, select the **Update Schedule** option.



2. Click **Manage**, if the update schedule is unmanaged. The device template will manage the update schedule for devices using this template.

   If you do not want a managed update schedule, click **Don't Manage**.
3. Configure the firmware update schedule:

   Download and install updates automatically – The HCP Anywhere Enterprise Portal downloads and installs firmware updates automatically. If you do not select this option, device owners must perform firmware updates manually.

   Restart automatically after installing new firmware – The HCP Anywhere Enterprise Portal automatically reboots after installing new firmware updates:

   As soon as possible – To reboot as soon as possible after a firmware update. In this case, the HCP Anywhere Enterprise Portal reboots as soon as it is recommended to do so. For example, the automatic reboot might be deferred, if the HCP Anywhere Enterprise Portal is undergoing system maintenance that should not be interrupted.

   During these hours – To reboot only during specific hours.

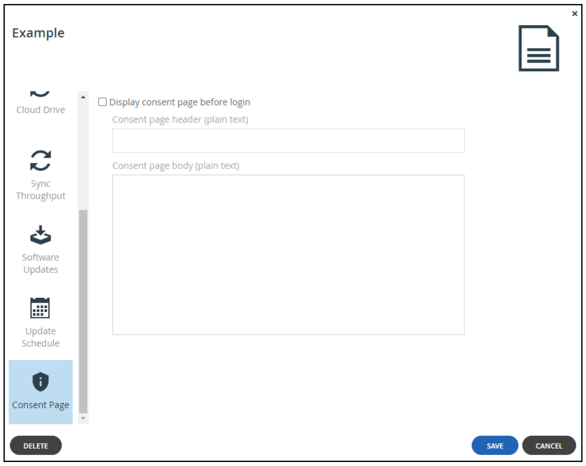
   On Days – To reboot on automatically on specified days.

Consent Page

You can configure devices that are connected to a HCP Anywhere Enterprise Portal to display a consent page before the user can log in to the device.

To configure a consent page:

1. In the configuration template window, select the **Consent Page** option**.**

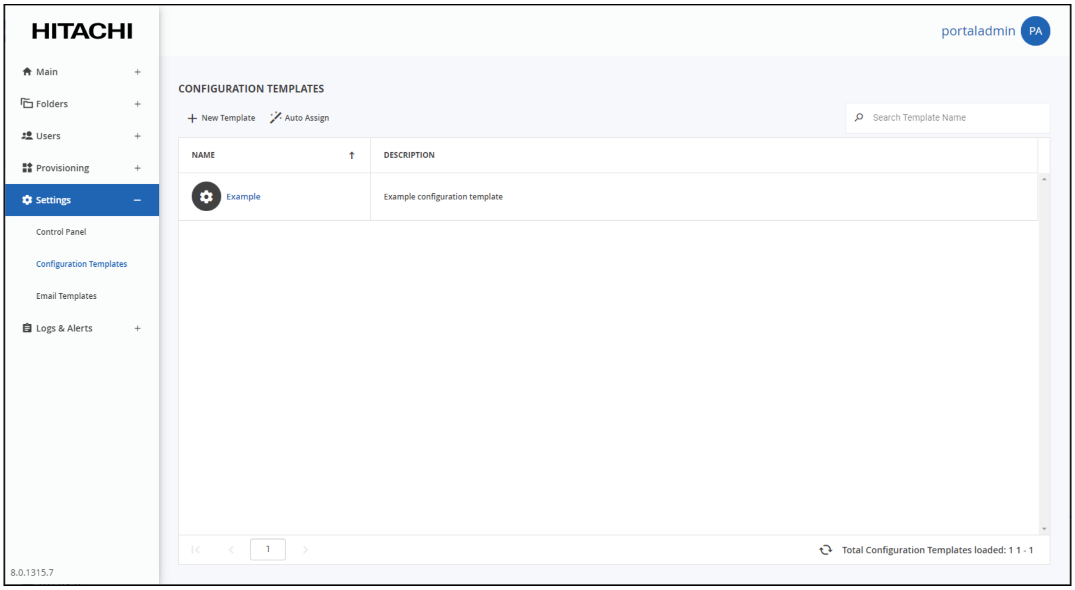


2. Check **Display consent page before login**. Before a user can access a device (such as an edge filer) that connects to the portal a consent page is displayed and only after the user accepts the terms in the consent page can the user log in.
3. Enter the text for the consent page heading, as plain text.
4. Enter the text for the consent page statement, as plain text.

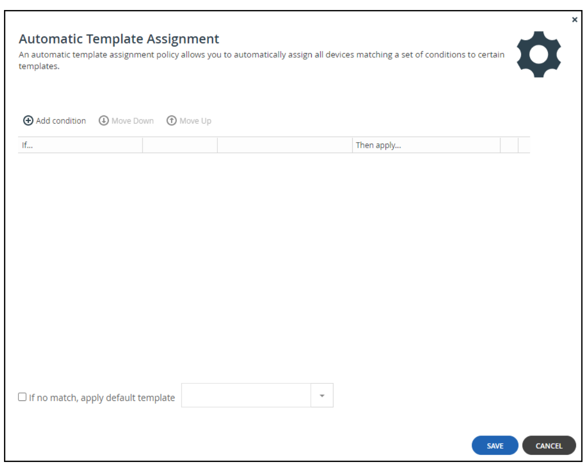
Configuring the Automatic Template Assignment Policy

To configure the automatic template assignment policy:

1. Select **Settings > Configuration Template** in the navigation pane.
   The **CONFIGURATION TEMPLATES** page is displayed.



2. Click **Auto Assign**.
   The **Automatic Template Assignment** window is displayed.



3. Define the conditions for a device to be assigned to a template, by doing the following for each condition:
   a) Click **Add condition**.
      A row is displayed in the table.
   b) Click the cell in the first column and select the condition parameter from the drop-down list.
   c) Click in the second column and select the condition operator from the drop-down list.
   d) Click in the third column, and complete the condition, by selecting values or entering the free-text value.

Multiple values must be separated by commas.
For example:

If you select **Installed Version** as the condition parameter in the first column, **equals** as the condition operator in the second column, and enter `7.0` in the third column, then the condition is met when the device's installed firmware version is *7.0*.

If you select **Owner Groups** as the condition parameter in the first column, **is one of** as the condition operator in the second column, and enter `groupA, groupB` in the third column, then the condition is met when the device owner's user account belongs to user group *groupA* or user group *groupB*.

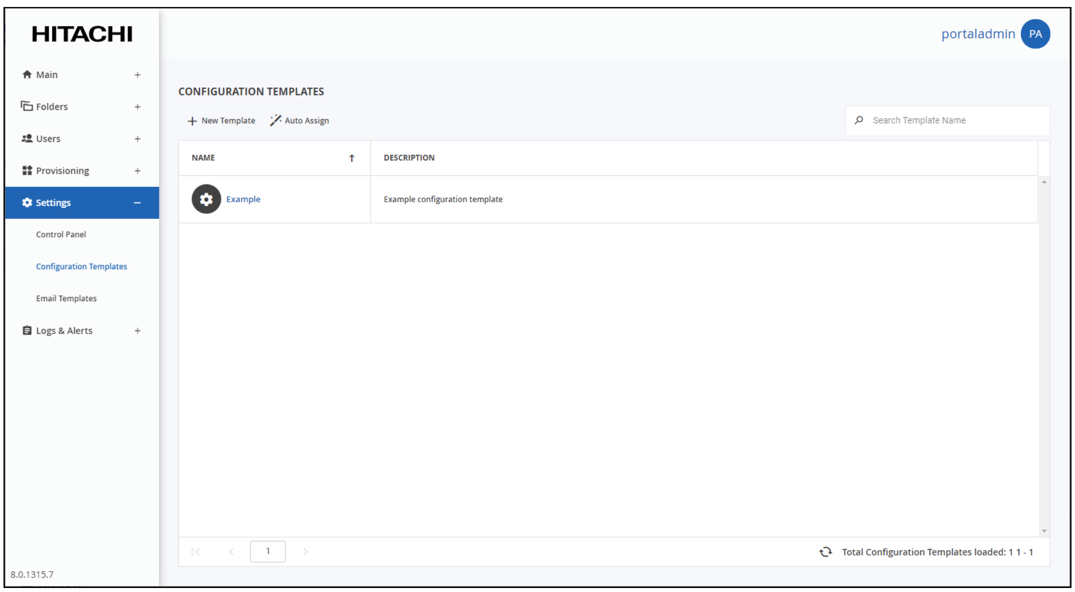
e) Click in the **Then apply** column, and select the template that is assigned when the condition is met.

4. To delete a condition, click in its row.
5. To specify that the policy should include a default device configuration template:
   a) Check **If no match, apply default template**.
   b) In the drop-down list, select the template to apply when none of the conditions are met.
6. Click **SAVE**.

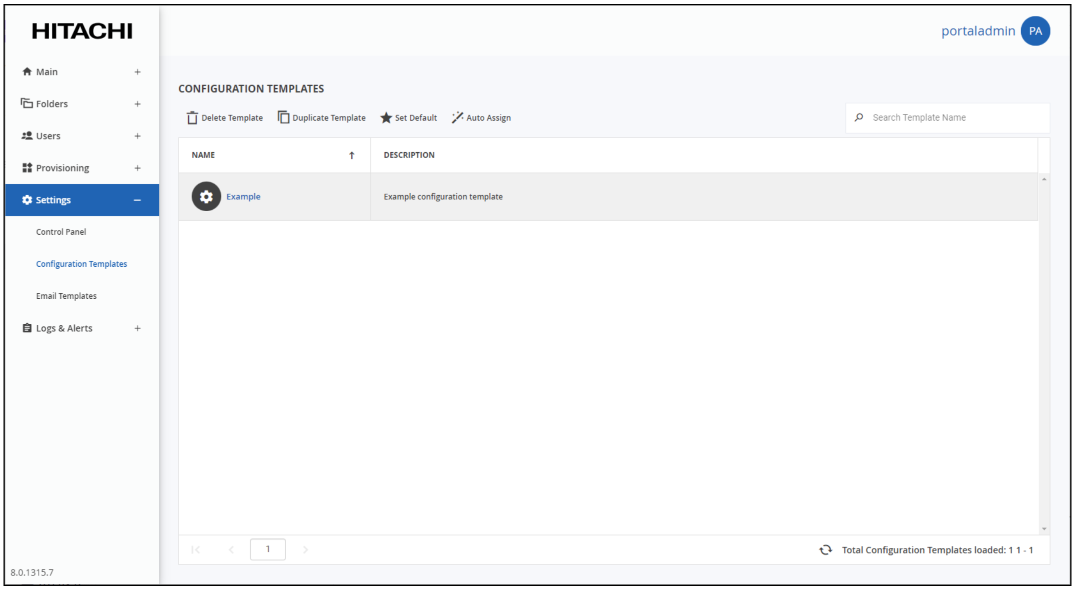
Setting the Default Device Configuration Template

To set a device configuration template as the default:

1. Select **Settings > Configuration Template** in the navigation pane.
   The **CONFIGURATION TEMPLATES** page is displayed.



2. Select the desired template's row.

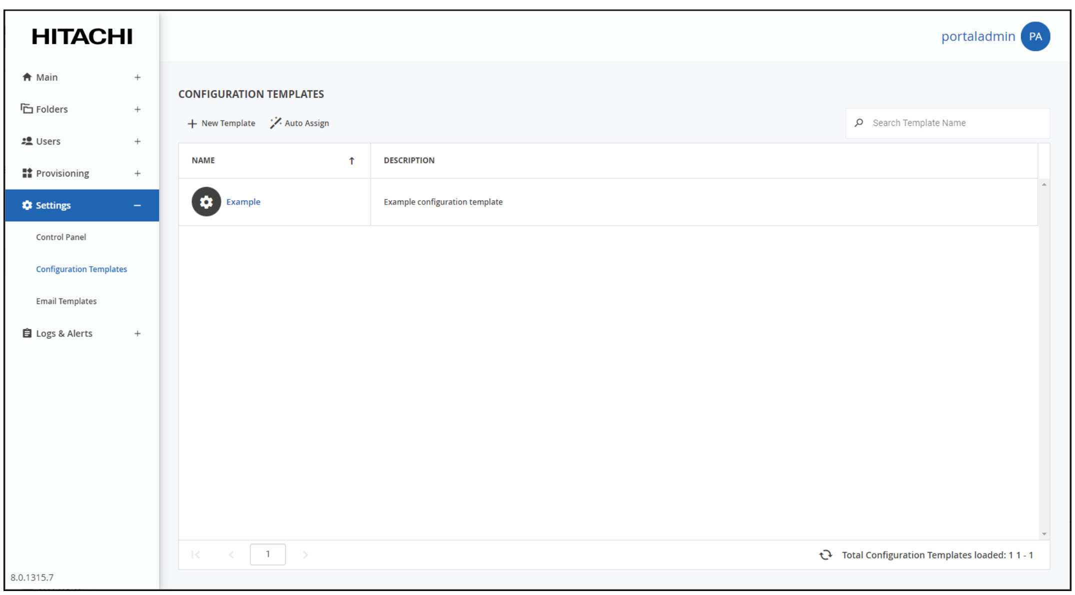


3. Click **Set Default**.

The selected template becomes the default template.

To stop a default template being the default:

1. Select **Settings > Configuration Template** in the navigation pane.
   The **CONFIGURATION TEMPLATES** page is displayed.



2. Either,
   - Select the default template's row and click **Remove Default**.
     No default template is configured.

   Or,
   - Select a different template's row to be the default template and click **Set Default.**

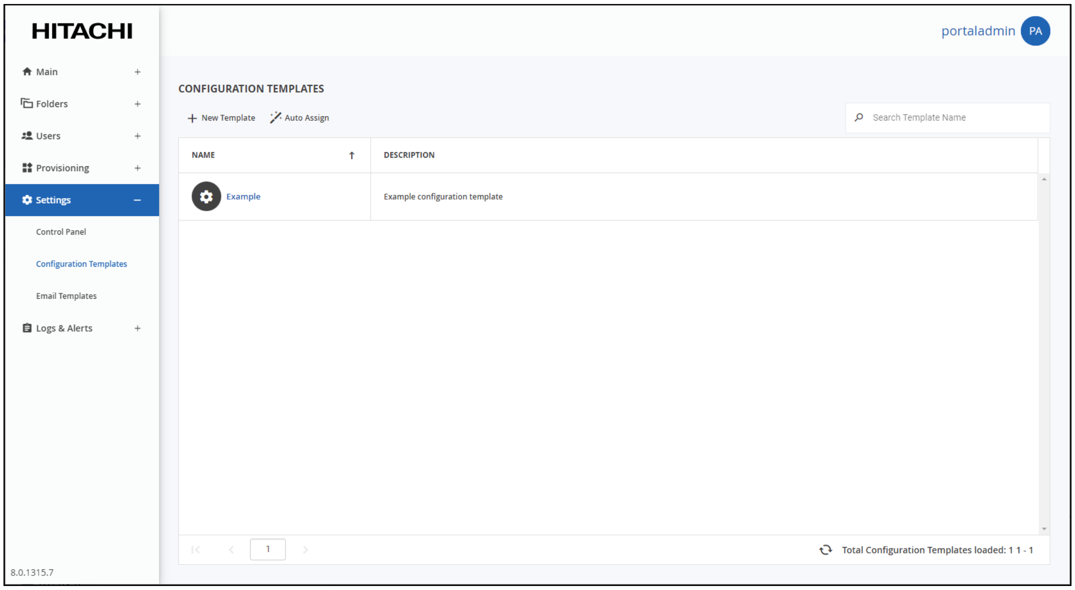
The newly selected template replaces the original template as the default template.

Duplicating Configuration Templates

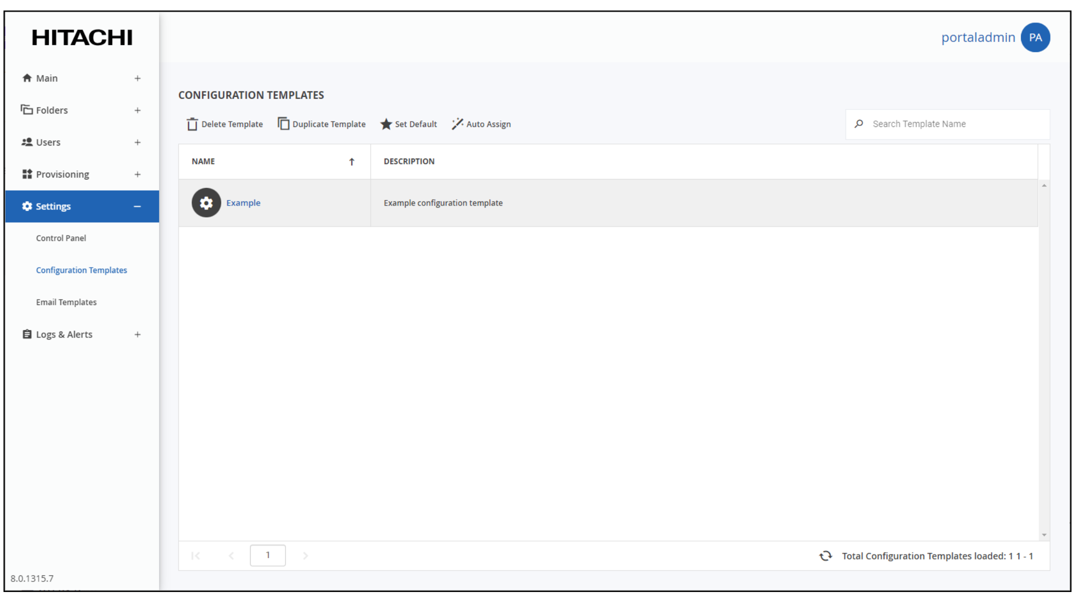
You can create a duplicate of an existing configuration template, then edit it as desired. All settings, except for the template name and description, are copied from the original template.

To duplicate a configuration template:

1. Select **Settings > Configuration Template** in the navigation pane.
   The **CONFIGURATION TEMPLATES** page is displayed.



2. Select the template's row.



3. Click **Duplicate Template**.

   A **New Configuration Template** window is displayed.
4. Enter the **Name** and, optionally, change the **Description** of the new template.
5. Click **SAVE**.

The new template is created with the same settings as the original template.

Chapter 17. Portal Logs

The portal **Log Viewer** includes the following logs:

Log	Content
System	Events that do not belong in other log categories.
Local Backup	This feature is currently not supported.
Cloud Sync	Cloud drive synchronization operations.
Access	User access to the HCP Anywhere Enterprise Portal events.
Audit	Changes to HCP Anywhere Enterprise Portal.
Agent	This feature is currently not supported.
Antivirus	Virus files detected by the portal antivirus function. This log is only displayed if the portal has an antivirus license.
Permanent Deletion	Log of folders and files permanently deleted.

Viewing logs for the HCP Anywhere Enterprise Portal system is available in the Global Administration View. Logs for team portals can be viewed in each virtual portal's view.

In this chapter

Understanding the Log Files

HCP Anywhere Enterprise products generate log messages upon various events. The log messages are divided by severity levels.

Level	Required Response
Emergency	System is unusable.
Alert	Action must be taken immediately.
Critical	Critical condition. A situation such as storage nearing full capacity has occurred. Action should be taken as soon as possible.
Error	Error condition. Action must be taken as soon as possible.
Warning	Warning messages. An indication that an error may occur if action is not taken.
Notice	Normal but significant condition.
Info	Informational message.
Debug	Debug-level messages, useful for debugging and troubleshooting.

Within each severity level, the log messages are divided in to topics. These topics enable you to understand the source of the message. For example, messages dealing with signing-in are included in the access topic.

Log messages are divided by one of the following topics:

- access
- accounting
- allTopics
- antivirus
- audit
- cloudsync
- files
- sync
- system

Example 1

Assume the following HCP Anywhere Enterprise Portal log message is received:

```
info,Login,Portal,,2023-10-11T01:32:05,,CTTP,Administration,Client
logged in to portal,172.21.1.15,,topic: access
```

- The first word indicates that this is an info message, and the next two words indicate that it is related to logging into the portal.
- The class is **UserLoggedInToPortal**
- The message is `Client logged in to portal`
- The additional attribute values are:
    - The protocol used – `CTTP`
    - The client IP address – `172.21.1.15`
    - The action – `Login`

The message is also timestamped (`2023-10-11T01:32:05`) with the type of message (`topic: access`).

Example 2

Assume the following HCP Anywhere Enterprise Portal log message is received:

```
error,Login,Portal,,2023-10-11T13:10:00,,,CTTP,Client login to portal
failed,,,failedPortal: portal.myportal.com reason: Login failed: Portal
portal.myportal.com does not exist failedDevice: IT topic: access
```

- The first word indicates that this is an error message, and the next two words indicate that it is related to logging into the portal.
- The class is UserLoggedInToPortalFailed
- The message is Client login to portal failed
- The additional attribute values are:
    - The client IP address – `172.21.1.15`

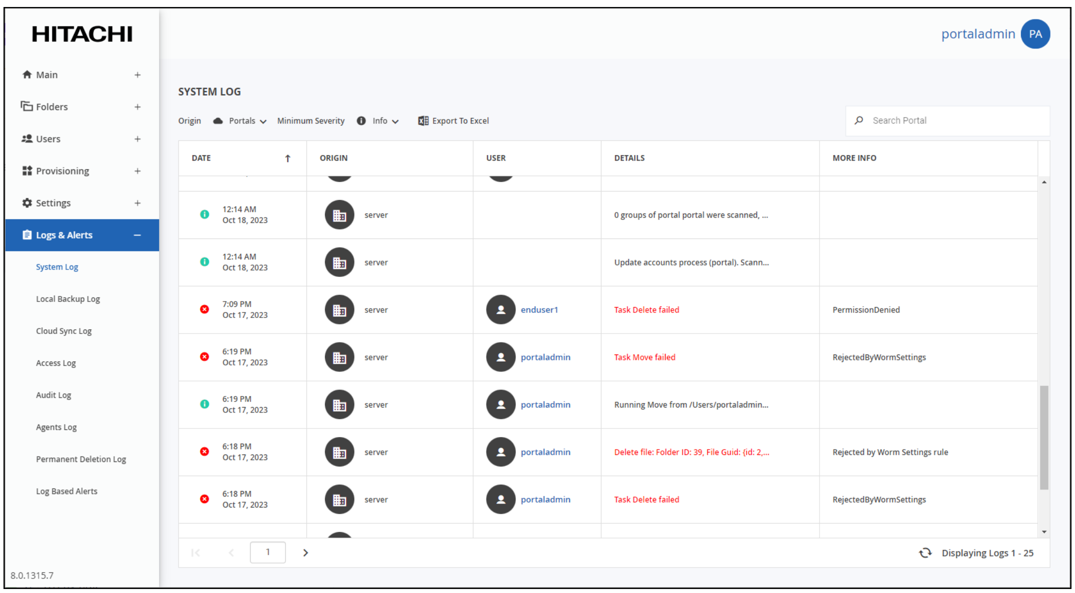
- The failed device – `IT`
- The portal that could not be logged in to – `portal.myportal.com`
- The reason – `Login failed: Portal portal.myportal.com does not exist`
- The protocol used – `CTTP`
- The action – `Login`

The message is also timestamped (`2023-10-11T13:10:00`) with the type of message (`topic: access`).

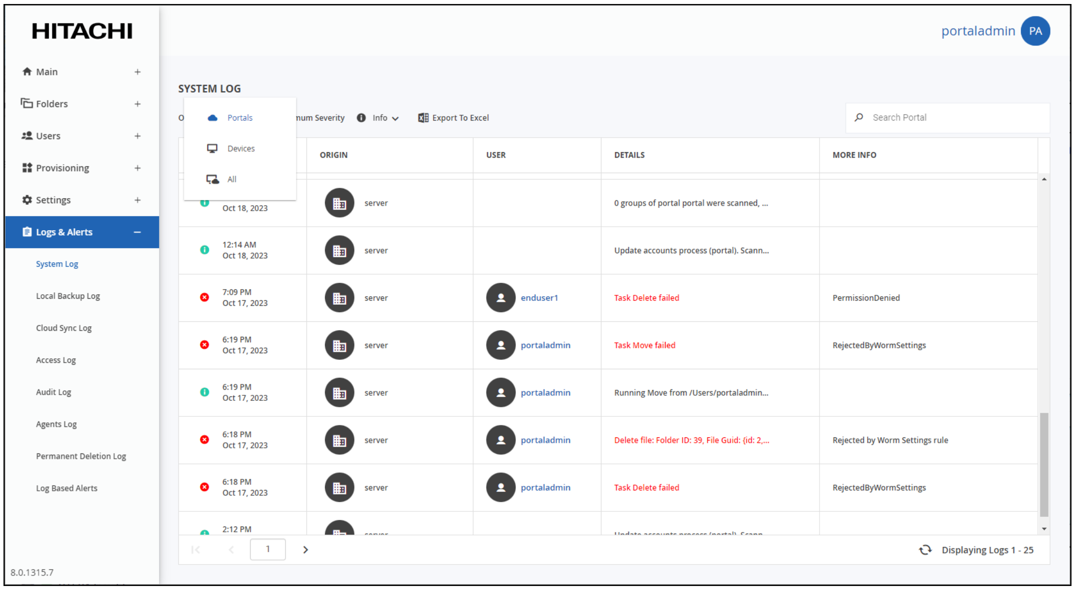
Viewing Logs

To view a log file in the user interface:

1. Select **Logs & Alerts** in the navigation pane.
   The **SYSTEM LOG** page opens, displaying the system log connected to the HCP Anywhere Enterprise Portal.



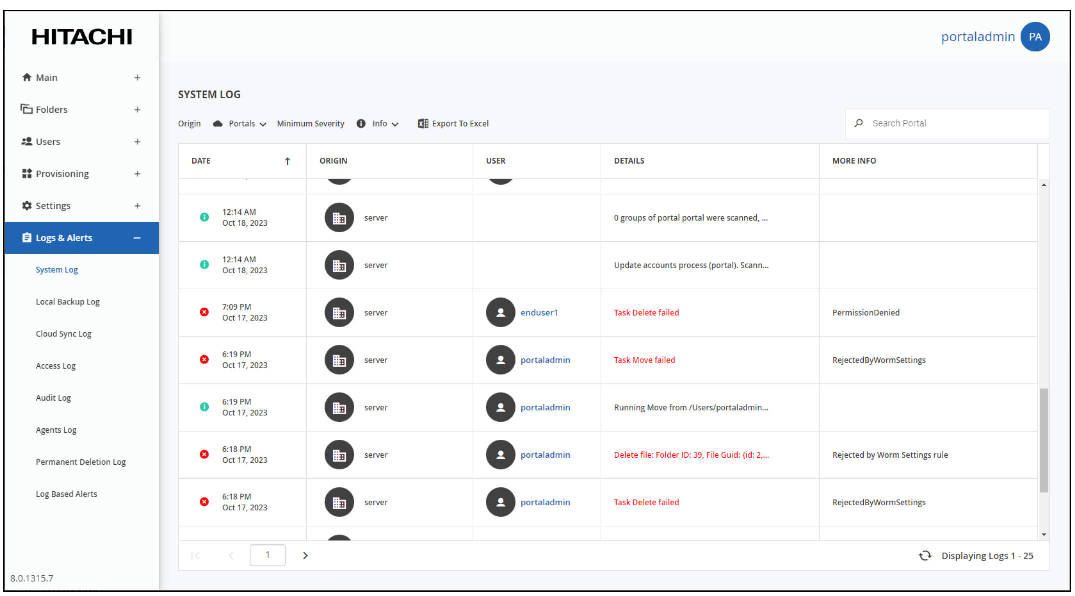
2. Select the log to view from the **Origin** list: **Portals**, **Devices**, or **All**.



The following logs are available:

- System Log
- Cloud Sync Log
- Access Log
- Audit Log
- Agent Log
- Antivirus Log
- Permanent Deletion Log

System Log



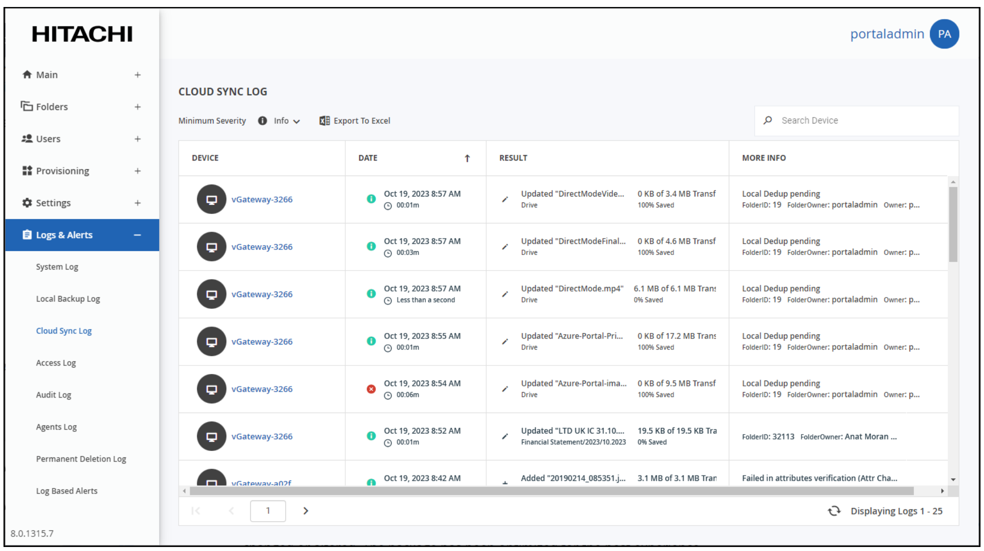
The information in the system log can be filtered by:

- The log origin: **Portals**, **Devices**, or **All** (both portal and devices).
- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **SYSTEM LOG** page includes the following columns:

Field	Display
DATE	The date and time at which the event occurred.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the user name.
DETAILS	A description of the event.
MORE INFO	A possible cause for the entry.

Cloud Sync Log



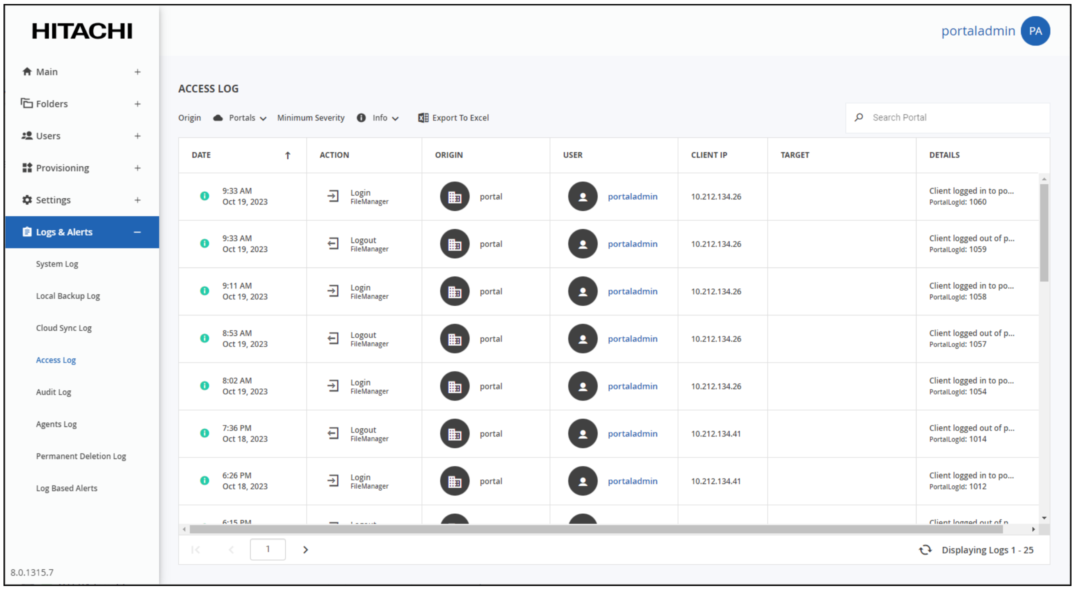
The information in the cloud sync log can be filtered by:

- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **CLOUD SYNC LOG** page includes the following columns:

Field	Display
DEVICE	The device name. To view details about the device, click the device name. The device details are displayed in a new browser window.
DATE	The date and time at which the event occurred.
RESULT	The result of the cloud sync.
MORE INFO	Additional information in cases where the sync was not successful.

Access Log



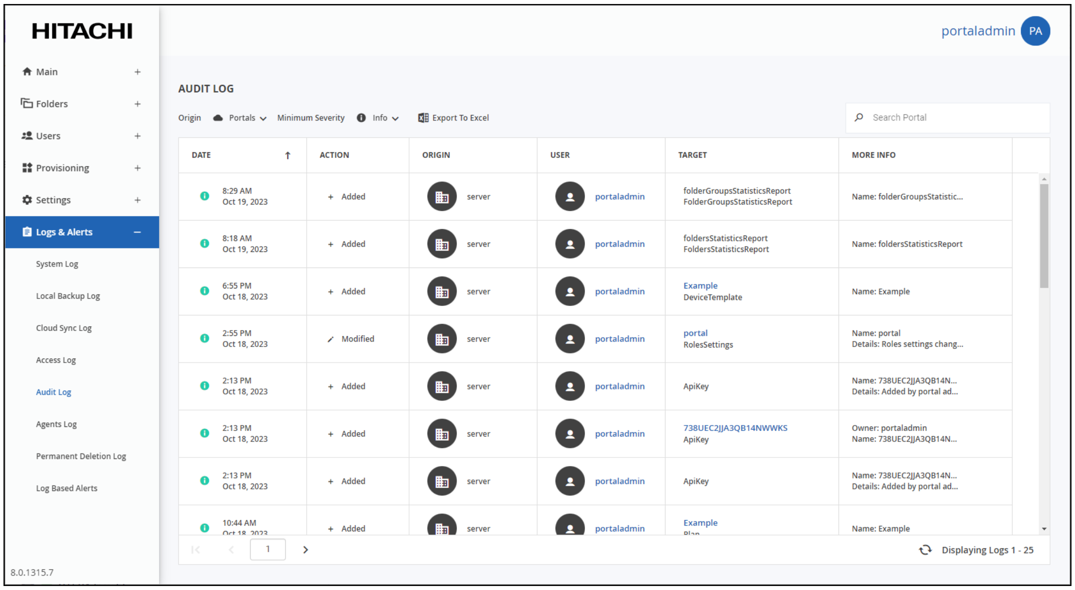
The information in the access log can be filtered by:

- The log origin: **Portals**, **Devices**, or **All** (both portal and devices).
- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **ACCESS LOG** page includes the following columns:

Field	Display
DATE	The date and time at which the event occurred.
ACTION	The action performed.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the user name.
CLIENT IP	The IP address from which the user triggered the event.
TARGET	The entity on which the action was performed.
DETAILS	A description of the event. For example, the user logged out and a file was shared for collaboration.

Audit Log



The information in the audit log can be filtered by:

- The log origin: **Portals**, **Devices**, or **All** (both portal and devices).
- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **AUDIT LOG** page includes the following columns:

Field	Display
DATE	The date and time at which the event occurred.
ACTION	The action performed: Added, Modified or Deleted.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the user name.
TARGET	The entity that was affected by the action. For example, a folder group or subscription plan, or user. To view details about the entity, click the entity name.
MORE INFO	Additional information about the event.

Agent Log

This feature is currently not supported.

The information in the Agent log can be filtered by:

- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **AGENTS LOG** page includes the following columns:

Field	Display
ACTION	The action performed.
DEVICE	The device name. To view details about the device, click the device name. The device details are displayed in a new browser window.
SOURCE	The user. To view details about the user, click the user name.
MORE INFO	Additional information about the event. For example, a software version was changed

Antivirus Log

Note: The Antivirus log is only available if the portal is licensed for antivirus and the subscription plan includes the antivirus option.

The information in the antivirus log can be filtered by:

- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **ANTIVIRYS LOG** page includes the following columns:

Field	Display
ACTION	The action performed.
FILE NAME	The name of the file moved to quarantine as a potential threat.
UPLOADER	The user who uploaded the file to the portal. To view details about the user, click the user name.
THREAT	The threat description.

Permanent Deletion Log

The information in the permanent deletion log can be filtered by:

- The minimum severity: **Debug**, **Info**, **Warning**, or **Error**.

The **PERMANENT DELETION LOG** page includes the following columns:

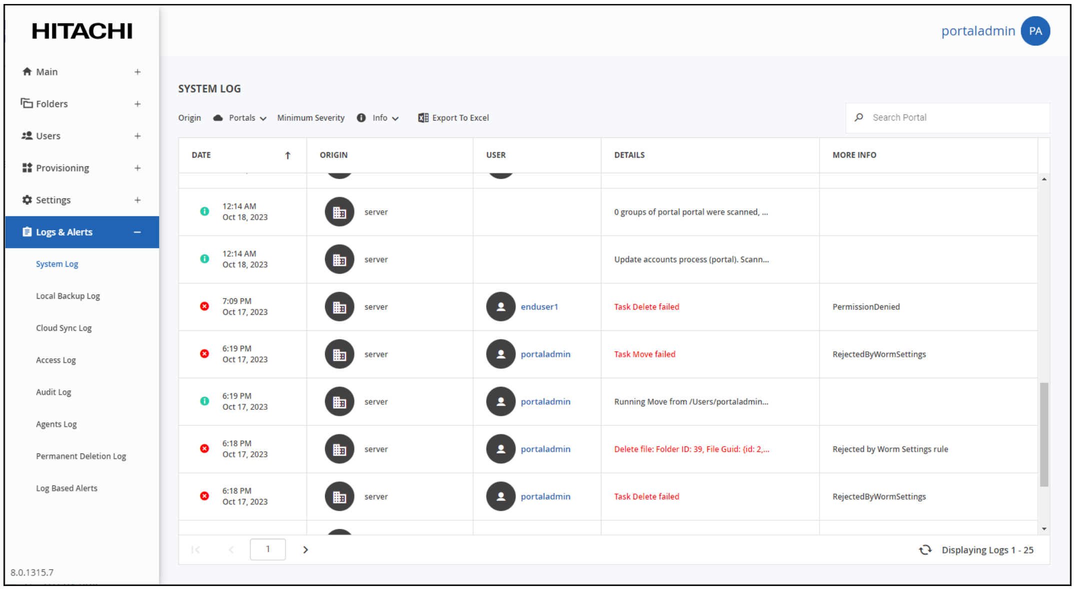
Field	Display
DATE	The date and time at which the event occurred.
USER	The user who triggered the deletion. To view details about the user, click the user name.
RESULT	The result of the deletion, whether successful or not.
REASON	The reason for the deletion that was entered in the **Permanent Deletion Wizard** in the **Verification** step.
ACTIONS	The actions performed. Clicking on **Details** displays the list of files deleted, with the file path and name and snapshot, last modified and more information about the deleted file.

Exporting Logs to Excel

You can export logs and their details to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export virtual portals to Excel:

1. Select the log to export under **Logs & Alerts** in the navigation pane.
   The log page, for example, the **SYSTEM LOG** page, is displayed.



2. Click **Export to Excel**.

The logs in the current log category are exported to your computer.

Managing Alerts Based on Log Events

You can configure the HCP Anywhere Enterprise Portal to automatically send email alerts to end users and administrators when specific log messages are generated.

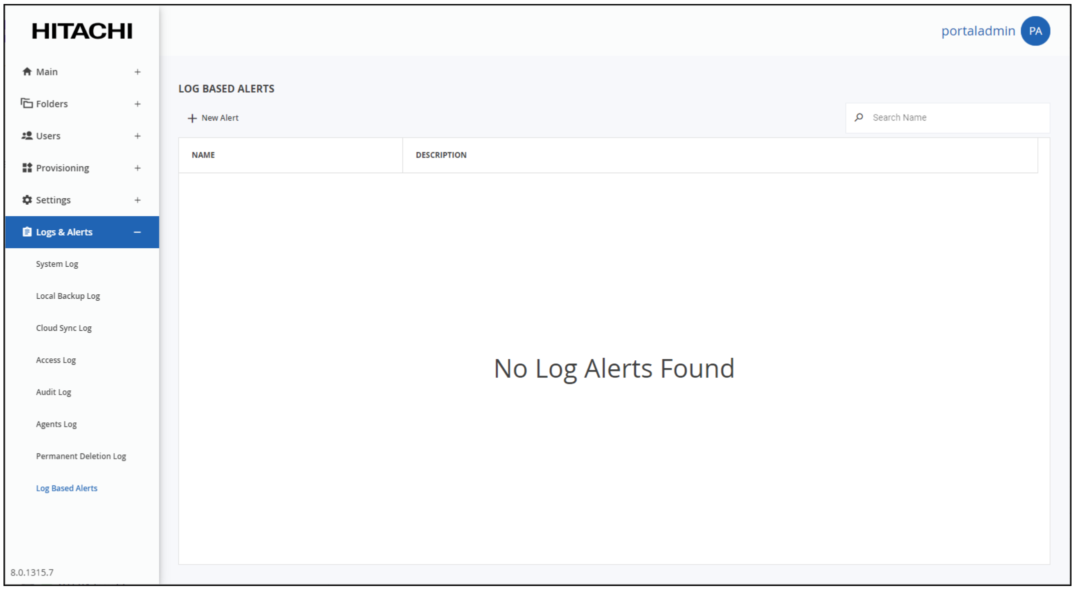
In this section

- Viewing Log Based Alerts
- Adding and Editing Alerts
- Deleting an Alert

Viewing Log Based Alerts

To view all log based alerts:

- Select **Logs & Alerts > Log Based Alerts** in the navigation pane.
  The **LOG BASED ALERTS** page is displayed.



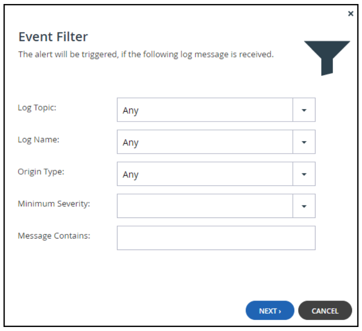
The page includes the following columns:

Field	Display
Name	The alert name.
Description	A description of the alert.

Adding and Editing Alerts

To add or edit an alert:

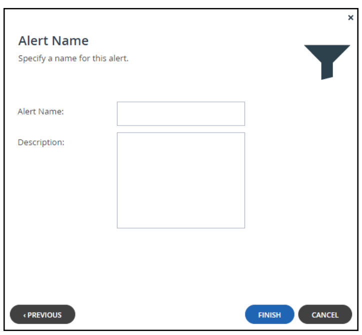
1. Select **Logs & Alerts > Log Based Alerts** in the navigation pane.
   The **LOG BASED ALERTS** page opens, displaying all the log based alerts.
2. To add a new alert-on, click **New Alert**.
   Or,
   To edit an existing alert, click the alert name**.**
   The **Event Filter** window is displayed.



3. Complete the fields.

   Log Topic – The category to trigger the alert. Select **Any** for any log category to trigger the alert.
   Log Name – The name of the log event to trigger the alert. Select **Any** for any event to trigger the alert.
   Origin Type – The entity from which a log must originate to trigger the alert. Select **Any** for any device or HCP Anywhere Enterprise Portal to trigger the alert.
   Minimum Severity – The minimum severity to trigger the alert.
   Message Contains – The text that the log message must contain to trigger the alert.
4. Click **NEXT**.

   The **Alert Name** window is displayed.



5. Complete the fields.

   Alert Name – A name for the alert.
   Description – A description of the alert.
6. Click **FINISH**.

Deleting an Alert

To delete an alert:

1. Select **Logs & Alerts > Log Based Alerts** in the navigation pane.
   The **LOG BASED ALERTS** page opens, displaying all the log based alerts.
2. Select the alert row.
3. Click **Delete.**

   A confirmation window is displayed.
4. Click **DELETE** to confirm.

The alert is deleted.

Chapter 18. Managing Reports

The HCP Anywhere Enterprise Portal provides reports for the following:

- Folders
- Folder Groups

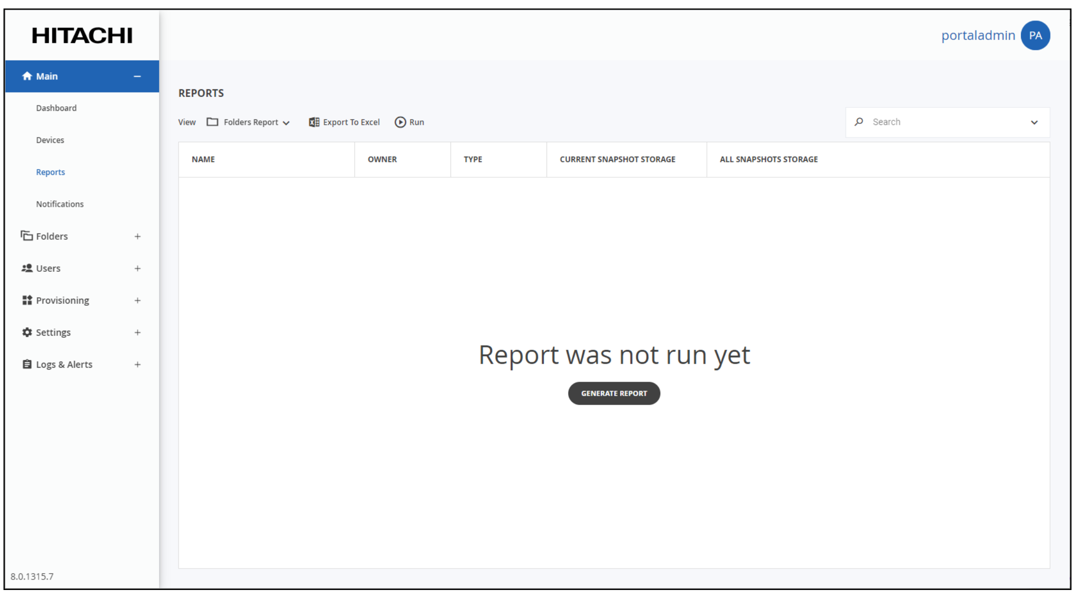
In this chapter

Viewing the Folders Report

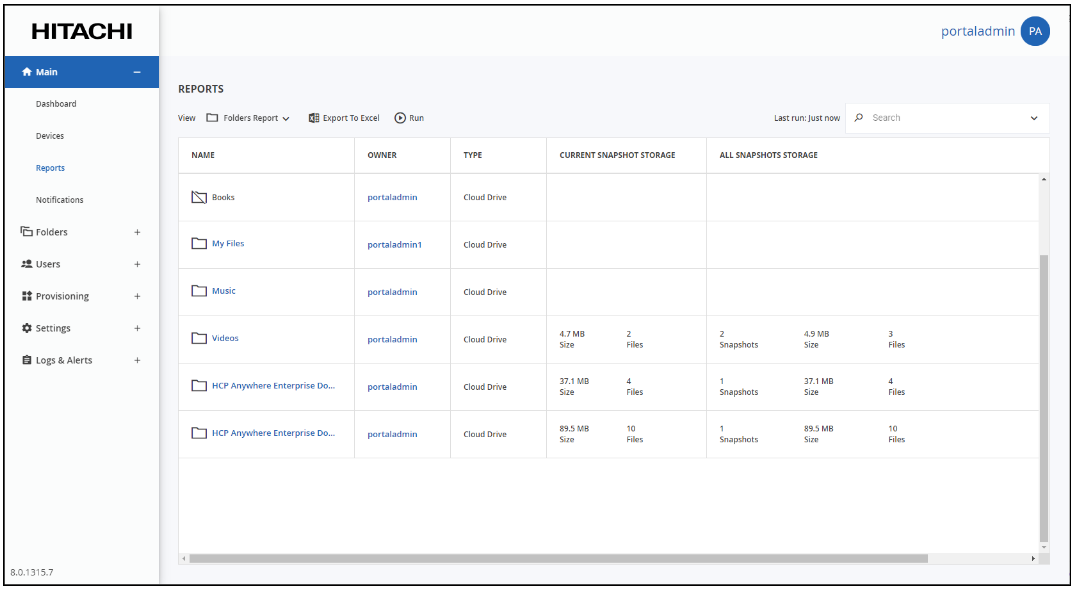
You can view detailed information about all folders, including deleted ones.

To view the Folders Report:

1. Select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.



2. Select **Folders Report** from the **View** drop-down list.
3. If a report was not yet run, click **GENERATE REPORT** or **Run**.



The following information is displayed.

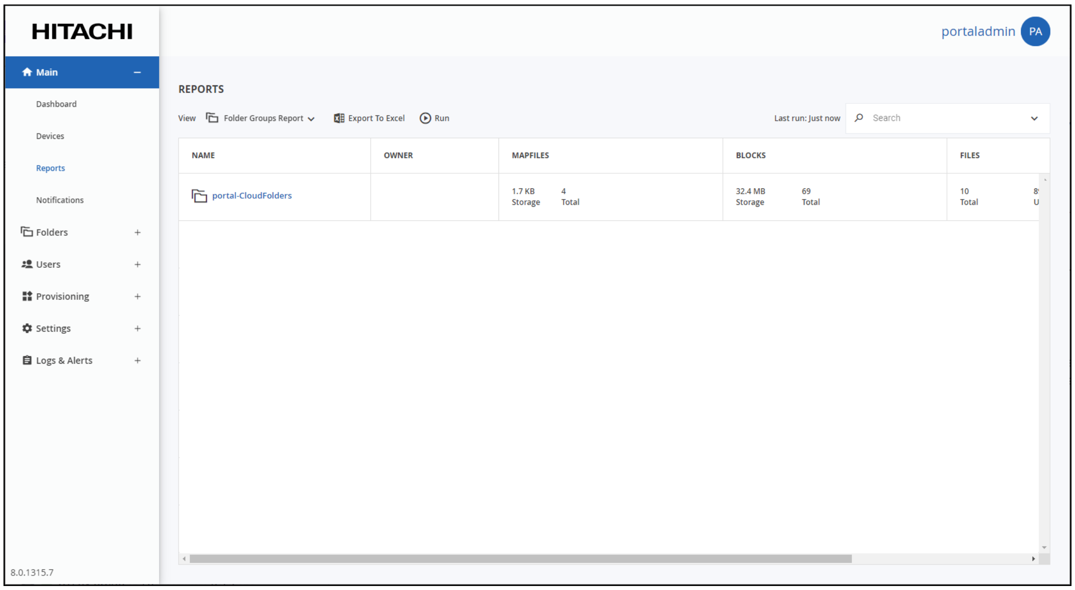
Field	Display
NAME	The folder's name.
OWNER	The folder's owner.
TYPE	The folder is a cloud drive folder.
CURRENT SNAPSHOT STORAGE	Details about the latest snapshot: • The storage quota allocated to this folder. If the quota is unlimited, this value is empty, otherwise, it displays the amount of the storage quota being used. The value is the logical storage before any deduplication, versioning and compression. • The amount of storage currently used by this folder. The value is the logical storage before any deduplication, versioning and compression. • The number of files in the current snapshot, the live file system, not including previous versions or deleted files, and the amount of storage required by these files.
ALL SNAPSHOT STORAGE	Details about all the snapshots storage for all devices: • The total number of snapshots that are currently maintained for this portal. The value depends on the retention policy. For details about the retention policy, see The Snapshot Retention Policy Options. • The size in bytes of the storage in the storage node for all the snapshots in the storage node for this portal. • The total number of files in all the snapshots. • The number of corrupted files, marked by FSCK. • Temporary files that represent incomplete uploads, in the *temp snapshot*. These files are automatically deleted within a few days. They are used for the purposes of keeping the blocks from being deleted so that HCP Anywhere Enterprise Portal is able to resume failed uploads.

Viewing the Folder Groups Report

You can view detailed information about all folder groups, including deleted ones.

To view the Folder Groups Report:

1. Select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.
2. Select **Folders Groups Report** from the **View** drop-down list.
3. If a report was not yet run, click **GENERATE REPORT** or **Run**.



The following information is displayed.

Field	Display
NAME	The folder's name.
OWNER	The folder's owner.
MAPFILES	Details about the mapfiles: • The amount of storage space consumed by this folder group. • The amount of space consumed by the mapfiles for this folder group. • The number of mapfiles currently being uploaded to folders belonging to this folder group. • The number of missing mapfiles in folders belonging to this folder group. • The total number of mapfiles in folders belonging to this folder group.

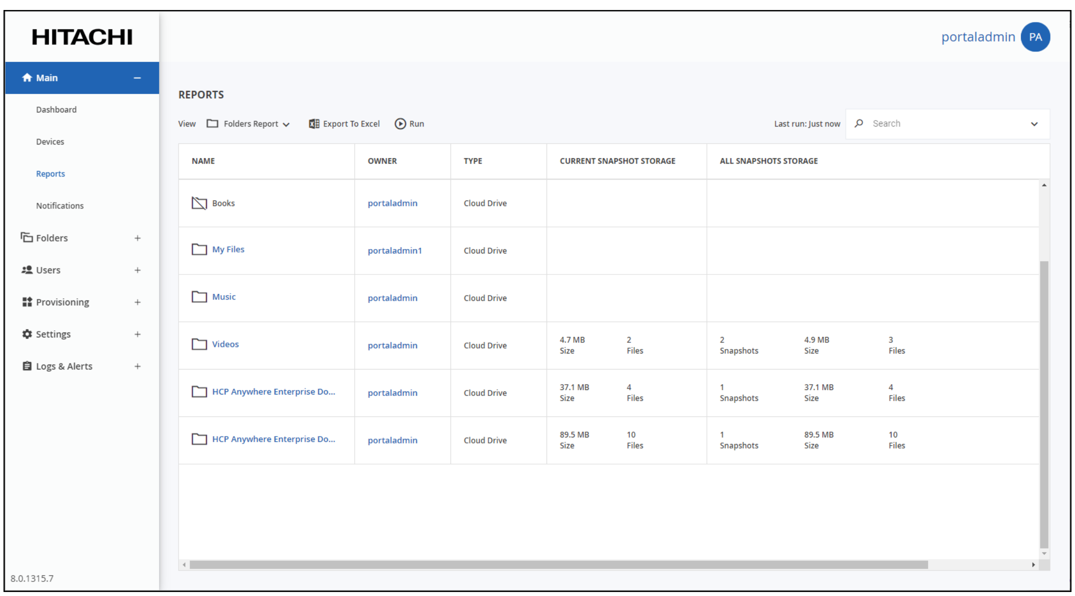
Field	Display
BLOCKS	Details about the blocks: • The total number of snapshots. • The number of uploaded blocks in folders belonging to this folder group. • The number of blocks currently being uploaded to folders belonging to this folder group. • The number of missing blocks in folders belonging to this folder group. • The number of files currently being uploaded.
FILES	• The total number of files in folders belonging to this folder group. • The number of folders belonging to this folder group. • The uncompressed size of the files in folders belonging to this folder group. • The number of files that are currently being uploaded to folders belonging to this folder group. • The size of files that are currently being uploaded to folders belonging to this folder group. • The number of corrupted files in folders belonging to this folder group.

Generating an Up-to-date Report

The **REPORTS** page shows the last time the report was generated. You can generate an up-to-date report.

To generate a report:

1. Select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.



2. Select the report to generate from the **View** drop-down list: **Folders Report** or **Folder Groups Report**.
3. Click **Run**.

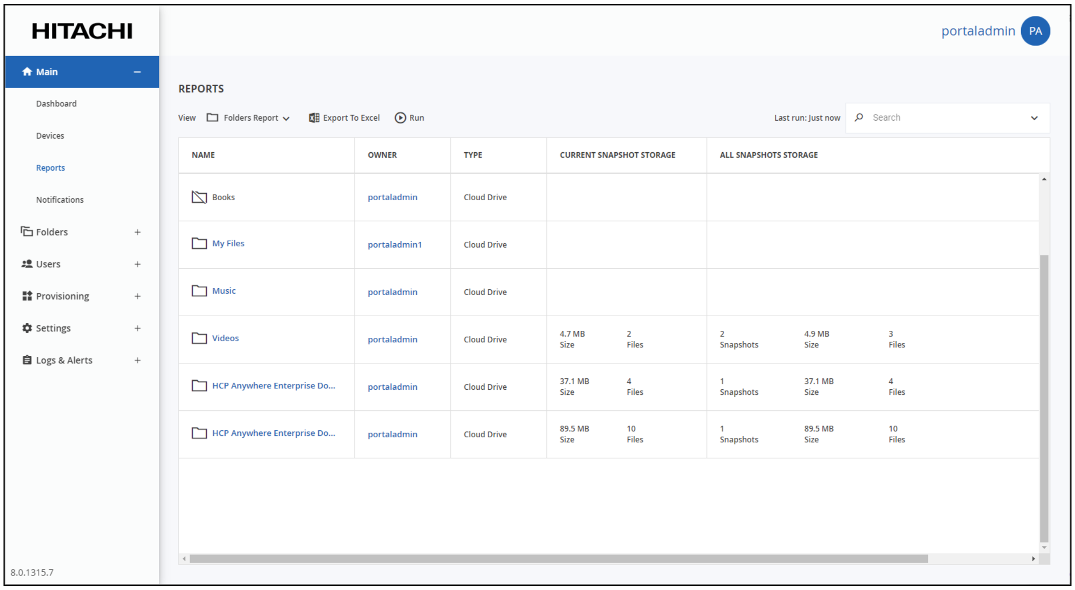
The up-to-date report is generated.

Exporting Reports to Excel

You can export the reports to a comma separated values (*.csv) Microsoft Excel file on your computer.

To export a report to Microsoft Excel:

1. Select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.



2. Select the report to be exported: **Folders Report** or **Folder Groups Report**.
3. Click **Export to Excel**.

The report is exported to your computer.

For the **Folders** report the following information is displayed.

Field	Description
Name	The folder's name.
Owner	The folder's owner.
Type	The type of folder.
Quota	The storage quota allocated to this folder. If the quota is unlimited, this value is zero (0). otherwise, it displays the amount of the storage quota being used.
Files	The number of files in the current snapshot.
Snapshots	The total number of snapshots.

Field	Description
Physical	The size in bytes of the storage in the storage node for all the snapshots in the storage node for this portal after deduplication and compression.
Files	The total number of files in all the snapshots.
Files in Upload	Temporary files that represent incomplete uploads, in the *temp snapshot*. These files are automatically deleted within a few days. They are used to keep the blocks from being deleted so that HCP Anywhere Enterprise Portal is able to resume failed uploads.
Bad Files	The number of corrupted files in the virtual portal, marked by FSCK.

For the **Folder Groups** report the following information is displayed.

Field	Display
Name	The folder's name.
Owner	The folder's owner.
Mapfile Overhead	The amount of space consumed by the mapfiles for this folder group in bytes.
Total Mapfiles	The total number of mapfiles in folders belonging to this folder group.
In Upload Mapfiles	The number of mapfiles currently being uploaded to folders belonging to this folder group.
Missing Mapfiles	The number of missing mapfiles in folders belonging to this folder group.
Blocks Storage Space	The amount of block storage space consumed by this folder group in bytes.
Uploaded Blocks	The number of uploaded blocks in folders belonging to this folder group.
In Upload Blocks	The number of blocks currently being uploaded to folders belonging to this folder group.
Total Files	The total number of files in folders belonging to this folder group.
Uncompressed Size	The uncompressed size of the files in folders belonging to this folder group.
Files in Upload	The number of files that are currently being uploaded to folders belonging to this folder group.
Bad Files	The number of corrupted files in folders belonging to this folder group.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com