Hitachi Content Platform Anywhere Enterprise

v8.0

Portal Global Administration Guide

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

MK-HCPAE003-01
December 2023

Contents

Preface

About this document

This book describes Hitachi Content Platform Anywhere Enterprise Portal for a global 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 Edge Filer users from a macOS PC.

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 HCP Anywhere Enterprise Portal Global Administration

HCP Anywhere Enterprise Portal is a scalable cloud service delivery platform that you install at your own data center or in a cloud environment and use to create, deliver and manage cloud storage applications, including a Global File System, file access via stubbing/caching, backup, and mobile collaboration.

HCP Anywhere Enterprise Portal facilitates access to cloud storage services; handles data protection and file sync & share services; used for provisioning and monitoring global file services. This is the beating heart of the system and is the component that will run in the customer's datacenter or VPC. 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. You extend the global file system to users, via HCP Anywhere Enterprise Edge Filers, HCP Anywhere Enterprise Drive Share (agents), and HCP Anywhere Enterprise 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 Portal enables you to create one or more tenants, called team or virtual portals. These tenants are accessed by end-users and management staff via web-based interfaces. HCP Anywhere Enterprise Edge Filers and endpoint HCP Anywhere Enterprise Agents 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 as well as individual endpoints – up to hundreds of thousands of connected devices – with no need for on-site IT presence in remote locations.

Files are centrally stored and protected, while users can easily access them everywhere. On top of the all-in-one global namespace/filesystem approach, Hitachi Vantara allows its customers to achieve the following goals:

Military-grade security – A private and secure architecture powered by end-to-end encryption, advanced authentication, anti-virus, DLP, and behind-the-firewall deployment.

Global deduplication – Most modern storage solutions apply deduplication only to centrally stored files. Hitachi Vantara has taken deduplication to the next level, applying the algorithms at both cloud and edge. Not only does the Portal support global deduplication, but HCP Anywhere Enterprise Edge Filers and HCP Anywhere Enterprise Drive Share clients offer source-based deduplication, greatly reducing the size of files being sent to the cloud and lowering storage costs substantially.

WAN optimization – To overcome bandwidth and latency limitations, a slew of optimization techniques are used in order to reduce file sizes and transfer times to/from any access point.

Intelligent caching – Every HCP Anywhere Enterprise Edge Filer and HCP Anywhere Enterprise Drive Share application comes with a built-in file cache. Caching accelerates remote access, plus it enables access points to “view” the full file storage space, and have on-demand access to every available file.

Managing a large global file system, with thousands of access points and tens of thousands of users, can be quite challenging. To simplify the process and support scale, to tens of thousands of users and sites, the HCP Anywhere Enterprise Portal comes with advanced management tools, including template-based automation. In addition, HCP Anywhere Enterprise Portal comes with rich activity dashboards and analytics, allowing administrators to observe, monitor and troubleshoot every aspect of their global file system.

A HCP Anywhere Enterprise Portal installation comprises a cluster of one or more VMs (servers). Each server can host any combination of the following services:

- **Main database**. Only one server can host the main database. The server that hosts the main database is called the primary server.
- **Secondary replication server**. A passive database service to replicate the primary server. During server installation, you can turn on the replication service and select the primary server from which to replicate.
- **Application service**. This server accepts connections and handles requests from Web and CTTP clients. Application servers are added to the cluster to increase client handling capacity. Any servers that are enabled as application servers automatically balance the connected clients between them, allowing for maximized capacity and availability.
- **Messaging server**. This server enables sending notifications from the HCP Anywhere Enterprise Portal to various consumers, for example the Varonis Data Security Platform, which is a connector running on top of the HCP Anywhere Enterprise Messaging Service. In production environments that use the messaging service, the HCP Anywhere Enterprise Portal must include three application servers defined as messaging servers.
- **Document preview server**. This server is used to process document preview requests. The document preview server supports high availability. You can install one or more servers, in order to ensure uninterrupted document preview generation and redundancy in the event of a server failure.

Team portals can be defined within a single HCP Anywhere Enterprise Portal installation. The global administrator manages the creation and default settings for team portals.

Team Portal (Tenant)

A team portal is designed for the needs of a company or team with multiple members. The users in the team portal are the team members.

Team portals are managed by team administrators, who are team members with the Administrator role. For information on managing team portals, see the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

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.

When multiple team portals are created, the HCP Anywhere Enterprise Portal global administrator can assign each team portal to a different organizational unit within the company or team. Each organizational unit can sign in to their own virtual portal and manage their settings. In contrast, the HCP Anywhere Enterprise Portal owner can access and manage the contents of any team portal, as well as manage global settings across all virtual portals.

Global Provisioning

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

The HCP Anywhere Enterprise Portal owner provisions each virtual portal owner with services and quotas. For example, it is possible to limit a virtual portal to use a total of up to 100GB of storage space.

The following provisioning methods are available for portal-level provisioning:

- **Global plans**
  In order to obtain services, virtual portals are assigned to a global plan which defines a set of services that the portal will receive, and which will subsequently be used by the portal's end users. Further, the plan can specify a maximum snapshot retention policy for the portal. See Managing Snapshots.
- **Global add-ons**
  In addition to the global plan, one or more global add-ons can be added to portals. Each global add-on defines a set of services that portals will receive in addition to the services specified in the global plan. For example, an add-on may include an additional 10 GB of storage space for the number of devices specified in the global plan. Add-ons can be set to expire after a specified time period and can be stacked as desired. For example, a portal may have a subscription plan for 100 GB of storage, as well as two add-ons for 10GB of storage and one add-on for 5GB of storage. While the add-ons are valid, the portal will be entitled to allocate up to 125GB of cloud storage to end users.

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 portal either on-premise or in a virtual private cloud (VPC) to keep your data within your network and 100% behind your firewall.
- 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.
- HCP Anywhere Enterprise Portal uses cryptographic libraries certified with FIPS 140-2.
- 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, EMM and DLP tools ensure that security and governance follow the data.

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.

Devices

HCP Anywhere Enterprise Portal connects to the following devices:

- HCP Anywhere Enterprise Edge Filers
- HCP Anywhere Enterprise Drive Share (Agents)
- HCP Anywhere Enterprise Drive Connect

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.

Chapter 2. Getting Started

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 HCP Anywhere Enterprise Portal
- Managing the servers on which HCP Anywhere Enterprise Portal is installed
- Creating and configuring virtual portals
- Provisioning the virtual portals

Each virtual team portal also has its own administration interface. As a global administrator, you can access the global administration interface and each virtual portal's administration interface to perform administration tasks for all virtual portals and also to perform specific administration tasks for a specific HCP Anywhere Enterprise Portal.

The interface includes the following views:

Administration view – Enables you to perform administration tasks that are global, affecting all virtual portals. The tasks described in this guide are performed in this view.

Virtual portal view – Enables you to perform administration tasks for each team portal. Administrators of a team portal can perform the same tasks via the team portal administration interface, which is almost identical to this view. For information about administering a team portal, see the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

Signing In To the HCP Anywhere Enterprise Portal

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

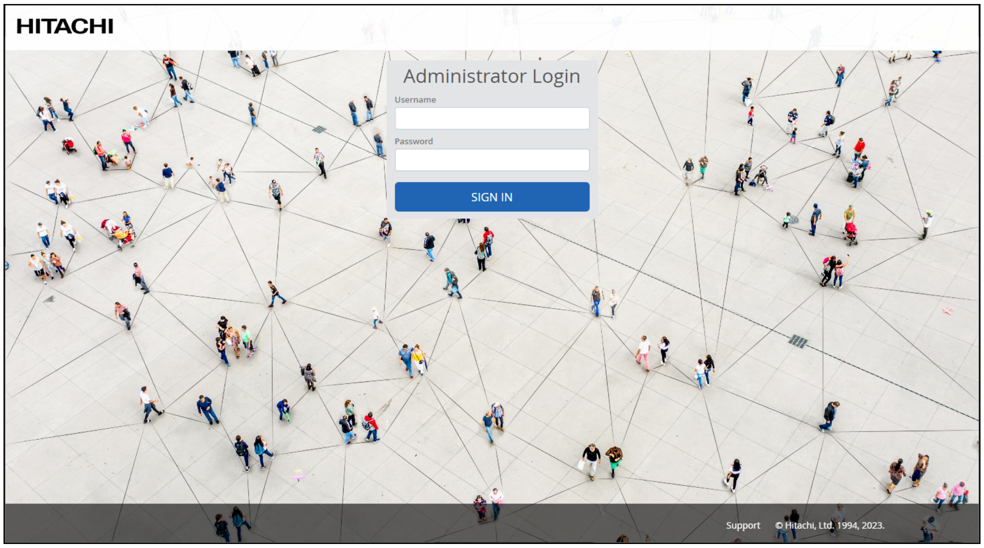
To sign in to the global administration interface you use the IP address of the HCP Anywhere Enterprise Portal server. If the DNS service is set up, you can use it with the HCP Anywhere Enterprise Portal's DNS suffix and, if changed from the default, the HTTPS access port number.

To sign in to the global administration interface:

1. In a Web browser open `http://<virtualportal_name>.<DNS_Suffix>/admin` where, *virtualportal_name* is the name of any one of the virtual portals defined in HCP Anywhere Enterprise Portal, and *DNS_Sufix* is the DNS suffix for the HCP Anywhere Enterprise Portal installation.

   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>/admin`
   where *HTTPS_port* is a customized port. See The HTTPS Access Port. For example, to connect to *Example*'s administration HCP Anywhere Enterprise Portal using HTTPS port 2222, use the following address:
   `https://CompanyPortal.example.com:2222/admin`.

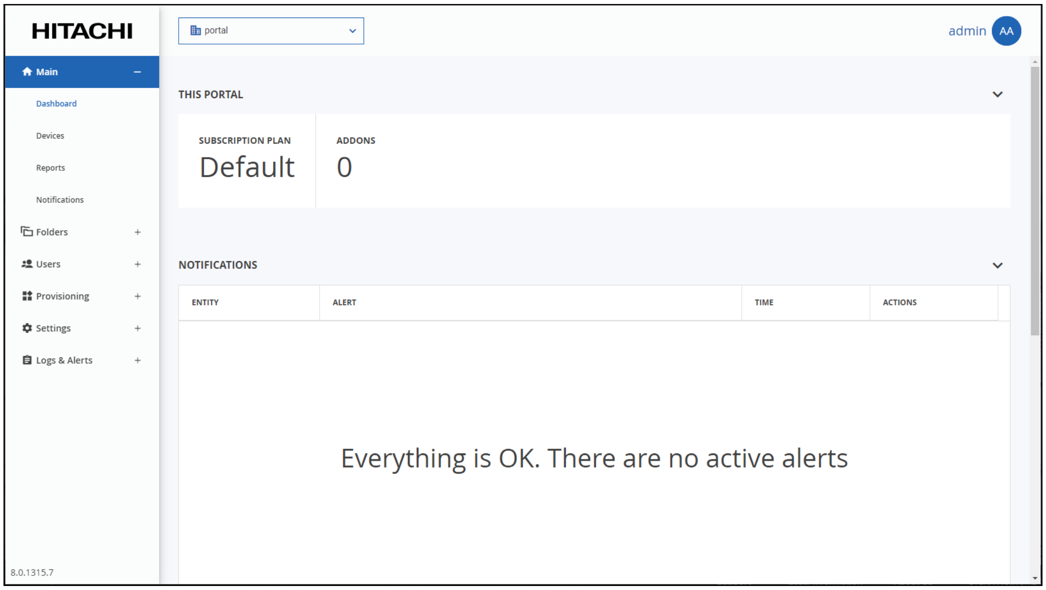
   Or,
   Open `http://<Portal_Server_IP>/admin` where *Portal_Server_IP* is the IP address of one of the HCP Anywhere Enterprise Portal servers. For example, to connect to the global administration view of a HCP Anywhere Enterprise Portal whose server IP address is 192.168.10.10, open `http://192.168.10.10`. This method enables you to gain access to the administration view, if the DNS service is not set up.
   After connecting, you can switch to any specific virtual portal view or back to the administration view, as described in Navigating Between Portal Views.
   The HCP Anywhere Enterprise Portal opens, displaying the sign in page.



If SAML Single Sign-on (SSO) is enabled, on your first access to the HCP Anywhere Enterprise Portal you are redirected to the SAML 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 administration interface opens displaying the **Main > Dashboard** page of the default team portal.



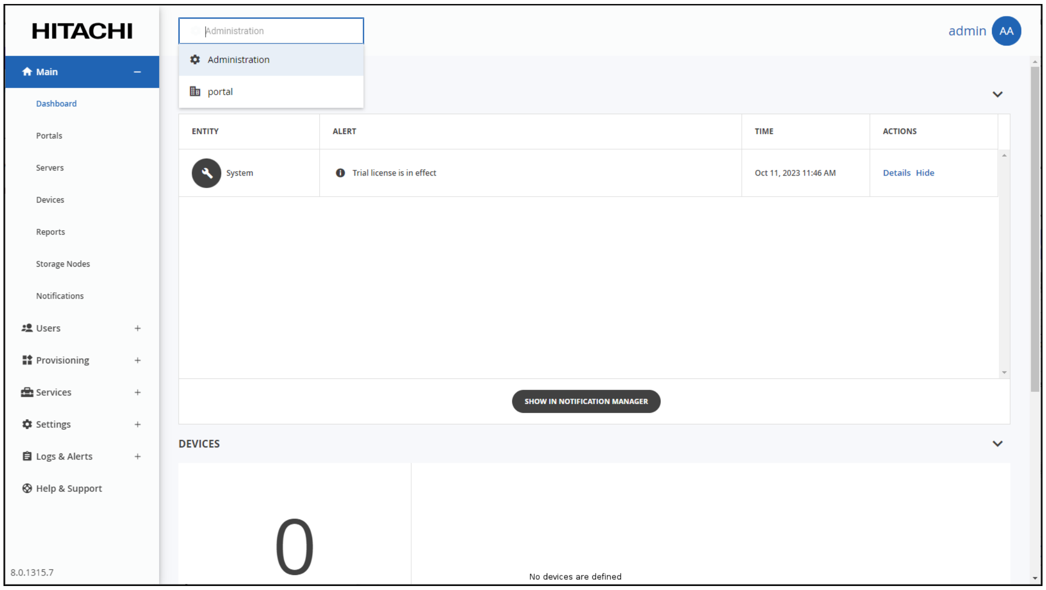
SUBSCRIPTION PLAN: Default
ADDONS: 0

ENTITY	ALERT	TIME	ACTIONS

Everything is OK. There are no active alerts

   For information about administering a team portal, see the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

3. In the view setting drop-down box at the top of the page, change the view to **Administration**.

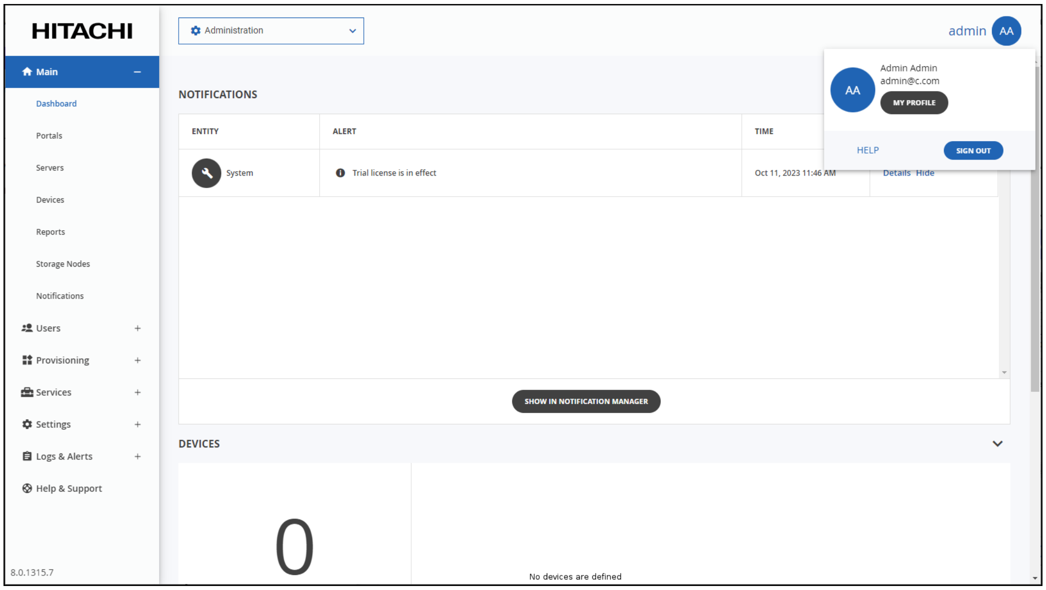


ENTITY	ALERT	TIME	ACTIONS
System	Trial license is in effect	Oct 11, 2023 11:46 AM	Details Hide

The Global Administrator User Interface

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

Top bar – The list of HCP Anywhere Enterprise Portals in a drop-down and the user name at the top right. Clicking the avatar or administrator initials next to the name displays additional controls, such as access to the documentation.



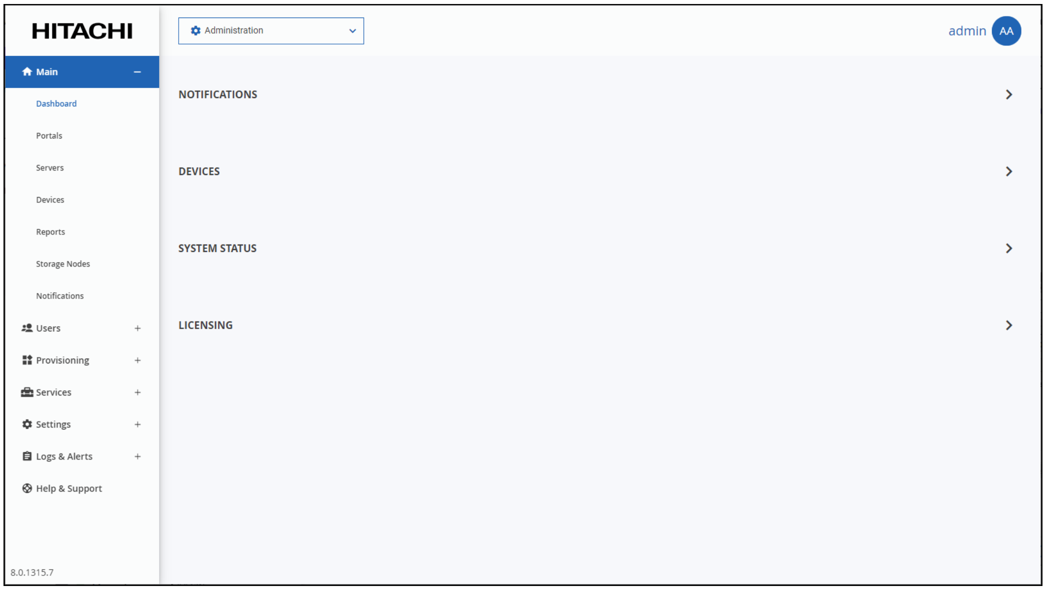
ENTITY	ALERT	TIME	
System	Trial license is in effect	Oct 11, 2023 11:46 AM	Details Hide

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

Content – Displays the HCP Anywhere Enterprise Portal pages.

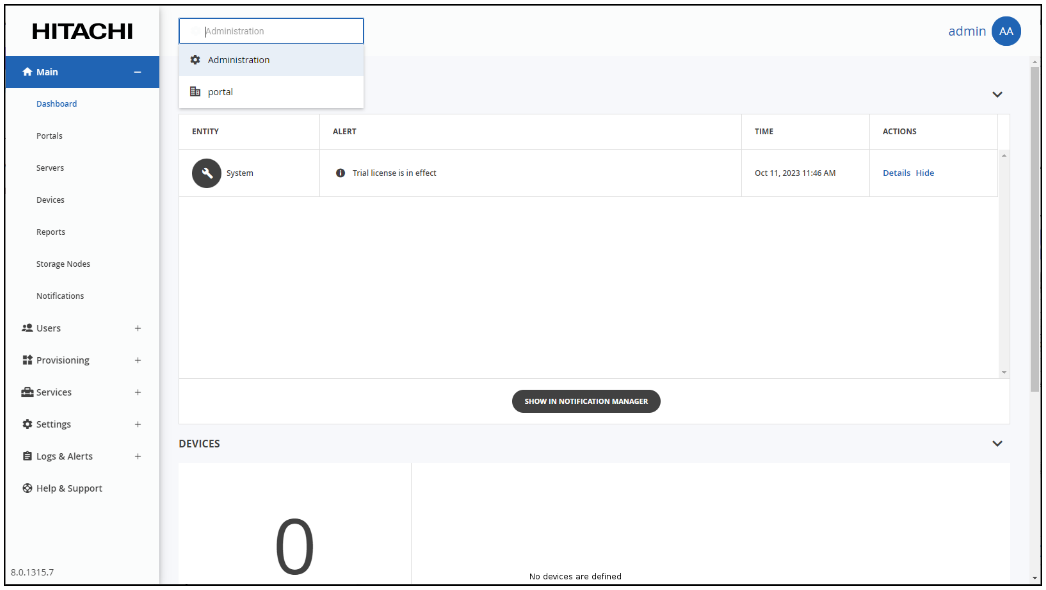
The Main Dashboard

The dashboard displays an overview of the HCP Anywhere Enterprise Portal.



Viewing Notifications in the Main Dashboard

The dashboard displays a summary of the highest priority active notifications.

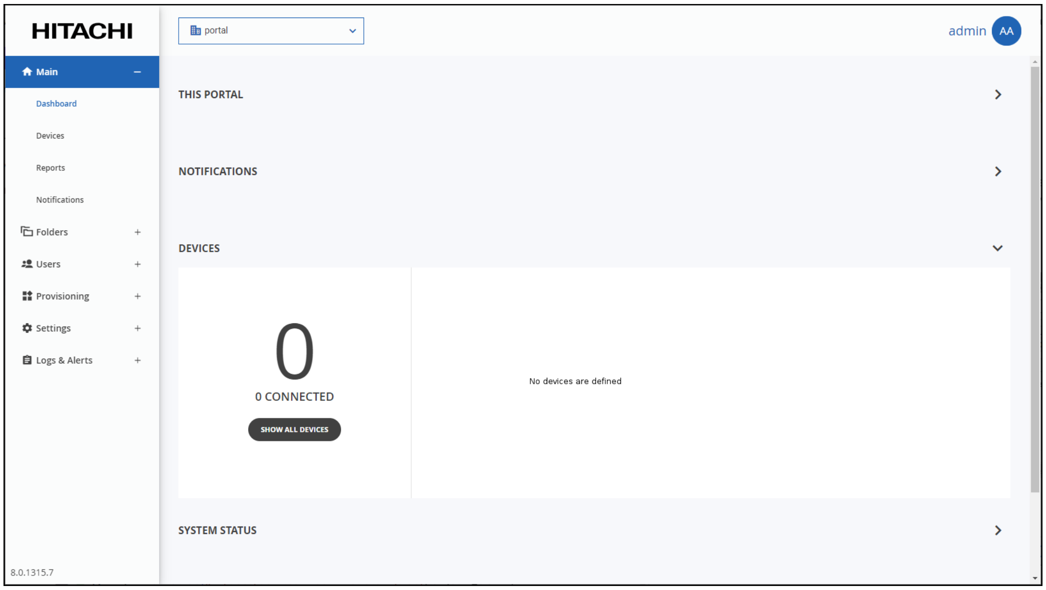


ENTITY	ALERT	TIME	ACTIONS
System	Trial license is in effect	Oct 11, 2023 11:46 AM	Details Hide

If there are notifications you can go directly to the **NOTIFICATIONS** page by clicking **SHOW IN NOTIFICATION MANAGER**. For more details about notifications, see Managing HCP Anywhere Enterprise Portal Notifications and Email Templates.

Viewing Devices in the Main Dashboard

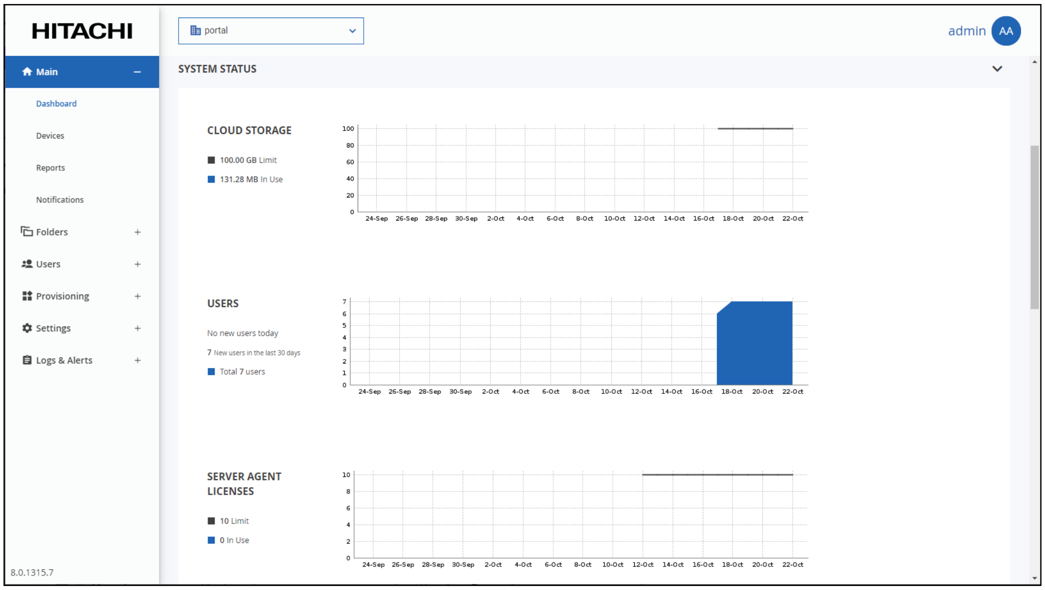
The dashboard displays a summary of devices registered with the HCP Anywhere Enterprise Portal. The information includes the total number of registered devices and the actual number connected at that time. A pie chart shows the different types of devices, such as server agents and different licensed HCP Anywhere Enterprise Edge Filers with the licenses (EV16, EV32, etc.).



You can go directly to the **DEVICES** page by clicking **SHOW ALL DEVICES**. For more details about notifications, see Managing Devices.

Viewing the System Status in the Main Dashboard

The dashboard displays a summary of the system over time, including the cloud storage limit and actual use, the number of users and how many new users for that day as well as details of the licenses usage.



SYSTEM STATUS

CLOUD STORAGE

- ■ 100.00 GB Limit
- ■ 131.28 MB In Use

USERS

No new users today

7 New users in the last 30 days

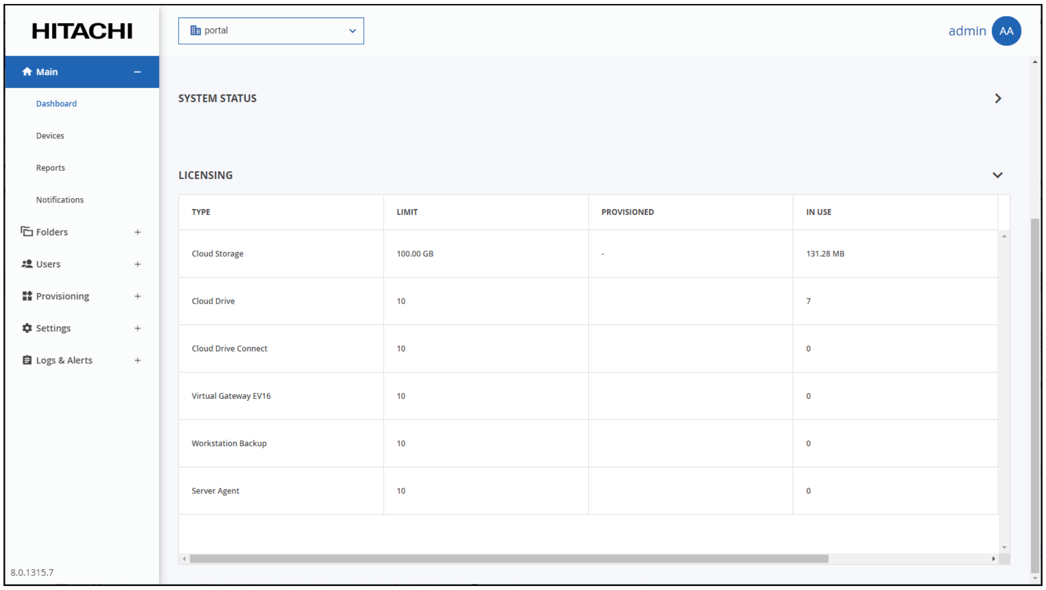
- ■ Total 7 users

SERVER AGENT LICENSES

- ■ 10 Limit
- ■ 0 In Use

Viewing Licensing in the Main Dashboard

The dashboard displays a summary of the each license limit, the licenses provisioned, the provisioned licenses used, and the remaining license available from the provisioned licenses.



SYSTEM STATUS

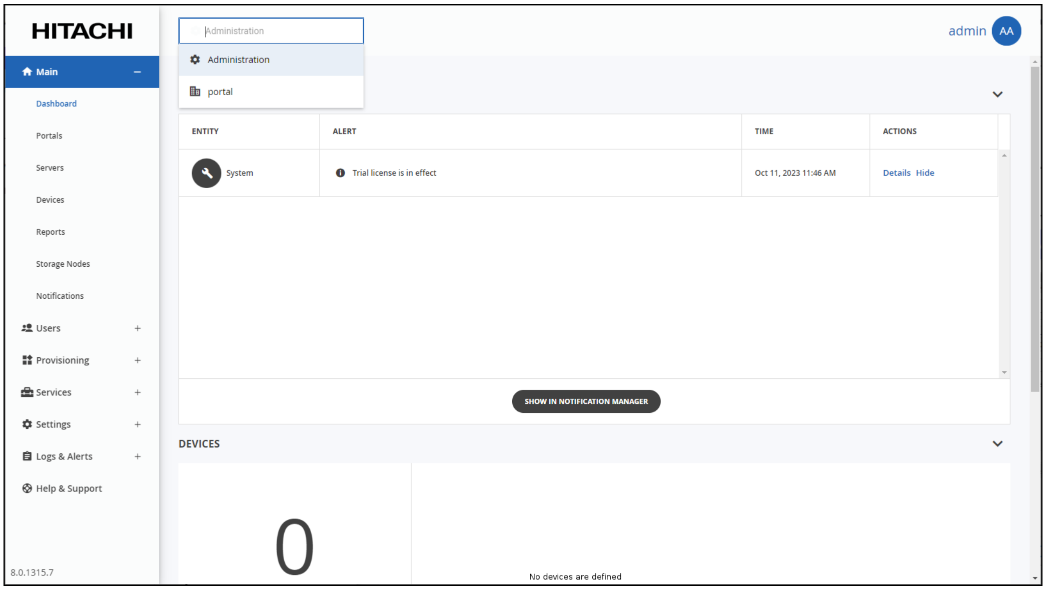
LICENSING

TYPE	LIMIT	PROVISIONED	IN USE
Cloud Storage	100.00 GB	-	131.28 MB
Cloud Drive	10		7
Cloud Drive Connect	10		0
Virtual Gateway EV16	10		0
Workstation Backup	10		0
Server Agent	10		0

Navigating Between Portal Views

To navigate between the administration view and a specific virtual portal view:

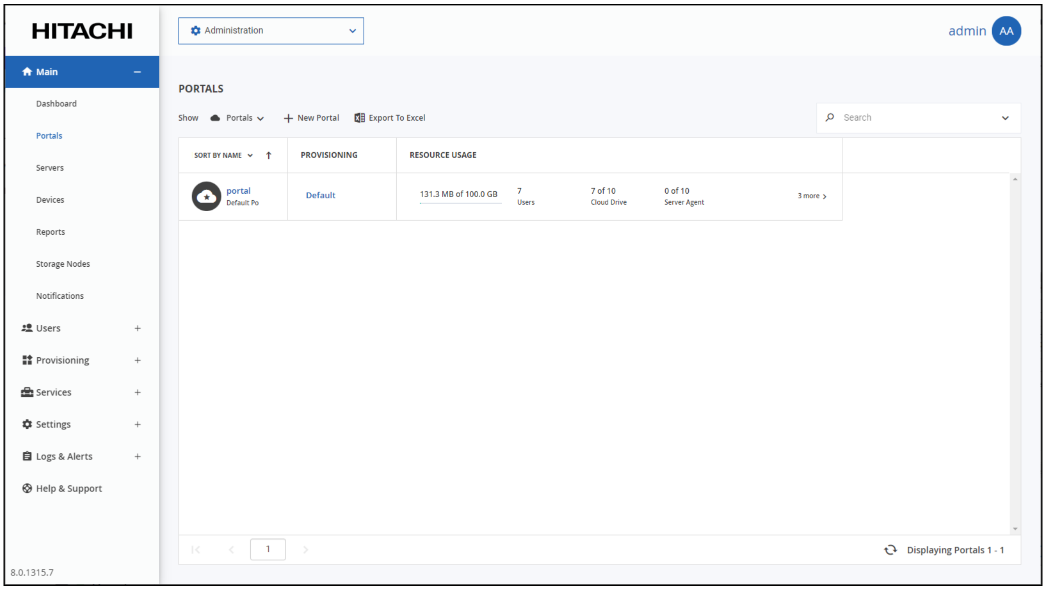
1. Open the HCP Anywhere Enterprise Portal drop-down list in the top bar.



ENTITY	ALERT	TIME	ACTIONS
System	Trial license is in effect	Oct 11, 2023 11:46 AM	Details Hide

2. Select **Administration** or the virtual portal you want to manage. You can start typing the name of the HCP Anywhere Enterprise Portal in the drop-down to filter the names displayed in the drop-down.

Note: If there are too many HCP Anywhere Enterprise Portals to list in the drop-down, you can also choose **Main > Portals** in the navigation pane of the administration view and scroll to the HCP Anywhere Enterprise Portal you want.



SORT BY NAME	PROVISIONING	RESOURCE USAGE				
portal Default Po	Default	131.3 MB of 100.0 GB	7 Users	7 of 10 Cloud Drive	0 of 10 Server Agent	3 more

Click the ✎ icon, which is displayed when moving the mouse over the name in the **SORT**

BY NAME column, to open the administration view for that HCP Anywhere Enterprise Portal.

For information about administering each team portal, see the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

Access URLs for Administrators and End Users

The global administration interface is accessible via the IP address of any of the HCP Anywhere Enterprise Portal servers. HCP Anywhere Enterprise recommends using IP address access for testing environments. For production environments, HCP Anywhere Enterprise recommends configuring the DNS service.

The URL for accessing a virtual portal as an end user or as an administrator, or for accessing the global administration interface of the HCP Anywhere Enterprise Portal may depend on:

- The Access Protocol
- The HTTPS Access Port

Note: A DNS suffix, used to create a virtual portal's DNS name, to access the HCP Anywhere Enterprise Portal, was set when the HCP Anywhere Enterprise Portal was installed, as described in the installation guide for the environment and in *Configuring Global Settings*.

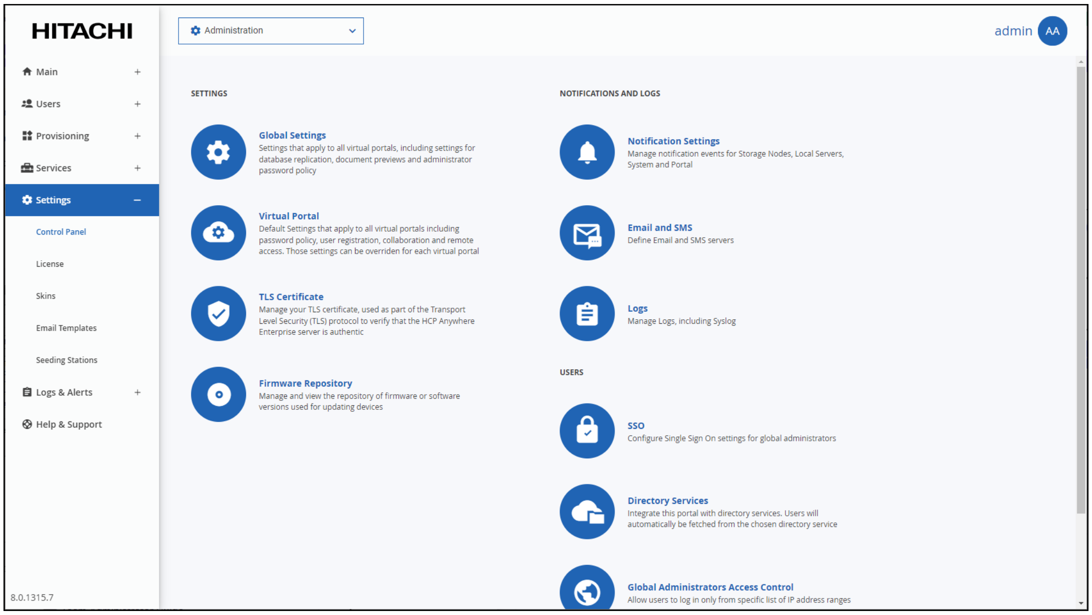
The Access Protocol

The global administration interface is accessible only via HTTPS.

The end user interface and team administrator interface is accessible via HTTP or HTTPS. You can enable automatic redirection of users from HTTP to HTTPS.

To enable automatic redirection from HTTP to HTTPS

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

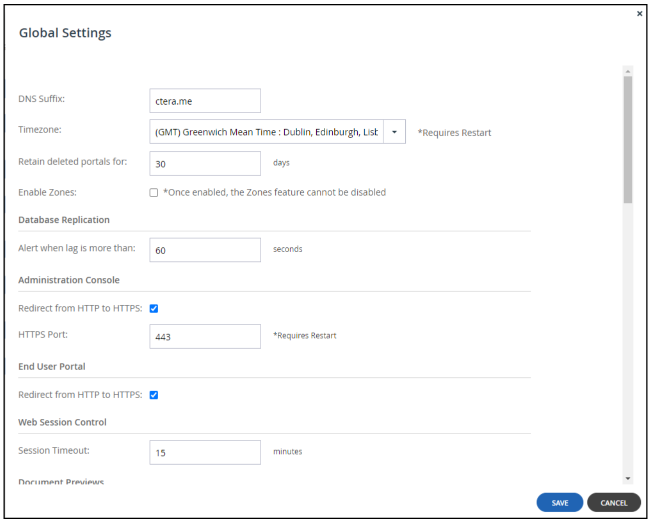
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Global Settings** under **SETTINGS** in the **Control Panel** page.
   The **Global Settings** window is displayed.



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisb *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: ☐ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

Web Session Control

Session Timeout: 15 minutes

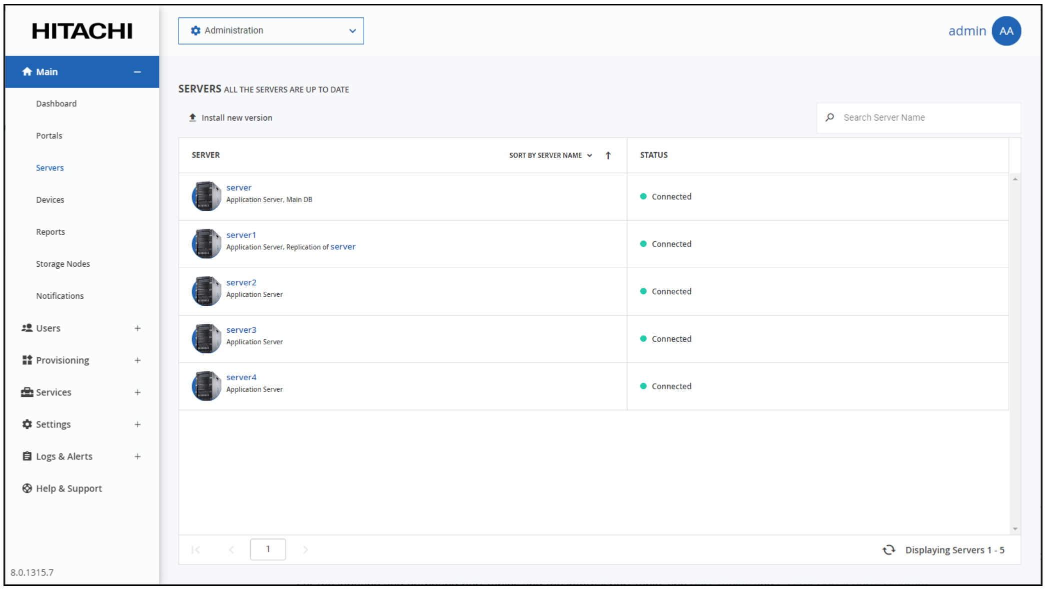
Document Previews

3. For administrators, make sure **Redirect from HTTP to HTTPS** is checked under

Administration Console.

4. For end users and team administrator, check **Redirect from HTTP to HTTPS** under **End-User Portal**.
5. Click **SAVE**.
6. Restart the HCP Anywhere Enterprise Portal servers.

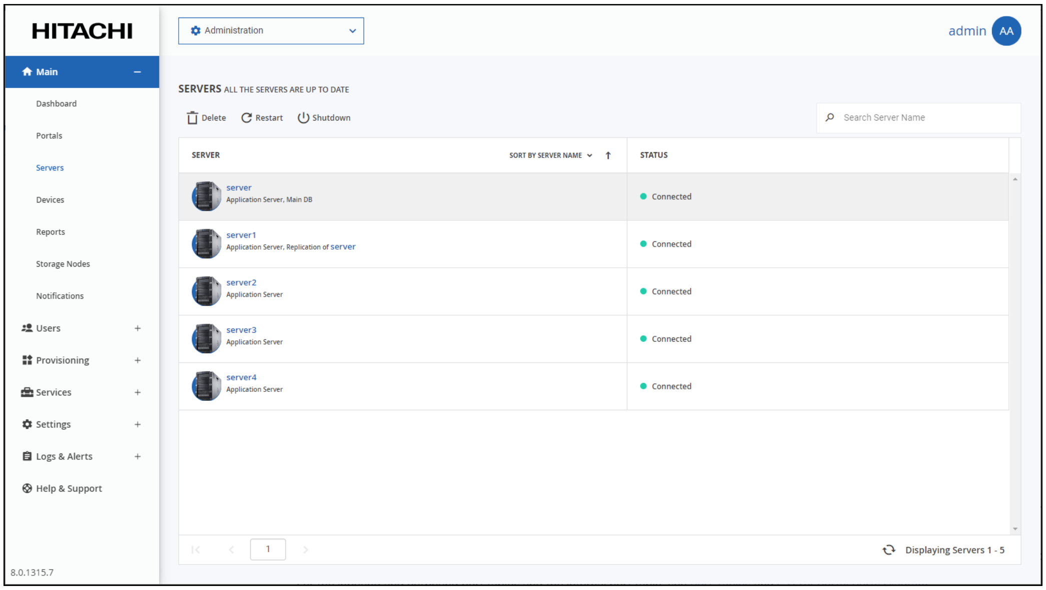
   a) In the global administration view, select **Main Servers** in the navigation pane.
   The **SERVERS** page is displayed.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

   b) Select each server in turn and click **Restart** for each server.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Restart the servers in the following order:
– Main database server.
– Replication database server, if available.

– All application or preview servers.

The change is implemented after the restart.

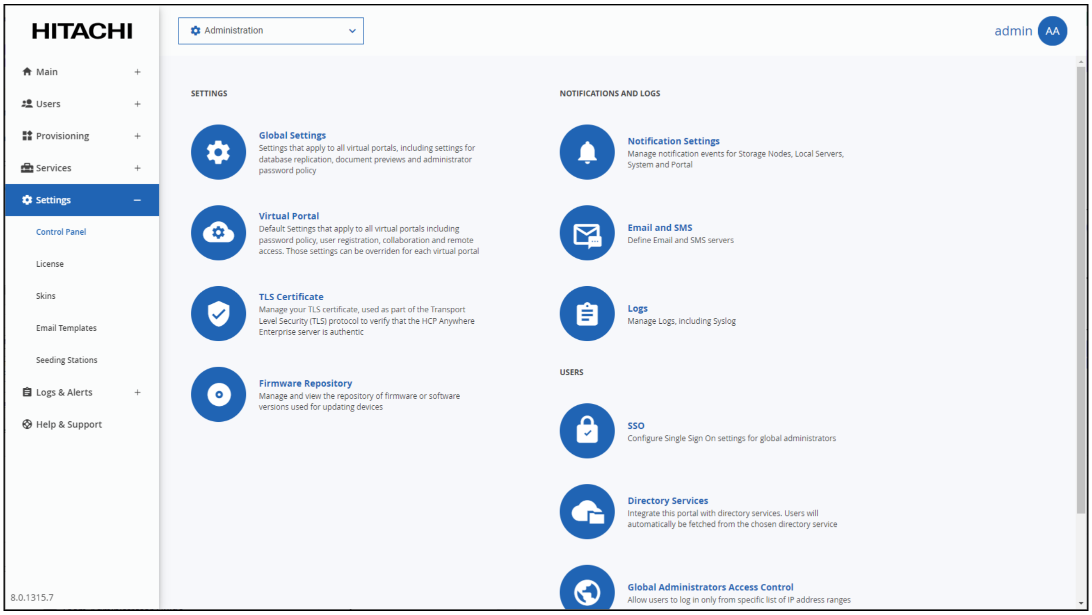
The HTTPS Access Port

By default, the administration portal is accessible via the standard HTTPS port, 443. However, you can change the HTTPS port. Changing the administration portal’s HTTPS access port can block undesired access to the HCP Anywhere Enterprise Portal. Once the HTTPS port is changed, the non standard port must be specified in the URL in order for the browser to access the HCP Anywhere Enterprise Portal.

To connect to the administration portal after changing the administration access port, append the port number to the FQDN of your HCP Anywhere Enterprise Portal. For example, to connect to *Example*’s administration portal using HTTPS port 2222, use the following address:
`https://example.hcp.me:2222/admin`

To customize the administration portal HTTPS access port:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

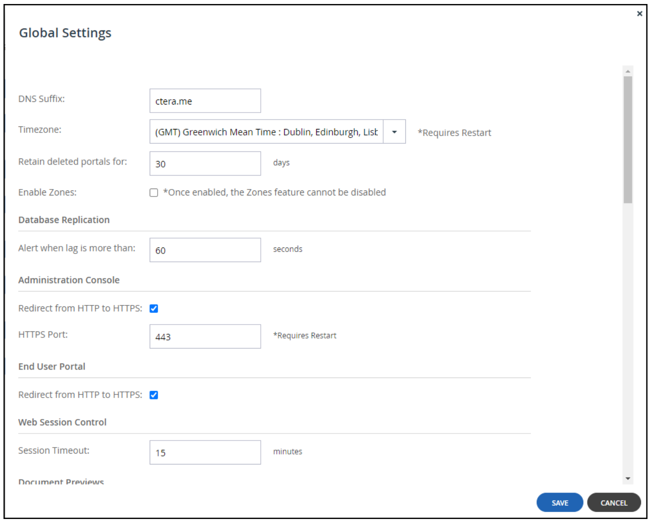
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Global Settings** under **SETTINGS** in the **Control Panel** page.
   The **Global Settings** window is displayed.



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, List *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: □ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

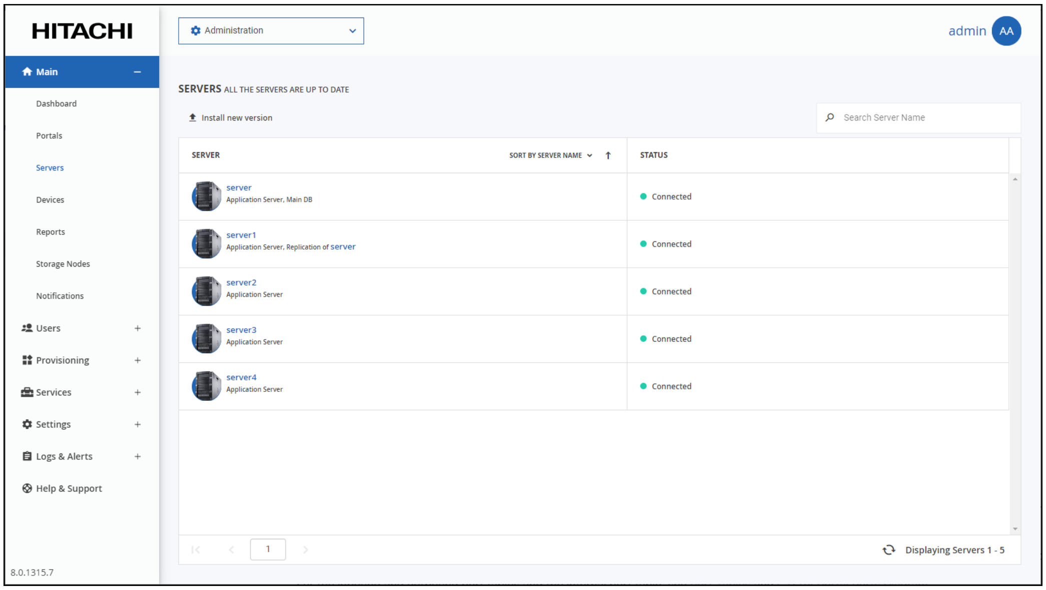
Web Session Control

Session Timeout: 15 minutes

Document Previews

3. In the **Administration Console** area, specify the new HTTPS port number in the **HTTPS Port** field.

   The allowed HTTPS ports are: 443, and from 1024 to 65535.
4. Click **SAVE**.
5. Restart the HCP Anywhere Enterprise Portal servers.
   a) In the global administration view, select **Main Servers** in the navigation pane.
   The **SERVERS** page is displayed.

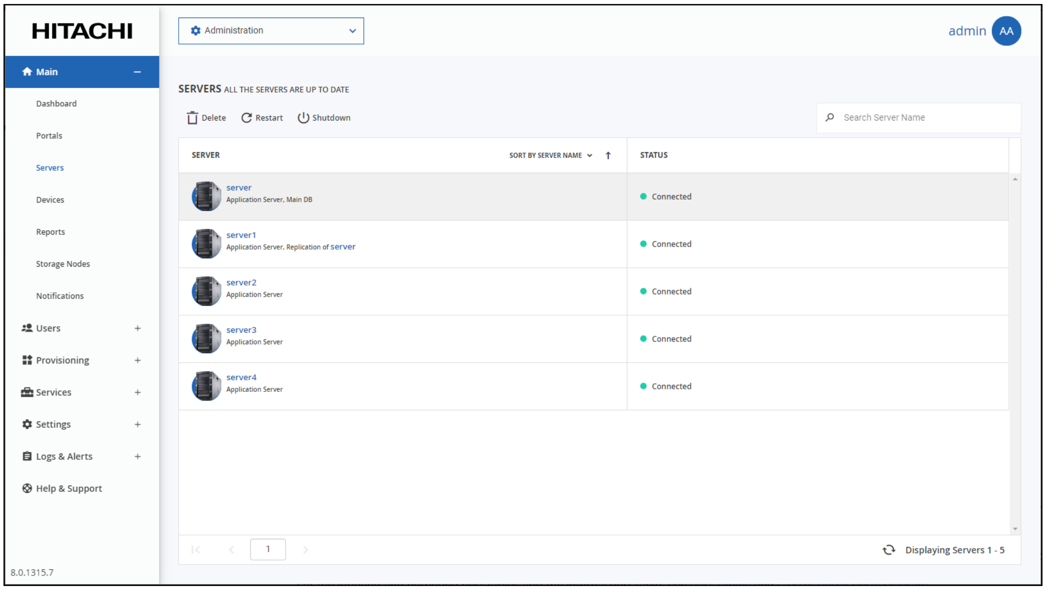


SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Displaying Servers 1 - 5

   b) Select each server in turn and click **Restart** for each server.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Restart the servers in the following order:

- Main database server.
- Replication database server, if available.
- All application or preview servers.

The change is implemented after the restart.

6. Configure the firewalls on the HCP Anywhere Enterprise Portal servers to enable TCP traffic between the servers on the customized HTTPS port. This is necessary because the customized HTTPS port is used for HCP Anywhere Enterprise server-to-server communications.

Note: Using **Redirect from HTTP to HTTPS** in addition to a customized HTTPS access port results in a redirect to the address that includes the custom port. For example, a redirect from `http://example.hcp.me/admin` to `https://example.hcp.me:2222/admin`.

Chapter 3. Managing Global Administrators

Global administrators have access to the HCP Anywhere Enterprise Portal global administration view, and to the administration view for all team portals.

At least one global administrator must be defined locally. Additional global administrators can also be defined from Active Directory, when Active Directory is set up, as described in Integrating HCP Anywhere Enterprise Portal with Active Directory.

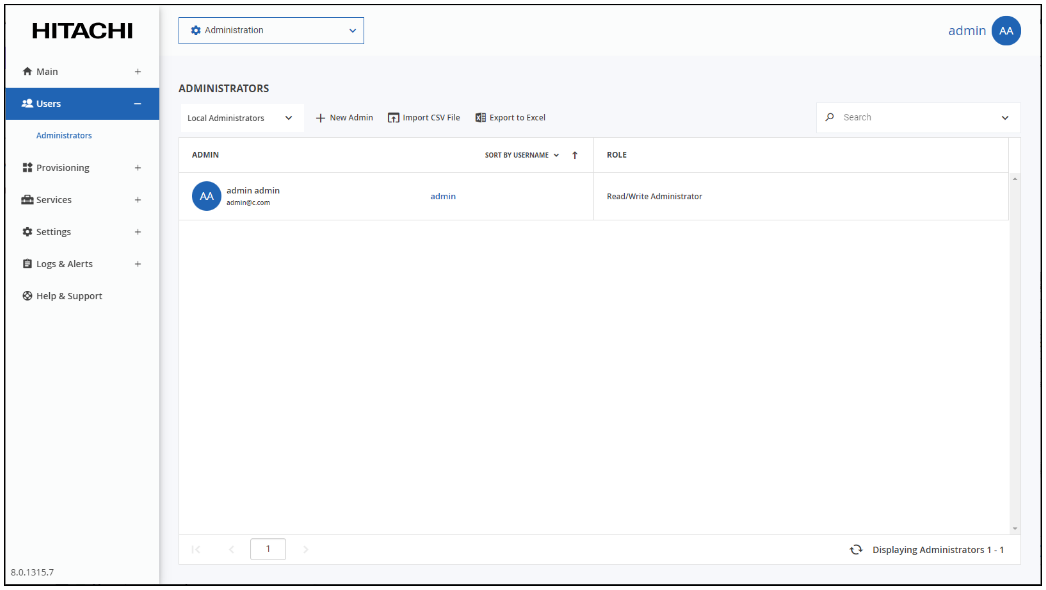
In this chapter

Viewing Global Administrators

To view all global administrators:

1. In the global administration view, select **Users > Administrators** in the navigation pane. The **ADMINISTRATORS** page is displayed. You can select to display **Local Administrators** or administrators from the connected Active Directory domain.

Local Administrators



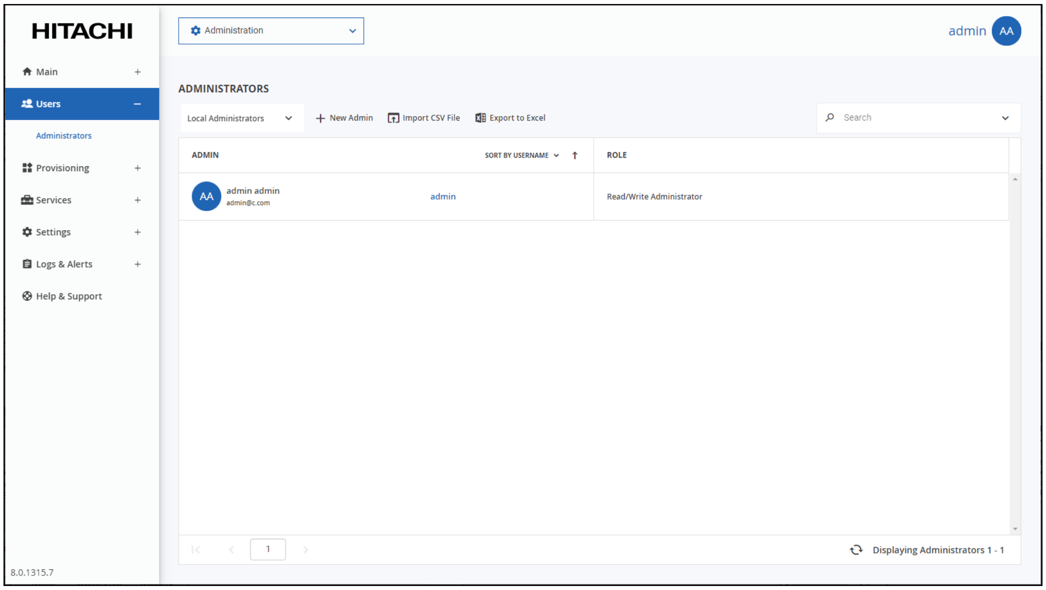
ADMIN		ROLE
AA admin admin admin@c.com	admin	Read/Write Administrator

The following information is displayed for each administrator:
ADMIN – The administrator's first and last names.

- **Email** (under the administrator name) – The administrator's email address.
- **Username** – The administrator’s user name.
- **Company** (under the administrator user name) – The name of the administrator's company.

ROLE – The administrator's role: Read/write administrator, read only administrator or support.

Active Directory Administrators



ADMIN		ROLE
AA admin admin admin@c.com	admin	Read/Write Administrator

The following information is displayed for each administrator:
ADMIN – The administrator's first and last names.

- **Email** (under the administrator name) – The administrator's email address.
- **Username** – The administrator’s user name.

ROLE – The administrator's role: Read/write administrator, read only administrator or support.

Adding, Editing, or Deleting Global Administrators

You can create an administrator and then configure what events and alerts you want to receive to the administrator email.

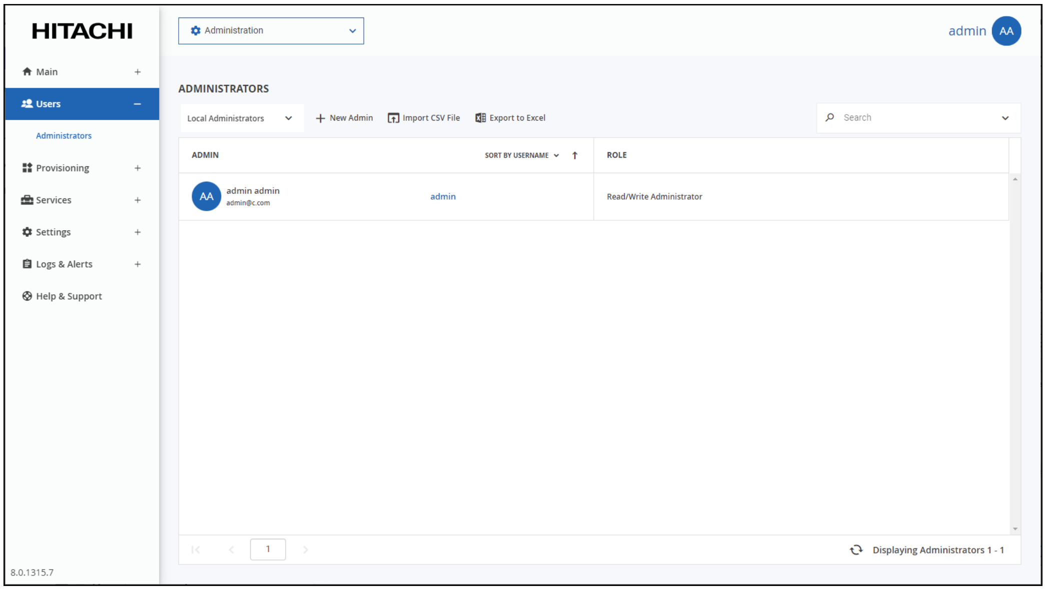
Note: When specifying user names for the global administrators, if you will be using SSO for the local administrator to log on to HCP Anywhere Enterprise Portal, the user names must match the SAML identity provider user names. For details about setting up SAML SSO, see Using SAML 2.0 For Single Sign-On.
A global administrator from Active Directory cannot log on using SAML, LDAPS or Kerberos.

Adding and Editing a Local Global Administrator

A global administrator can be defined in Active Directory. For details, see Adding a Global Administrator From Active Directory.

To add or edit a local global administrator:

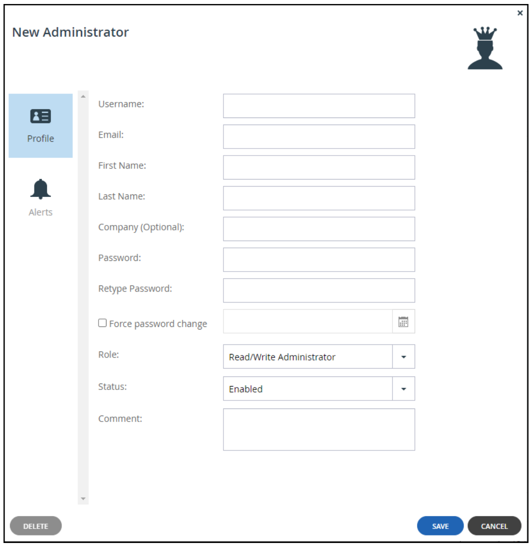
1. In the global administration view, select **Users > Administrators** in the navigation pane. The **ADMINISTRATORS** page is displayed.



ADMIN		ROLE
AA admin admin admin@c.com	admin	Read/Write Administrator

2. Make sure that *Local Administrators* is displayed.
3. Either,

   Add an administrator, click **New Admin**.
   The **New Administrator** window is displayed.



Username:	
Email:	
First Name:	
Last Name:	
Company (Optional):	
Password:	
Retype Password:	
☐ Force password change	
Role:	Read/Write Administrator
Status:	Enabled
Comment:	

Or,

Edit an existing administrator, click the administrator's name. The administrator window is displayed with the username of the administrator as the window title and account details: The creation date of the account and the last login.

4. Enter the **Profile** details:

   Username – A user name for the administrator.
   Email – The administrator's email address.
   First Name – The administrator's first name.
   Last Name – The administrator's last name.
   Company (Optional) – The name of the administrator's company.
   Password – A password for the administrator. By default, the password must be at least 7 characters long. The minimum password length can be changed. See Administrators Password Policy.
   Retype Password – Retype the password.
   Force password change – To specify an expiration date for the administrator password. When the password has expired, the administrator must specify a new password on the next login.
   Role – Specify the administrator's role. HCP Anywhere Enterprise Portal includes built-in global administrator roles:

   - **Disabled** – The administrator role is disabled.
   - **Read/Write Administrator** – The administrator has read-write permissions throughout the HCP Anywhere Enterprise Portal.
   - **Read Only Administrator** – The administrator has read-only permissions throughout the HCP Anywhere Enterprise 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 HCP Anywhere Enterprise Portal.
   - **Compliance Officer** -The administrator can access the end user portal view as an administrator with read-write permissions and also manage compliance settings for cloud drive folders.

   Note: You can customize these roles, adding or removing permissions as described in Customizing Administrator Roles.

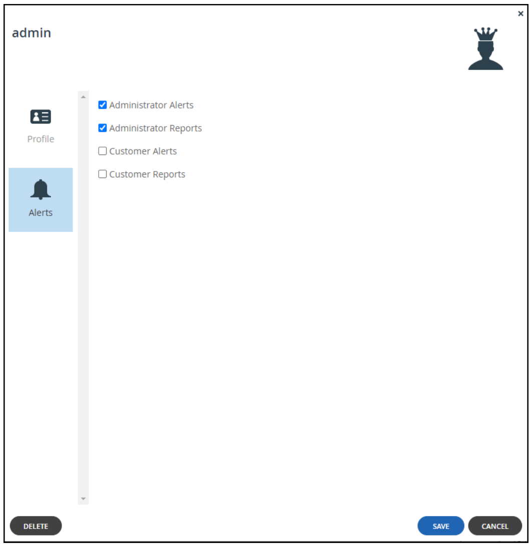
   Status – The administrator status.

   - **Enabled** – The account is enabled, and the administrator can access the HCP Anywhere Enterprise Portal.
   - **Disabled** – The account is disabled, and the administrator cannot access the HCP Anywhere Enterprise Portal. The default value for new administrators is *Enabled*.

   Note: The currently logged in administrator cannot be disabled.

   Comment – A description of the administrator.

5. Optionally, select the **Alerts** option.


admin

☑ Administrator Alerts

☑ Administrator Reports

☐ Customer Alerts

☐ Customer Reports

6. Check the types of alerts to receive:

   Administrator Alerts – Notifications about HCP Anywhere Enterprise Portal-level problems.
   Administrator Reports – Notifications reporting HCP Anywhere Enterprise Portal-level activity.
   Customer Alerts – Notifications about device-level problems.
   Customer Reports – Notifications about customer activity.
7. Click **SAVE**.

Adding a Global Administrator From Active Directory

HCP Anywhere Enterprise Portal can be integrated with 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 HCP Anywhere Enterprise Portal installation guide are opened.

Global administrator accounts are automatically fetched and refreshed from Active Directory, and authentication is performed using Active Directory.

Note: Global Administrators must have an email address, as well as a first and last name, defined in Active Directory. Users without one of these attributes cannot log in to the portal and will cause synchronization to fail.
A global administrator from Active Directory cannot log on using SAML, LDAPS or Kerberos.
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 Active Directory administrators are fetched, they can be viewed in the portal. The administrator from Active Directory cannot be edited in the HCP Anywhere Enterprise Portal, except to change the **Status** to **Disabled**.

When integrated with Active Directory, the HCP Anywhere Enterprise Portal first checks if the global administrator is defined locally before checking Active Directory.

Integrating HCP Anywhere Enterprise Portal with Active Directory

Before integrating the portal to Active Directory, to set up integration with TLS:

- LDAPS (TCP port 636) and Global Catalog TLS (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 run the command: `portal-cert.sh import -f <certificate>.cer <Alias_Name>`
  where *certificate* is a name for the certificate and *Alias_Name* is a name you can use to identify the certificate.

  Note: You only need to import the certificate and not the whole certificate chain.

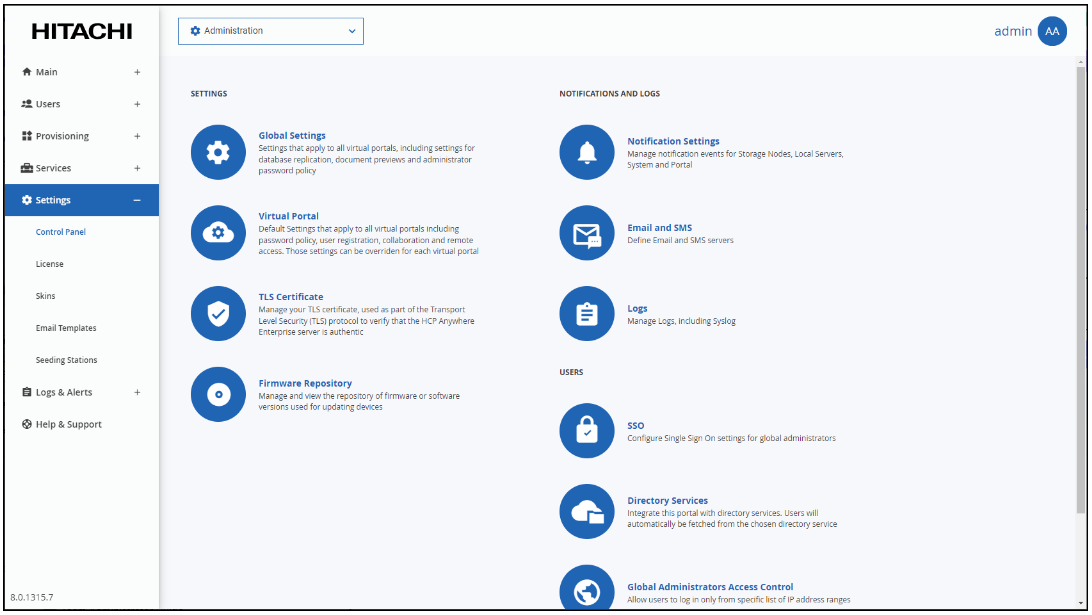
  c) After importing the certificate to each HCP Anywhere Enterprise Portal application server, run the command to start the portal: portal-manage.sh restart

  d) Follow the instructions in the **To set up defining an administrator from Active Directory:** procedure, below, checking Use TLS.

  e) Remove access to ports TCP 389 and TCP 3268.

To set up defining an administrator from Active Directory:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

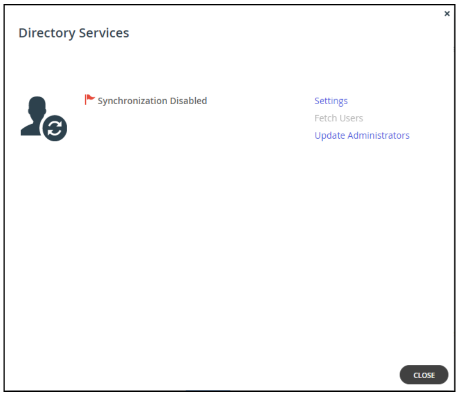
Logs
Manage Logs, including Syslog

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

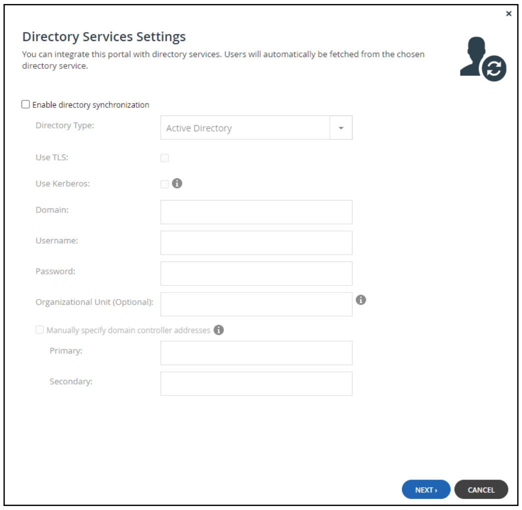
Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

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 Global Administrators From Active Directory]().

   After clicking **Settings**, the **Directory Services Settings** window is displayed.



Directory Services Settings

You can integrate this portal with directory services. Users will automatically be fetched from the chosen directory service.

□ Enable directory synchronization

Directory Type: Active Directory

Use TLS: □

Use Kerberos: □

Domain:

Username:

Password:

Organizational Unit (Optional):

□ Manually specify domain controller addresses

Primary:

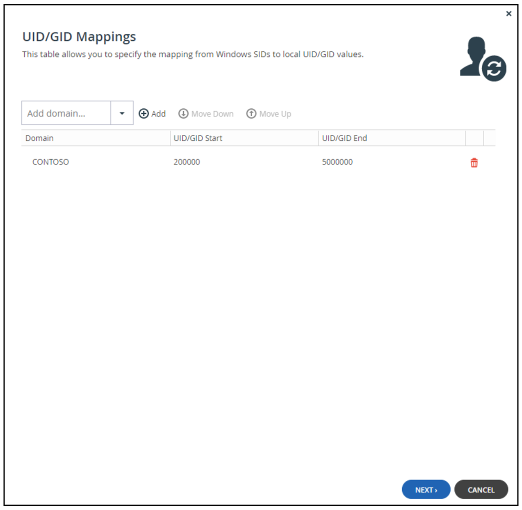
Secondary:

Enable Directory Synchronization – Enable integration with a directory domain.
Directory Type – Integration is with Active Directory.
Use TLS – Connect to the Active Directory domain using TLS.
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.
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.

4. Click **NEXT**.

The HCP Anywhere Enterprise Portal connects to the domain and the **UID/GID Mappings** window is displayed.



UID/GID Mappings

This table allows you to specify the mapping from Windows SIDs to local UID/GID values.

Domain	UID/GID Start	UID/GID End
CONTOSO	200000	5000000

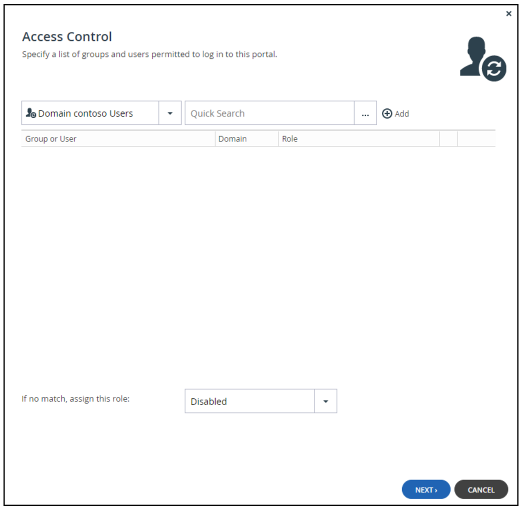
5. To add the other Active Directory domains in the tree/forest, do the following for each one:

a) 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 and 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.

b) 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.

6. Click **NEXT**.

The **Access Control** window is displayed.



Access Control

Specify a list of groups and users permitted to log in to this portal.

Domain contoso Users

Group or User	Domain	Role

If no match, assign this role: Disabled

7. Add each global administrator 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.
8. To remove a user or group, select the row and click 🗑.

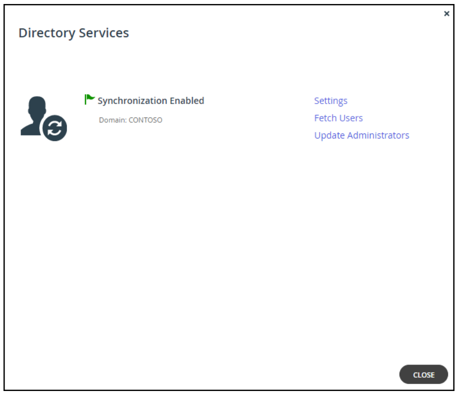
   The user or user group is removed.
9. In each user and user group's row, click in the Role column, then select the user role from the drop-down list.

   Disabled – The user account is disabled. The user cannot access the end user portal view.
   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 administrator 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.
10. To assign a role for a global administrator with no match in the access control list, select the user role from the **If no match, assign this role** drop-down list: **Disabled**, **Read/Write Administrator**, **Read Only Administrator**.
11. Click **NEXT**.

    The **Wizard Completed** window is displayed.
12. 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**.
13. Click **CLOSE**.

Synchronization with the directory server is enabled.
Click **Fetch Users** to retrieve the users from the directory, to use in the portal.



Directory Services

Synchronization Enabled
Domain: CONTOSO

14. Click **CLOSE**.

The global administrators in the portal are automatically updated at midnight of every night with the users in Active Directory. To immediately fetch the global administrators, see Manually Fetching Global Administrators From Active Directory.

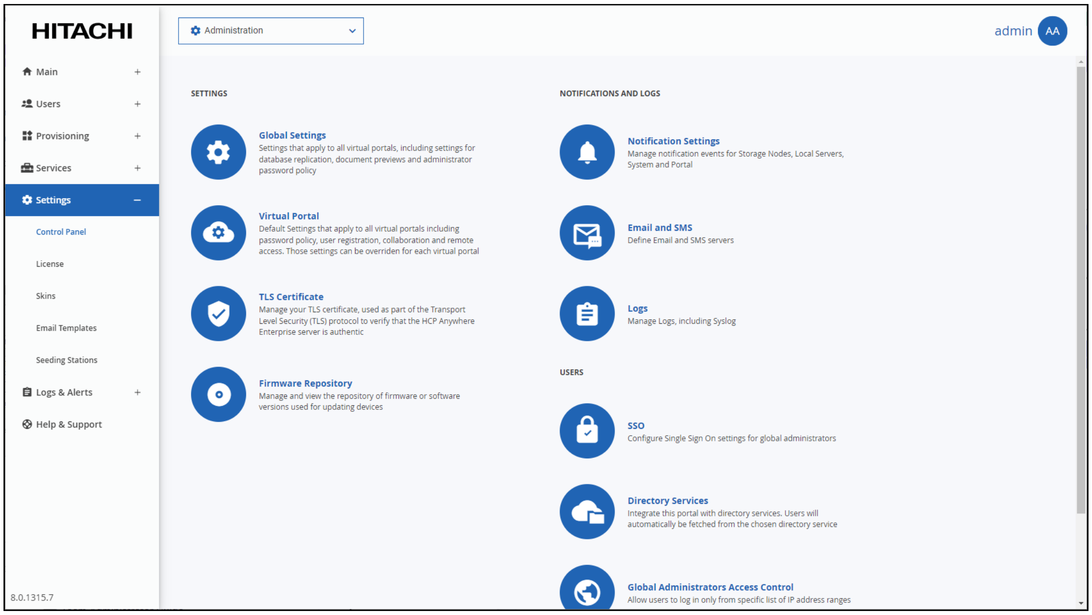
Manually Fetching Global Administrators From Active Directory

You can manually fetch user data from an integrated directory, after the connection with the directory service is established 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 an administrator 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 manually fetch user data:

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



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

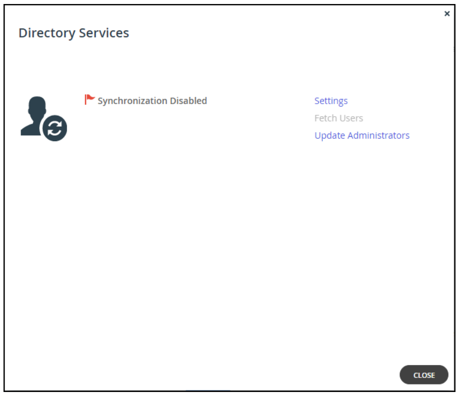
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

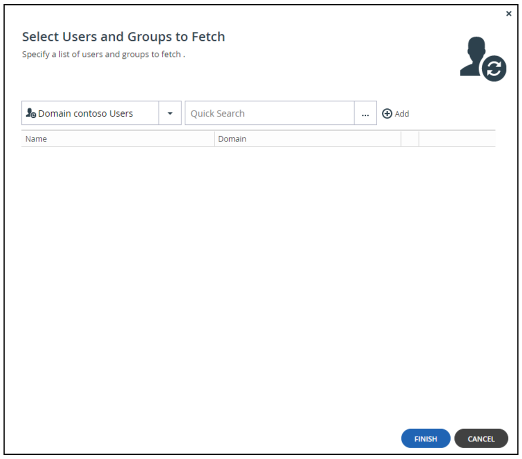
2. Select **Directory Services** under **USERS** in the **Control Panel** page.
   The **Directory Services** window is displayed.



3. Either,

   Click **Update Administrators**.
   Or,

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


Select Users and Groups to Fetch

Specify a list of users and groups to fetch .

b) Add each global administrator allowed to access the portal:
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.

Select the global administrator 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. 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.

c) Click **FINISH.**

The administrators are 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**.

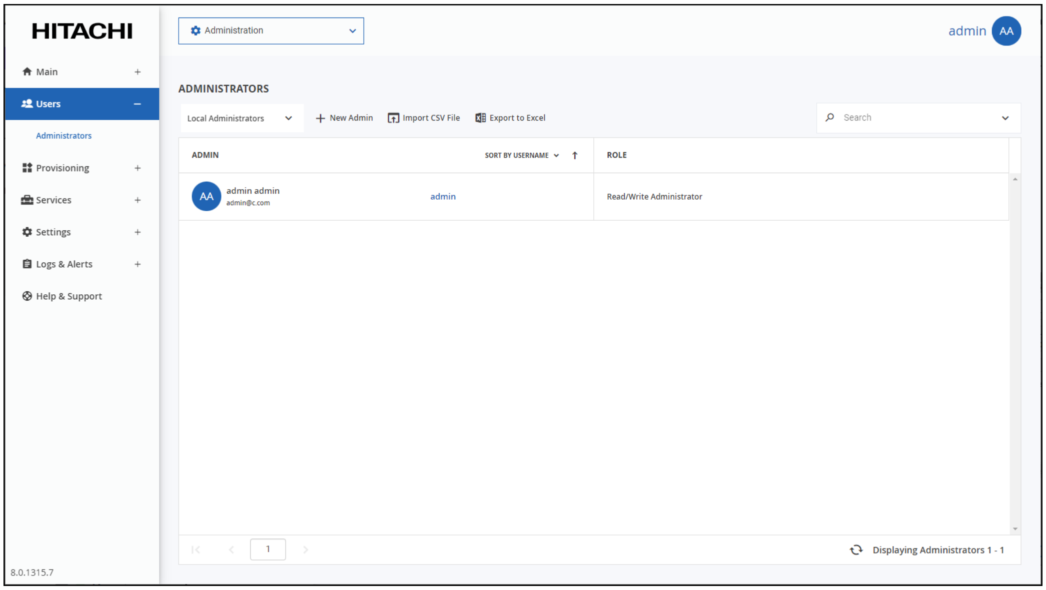
6. Click **CLOSE**.

Deleting Global Administrators

You cannot delete the administrator that is currently logged in to the HCP Anywhere Enterprise Portal.

To delete a global administrator:

1. In the global administration view, select **Users > Administrators** in the navigation pane. The **ADMINISTRATORS** page is displayed.



ADMIN		ROLE
AA admin admin admin@c.com	admin	Read/Write Administrator

2. Either,
   a) Select the administrator to delete and click **Delete Administrator**.
   A confirmation window is displayed.
   b) Click **DELETE ADMINISTRATOR** to confirm.
   Or,
   a) Click any of the **ADMIN** values: First and last name, email address, or username.
   The administrator window is displayed with the username of the administrator as the window title.
   b) Click **DELETE**.
   A confirmation window is displayed.
   c) Click **YES** to confirm.

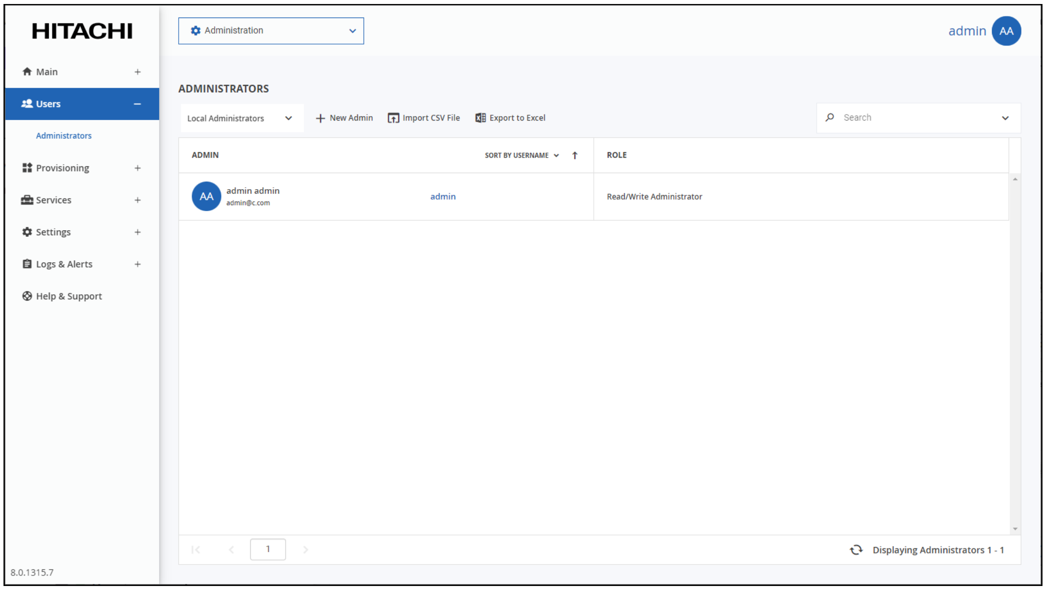
The administrator is deleted.

Exporting Global Administrators To an Excel File

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

To export the list of administrators to an Excel file:

1. In the global administration view, select **Users > Administrators** in the navigation pane. The **ADMINISTRATORS** page is displayed.



ADMIN		ROLE
admin admin admin@c.com	admin	Read/Write Administrator

2. Click **Export to Excel**.

The administrator list is downloaded to your computer.

Importing Global Administrators from a File

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

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

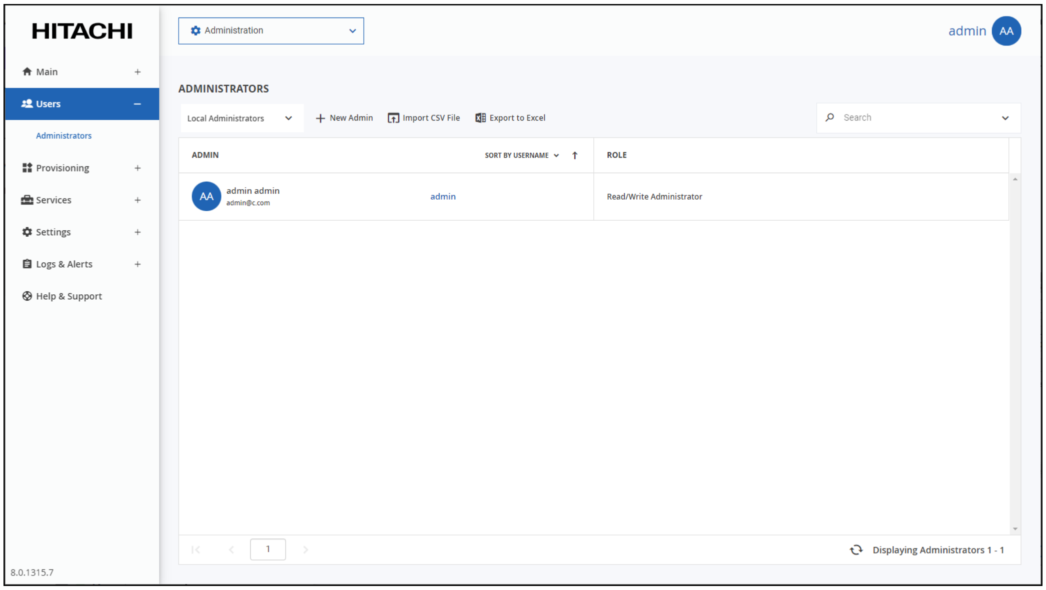
1. Username
2. First name
3. Last name
4. Email address
5. Company (Optional)
6. Password
7. Role
8. — (this column must not contain a value)
9. — (this column must not contain a value)
10. — (this column must not contain a value)

11. Comment (Optional)
12. Status (Optional)

Optional fields can be left blank.

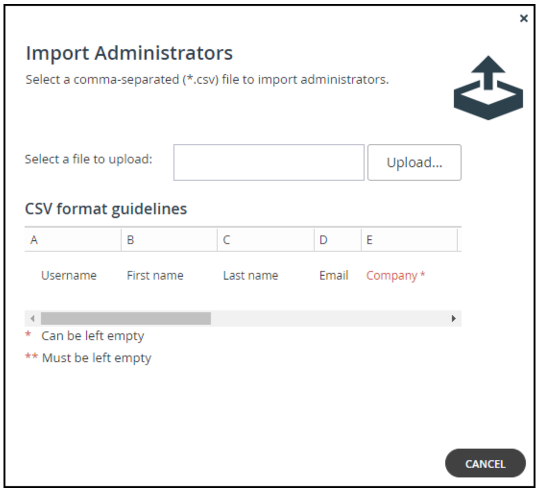
To import administrators from a *.csv file:

1. In the global administration view, select **Users > Administrators** in the navigation pane. The **ADMINISTRATORS** page is displayed.



ADMIN		ROLE
admin admin admin@c.com	admin	Read/Write Administrator

2. Click **Import CSV File**.
   The **Import Administrators** window is displayed.



Import Administrators

Select a comma-separated (*.csv) file to import administrators.

Select a file to upload:

CSV format guidelines

A	B	C	D	E
Username	First name	Last name	Email	Company *

* Can be left empty
** Must be left empty

3. Click **Upload** and select the file with the administrator details to upload.
4. Click **Open**.
   The file is uploaded and the **Import Completed** window is displayed.
5. Click **FINISH**.

Customizing Administrator Roles

By default, HCP Anywhere Enterprise Portal includes built-in roles for administrators. HCP Anywhere Enterprise Portal includes the following roles for global administrators:

Compliance Officer – The administrator can manage HCP Anywhere Enterprise Vault on folders.

Read/Write Administrator – The administrator has read/write permissions throughout the HCP Anywhere Enterprise Portal.

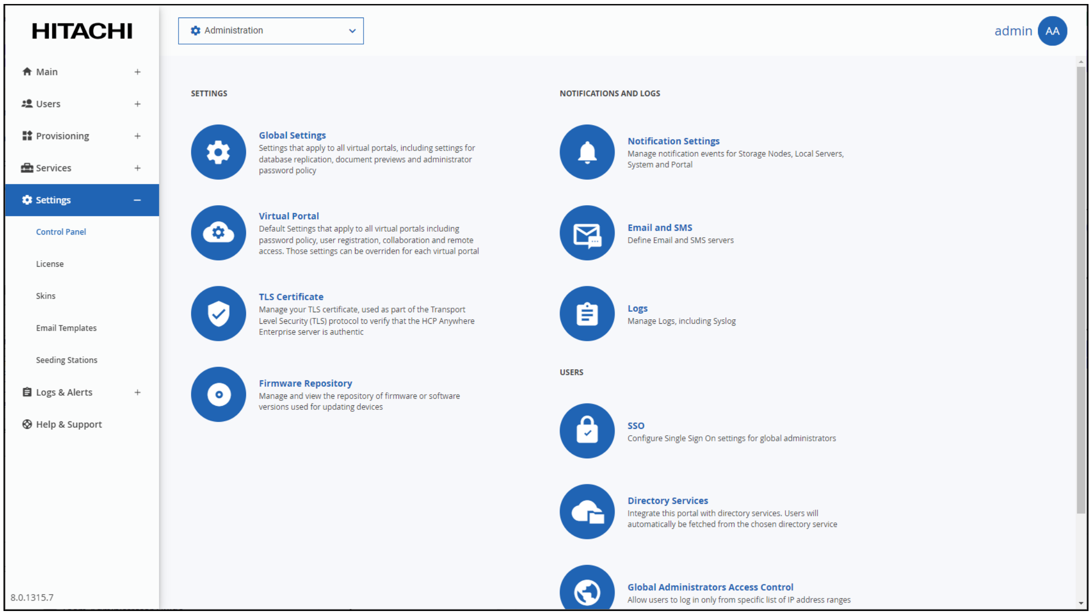
Read Only Administrator – The administrator has read-only permissions throughout the HCP Anywhere Enterprise Portal.

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 HCP Anywhere Enterprise Portal.

You can customize these roles, adding or removing permissions.

To customize an administrator role:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

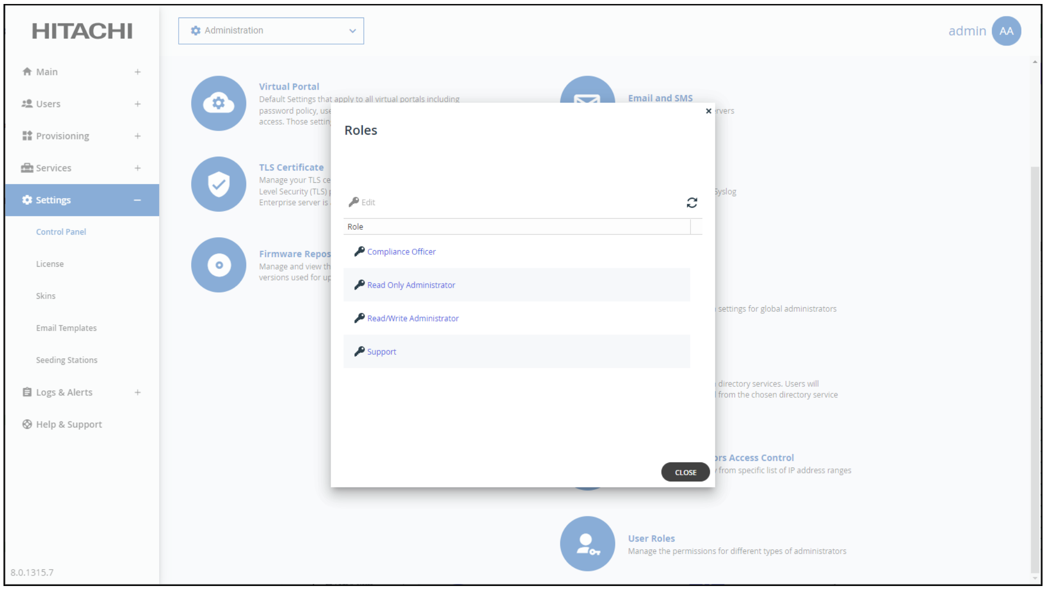
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

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

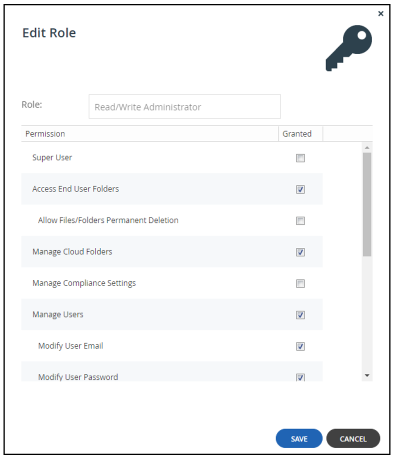


Roles

Role
Compliance Officer
Read Only Administrator
Read/Write Administrator
Support

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

   The **Edit Role** window is displayed.



Edit Role

Role: Read/Write Administrator

Permission	Granted
Super User	□
Access End User Folders	☑
Allow Files/Folders Permanent Deletion	□
Manage Cloud Folders	☑
Manage Compliance Settings	□
Manage Users	☑
Modify User Email	☑
Modify User Password	☑

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 and modify end user files and 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.

   > A**llow Files/Folders Permanent Deletion** – Allow administrators to permanently delete end users files and folders. 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 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 remove, rename and change the owner of 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, backup folders 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.

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* in the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

Note: The Compliance Officer rold 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.

Allow Seeding Export – This feature is currently not supported.

Allow Seeding Import – This feature is currently not supported.

Manage Log Settings – Allow administrators to access the log settings.

5. Click **SAVE**.

Permissions Available to Roles

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

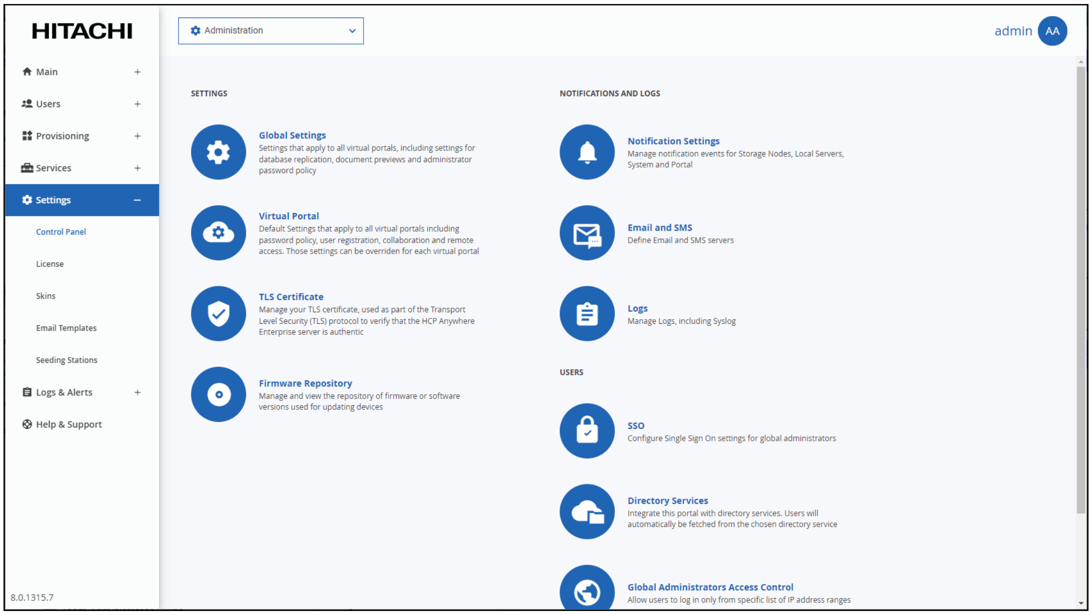
Permission	Compliance Officer	Read/Write Administrator	Read Only Administrator	Support
Manage Users	Yes	Yes	No	Yes
Modify User Email	Yes	Yes	No	Yes
Modify User Password	Yes	Yes	No	Yes
Manage Plans	Yes	Yes	No	Yes
Modify Virtual Portal Settings	Yes	Yes	No	Yes (Default is No)
Modify Roles	Yes	Yes	No	Yes (Default is No)
Allow Single Sign On to Devices	Yes (Default is No)	Yes (Default is No)	Yes (Default is No)	Yes (Default is No)
Allow remote wipe for devices	—	—	—	—
Allow Seeding Export	—	—	—	—
Allow Seeding Import	—	—	—	—
Manage Log Settings	Yes	Yes	No	Yes (Default is No)

Configuring an IP-Based Access Control List

You can configure an IP-based access control list, specifying the IP address ranges from which administrators can access the HCP Anywhere Enterprise Portal interface.

To configure an IP-based access control list:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



HITACHI

Administration

admin AA

Main +
Users +
Provisioning +
Services +
Settings −
Control Panel
License
Skins
Email Templates
Seeding Stations
Logs & Alerts +
Help & Support

8.0.1315.7

SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

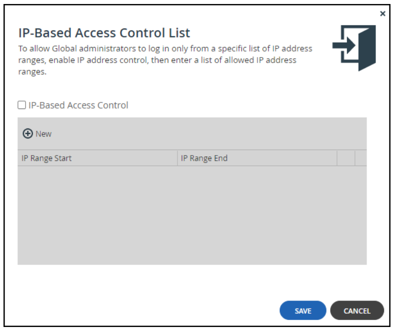
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Global Administrators Access Control**, under **USERS** in the **Control Panel** page.
   The **IP-Based Access Control List** window is displayed.



×

IP-Based Access Control List

To allow Global administrators to log in only from a specific list of IP address ranges, enable IP address control, then enter a list of allowed IP address ranges.

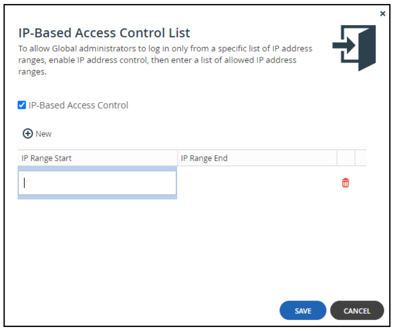
□ IP-Based Access Control

⊕ New

IP Range Start	IP Range End

SAVE CANCEL

3. Check the **IP-Based Access Control** box.
   The IP-based access control list is enabled.
4. Click **New** to add an IP address range from which access to the HCP Anywhere Enterprise Portal interface is allowed.
   A new row is added to the IP-based access control list.



IP-Based Access Control List

To allow Global administrators to log in only from a specific list of IP address ranges, enable IP address control, then enter a list of allowed IP address ranges.

☑ IP-Based Access Control

IP Range Start	IP Range End	

5. Click in the **IP Range Start** field, and enter the start IP address.
6. Click in the **IP Range End** field, and enter the end IP address.

   Note: To remove an IP address range, in the IP address range's row, click 🗑. The IP address range is removed.
7. Click **SAVE**.

Chapter 4. Managing the HCP Anywhere Enterprise Portal License

The HCP Anywhere Enterprise Portal license limits the number of HCP Anywhere Enterprise Edge Filer licenses, HCP Anywhere Enterprise Drive Share (Agent) licenses, and Cloud Drive licenses, that can be provisioned throughout the HCP Anywhere Enterprise Portal.

The HCP Anywhere Enterprise Portal includes a 30-day evaluation license. Hitachi Vantara recommends installing a full license when installing the HCP Anywhere Enterprise Portal.

Once the trial license has expired, or if you require additional licensing, you must install a new license key. Also, a HCP Anywhere Enterprise Portal with a trial license cannot be upgraded to a newer version.

When a HCP Anywhere Enterprise Portal license is about to expire, notifications appear on the notifications page of HCP Anywhere Enterprise Portal's administration interface, and emails are sent to the HCP Anywhere Enterprise Portal administrators. If the HCP Anywhere Enterprise Portal license expires, the HCP Anywhere Enterprise Portal continues to function but adding new devices is disabled.

In this chapter

How the HCP Anywhere Enterprise Portal License Works

The HCP Anywhere Enterprise Portal license specifies license quotas for each of the following:

- **HCP Anywhere Enterprise Portal License**
  The amount of storage allowed, in blocks of 50TB.
  The storage considered towards the licensed storage allowed is the data existing in the current snapshot for all cloud and backup folders before deduplication and compression.
- **HCP Anywhere Enterprise Edge Filer licenses**
  The number of HCP Anywhere Enterprise Edge Filer licenses that can be provisioned. A HCP Anywhere Enterprise Edge Filer license is consumed by a HCP Anywhere Enterprise Edge Filer connected to a HCP Anywhere Enterprise Portal user account.
- **HCP Anywhere Enterprise Drive Share (Agent) Licenses**
  The number of HCP Anywhere Enterprise Drive Server licenses that can be provisioned. A HCP Anywhere Enterprise Drive Server license applies to a HCP Anywhere Enterprise Drive Share (Agent) installed on a server.
- **HCP Anywhere Enterprise Cloud Drive Licenses**
  The number of Cloud Drive licenses that can be provisioned. Each HCP Anywhere Enterprise Cloud Drive license enables use of the Cloud Drive service for a single user account.
- **HCP Anywhere Enterprise Cloud Drive Connect License**s

The number of Cloud Drive Connect licenses that can be provisioned. This license is a subset of the full *Cloud Drive* license and entitles a user per license to access the HCP Anywhere Enterprise Portal without full sync and share capabilities. This is useful for users who do not need to collaborate on shared documents and folders with other users, and for access after a HCP Anywhere Enterprise Edge Filer disaster.

The license is subdivided when you allocate quotas to virtual portals, by assigning the virtual portals to global plans and add-ons. For example, if the HCP Anywhere Enterprise Portal license includes 20 HCP Anywhere Enterprise Edge Filer licenses, and 20 cloud drive licenses, and there are two virtual portals, you may choose to allocate half of the HCP Anywhere Enterprise Edge Filer and cloud drive quotas to each virtual portal. In this case, each virtual portal is allocated quotas for 10 HCP Anywhere Enterprise Edge Filers and 10 cloud drives.

With each virtual portal, the HCP Anywhere Enterprise Portal license can be further subdivided, when quotas are allocated to user accounts via plans and add-ons.

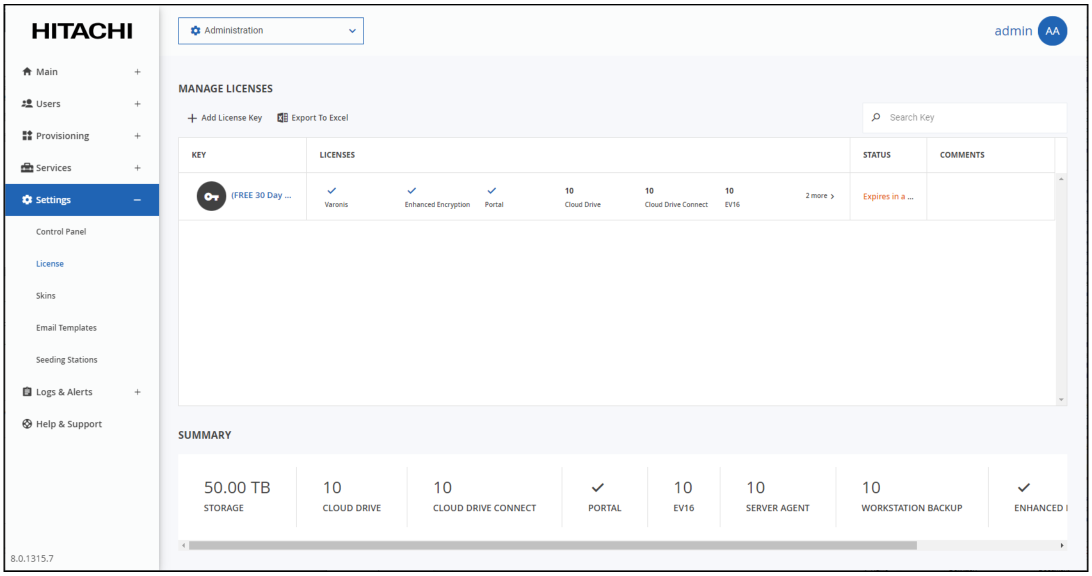
Licenses provisioned to a specific team portal, except for storage, are immediately consumed from the HCP Anywhere Enterprise Portal license. You can oversubscribe team portal storage and storage is consumed from the license limit as it is actually used up to the license limit. Within the team portal you can optionally limit how many licenses or storage each user can consume, by assigning a plan to the user.

The number of licenses in use must be less than or equal to the number provisioned for the team portal. The number provisioned for the team portal is the limit for that portal.

Viewing HCP Anywhere Enterprise Portal License Information

To view HCP Anywhere Enterprise Portal license information:

1. In the global administration view, select **Settings > License** in the navigation pane.
   The **MANAGE LICENSES** page is displayed.



KEY	LICENSES	STATUS	COMMENTS
(FREE 30 Day ...	✓ Varonis ✓ Enhanced Encryption ✓ Portal 10 Cloud Drive 10 Cloud Drive Connect 10 EV16 2 more ›	Expires in a ...	

SUMMARY

50.00 TB	10	10	✓	10	10	10	✓
STORAGE	CLOUD DRIVE	CLOUD DRIVE CONNECT	PORTAL	EV16	SERVER AGENT	WORKSTATION BACKUP	ENHANCED I

The following information is displayed for each license:

KEY – The license key.

LICENSES – The license details.

Antivirus – The license includes the antivirus service.

Varonis – The license includes the Varonis service.

Enhanced Encryption – The license includes the Key Management service.

Portal– The HCP Anywhere Enterprise Portal license is operational or not.

Cloud Drive – The number of cloud drive licenses included in the license key. Cloud drive licenses are per HCP Anywhere Enterprise Portal user. There is no limit to the number of HCP Anywhere Enterprise Drive Share (Agents) that can synchronize to each user's cloud drive.

Cloud Drive Connect – The number of cloud drive connect licenses included in the license key.

EV8 – The number of EV8 HCP Anywhere Enterprise Edge Filer licenses included in the license key. You cannot define more than this number of edge filers with an EV8 license in the HCP Anywhere Enterprise Portal.

EV16 – The number of EV16 HCP Anywhere Enterprise Edge Filer licenses included in the license key. You cannot define more than this number of edge filers with an EV16 license in the HCP Anywhere Enterprise Portal.

EV32 – The number of EV32 HCP Anywhere Enterprise Edge Filer licenses included in the license key. You cannot define more than this number of edge filers with an EV32 license in the HCP Anywhere Enterprise Portal.

EV64 – The number of EV64 HCP Anywhere Enterprise Edge Filer licenses included in the license key. You cannot define more than this number of edge filers with an EV64 license in the HCP Anywhere Enterprise Portal.

EV128 – The number of EV128 HCP Anywhere Enterprise Edge Filer licenses included in the license key. You cannot define more than this number of edge filers with an EV128 license in the HCP Anywhere Enterprise Portal.

EV256 – The number of EV256 HCP Anywhere Enterprise Edge Filer licenses included in the license key. You cannot define more than this number of edge filers with an EV256 license in the HCP Anywhere Enterprise Portal.

Server Agent – The number of HCP Anywhere Enterprise Drive Share (Agent) licenses included in the license key.

STATUS – The license key's status.

OK – The license is current.

Expired on *date* – The license expired on the specified date.

Expires in *X* days – The license will expire X days from now.

COMMENTS – Any comment about the license key.

Adding and Removing Licenses

As a prerequisite, you must purchase a license key from your HCP Anywhere Enterprise authorized reseller, specifying your HCP Anywhere Enterprise Portal's DNS suffix, antivirus requirements, and the number of required HCP Anywhere Enterprise Edge Filers, HCP Anywhere Enterprise Drive Share (Agent) licenses. You receive one or more license keys.

Note: You can view your HCP Anywhere Enterprise Portal's DNS suffix, in the global administration view's **Settings > Control Panel > Global Settings** page. This DNS suffix was set up when you installed the HCP Anywhere Enterprise Portal, as described in the installation guide for your environment.

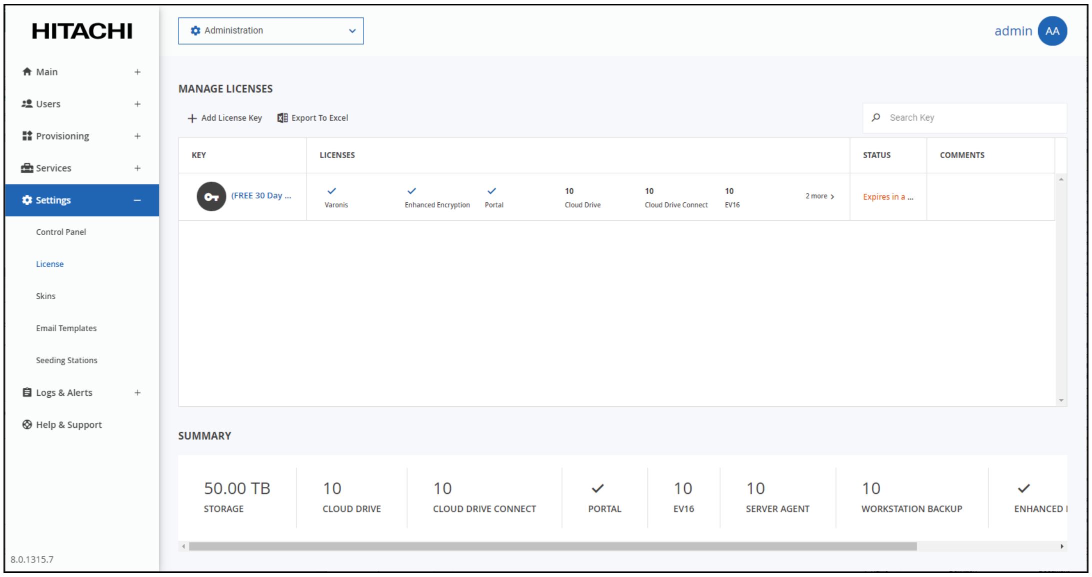
To extend a trial license requires Internet access. If this is a problem, contact Hitachi

Vantara support.

Adding a License

To add a license:

1. In the global administration view, select **Settings > License** in the navigation pane.
   The **MANAGE LICENSES** page is displayed.



MANAGE LICENSES

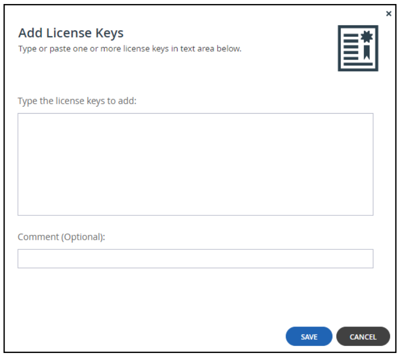
KEY	LICENSES							STATUS	COMMENTS
(FREE 30 Day ...	✓ Varonis	✓ Enhanced Encryption	✓ Portal	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	2 more ›	Expires in a ...	

SUMMARY

50.00 TB	10	10	✓	10	10	10	✓
STORAGE	CLOUD DRIVE	CLOUD DRIVE CONNECT	PORTAL	EV16	SERVER AGENT	WORKSTATION BACKUP	ENHANCED I

2. Click **Add License Key**.

   The **Add License Keys** window opens.



Add License Keys

Type or paste one or more license keys in text area below.

Type the license keys to add:

Comment (Optional):

3. Copy the license key you received from HCP Anywhere Enterprise, and paste it into the text box.

   To add more than one key, paste each key on a new line.
   The system verifies and activates the license keys by contacting the HCP Anywhere Enterprise Activation service. As each license key is activated, it is associated with this installation of HCP Anywhere Enterprise Portal.
4. Optionally add a comment in the **Comment** field. The comment is displayed in the **MANAGE LICENSES** page.

   Note: You can use this comment to document information such as the purchase order number associated with the license.

5. Click **SAVE**.

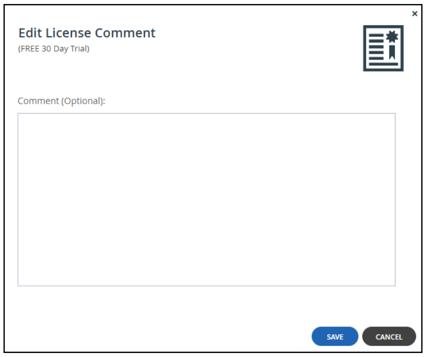
HCP Anywhere Enterprise Portal connects to the license server over HTTPS to activate the key.

Adding or Editing a Comment for a License

To add or edit a license comment:

1. In the global administration view, select **Settings > License** in the navigation pane.
   The **MANAGE LICENSES** page is displayed.
2. Click the license key.

   The **Edit License Comment** window is displayed.



Edit License Comment
(FREE 30 Day Trial)

Comment (Optional):

3. Optionally, add or edit the contents of the **Comment** field.
4. Click **SAVE**.

Removing Licenses

To remove a license:

1. In the global administration view, select **Settings > License** in the navigation pane.
   The **MANAGE LICENSES** page is displayed.
2. Select the license key and click **Delete License**.

   A confirmation window is displayed.
3. Click **DELETE LICENSE**.

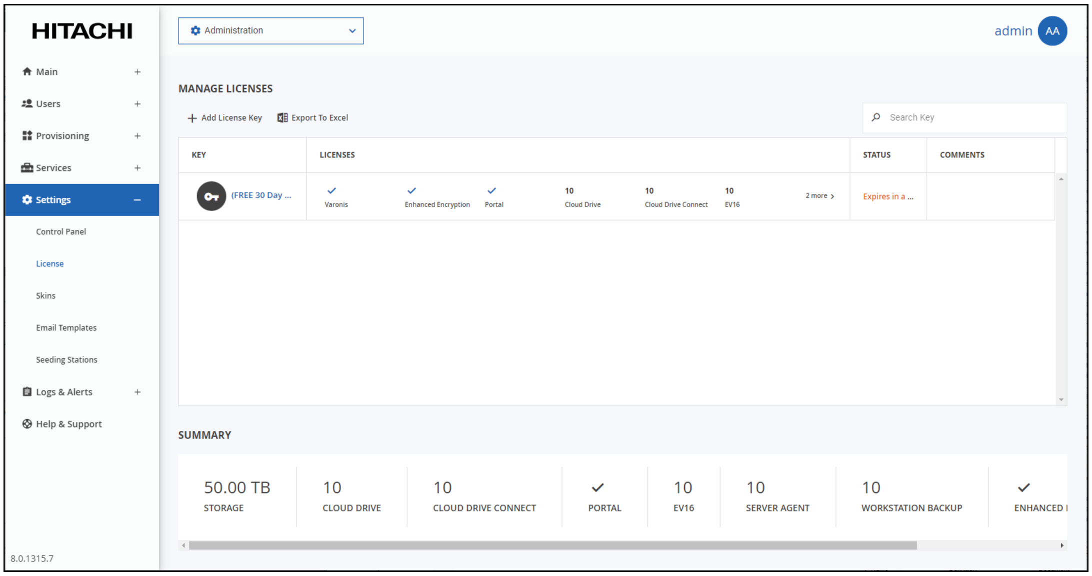
   The license key is deleted.

Exporting License Details to Excel

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

To export license keys:

1. In the global administration view, select **Settings > License** in the navigation pane. The **MANAGE LICENSES** page is displayed.



MANAGE LICENSES

KEY	LICENSES							STATUS	COMMENTS
(FREE 30 Day ...	✓ Varonis	✓ Enhanced Encryption	✓ Portal	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	2 more ›	Expires in a ...	

SUMMARY

50.00 TB	10	10	✓	10	10	10	✓
STORAGE	CLOUD DRIVE	CLOUD DRIVE CONNECT	PORTAL	EV16	SERVER AGENT	WORKSTATION BACKUP	ENHANCED I

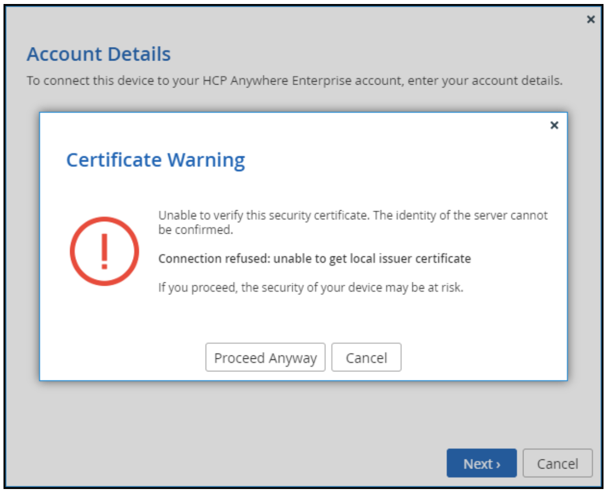
2. Click Export to Excel.

The details of the license are exported to an excel file on your computer.

Chapter 5. Managing Certificates

Certificates are used as part of the Transport Level Security (TLS) protocol. They enable using Web browsers, HCP Anywhere Enterprise Edge Filers, and HCP Anywhere Enterprise Drive Share (Agents) to verify that the HCP Anywhere Enterprise Portal server with which they are communicating is authentic and not spoofed.

If the HCP Anywhere Enterprise Portal does not have a valid certificate installed, a warning is displayed to the end user when logging a device into the HCP Anywhere Enterprise Portal, offering the option to proceed anyway.


Account Details

To connect this device to your HCP Anywhere Enterprise account, enter your account details.

Certificate Warning

Unable to verify this security certificate. The identity of the server cannot be confirmed.

Connection refused: unable to get local issuer certificate

If you proceed, the security of your device may be at risk.

This warning is presented every time a user connects a device to the HCP Anywhere Enterprise Portal, until a valid certificate is installed.

Note: During the configuration of the primary server, for a production environment, you should have installed a valid certificate, as described in *Installing a TLS Certificate* in the installation guide for your platform.

A valid TLS certificate must meet the following requirements:

- If multiple virtual portals are configured, then each virtual portal has its own DNS name. In this case, the SSL certificate should be a wildcard certificate, that is, the DNS name embedded in the certificate should start with "*". For example, if the HCP Anywhere Enterprise Portal's DNS suffix is *myportal.com*, and there are two virtual portals, *portal1.myportal.com* and *portal2.myportal.com*, you need a wildcard certificate for **.myportal.com*.
- If you have only one HCP Anywhere Enterprise Portal, and do not intend to configure multiple virtual portals, then a regular SSL certificate is preferable and not a wildcard certificate. For example, if your HCP Anywhere Enterprise Portal's DNS name is *portal1.myportal.com*, then you need a certificate for *portal1.myportal.com*.
- It is possible to specify multiple alternative names, using the `subjectAltName` certificate extension.
- The certificate must in *.zip format and contain certificate files in *.pem format.

You can automatically generate a certificate request to send to any public TLS certificate authority, such as GoDaddy, which Hitachi Vantara recommends, Verisign, or Thawte, as described in Generate a Certificate Signing Request. Once you have received a certificate from the certificate authority, you must the install it, as described in the installation guide for your platform.

Alternatively, you can export a certificate from another HCP Anywhere Enterprise Portal, described in Exporting the Installed TLS Certificate, and install it on this HCP Anywhere Enterprise Portal, described in Importing a TLS Certificate.

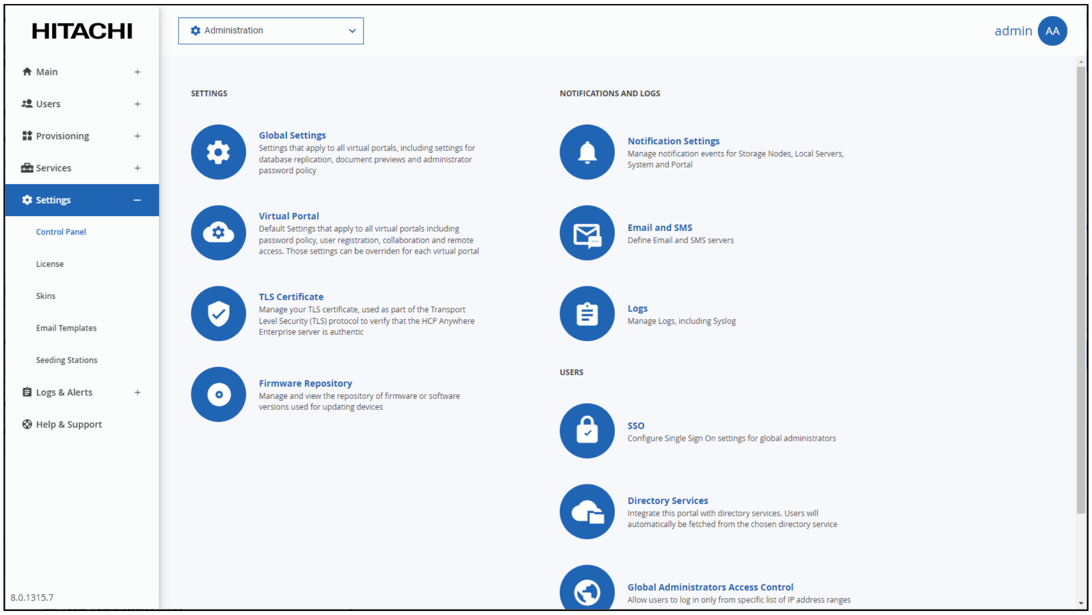
Note: When generating a certificate request and installing the received certificate, the private key is generated on the portal and never leaves it. In contrast, when exporting and importing certificates, the private key is exported and imported along with the certificate, and it is therefore important to keep the exported file confidential.

Exporting the Installed TLS Certificate

You can export the installed SSL certificate chain together with the corresponding private key.

To export the installed TLS certificate:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

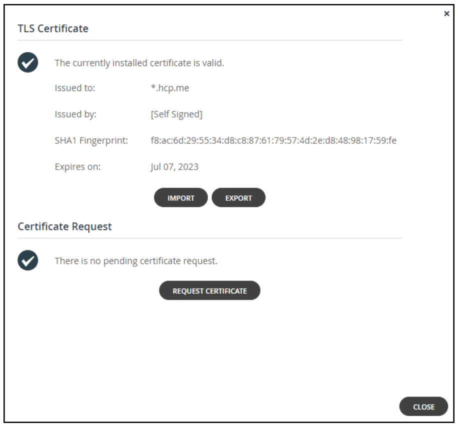
SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **TLS Certificate** under **SETTINGS** in the Control Panel page.

   The **TLS Certificate** window is displayed.



The currently installed certificate is valid.

Issued to: *.hcp.me

Issued by: [Self Signed]

SHA1 Fingerprint: f8:ac:6d:29:55:34:d8:c8:87:61:79:57:4d:2e:d8:48:98:17:59:fe

Expires on: Jul 07, 2023

There is no pending certificate request.

3. Click **EXPORT**.

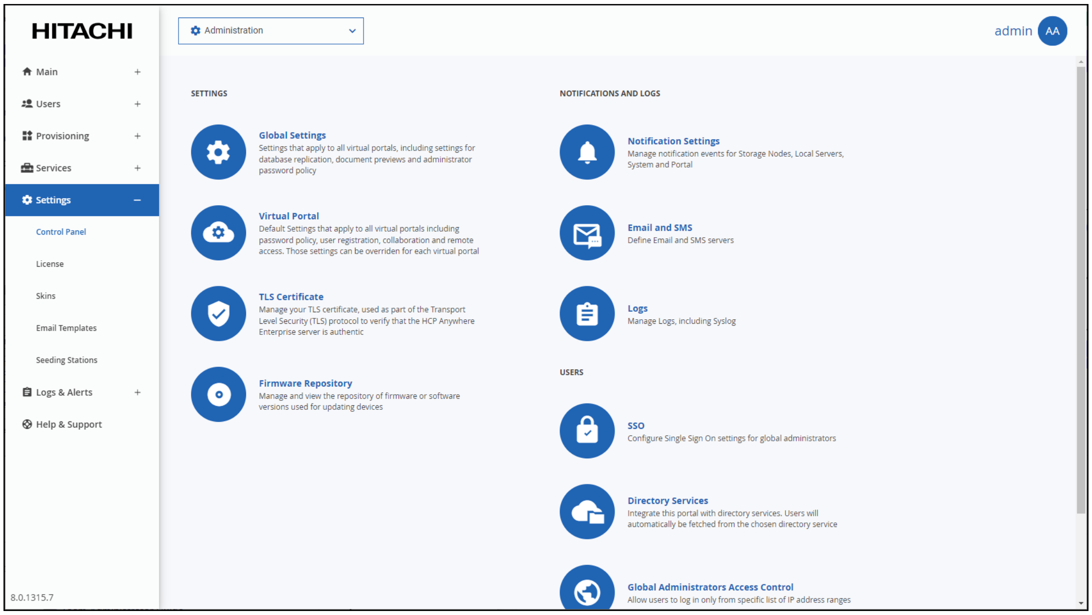
   A ZIP file, including the certificate and private key, is downloaded to your computer.

   Warning: This file is security sensitive, and sending it over an insecure link may enable the server to be compromised.

Importing a TLS Certificate

To import a TLS certificate:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



Global Settings Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository Manage and view the repository of firmware or software versions used for updating devices

Notification Settings Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS Define Email and SMS servers

Logs Manage Logs, including Syslog

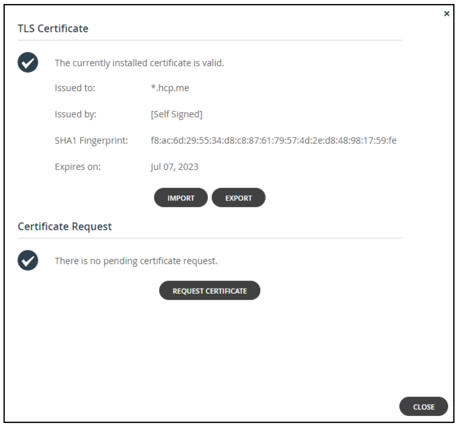
SSO Configure Single Sign On settings for global administrators

Directory Services Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control Allow users to log in only from specific list of IP address ranges

2. Select **LS Certificate** under **SETTINGS** in the **Control Panel** page.

   The **TLS Certificate** window is displayed.



TLS Certificate

✓ The currently installed certificate is valid.

Issued to: *.hcp.me

Issued by: [Self Signed]

SHA1 Fingerprint: f8:ac:6d:29:55:34:d8:c8:87:61:79:57:4d:2e:d8:48:98:17:59:fe

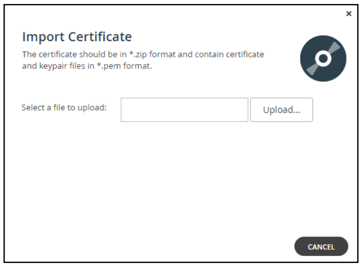
Expires on: Jul 07, 2023

Certificate Request

✓ There is no pending certificate request.

3. Click **IMPORT**.

   The **Import Certificate** window is displayed.



Import Certificate

The certificate should be in *.zip format and contain certificate and keypair files in *.pem format.

Select a file to upload:

4. Click **Upload** and browse to the ZIP file containing the certificate components.
5. Click **Open** and then **FINISH**.

Chapter 6. Managing Storage Nodes

HCP Anywhere Enterprise Portal can write your data to storage nodes from many different vendors. The **STORAGE NODES** page in the global administration view enables you to easily add new storage nodes, dedicate storage nodes to virtual portals, stop and start writing to different storage nodes, and migrate data seamlessly from one storage node to another storage node.

Note: Hitachi Vantara recommends that whenever you create a new S3 bucket to use as the backend storage for a storage node, you enable *object lock* on the bucket.

In this chapter

HCP Anywhere Enterprise provides a storage node with the installation, Local Filesystem, which can be used up to a maximum of 20TB.

Using More than One Storage Node

You can define multiple storage nodes. When there are multiple storage nodes, HCP Anywhere Enterprise manages the writes so that the nodes are balanced in the following cases:

- When multiple storage nodes are defined that are not dedicated to specific virtual portals. If a storage node is down, data is not written to that node, but to the other storage nodes that are up.
- When multiple storage nodes are dedicated to the same virtual portal. If a storage node dedicated to the virtual portal is down, data is not written to that node, but to the other storage nodes dedicated to the same virtual portal, that are up.

Cloud Storage Routing: Grouping Storage Nodes in a Storage Class

Cloud storage routing uses storage classes, which represent a group of one or more storage nodes that share a similar business requirement, such as location. For example, a storage class can consist of a number of storage nodes all in the same location. Each cloud folder group can be assigned to a storage class to enable the cloud folder group content to be written to a specific storage node.

Storage classes can be used to provide the following main benefits:

- Data Sovereignty (GDPR)
- Cost Savings

- Business Efficiency

Data Sovereignty

Data sovereignty has become critical as strict rules dictate where data is stored and how it is moved, including differing laws and regulations across countries and regions. With HCP Anywhere Enterprise Cloud Storage Routing, organizations can maintain data sovereignty, as well as compliance with GDPR and other regulations.

Cost Savings

By being able to select the cloud provider that exists nearest where the data creation is, huge cost savings can be achieved. Also, you can configure the routing to ensure that folder group content that is not accessed regularly, such as archived data, is always written to cheaper storage.

Business Efficiency

Your organization needs quick access to data in order to function efficiently. Until now, this hasn? always been possible, with data often stored in different places and especially when utilizing cloud data storage providers. HCP Anywhere Enterprise Cloud Storage Routing provides low- latency access to data, ensuring that your teams always have access to the data they need.

The team portal administrator can define cloud folder groups to write to a specific storage class, optimizing use of that cloud folder group with one or more of the benefits outlined above.

Storage classes are defined using CLI. The storage nodes are assigned initially to a default storage class. The storage class can be changed from the default when the storage node is defined. After the storage node is defined the storage class cannot be changed.

Defining a Storage Class

Storage classes are defined using CLI. To run the CLI from the portal user interface, see Execute CLI Commands from the Global Admin User Interface. Use the following CLI to create a storage class: `add /storageClasses/ name <name>`

where *name* is the name you call the storage class.

Assigning a Storage Class to a Storage Node

After defining the storage class, as described above in Defining a Storage Class, you can assign it to a specific storage node as part of the general storage node definition, described in Adding and Editing Storage Nodes

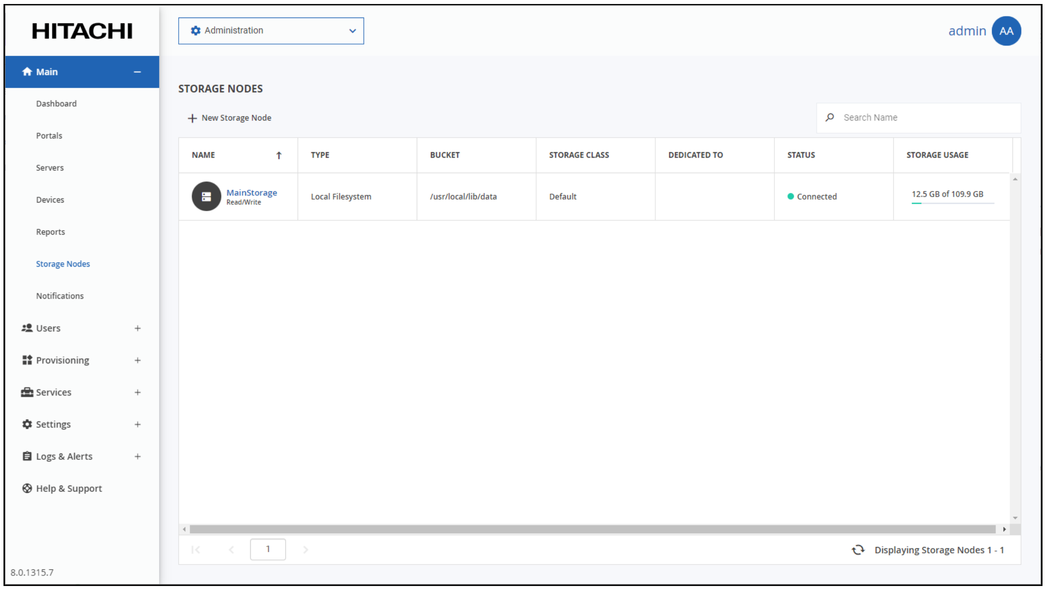
Changing the Name of a Storage Class

After defining a storage class, as described above in Defining a Storage Class, you can change the name using the following CLI:
`set /storageClasses/<currentSCName>/ name <newSCName>` where <*currentSCName*> is the name of the storage class to change and <*newSCName*> is the name to change it to.

Viewing Storage Nodes

To view all storage nodes in the system:

- In the global administration view, select **Main > Storage Nodes** in the navigation pane.
  The **STORAGE NODES** page is displayed.



STORAGE NODES

New Storage Node

Search Name

NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		● Connected	12.5 GB of 109.9 GB

Displaying Storage Nodes 1 - 1

The following information is displayed for each storage node:

NAME – The storage node's name.

Status (under the name) – Whether the storage node is read/write enabled or read and delete only.

TYPE – The storage node's type.

BUCKET – The name of the storage node's bucket.

STORAGE CLASS – The group of one or more storage nodes to which this storage node belongs.

DEDICATED TO – The name of a single team portal to which the storage node is dedicated, if applicable. The storage node is used for this team portal and no other team portal uses it. The team portal will only write to storage nodes that are dedicated to it and not to other storage nodes.

STATUS – The storage node's current status. This can be either of the following:

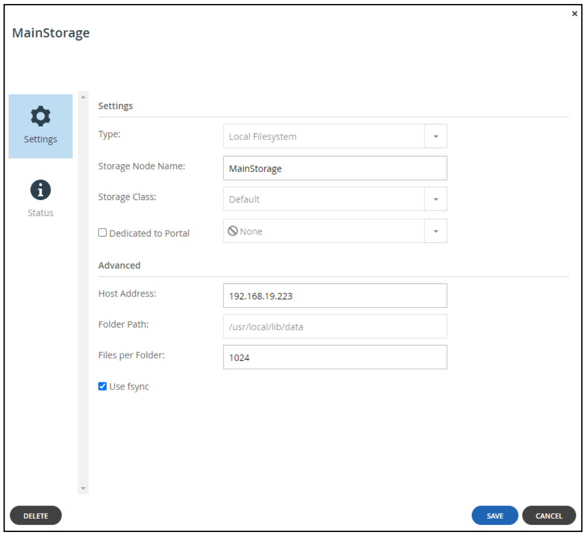
- Connected
- Not Connected

The HCP Anywhere Enterprise Portal does not attempt to store new blocks in storage nodes that are not connected.

STORAGE USAGE – The amount of storage available, followed by the amount of used storage. This field is only relevant for the **Local Filesystem** storage node, which is the default storage node when setting up the HCP Anywhere Enterprise Portal.

To view details of a specific node:

- Click the node name on the **STORAGE NODES** page.
  The storage node window is displayed with the storage node name as the window title.



MainStorage

Settings

Type: Local Filesystem

Storage Node Name: MainStorage

Storage Class: Default

☐ Dedicated to Portal: None

Advanced

Host Address: 192.168.19.223

Folder Path: /usr/local/lib/data

Files per Folder: 1024

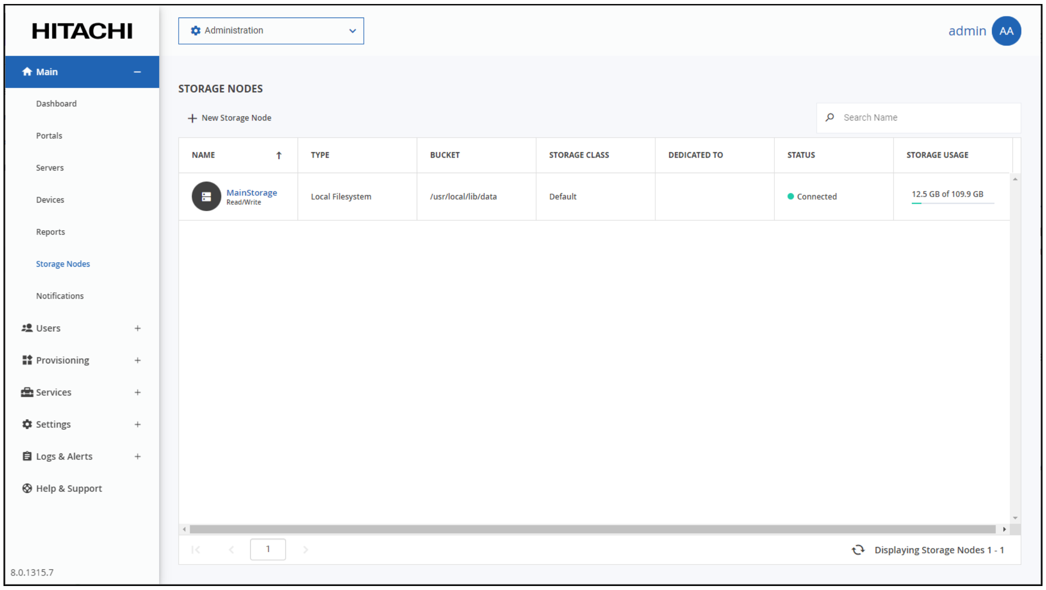
☑ Use fsync

The details displayed depend on the type of storage node.

Adding and Editing Storage Nodes

To add or edit a storage node:

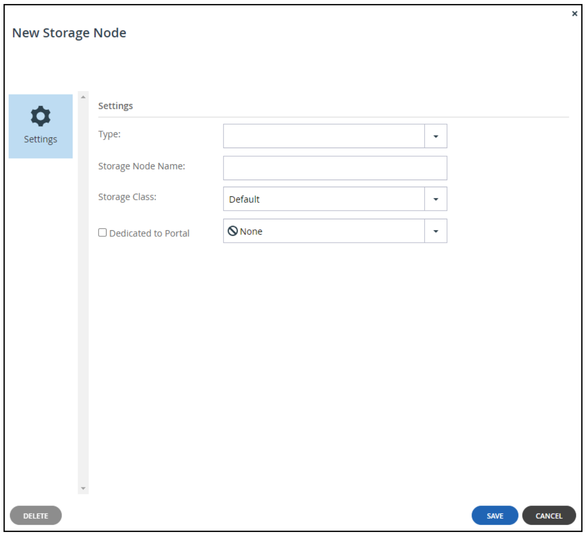
1. For the **Generic (NFS)** storage node:
   - **a)** Log in to the server as root, using SSH.
   - **b)** Create a folder for the NFS mount on the server.
   - **c)** Mount the NFS storage node to each server, except the preview server, by running the following script on each server:
     `portal-mount.sh mount_storage_node` *`NFS_IP`*`:/`*`NFS_FOLDER`*
     where *NFS_IP* is the IP address of the NFS mount point, and *NFS_FOLDER* is the name of the folder you created on the NFS server.
2. In the global administration view, select **Main > Storage Nodes** in the navigation pane.
   The **STORAGE NODES** page is displayed.



NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		● Connected	12.5 GB of 109.9 GB

3. Either,

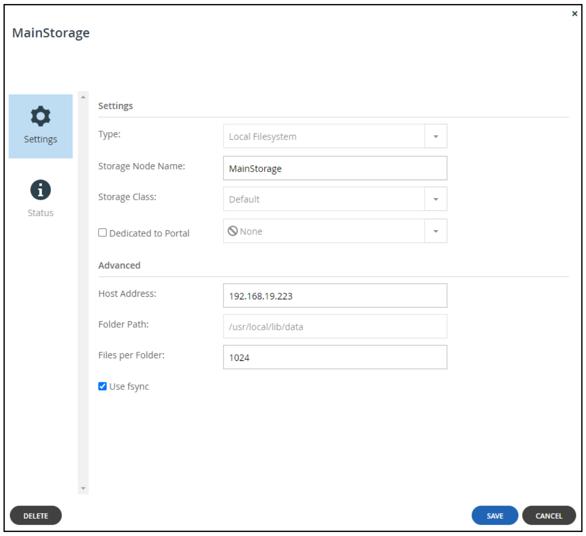
- Add a storage node, click **New Storage Node**.
  The **New Storage Node** window is displayed.



Type:	
Storage Node Name:	
Storage Class:	Default
□ Dedicated to Portal	None

Or,

- Edit an existing storage node; click the node's name**.**
  The storage node window is displayed with the storage node name as the window title.



Settings

Type: Local Filesystem

Storage Node Name: MainStorage

Storage Class: Default

☐ Dedicated to Portal: None

Advanced

Host Address: 192.168.19.223

Folder Path: /usr/local/lib/data

Files per Folder: 1024

☑ Use fsync

The details displayed depend on the type of storage node. When editing a storage node you can only edit enabled values, such as **Storage Node Name**.

4. Enter the generic details for the storage node. These details are the same for every type of storage node.

Type – The type of storage node you are adding. When you select the type, more fields are displayed so that you can add the specific details for the storage node, as described for each storage node listed in step .
Storage Node Name – A unique name to identify the storage node.
Storage Class – The storage class that will include this storage node. After defining the storage node, the storage class cannot be changed.
Note: The storage classes are defined using CLI. For details, see Defining a Storage Class.
Dedicated to Portal – Dedicate the storage node to one team portal selected from the drop-down list. The storage node is used for this team portal and no other team portal uses it. The team portal will only write to storage nodes that are dedicated to it and not to other storage nodes.

5. Complete the additional fields that are displayed when you choose the type.

- Amazon S3
- Generic (NFS)
- Generic (S3)
- GenericS3V4
- Google Cloud Storage (S3)
- Hitachi HCP
- HCP Hitachi Vantara (S3)
- Local Filesystem
- Microsoft Azure Blob Storage

Note: Other storage nodes in the list are currently not supported.

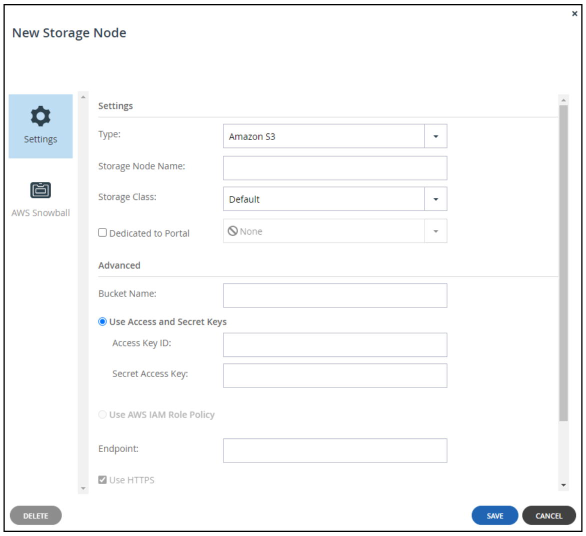
6. Click **SAVE**.

Note: All data in transit to and from a storage node, and stored in the storage node is encrypted by the HCP Anywhere Enterprise Portal.

Amazon S3

All AWS S3 buckets that support instant access, including *Standard*, *Standard-IA*, *Intelligent-Tiering*, and *Glacier Instant Retrieval*, are supported. Refer to AWS documentation for the differences between these storage types.

Note: All data in transit to and from a storage node and at rest, stored in the Amazon S3 storage node, is encrypted. In addition, SSE-S3 encryption is automatically set on all S3 buckets. You can also use AWS Key Management Service (SSE-KMS) keys to further encrypt your data (SSE-KMS).
Hitachi Vantara recommends that in order to keep the log clean of CloudWatch based errors, Amazon CloudWatch should be associated with the user creating the Amazon S3 storage node.



New Storage Node

Settings

Type: Amazon S3

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal — None

Advanced

Bucket Name:

● Use Access and Secret Keys

Access Key ID:

Secret Access Key:

○ Use AWS IAM Role Policy

Endpoint:

☑ Use HTTPS

Note: As soon as you specify that the storage node is Amazon S3, an **AWS Snowball** option is added to the **New Storage Node** window. For details, see Setting Up the HCP Anywhere Enterprise Portal with AWS Snowball.

Bucket Name – The unique name of the Amazon S3 bucket that you want to add as a storage node.

Use Access and Secret Keys – Use Amazon S3 access credentials for the storage node.
Access Key ID – The AWS S3 access key ID.
Secret Access Key – The AWS S3 secret access key.

Use AWS IAM Role Policy – When the portal is also running as an AWS EC2 instance, you can define an IAM policy and then assign this policy to an EC2 role which is then attached to the portal instance, via Instance **Settings > Attach/Replace IAM Role** in the AWS Management Console. If you set up this type of policy, you do not need to specify the Access and Secret keys to access the storage node.

Endpoint – The private endpoint name of the S3 service. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

Use HTTPS – Use HTTPS to connect with the storage node.

Trust all certificates – Do not validate the certificate of the object storage. Normally this is unchecked.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

Note: Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Add Metadata Tags – Use custom metadata to support information lifecycle management rules (ILM) on the storage node. Checking **Add Metadata Tags** implements the ILM, enabling storage tiering so that data can be routed across different object storages.

Using Amazon S3 Versioning to Protect Against Ransomware Attacks

Amazon S3 Versioning is a version control feature for S3 that enables you to revert to older versions of an S3 object, which helps provide protection against accidental or malicious deletion such as from a ransomware attack.

You can protect these versions from ransomware attacks in the following ways:

- You can define a bucket policy to grant permissions and ensure that only users with the necessary permissions will be able to permanently delete an object from a previous version. In this way you will be able to restore your data from a previous version, safeguarding your environment from ransomware attacks.
- When working with S3 Versioning in Amazon S3 buckets, you can optionally add another layer of security by configuring a bucket to enable MFA (multi-factor authentication) delete. When you do this, the bucket owner must include two forms of authentication in any request to delete a version or change the versioning state of the bucket. MFA delete requires additional authentication to change the versioning state of your bucket or to permanently deleting an object version. Both your security credentials and the concatenation of a valid serial number, a space, and the six-digit code displayed on an approved authentication device are required together to permanently delete an object version. MFA delete thus provides added security if, for example, your security credentials are compromised. MFA delete can help prevent accidental bucket deletions by requiring the user who initiates the delete action to prove physical possession of an MFA device with an MFA code. To use MFA delete, you can use either a hardware or virtual MFA device to generate an authentication code.

You can use either or both of these options to protect your data.

For details about setting up S3 versioning, see Configuring Amazon S3 Versioning.

Configuring Amazon S3 Versioning

Amazon S3 Versioning is a version control feature for S3 that enables you to revert to older versions of an S3 object, which helps provide protection against accidental or malicious deletion such as from a ransomware attack.

Versioning keeps multiple versions of an object in the same bucket. When you enable it on a bucket, Amazon S3 automatically adds a unique version ID to every object stored in the bucket. At that point, a simple DELETE action does not permanently delete an object version; it merely associates a delete marker with the object. You can then use the versioning features to retrieve the deleted object or an earlier version of the object if needed. If you want to permanently delete an object version, you must specify its version ID in your DELETE request.

You can define a bucket policy to grant permissions and ensure that only users with the necessary permissions will be able to permanently delete an object from a previous version.

Note: Bucket policy can be attached to your bucket on creation, or at any time afterwards. When a bucket policy is defined for the bucket along with a lifecycle rule to change the bucket storage class, as described in Using AWS S3 Intelligent-Tiering For Storage, the policy is transferred to the new storage class.

To set up versioning:

Note: The following procedure does not protect the versions from ransomware attacks

1. From your Amazon Web Services account, sign-in to the AWS Management Console and select Services.
2. Under **Storage** select **S3**.
3. Click the HCP Anywhere Enterprise Portal bucket from the S3 buckets list and then select the **Properties** tab to check that **Versioning** is enabled.

   The properties for the bucket are displayed.
4. Under **Bucket Versioning** click **Edit** and then chose **Enable**.
5. Click **Save changes**.

Note: When **Versioning** is enabled, you are paying for multiple versions of the same document, which you will want to remove in line with the HCP Anywhere Enterprise Portal retention policy.

To set a bucket policy to safeguard versions against ransomware attacks:

1. From your Amazon Web Services account, click the HCP Anywhere Enterprise Portal bucket from the S3 buckets list and then select the **Permissions** tab.
   The permissions details for the bucket are displayed.
2. Scroll to **Bucket policy** and click **Edit**.
3. Paste the following policy document into the Bucket policy area:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyDeletePreviousVersions",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:DeleteObjectVersion",
            "Resource": "arn:aws:s3:::<bucketname>/*",
            "Condition": {
                "Null": {
                    "s3:VersionId": "true"
                }
            }
        }
    ]
}
```

where *bucketname* is the name of the bucket.
With this policy, previous versions can only be deleted by removing the policy, by an administrator with the necessary permissions. After a ransomware attack, a previous version can be restored in place of the current version that is no longer accessible after a ransomware attack.

4. Click **Save changes**.

To Enable MFA delete:

You can only enable MFA delete via AWS CLI or REST API. The bucket owner, the AWS account that created the bucket (root account), and all authorized users can enable versioning. However, only the bucket owner (root account) can enable MFA delete.

For details about how to configure MFA delete, see https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiFactorAuthenticationDelete.html.

To set up versioning and to allow deleting files after a fixed number of days:

Note: The following procedure does not protect the versions from ransomware attacks

1. From your Amazon Web Services account, click the HCP Anywhere Enterprise Portal bucket from the S3 buckets list and then select the Management tab.
   The management details for the bucket are displayed.
2. Click **Create lifecycle rule**.

   The **Create lifecycle rule** page is displayed.
3. Enter a name for the rule and chose **Apply to all objects in the bucket**.
4. Check the acknowledgment that is displayed.
5. Under **Lifecycle rule actions** check **Permanently delete noncurrent versions of objects** and **Delete expired delete markers or incomplete multiple uploads**.

   The page changes to display **Permanently delete noncurrent versions of objects** and **Delete expired object delete markers or incomplete multipart uploads** sections.
6. Specify the number of days in **Days after objects become noncurrent**, after which the noncurrent versions of objects are permanently deleted.

   Hitachi Vantara recommends that you retain versioned objects for the same number of days that the metadata of deleted objects is retained by the HCP Anywhere Enterprise Portal (the default is 30 days).
7. Check **Delete expired object delete markers**.
8. Review the details of the rule and if satisfied, click Create rule.

   Lifecycle rules run once a day at midnight UTC.

   Note: The first time the rule runs, it can take up to 48 hours.

Using AWS Intelligent Tiering For HCP Anywhere Enterprise Portal Storage

Each object in Amazon S3 has an Amazon S3 storage class associated with it. Amazon S3 offers a range of S3 storage classes for the objects that you store. You choose a class depending on your use case scenario and performance access requirements.

The **S3 Standard** storage class is the default storage class if you don't specify a storage class when you upload an object to AWS. However, Amazon also offer a storage class that automatically optimizes frequently and infrequently accessed objects, the **S3 Intelligent-Tiering** storage class.

The **S3 Intelligent-Tiering** storage class is designed to optimize storage costs by automatically moving data to the most cost-effective storage access tier, without performance impact or operational overhead.

How Does Intelligent Tiering Work?

The **S3 Intelligent-Tiering** storage class is suitable for objects larger than 128 KB that you plan to store for at least 30 days. The storage class stores objects in two access tiers: one tier that is optimized for frequent access and another lower-cost tier that is optimized for infrequently accessed data. Amazon S3 monitors access patterns of the objects in the storage class and moves data on a granular object level that has not been accessed for 30 consecutive days to the infrequent access tier.

With intelligent tiering, you are charged a monthly monitoring and automation fee per object instead of retrieval fees. If an object in the infrequent access tier is accessed, it is automatically moved back to the frequent access tier, but no fees are applied when objects are moved between access tiers within the S3 Intelligent-Tiering storage class.

The bigger the block size, the larger the savings. Hitachi Vantara recommends using the **S3 Intelligent-Tiering** storage class when the block size is set to 1MB or larger. If the block size is less than 1MB, contact Hitachi Vantara support to see whether there is a saving. The larger the average object size the more negligible is the monitoring and automation fee as part of the whole fee. Whether you use intelligent tiering or not is mainly dependent on the following considerations:

- The average block size of your objects. The **S3 Intelligent-Tiering** storage class is suitable for objects larger than 128KB. In HCP Anywhere Enterprise Portal files are broken down in to blocks and the block size is controlled by the **Average Block Size** setting in the **Virtual Portal Settings**. The default average block size is 512KB.

  Note: Use **Fixed Block Size** if direct mode is defined for the storage node and Hitachi Vantara recommends keeping the default 4MB fixed block size.
  HCP Anywhere Enterprise Portal file maps are typically small and are not included in the intelligent tiering transition rule.
- The percentage of infrequently accessed data.
- The percentage of objects stored for less than 30 days. The **S3 Intelligent-Tiering** storage class is suitable for objects that you plan to store for at least 30 days and if you delete an object before the end of the 30-day minimum storage duration period, you are charged for 30 days. HCP Anywhere Enterprise Portal retains deleted files for at least 30 days, to enable undeleting a file, meaning that this requirement can be ignored.

Changing Storage to Intelligent Tiering

Before transitioning storage to the **S3 Intelligent-Tiering** storage class, Hitachi Vantara recommends checking the average size of the objects being stored and the days they are held in storage.

Note: When a version is defined for the bucket with a policy to rectify a ransomware attack, as described in Integrating HCP Anywhere Enterprise Portal with S3-Versioned Buckets, the policy is transferred to the **S3 Intelligent-Tiering** storage class.

To transition storage to intelligent tiering storage:

1. From your Amazon Web Services account, sign in to the AWS Management Console and select **Services**.
2. Under **Storage**, select **S3**.
3. Click the HCP Anywhere Enterprise Portal bucket from the S3 buckets list and then select the **Management** tab.

   The management details for the bucket are displayed.
4. Click **Create lifecycle rule**.

   The **Create Lifecycle rule** wizard is displayed.
5. Enter a name for the rule, make sure **Limit the scope of this rule using one or more filters** is chosen and in the **Filter type prefix** text box enter `blocks`.
6. Under **Lifecycle rule actions** check **Move current versions of objects between storage classes**.

   The page changes to display **Transition current versions of objects between storage classes** section.
7. For **Choose storage class transitions** select `Intelligent-Tiering` and specify the number of days for the transition after the object is created. For example, 7.
8. Review the details of the rule and if satisfied, click **Create rule**.

Lifecycle rules run once a day at midnight UTC.

Note: The first time the rule runs, it can take up to 48 hours.

Use management metrics to validate the storage transition.

To access management metrics for an S3 bucket:

1. From your Amazon Web Services account, sign in to the AWS Management Console and select **Services**.
2. Under **Storage**, select **S3**.
3. Click the HCP Anywhere Enterprise Portal bucket from the S3 buckets list and then select the **Metrics** tab.

   The metrics for the bucket are displayed. Graphs are displayed after transitioning to the **S3 Intelligent-Tiering** storage class.

Setting Up the HCP Anywhere Enterprise Portal with AWS Snowball

The AWS Snowball service is part of the AWS Snow Family and uses physical storage devices, Snowball Edge devices, to transfer large amounts of data between your on-premise storage and Amazon S3 storage in the cloud at faster-than-Internet speeds. By working with AWS Snowball, you can save time and money when ingesting large quantities of data from an edge filer to an AWS S3 storage node managed by a HCP Anywhere Enterprise Portal. You install one or more AWS Snowball Edge devices on the same network as the HCP Anywhere Enterprise Edge Filer so that the data is first moved from the HCP Anywhere Enterprise Edge Filer to the Snowball Edge device and from there to the AWS account where it is managed by Amazon to move it to the appropriate AWS S3 storage bucket.

Note: Snowball is intended for transferring large amounts of data. If you want to ingest less than tens of TB of data, Snowball might not be your most economical choice.

An AWS Snowball Edge device can handle around 80TB of data. If you are transferring more than the maximum storage for a Snowball Edge device, you need multiple Snowball Edge devices. Each Snowball Edge device must be associated with a different AWS S3 bucket. Therefore, for each Snowball Edge device required, a separate Amazon S3 storage node is required, with each storage node associated with a different AWS S3 bucket.

After all the data has been written to the Snowball Edge devices it is transferred to Amazon, using an AWS courier and Amazon is responsible for populating the S3 buckets with the data. When the data is stored on multiple Snowball Edge devices, all the devices **must** be shipped at the same time.

You associate each Amazon S3 storage node defined in the HCP Anywhere Enterprise Portal with an AWS Snowball Edge device.

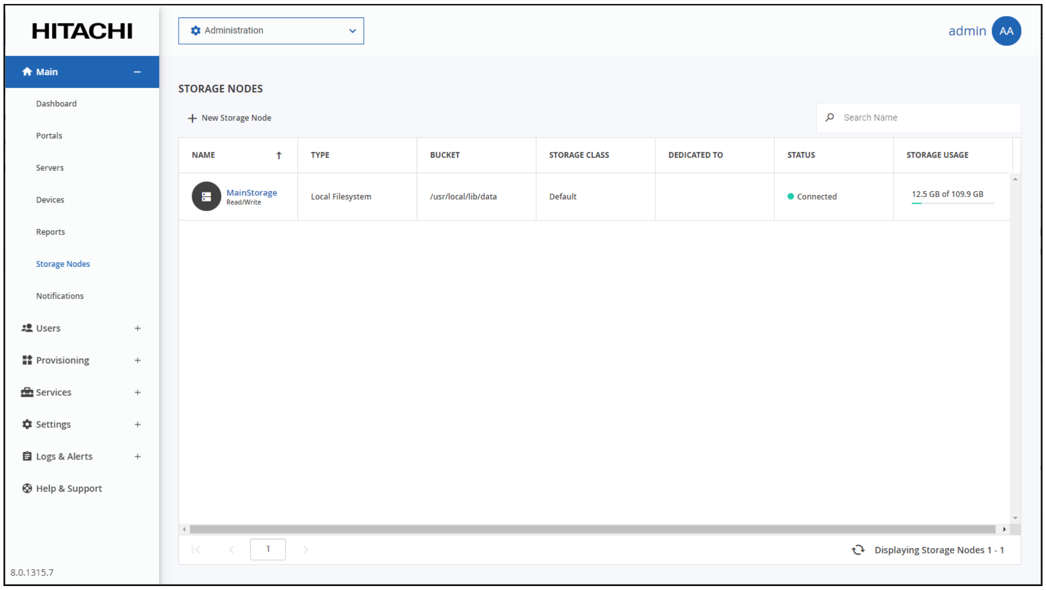
To set up Snowball Edge devices:

- Refer to AWS documentation.
  Hitachi Vantara requires that each Snowball Edge device must be connected to a single AWS S3 bucket. You need to know for each server the respective bucket when you set up the HCP Anywhere Enterprise Portal. Also, the Snowball Edge devices must be on the same network as the HCP Anywhere Enterprise Edge Filer.

To set up Snowball usage in the HCP Anywhere Enterprise Portal:

1. Calculate how many AWS Snowball Edge devices and Amazon S3 storage node are required. Divide the amount of storage to migrate to HCP Anywhere Enterprise Portal by the maximum usable storage possible on one AWS Snowball Edge device.
   For example, if the existing file server holds 460TB of data you need 6 AWS Snowball Edge devices to handle the data and therefore 6 AWS storage buckets, with each storage bucket assigned an Amazon S3 storage node.

   Note: Deduplication and compression often reduce the final amount of storage required by the storage nodes at the end of the process.
2. Define the Amazon S3 storage node or nodes, one node for each AWS bucket.
   a) In the global administration view, select **Main > Storage Nodes** in the navigation pane.
   The **STORAGE NODES** page is displayed.



STORAGE NODES

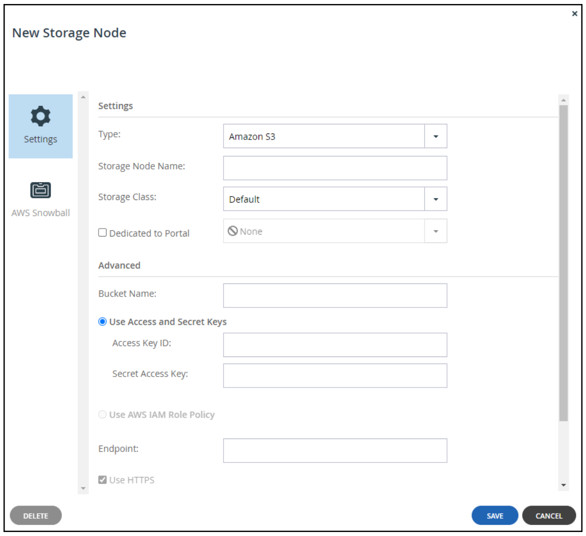
NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		● Connected	12.5 GB of 109.9 GB

Displaying Storage Nodes 1 - 1

b) Click **New Storage Node**.
The **New Storage Node** window is displayed.

c) Enter the generic details for the storage node.
Type – The type of storage node. Select Amazon S3 from the drop-down text box.
As soon as you specify that the storage node is Amazon S3, an **AWS Snowball** option is added to the **New Storage Node** window.
Storage Node Name – A unique name to identify the storage node.
Dedicated to Portal – When using Snowball, you **must** dedicate the storage node to one virtual portal selected from the drop-down list.

d) Complete the additional fields that are displayed.



Settings

Type: Amazon S3

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal   None

Advanced

Bucket Name:

● Use Access and Secret Keys

Access Key ID:

Secret Access Key:

○ Use AWS IAM Role Policy

Endpoint:

☑ Use HTTPS

Bucket Name – The unique name of the Amazon S3 bucket that you want to add as a storage node.
Use Access and Secret Keys – Use Amazon S3 access credentials for the storage node. These are the credentials for the bucket in AWS S3, and not for the bucket on the Snowball

Edge device.

Access Key ID – The AWS S3 access key ID.

Secret Access Key – The AWS S3 secret access key.

Use AWS IAM Role Policy – When the portal is also running as an AWS EC2 instance, you can define an IAM policy and then assign this policy to an EC2 role which is then attached to the portal instance, via Instance **Settings > Attach/Replace IAM Role** in the AWS Management Console. If you set up this type of policy, you do not need to specify the Access and Secret keys to access the storage node.

Endpoint – The endpoint name of the S3 service. The default value for Amazon S3 is s3.amazonaws.com. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

Use HTTPS – Use HTTPS to connect with the AWS S3 storage node.

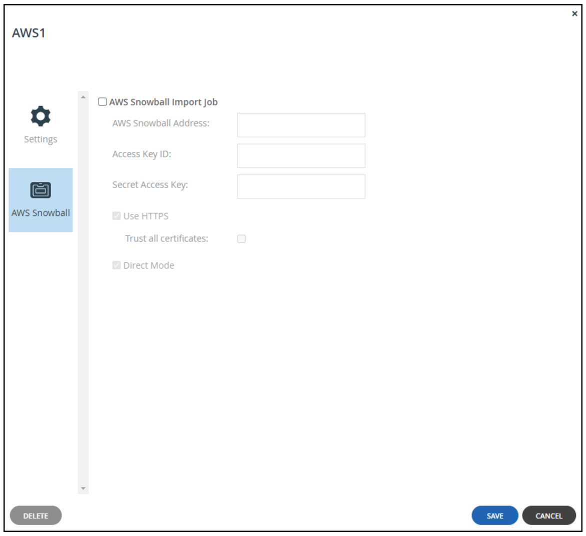
Trust all certificates – Do not validate the certificate of the object storage. Normally this is unchecked.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. Direct mode **must** be defined for the storage node. Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size.

Note: Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Add Metadata Tags – For internal use. This must be unchecked.

3. Click **AWS Snowball**.
4. The AWS Snowball window is displayed.



AWS1

☐ AWS Snowball Import Job

AWS Snowball Address:

Access Key ID:

Secret Access Key:

☑ Use HTTPS

Trust all certificates: ☐

☑ Direct Mode

5. Check **AWS Snowball Import Job** and then specify the Snowball Edge device details:

AWS Snowball Address – The address of the Snowball Edge device, including the port, either 8443 when using HTTPS or 8080 when using HTTP.

Access Key ID – The AWS Snowball Edge device access key ID.

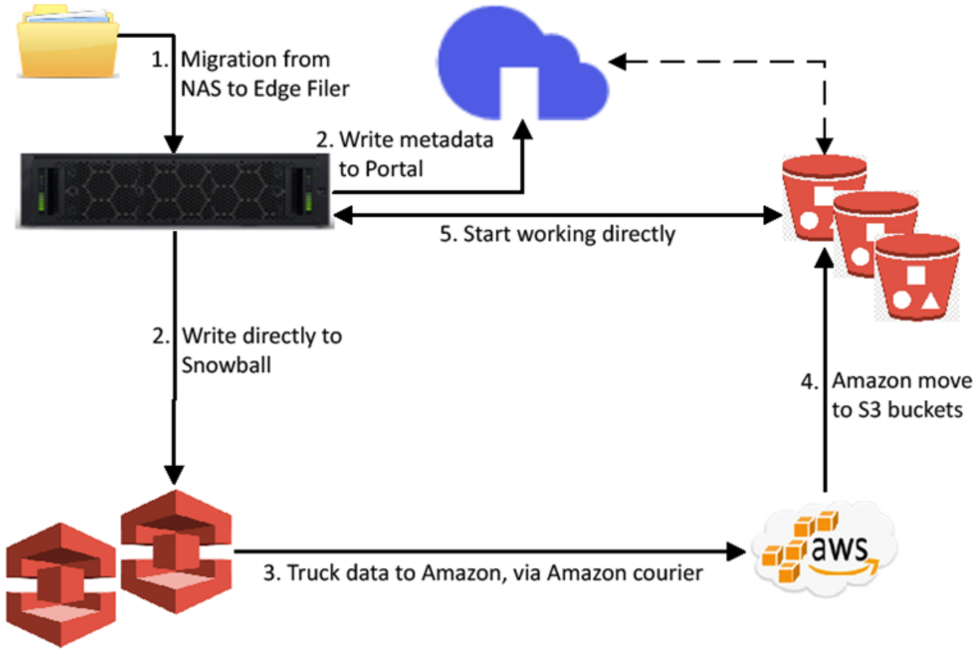
Secret Access Key – The AWS Snowball Edge device secret access key.

Use HTTPS – Use HTTPS to connect with the storage node. Only check this box if SSL is configured on the Snowball Edge device and you require high security. Typically, since the Snowball Edge device is on the local network this can be left unchecked.

Trust all certificates – Trust any security certificate installed on the Snowball Edge device. Since the Snowball Edge device certificate is typically untrusted, this should be checked.

Direct Mode – Data is uploaded directly to the Snowball Edge device. You cannot change this setting.

6. Click **SAVE**.


1. Migration from NAS to Edge Filer
2. Write metadata to Portal
5. Start working directly
2. Write directly to Snowball
4. Amazon moves data to S3 buckets
3. Truck data to Amazon, via Amazon courier
aws

When the HCP Anywhere Enterprise Edge Filer is connected to the HCP Anywhere Enterprise Portal, you can optionally use the HCP Anywhere Enterprise Edge Filer Migration Tool to migrate the data from the existing file server to the HCP Anywhere Enterprise Edge Filer, step 1 in the diagram, which then writes the data directly to the Snowball Edge devices, step 2 in the diagram. At the same time the HCP Anywhere Enterprise Edge Filer writes the metadata to the HCP Anywhere Enterprise Portal, step 2 in the diagram.

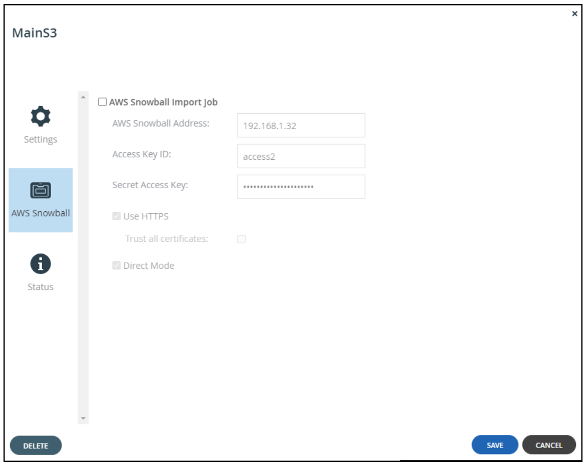
Note: While the data is being written to the Snowball Edge devices, it can be accessed from the HCP Anywhere Enterprise Edge Filer but not from the HCP Anywhere Enterprise Portal or other HCP Anywhere Enterprise Edge Filers which do not have access to the Snowball Edge device. If you want to access the data from the HCP Anywhere Enterprise Edge Filer, you have to disable streaming of data until the data has been fully moved to the HCP Anywhere Enterprise Portal, step 5 in the diagram, described in Managing Streaming to the HCP Anywhere Enterprise Edge Filer.

After all the data has been written to the Snowball Edge devices it is transferred to Amazon, using an AWS courier, step 3 in the diagram. Amazon is responsible for populating the S3 buckets with the data, step 4 in the diagram. When the data is stored on multiple Snowball Edge devices, all the devices **must** be shipped at the same time.

Note: While the data is being transferred to Amazon and moved in to the S3 buckets, it **cannot** be accessed from any HCP Anywhere Enterprise Edge Filer nor from the HCP Anywhere Enterprise Portal.

When the process is complete the job completion report is available from the AWS Management console. Verify that the job completed successfully, from the job report, or if there were errors, check these errors in the *Download failure log*. For details, refer to AWS documentation.

After Amazon completes the job of moving your data into the S3 buckets, you must uncheck **AWS Snowball Import Job** in each of the storage nodes.



MainS3

□ AWS Snowball Import Job

AWS Snowball Address: 192.168.1.32

Access Key ID: access2

Secret Access Key: ••••••••••••••••••••••

☑ Use HTTPS

Trust all certificates: □

☑ Direct Mode

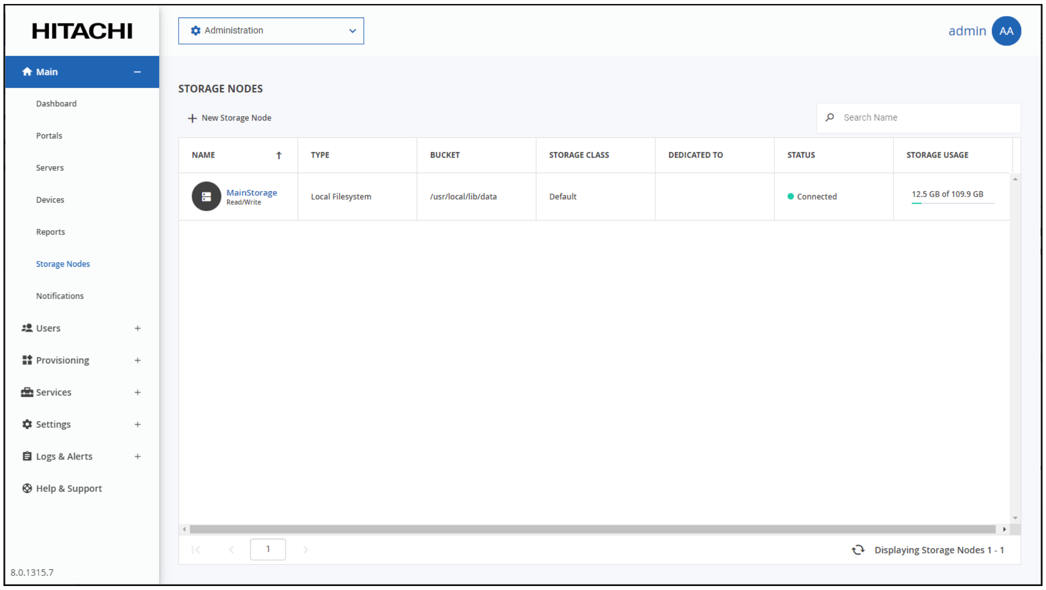
Unchecking **AWS Snowball Import Job** causes the Amazon S3 storage nodes to be treated as standard storage nodes so that the data can be accessed from the HCP Anywhere Enterprise Portal and any HCP Anywhere Enterprise Edge Filer, or HCP Anywhere Enterprise Drive Share (Agents) connected to the portal.

Warning: **If you keep *AWS Snowball Import Job* checked, files that have blocks on the storage node checked as Snowball will be inaccessible from the HCP Anywhere Enterprise Portal or from any HCP Anywhere Enterprise Edge Filers, HCP Anywhere Enterprise Drive Share (Agents) connected to the HCP Anywhere Enterprise Portal.**

After the migration has completed, optionally define all the Amazon S3 storage nodes as read-only except for one which will remain a read/write node.

To optionally define storage nodes as read-only:

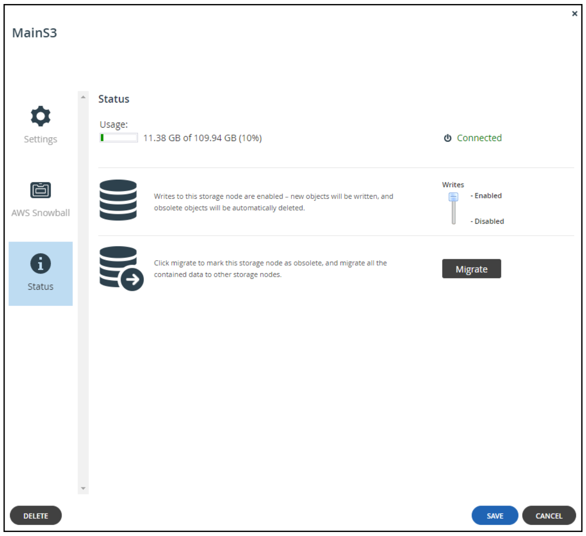
1. In the global administration view, select **Main > Storage Nodes** in the navigation pane. The **STORAGE NODES** page is displayed.



STORAGE NODES

NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		Connected	12.5 GB of 109.9 GB

2. For each Amazon S3 storage node, except for one, click the **Status** option.
3. Move the **Writes** slider to **Disabled**.



Status

Usage:
11.38 GB of 109.94 GB (10%)

Connected

Writes to this storage node are enabled – new objects will be written, and obsolete objects will be automatically deleted.

Click migrate to mark this storage node as obsolete, and migrate all the contained data to other storage nodes.

Managing Streaming to the HCP Anywhere Enterprise Edge Filer

While the data is being written to the Snowball Edge devices, it can be accessed from the edge filer but not from the portal or other edge filers which do not have access to the Snowball Edge device. If you want to access the data from the edge filer, you have to manage streaming data.

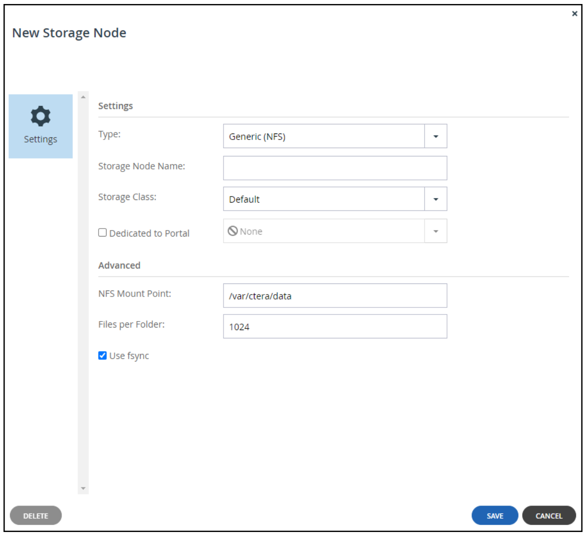
To manage streaming data:

- Run the following CLI in the HCP Anywhere Enterprise Edge Filer:
  ```
  set /config/cloudsync/cloudExtender/minFileSizeForStreamingInMB
  2147483646
  ```

After the data has been moved to the HCP Anywhere Enterprise Portal, enable streaming from the HCP Anywhere Enterprise Portal by running the following CLI in the HCP Anywhere Enterprise Edge Filer: `set /config/cloudsync/cloudExtender/minFileSizeForStreamingInMB 10`

Generic (NFS)

Note: You cannot use a **Generic (NFS)** storage node for storage that exceeds 100TB.



New Storage Node

Settings

Type:	Generic (NFS)
Storage Node Name:	
Storage Class:	Default
□ Dedicated to Portal	None

Advanced

NFS Mount Point:	/var/ctera/data
Files per Folder:	1024

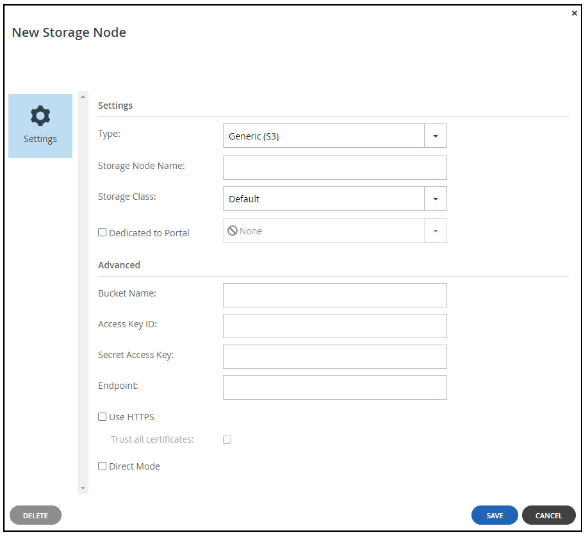
☑ Use fsync

The NFS Mount Point – The name of the NFS mount folder.

Files per Folder – The maximum number of files to store in a folder. The default value is 1024.

Use fsync – Blocks of data should be flushed to disk immediately. Using fsync prevents data loss in the event of a power failure.

Generic (S3)



New Storage Node

Settings

Type: Generic (S3)

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal None

Advanced

Bucket Name:

Access Key ID:

Secret Access Key:

Endpoint:

□ Use HTTPS

Trust all certificates: □

□ Direct Mode

Bucket Name – The unique name of the S3 bucket that you want to add as a storage node.

Access Key ID – The S3 access key ID.

Secret Access Key – The S3 secret access key.

Endpoint – The endpoint name of the S3 service. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

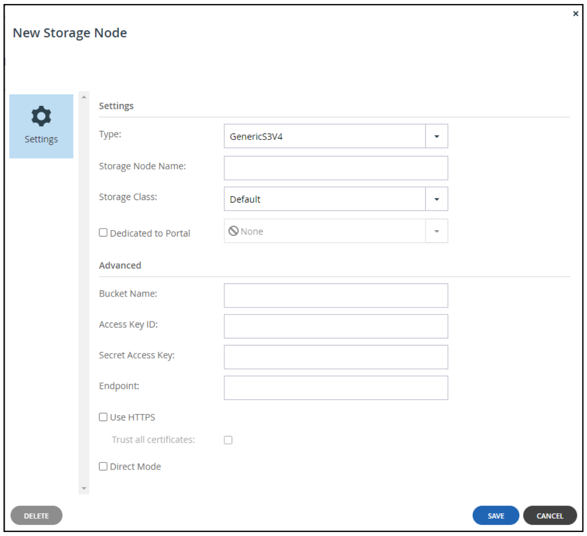
Use HTTPS – Use HTTPS to connect with the storage node.

Trust all certificates – Do not validate the certificate of the object storage. Normally this is unchecked.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

Note: Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

GenericS3V4



Settings

Type: GenericS3V4

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal None

Advanced

Bucket Name:

Access Key ID:

Secret Access Key:

Endpoint:

□ Use HTTPS

Trust all certificates: □

□ Direct Mode

Bucket Name – The unique name of the S3 bucket that you want to add as a storage node.

Access Key ID – The S3 access key ID.

Secret Access Key – The S3 secret access key.

Endpoint – The endpoint name of the S3 service. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

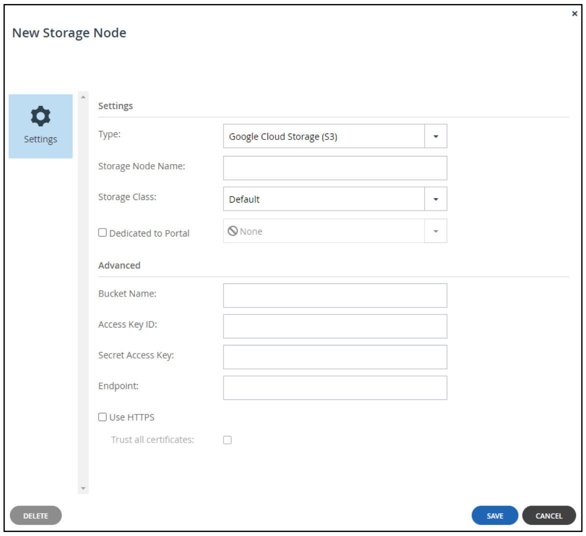
Use HTTPS – Use HTTPS to connect with the storage node.

> **Trust all certificates** – Do not validate the certificate of the object storage. Normally this is unchecked.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

> **Note:** Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Google Cloud Storage (S3)



New Storage Node

Settings

Type: Google Cloud Storage (S3)

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal None

Advanced

Bucket Name:

Access Key ID:

Secret Access Key:

Endpoint:

□ Use HTTPS

Trust all certificates: □

Bucket Name – The unique name of the S3 bucket that you want to add as a storage node.

Access Key ID – The S3 access key ID.

Secret Access Key – The S3 secret access key.

Endpoint – The endpoint name of the S3 service. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

Use HTTPS – Use HTTPS to connect with the storage node.

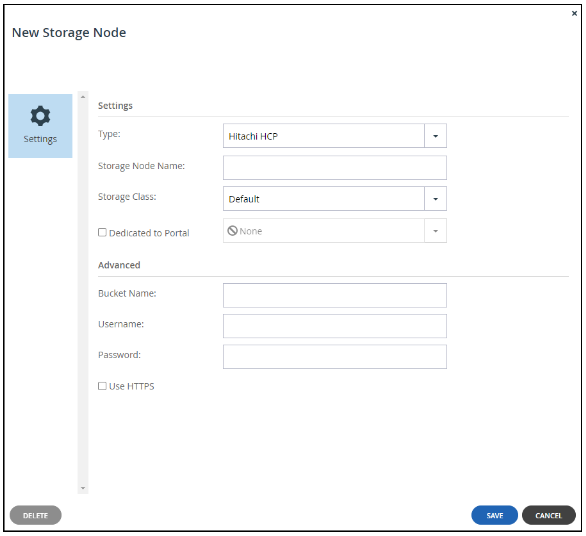
Trust all certificates – Do not validate the certificate of the object storage. Normally this is unchecked.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

Note: Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Hitachi HCP

The minimum version of Hitachi HCP supported by HCP Anywhere Enterprise Portal is 7.0.



New Storage Node

Settings

Type: Hitachi HCP

Storage Node Name:

Storage Class: Default

☐ Dedicated to Portal None

Advanced

Bucket Name:

Username:

Password:

☐ Use HTTPS

Bucket Name – The name of your Hitachi HCP bucket.

User – The user ID for accessing Hitachi HCP.

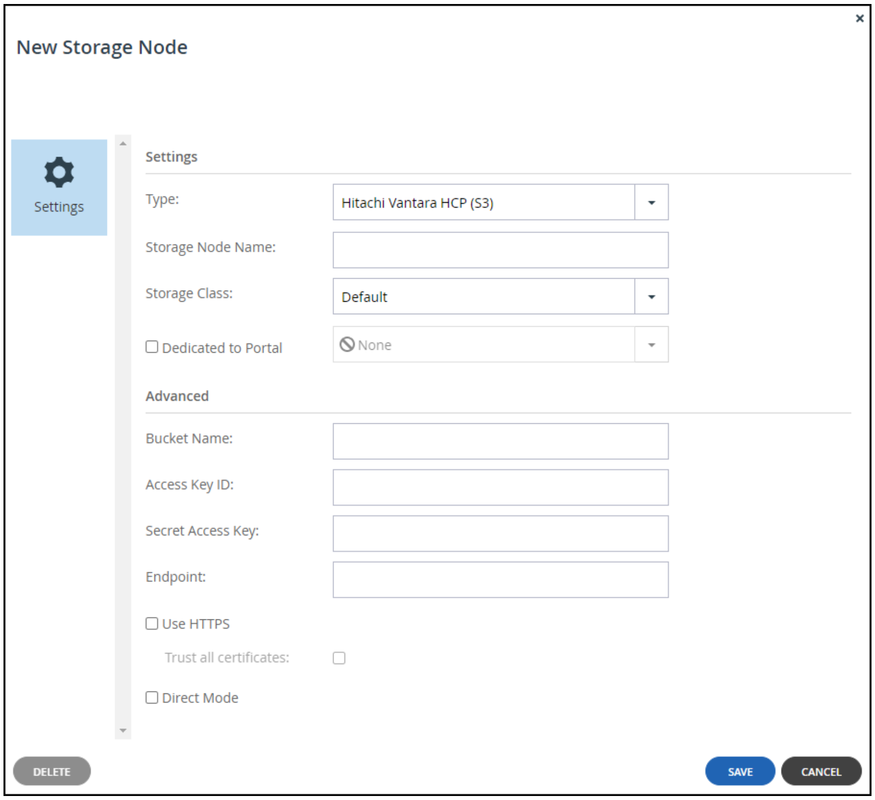
Password – The password for accessing Hitachi HCP.

Use HTTPS – Use HTTPS to connect with the storage node. If this option is not selected, HTTP will be used instead.

Note: Enabling HTTPS reduces performance.

HCP Hitachi Vantara (S3)

The minimum version of Hitachi Vantara HCP (S3) supported by HCP Anywhere Enterprise Portal is version 9.6.1.3.



New Storage Node

Settings

Type: Hitachi Vantara HCP (S3)

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal — None

Advanced

Bucket Name:

Access Key ID:

Secret Access Key:

Endpoint:

□ Use HTTPS

Trust all certificates: □

□ Direct Mode

Bucket Name – The unique name of the S3 bucket that you want to add as a storage node.

Access Key ID – The S3 access key ID.

Secret Access Key – The S3 secret access key.

Endpoint – The endpoint name of the S3 service. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

Use HTTPS – Use HTTPS to connect with the storage node.

> **Trust all certificates** – Do not validate the certificate of the object storage. Normally this is unchecked.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

> **Note:** Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Local Filesystem

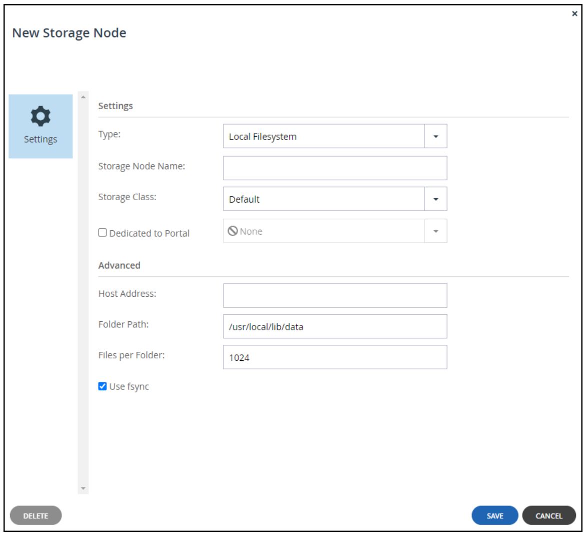
The **Local Filesystem** storage node is the default storage node after installing HCP Anywhere Enterprise Portal.

Note: You cannot use a **Local Filesystem** storage node for storage that exceeds 20TB.

When using a **Local Filesystem** storage node, data blocks are stored in a specific folder in the primary HCP Anywhere Enterprise Portal server's local file system.

HCP Anywhere Enterprise Portal servers set to secondary mode access the storage node by communicating through the primary HCP Anywhere Enterprise Portal server.

Note: Hitachi Vantara recommends setting the deduplication block size to 512KB or larger. Set the block size in the **Virtual Portal Settings** window. Access the **Virtual Portal Settings** window by selecting **Settings** in the navigation pane and then selecting **Virtual Portal**, under **SETTINGS** in the **Control Panel** content page. In the **Virtual Portal Settings** window, set the **Average Block Size field**, under **Default Settings for New Folder Groups**. The default block size is 512KB.



New Storage Node

Settings

Type: Local Filesystem

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal None

Advanced

Host Address:

Folder Path: /usr/local/lib/data

Files per Folder: 1024

☑ Use fsync

Host Address – The host address of the primary server.

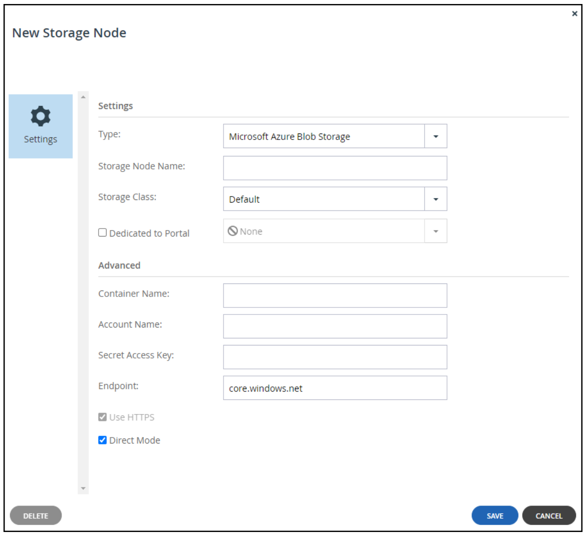
Folder Path – The path in where files should be stored in the local file system.

Files per Folder – The maximum number of files to store in a folder. The default value is 1024.

Use fsync – Blocks of data should be flushed to disk immediately. Using fsync prevents data loss in the event of a power failure.

Microsoft Azure Blob Storage

Both Hot and Cool Blob Storage is supported. Refer to Microsoft Azure documentation for the differences between these storage types.



Settings

Type: Microsoft Azure Blob Storage

Storage Node Name:

Storage Class: Default

□ Dedicated to Portal — None

Advanced

Container Name:

Account Name:

Secret Access Key:

Endpoint: core.windows.net

☑ Use HTTPS

☑ Direct Mode

Container Name – The name of a Microsoft Azure blob container.

Account Name – The Microsoft Azure account name.

Secret Access Key – The Microsoft Azure account key.

Endpoint – The endpoint name of the service. The default value for iscore.windows.net. Normally, this value should not be changed. The port for the endpoint can be customized by adding the port after the URL, using a colon (:) separator. The default port is 80.

Use HTTPS – Use HTTPS to connect with the storage node. If this option is not selected, HTTP will be used instead.

Note: Enabling HTTPS reduces performance.

Direct Mode – Data is uploaded and downloaded directly to and from the storage node and not via the portal. If direct mode is defined for the storage node, Hitachi Vantara recommends setting the deduplication method to fixed blocks and keeping the default 4MB fixed block size. For details, see Default Settings for New Folder Groups.

Note: Once **Direct Mode** is set, the **Use HTTPS** option is also checked and cannot be unchecked.

Using Tiering For HCP Anywhere Enterprise Portal Storage

Each object in Azure Blob Storage has an access tier associated with it:

Hot – Optimized for storing data that is accessed frequently.
Cool – Optimized for storing data that is infrequently accessed and stored for at least 30 days.
Archive – Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

HCP Anywhere Enterprise Portal Azure Blob Storage can use both **hot** and **cool** tiers. Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs. You configure your Azure Blob Storage bucket to tier data that is not frequently accessed in the cool tier with Azure Blob Storage lifecycle management to create a rule-based policy to transition your data to the best access tier. For more details, see https://azure.microsoft.com/en-us/blog/azure-blob-storage-lifecycle-management-now-generally-available/.

For example, the following sample policy manages the lifecycle for such data. It applies to block blobs in container *portalsn* and tiers tier blobs to cool storage 7 days after the last modification.

```
{
  "rules": [
  {
    "name": "rulePortalsn",
    "enabled": true,
    "type": "Lifecycle",
    "definition": {
      "filters": {
        "blobTypes": [ "blockBlob" ],
        "prefixMatch": [ "portalsn" ]
      },
      "actions": {
        "baseBlob": {
          "tierToCool": { "daysAfterModificationGreaterThan": 7 },
        }
      }
    }
  }
  ]
}
```

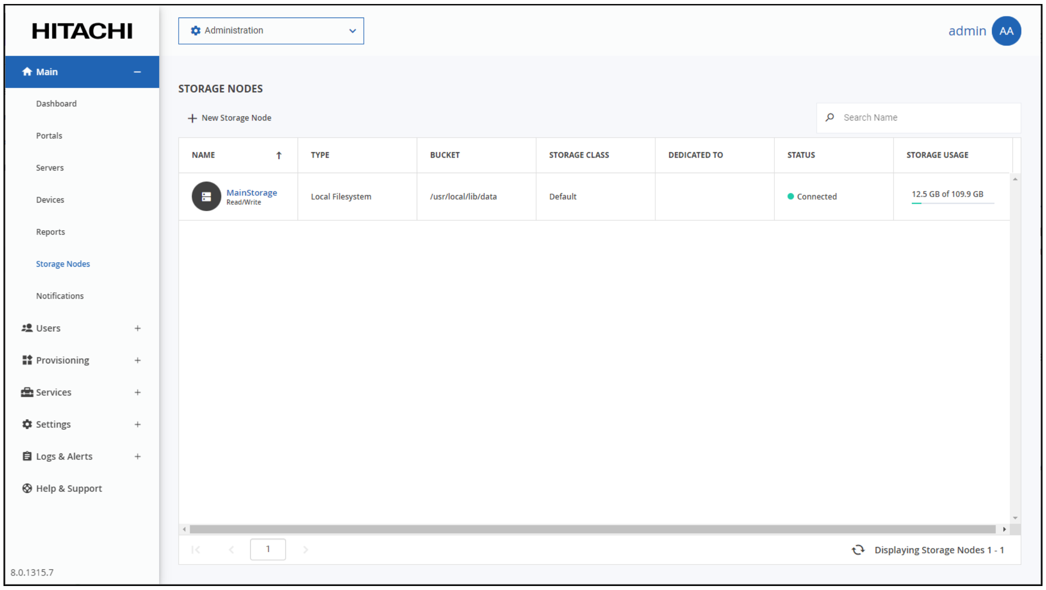
Enabling and Disabling Writes to a Storage Node

When you create a storage node, the node is by default in read/write mode.

You can enable or disable writes to a storage node whenever needed, such as when you are about to replace a storage node and you want to stop new data blocks from being written to the node. While writes are disabled on a node, any new data blocks to be written are directed to other storage nodes that are write-enabled. Also, the node goes into read-delete mode, in which HCP Anywhere Enterprise Portal deletes any blocks on the node deemed to be no longer in use.

To enable or disable writes to a storage node:

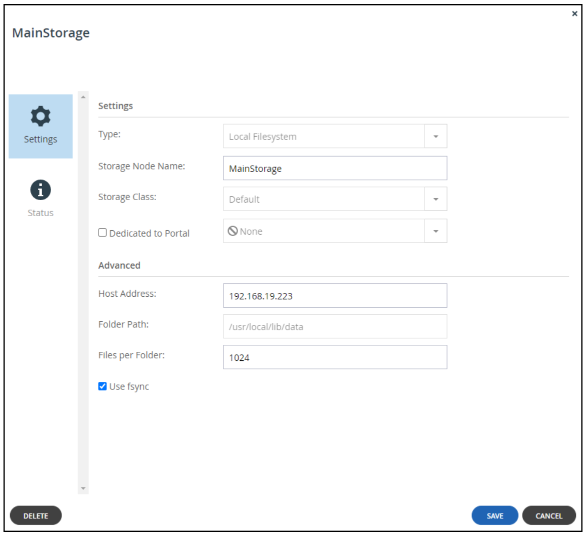
1. In the global administration view, select **Main > Storage Nodes** in the navigation pane. The **STORAGE NODES** page is displayed.



STORAGE NODES

NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		● Connected	12.5 GB of 109.9 GB

2. Click the storage node name.
   The storage node window is displayed with the storage node name as the window title.



MainStorage

Settings

Type: Local Filesystem

Storage Node Name: MainStorage

Storage Class: Default

☐ Dedicated to Portal: None

Advanced

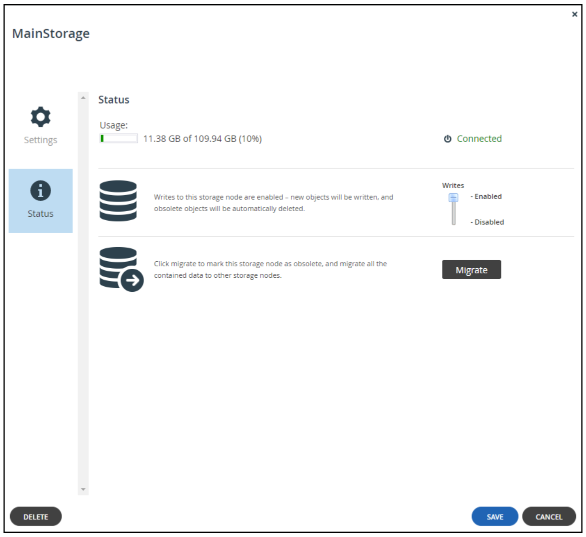
Host Address: 192.168.19.223

Folder Path: /usr/local/lib/data

Files per Folder: 1024

☑ Use fsync

3. Select the **Status** option.



MainStorage

Status

Usage: 11.38 GB of 109.94 GB (10%)

Connected

Writes to this storage node are enabled – new objects will be written, and obsolete objects will be automatically deleted.

Writes - Enabled - Disabled

Click migrate to mark this storage node as obsolete, and migrate all the contained data to other storage nodes.

4. Slide the Writes bar to **Enabled** or **Disabled**.

Migrating a Storage Node

HCP Anywhere Enterprise Portal is a storage-agnostic platform that supports a variety of block and object storage vendors. By abstracting the backend storage using a software-defined storage architecture. HCP Anywhere Enterprise Portal can migrate data between storage nodes, including between on- premises and cloud storage block/object storage nodes. This helps you to manage and implement infrastructure changes, hardware retirement policies, and business objectives. The migration does not require down time, as it is performed in the background while the service remains fully operational. Users can continue to access, backup, sync, and share data during the data migration process.

Migrating to Multiple Non-dedicated Storage Nodes

If more than one storage node is available and the storage node is not dedicated to a virtual portal, data is migrated to all the storage nodes that are online and that are not defined as dedicated storage nodes and are write-enabled. For details about migrating a storage node that is dedicated to a portal, see Migrating from a Dedicated Storage Node. For details about defining a storage node as write enabled, the default, see Enabling and Disabling Writes to a Node.

Migrating from a Storage Node in a Storage Class

If the source storage node is in a storage class, its data is migrated only to other storage nodes that are online and are in that storage class and are write-enabled. For details about defining a dedicated storage node, see Adding and Editing Storage Nodes. You cannot migrate a storage node that is the only storage node in a storage class.

Migrating from a Dedicated Storage Node

If the source storage node is dedicated to a virtual portal, its data is migrated only to other storage nodes that are dedicated to the same portal. If more than one dedicated storage node is connected to the portal, data is migrated to all the dedicated storage nodes that are online and that are write-enabled. For details about defining a dedicated storage node, see Adding and Editing Storage Nodes.

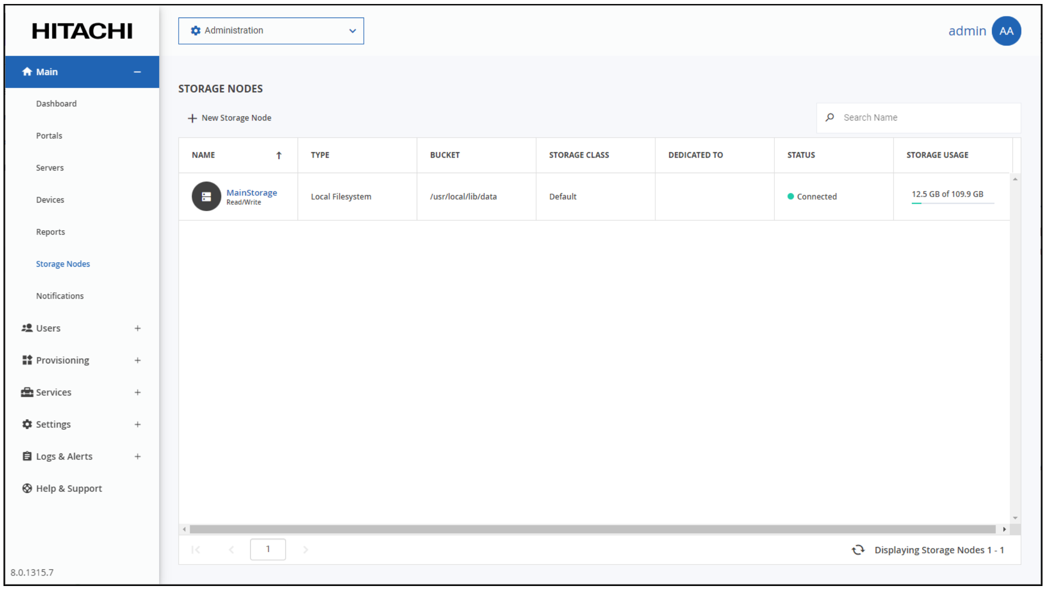
Migrating from a Dedicated Storage Node in a Storage Class

If the source storage node is in a storage class and is dedicated to a virtual portal, its data is migrated only to other storage nodes that are online in that storage class, that are also dedicated to the portal and that are write-enabled. For details about defining a dedicated storage node, see Adding and Editing Storage Nodes.

The Migration Procedure

To migrate a storage node:

1. In the global administration view, select **Main > Storage Nodes** in the navigation pane. The **STORAGE NODES** page is displayed.

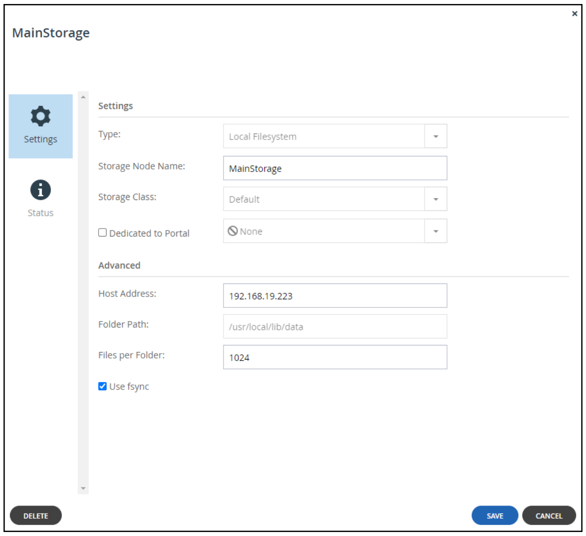


STORAGE NODES

NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		Connected	12.5 GB of 109.9 GB

2. Click the storage node name.

   The storage node window is displayed with the storage node name as the window title.



MainStorage

Settings

Type: Local Filesystem

Storage Node Name: MainStorage

Storage Class: Default

☐ Dedicated to Portal: None

Advanced

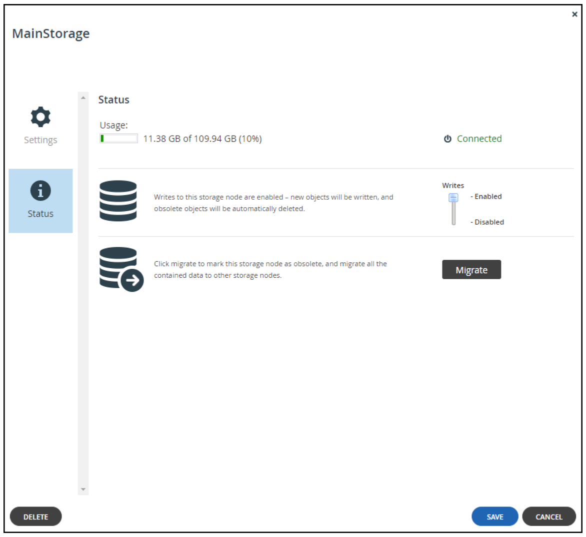
Host Address: 192.168.19.223

Folder Path: /usr/local/lib/data

Files per Folder: 1024

☑ Use fsync

3. Select the **Status** option.



MainStorage

Status

Usage:
11.38 GB of 109.94 GB (10%)

Connected

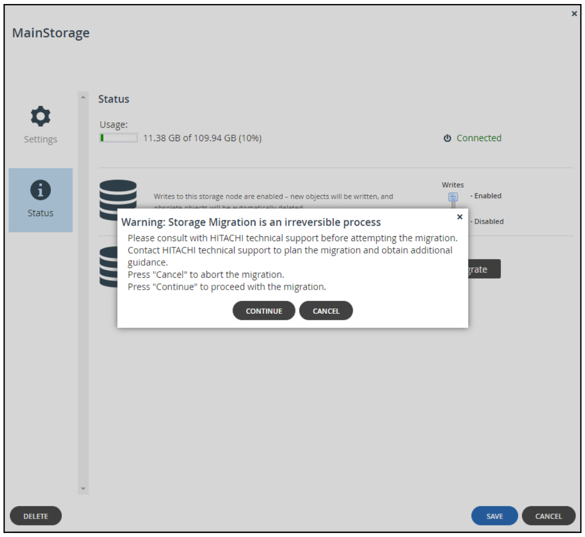
Writes to this storage node are enabled – new objects will be written, and obsolete objects will be automatically deleted.

Writes
- Enabled
- Disabled

Click migrate to mark this storage node as obsolete, and migrate all the contained data to other storage nodes.

4. Click **Migrate**.

   A message is displayed, recommending contacting HCP Anywhere Enterprise support before starting the migration.



MainStorage

Status

Usage:
11.38 GB of 109.94 GB (10%)

Connected

Writes to this storage node are enabled – new objects will be written, and

Writes
- Enabled
- Disabled

Warning: Storage Migration is an irreversible process

Please consult with HITACHI technical support before attempting the migration.
Contact HITACHI technical support to plan the migration and obtain additional guidance.
Press "Cancel" to abort the migration.
Press "Continue" to proceed with the migration.

5. If you have already contacted HCP Anywhere Enterprise Support and understand the implications of the migration, click **CONTINUE**, otherwise, click **CANCEL**.

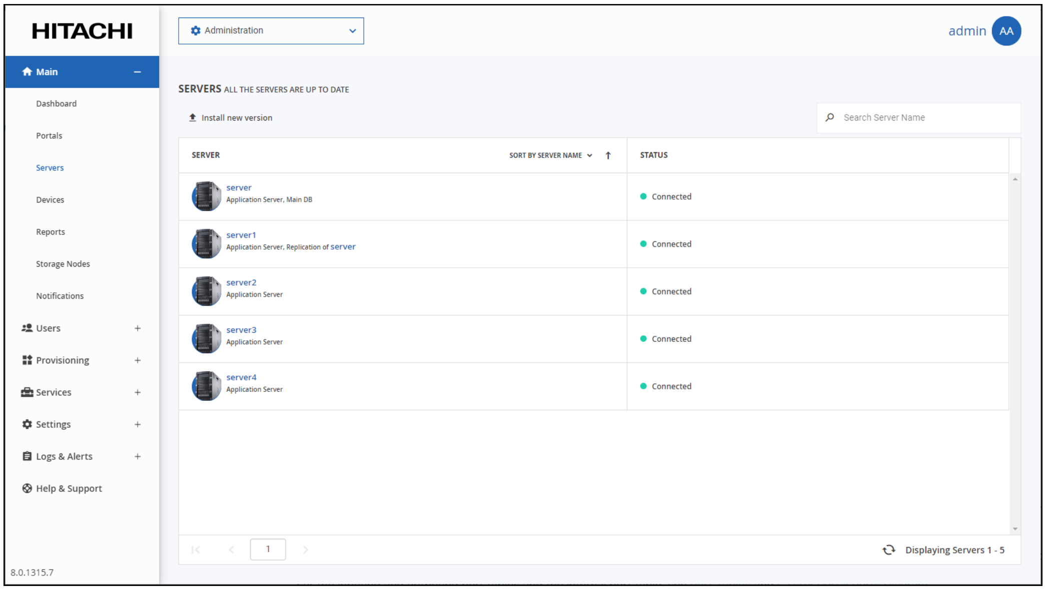
All of the data on the storage node is transferred to the other available write-enabled nodes.

Monitoring the Migration

The migration process can be monitored in the **Activity** tab of the server manager. To open the server manager, click the server's name in the **Main > Servers** page. Select the **Activity** tab.

To monitor a migration operation:

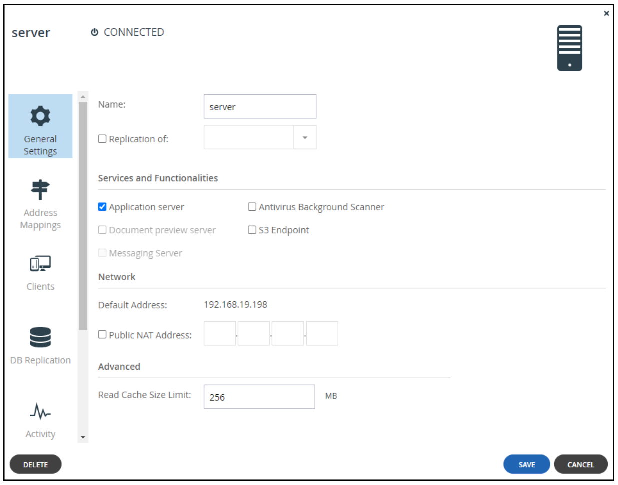
1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

2. Click the server hosting the storage node being migrated.
   The server window is displayed with the server name as the window title.



Name: server

☐ Replication of:

Services and Functionalities

☑ Application server
☐ Antivirus Background Scanner
☐ Document preview server
☐ S3 Endpoint
☐ Messaging Server

Network

Default Address: 192.168.19.198

☐ Public NAT Address:

Advanced

Read Cache Size Limit: 256 MB

3. Click the **Activity** option and scroll down to the graphs displaying the migration operation:
   - The amount of storage migration traffic, in KB/second.
     You can use this information together with the total storage that needs to be migrated, which is displayed in the storage node status option, to calculate approximately how long the migration will take to complete.

- The number of blocks migrated, in blocks/second.

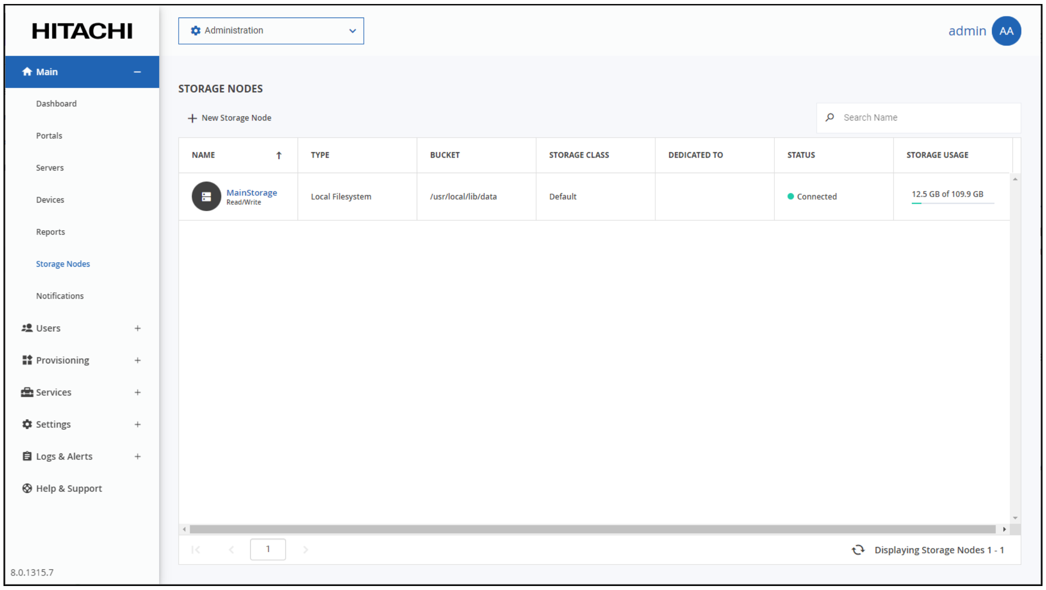
Deleting a Storage Node

You cannot delete a storage node that has data. An error, `Storage node can't be deleted. There is stored data on that storage` is displayed. To delete the node, first migrate the data from the node. For details about migrating a storage node, see Migrating a Storage Node.

Note: You also cannot delete a storage node that is the only storage node in a storage class.

To delete a storage node:

1. In the global administration view, select **Main > Storage Nodes** in the navigation pane.
   The **STORAGE NODES** page is displayed.



NAME	TYPE	BUCKET	STORAGE CLASS	DEDICATED TO	STATUS	STORAGE USAGE
MainStorage Read/Write	Local Filesystem	/usr/local/lib/data	Default		Connected	12.5 GB of 109.9 GB

2. Either,
   a) Select the storage node row for the storage node to delete and click **Delete**.
      A confirmation window is displayed.
   b) Click **DELETE STORAGE** to confirm.

   Or,
   a) Click the storage node name.
      The storage node window is displayed with the storage node name as the window title.
   b) Click **DELETE**.
      A confirmation window is displayed.
   c) Click **YES** to confirm.

The storage node is deleted.

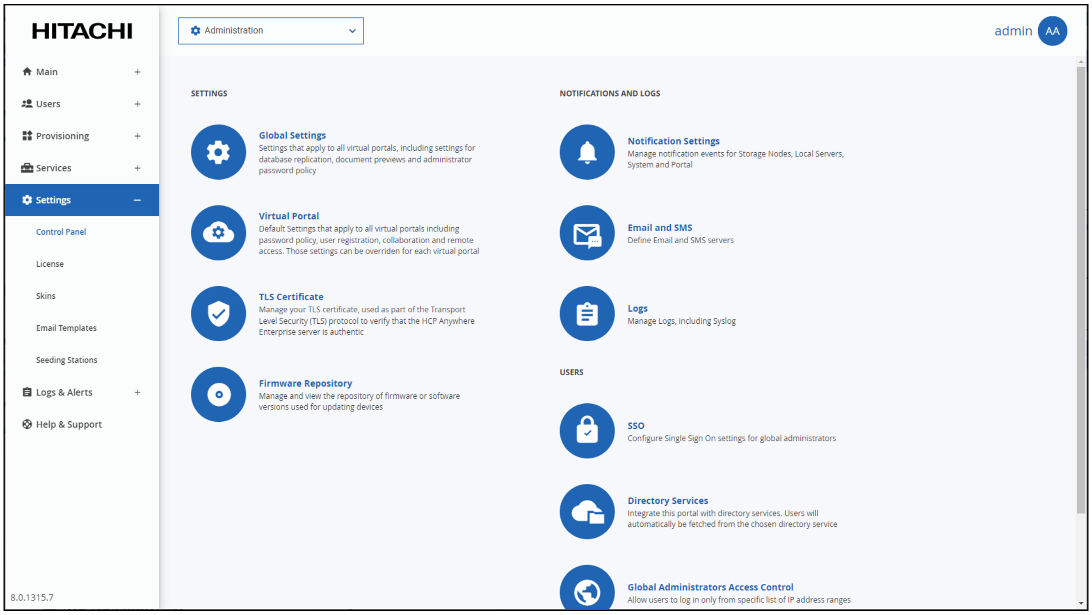
Chapter 7. Configuring Global Settings

Global settings apply across all team portals:

- The DNS suffix that is appended to each virtual portal's name, in order to create the team portal's DNS name.
- The HCP Anywhere Enterprise Portal time zone.
- The amount of time a deleted portal should be saved before it is permanently deleted.
- Enable Zones.
- Database replication lag time.
- Redirects from HTTP to HTTPS for administrators and end users.
- Session timeout when no activity.
- Document preview settings.
- Password policy for portal administrators.
- Settings for the HCP Anywhere Enterprise Portal behind a proxy server.
- Consent page prior to login.

To configure global settings:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

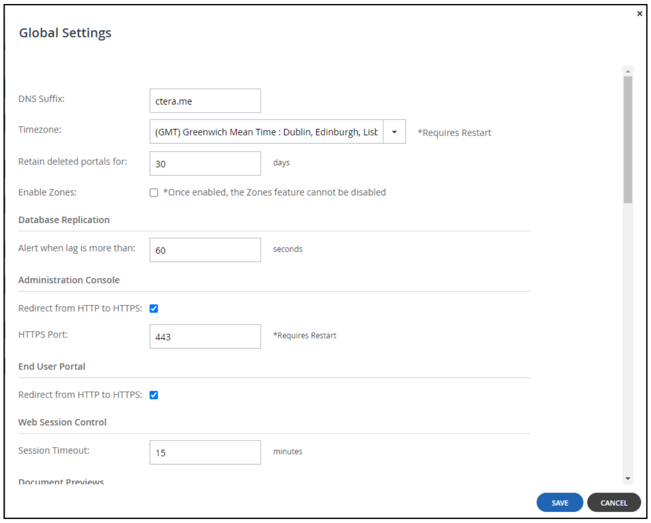
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Global Settings** under **SETTINGS** in the **Control Panel** page.
   The **Global Settings** window is displayed.



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, List *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: □ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

Web Session Control

Session Timeout: 15 minutes

Document Previews

3. Make changes as needed.

   DNS Suffix – The global DNS suffix to use for all virtual portals. The DNS suffix was set when the HCP Anywhere Enterprise Portal was installed, as described in the installation guide for the environment.

   Warning: Changing the DNS suffix from the suffix specified when the portal was installed, requires Hitachi Vantara to issue a new license as well as possible changes to system settings, such as the hosts file.

   The DNS suffix is the suffix that is appended to each team portal's name, in order to create the team portal's DNS name. For example, if a team portal's name is *myportal*, and the DNS suffix is *example.com*, then the team portal's DNS name will be *myportal.example.com*. The DNS name is used to connect directly to a team portal.

   Note: The name of each virtual portal is configurable in the **Main > Portals** page. Click the portal name to change the name.

   Timezone – The HCP Anywhere Enterprise Portal's time zone.

   Note: If you change the **Timezone**, you need to restart the HCP Anywhere Enterprise Portal servers for the change to take effect. Restart the HCP Anywhere Enterprise Portal servers in the following order:
   – Main database server.
   – Replication database server, if available.
   – All application or preview servers.
   The **Timezone** change is implemented after the restart.

   Retain deleted portals for – The number of days to retain a deleted team portal. During this retention period, the administrator can undelete the portal, but after this period, the portal is permanently deleted along with the portal content. For details, see Deleting and Undeleting Virtual Portals.

   Enable Zones – 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 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. For details, see the *Hitachi Content Platform Anywhere*

Enterprise Portal Team Administration Guide.

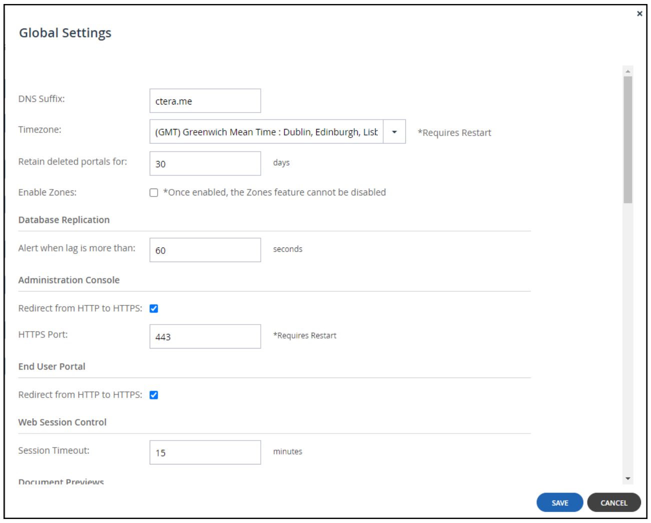
Note: Once this setting is enabled and saved, the **Zones** option is available for all team portals and cannot be disabled.

4. Make necessary changes to the other sections.

   Database Replication
   Administration Console
   End User Portal
   Web Session Control
   Document Previews
   Administrators Password Policy
   Proxy Settings
   Consent Page

5. Click **SAVE**.

Database Replication



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisb *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: □ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

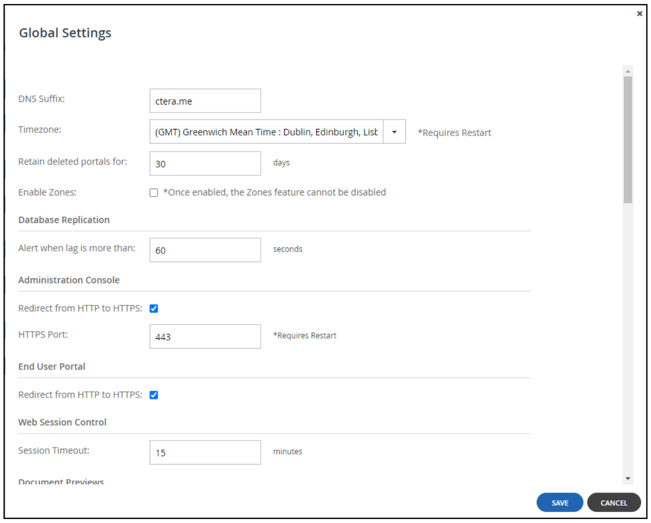
Web Session Control

Session Timeout: 15 minutes

Document Previews

Alert when lag is more than – In the event that replication falls behind, portal administrators are notified via email after a lag time of specified number of seconds.

Administration Console



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisb *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: □ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

Web Session Control

Session Timeout: 15 minutes

Document Previews

Redirect from HTTP to HTTPS – Enable automatic redirection between HTTP and HTTPS.

HTTPS Port – An HTTPS port number to change the administration portal HTTPS access port. The following HTTPS ports are allowed: 443, 1024 to 65535.

Note: If you change the **HTTPS Port**, you need to restart the HCP Anywhere Enterprise Portal servers for the change to take effect. Restart the HCP Anywhere Enterprise Portal servers in the following order:

a) Main database server.

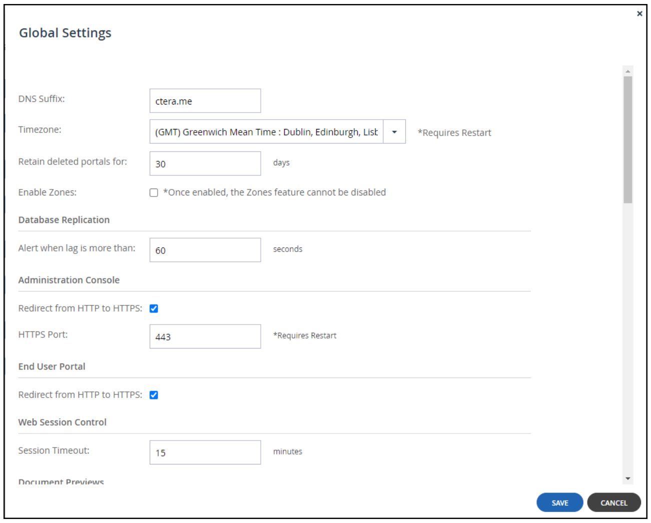
b) Replication database server, if available.

c) All application or preview servers.

The **HTTPS Port** change is implemented after the restart.

For more information, see Access URLs for Administrators and End Users.

End User Portal



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisb *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: □ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

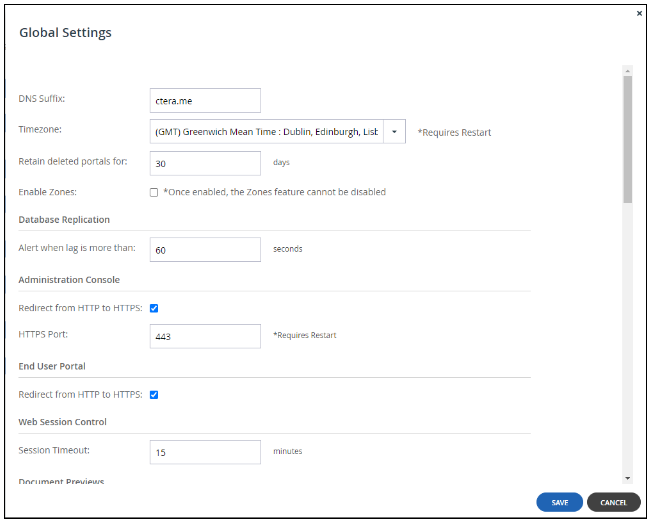
Web Session Control

Session Timeout: 15 minutes

Document Previews

Redirect from HTTP to HTTPS – Enable automatic redirection of end users between HTTP and HTTPS.

Web Session Control



Global Settings

DNS Suffix: ctera.me

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisb *Requires Restart

Retain deleted portals for: 30 days

Enable Zones: □ *Once enabled, the Zones feature cannot be disabled

Database Replication

Alert when lag is more than: 60 seconds

Administration Console

Redirect from HTTP to HTTPS: ☑

HTTPS Port: 443 *Requires Restart

End User Portal

Redirect from HTTP to HTTPS: ☑

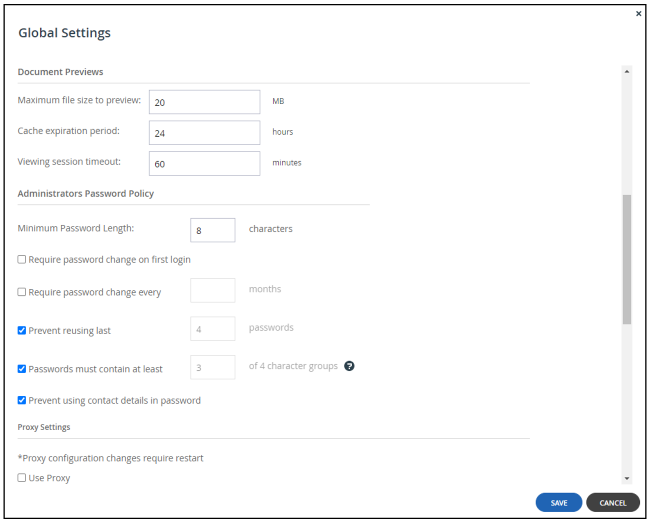
Web Session Control

Session Timeout: 15 minutes

Document Previews

Session Timeout – The amount of time the session remains open when there is no activity.

Document Previews



Global Settings

Document Previews

Maximum file size to preview: 20 MB

Cache expiration period: 24 hours

Viewing session timeout: 60 minutes

Administrators Password Policy

Minimum Password Length: 8 characters

□ Require password change on first login

□ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Proxy Settings

*Proxy configuration changes require restart

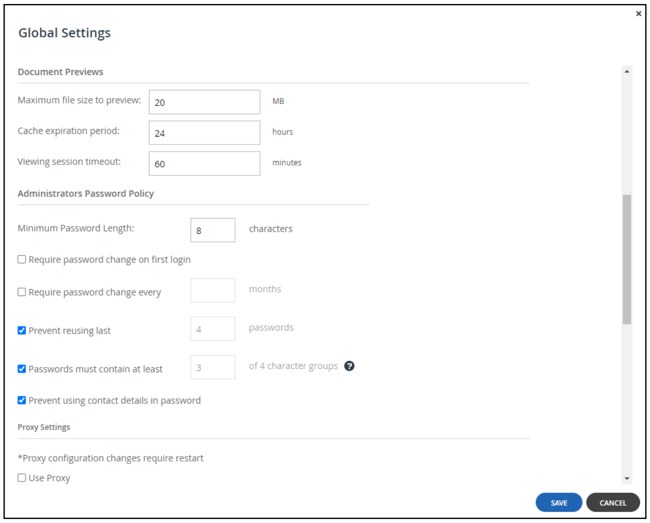
□ Use Proxy

Maximum file size to preview – The maximum file size HCP Anywhere Enterprise Portal end users can preview using the online file viewer.

Cache expiration period – The time for which a file is stored in the Preview server cache after it is previewed, which causes the next preview of the same file to be faster.

Viewing session timeout – The amount of time after a file is previewed that the preview session is closed. After this amount of time, the user can no longer scroll through the document. If the user wishes to continue previewing the document, the user must close the preview window and open it again.

Administrators Password Policy



Global Settings

Document Previews

Maximum file size to preview: 20 MB

Cache expiration period: 24 hours

Viewing session timeout: 60 minutes

Administrators Password Policy

Minimum Password Length: 8 characters

□ Require password change on first login

□ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Proxy Settings

*Proxy configuration changes require restart

□ Use Proxy

Minimum Password Length – The minimum number of characters that must be used in a HCP Anywhere Enterprise Portal administrator's account password.

Require password change on first login – Require administrators to change their password on their first login.

Require password change every – Require administrators to change their password after a certain number of months, then specify the desired number of months in the field provided. When the specified number of months has elapsed, the administrator's password will expire, and they will be required to configure a new password upon their next login.

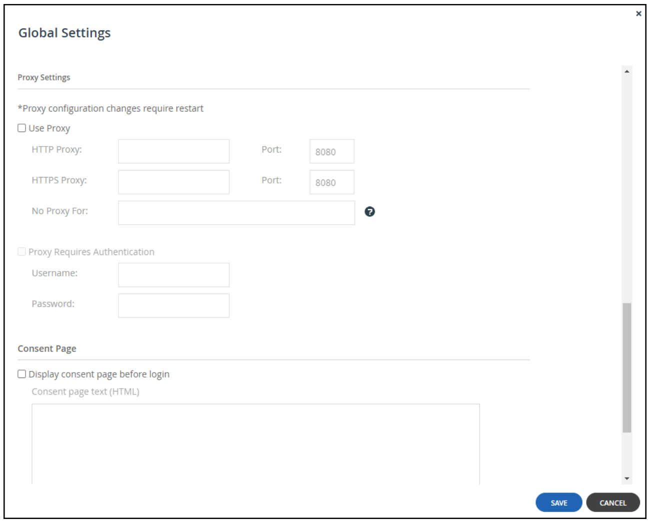
Prevent reusing last... passwords – Prevent administrators from reusing a specified number of their previous passwords when they change their password. Specify the number of previous passwords you want this to apply to.

Passwords must contain at least.... of 4 character groups – Require administrators 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 administrators from using their personal details in their password, including first name, last name, email, username, and company name. After checking this page, edit the content of the consent page.

Proxy Settings



Global Settings

Proxy Settings

*Proxy configuration changes require restart

□ Use Proxy

HTTP Proxy:		Port:	8080
HTTPS Proxy:		Port:	8080
No Proxy For:			

□ Proxy Requires Authentication

Username:	
Password:	

Consent Page

□ Display consent page before login

Consent page text (HTML)

You can configure the HCP Anywhere Enterprise Portal behind a Proxy Server. When configured, external connections go through the proxy server, such as storage nodes, and antivirus servers.

Use Proxy – Check the Use Proxy option to configure the HCP Anywhere Enterprise Portal behind a proxy server. If checked either an HTP proxy server or an HTTPS proxy server or both must be configured.

- **HTTP Proxy** – The address of the HTTP proxy server.

    - **Port** – The HTTP proxy server port number. The port number must be between 1 and 65535.
- **HTTPS Proxy** – The address of the HTTPS proxy server.
    - **Port** – The HTTPS proxy server port number. The port number must be between 1 and 65535.
- **No Proxy For** – A comma separated list of IP addresses and DNS names that will not go through the proxy server. For example, when a storage node in the cloud is used as well as an on-premises storage node, only the storage node in the cloud should go through the proxy server. In this type of scenario, the address of the on-premises storage node should be specified here.

  Note: When the HCP Anywhere Enterprise Messaging service is used, make sure that each messaging server IP is included in the **No Proxy For** list.

Proxy Requires Authentication – Check to specify that the proxy server requires authentication via a username and password.

Username – The username for authenticating to the proxy server.

Password – The password for authenticating to the proxy server.

Note: If you configure a proxy server or change the proxy server settings, you need to restart the HCP Anywhere Enterprise Portal servers for the change to take effect. Restart the HCP Anywhere Enterprise Portal servers in the following order:

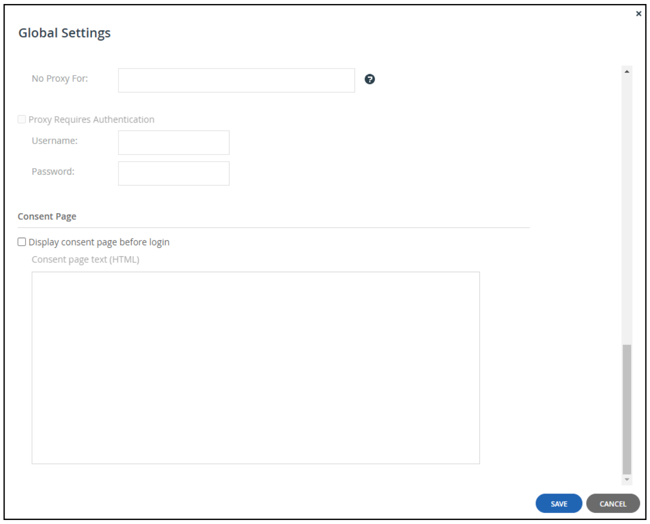
a) Main database server.

b) Replication database server, if available.

c) All application or preview servers.

The proxy server settings are implemented after the restart.

Consent Page



Display consent page before login – Before logging in to the portal a consent page is displayed and only after the user accepts the terms in the consent page can the user access the portal. The consent page is enforced on all types of sign-in, such as via Active Directory, a Common Access Card (CAC) or via SAML single sign-on. The consent page text is created using HTML.

Chapter 8. Setting Up Single Sign-on (SSO)

You set up Single Sign-On, SSO, for global administrators.

Note: You can define Single Sign-On, SSO, for a team 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. For details, refer to the *Hitachi Content Platform Anywhere Enterprise Team Administration Guide*.

HCP Anywhere Enterprise Portal supports user identity federation over SAML 2.0. SAML enables you to provide Single Sign-On (SSO) capabilities for the global administrators. To set SSO for global administrators, you must create global administrators that have user names corresponding to the SAML identity provider user names. For details about adding global administrators, see Adding, Editing, or Deleting Global Administrators.

Note: Global administrator are defined locally on the HCP Anywhere Enterprise Portal and the passwords are stored on HCP Anywhere Enterprise Portal to enable the administrator to bypass the SAML authentication in the event of misconfiguration of the identity provider's login page or in case the identity provider's login page is temporarily unavailable. For details, see Bypassing SAML Authentication.
Enabling SAML SSO for a global administrator does **not** enable SAML SSO for team and reseller portals. To set up SS for team and reseller portals, refer to the *Hitachi Content Platform Anywhere Enterprise Team Administration Guide*.

In this chapter

Using SAML 2.0 For Single Sign-On

To configure SAML SSO, you need a 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)
- Microsoft Entra ID (Azure Active Directory)
- Okta
- OneLogin
- Swivel AuthControl Sentry

Before setting up SAML in the HCP Anywhere Enterprise Portal:

- The global administrators must be defined. For details, see Adding, Editing, or Deleting Global Administrators.
- 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.

Identity Provider Details

You need to set up the HCP Anywhere Enterprise Portal as a SAML application in the identity provider. The following sections outline the procedures for each of the providers certified by Hitachi Vantara.

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

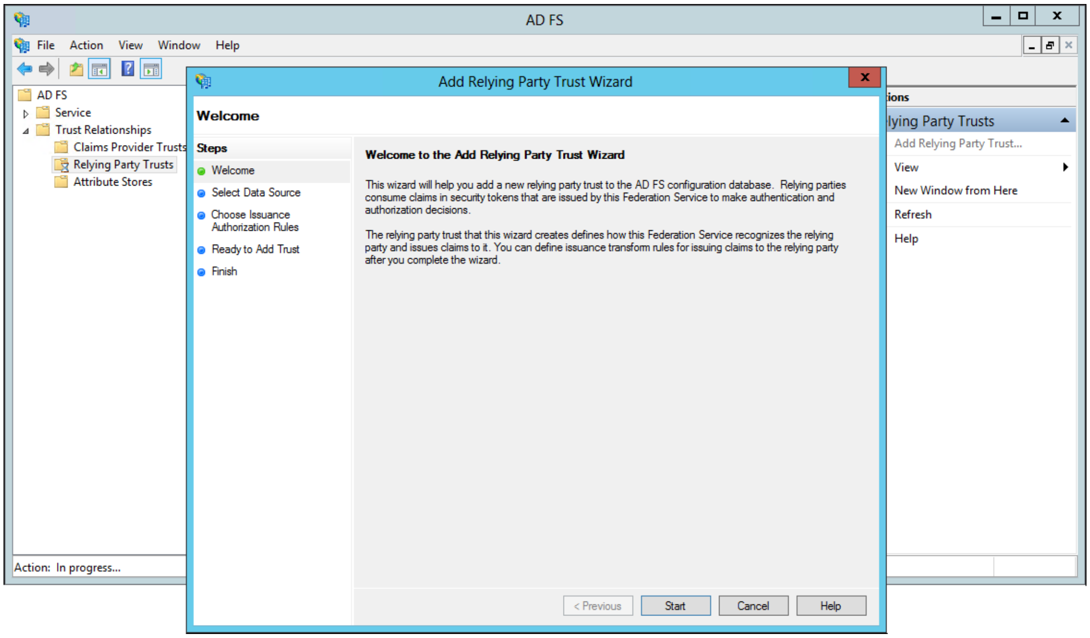
Configuring Microsoft ADFS to Work with HCP Anywhere Enterprise Portal

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**.

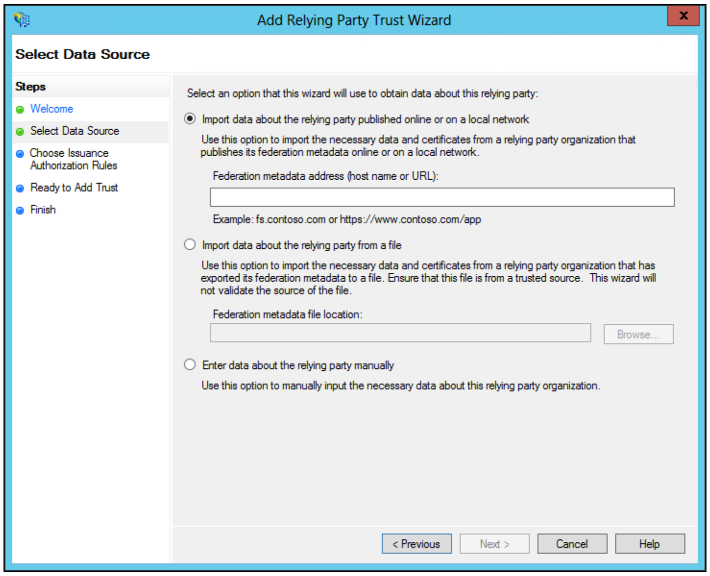


Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

5. Click **Start**.



Select an option that this wizard will use to obtain data about this relying party:

● Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

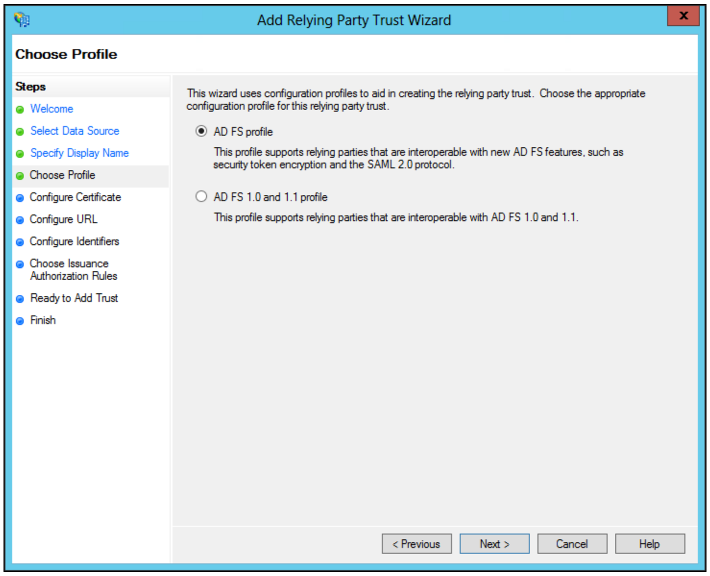
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

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**.



Choose Profile

This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

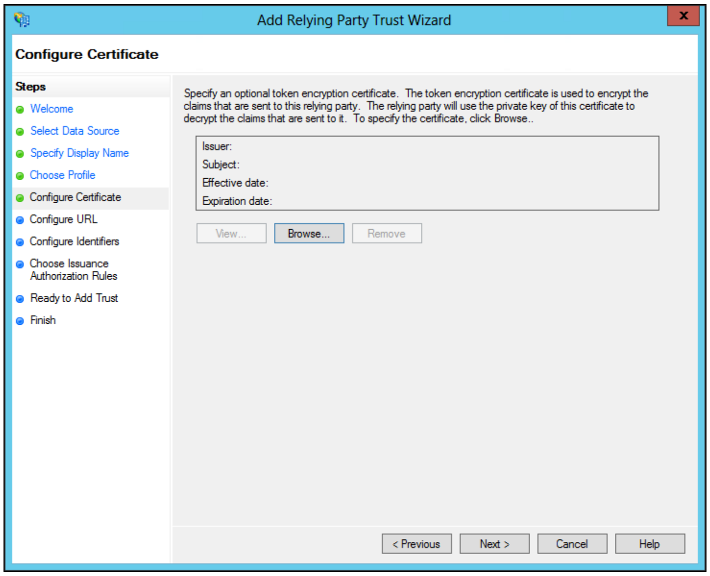
● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

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



Configure Certificate

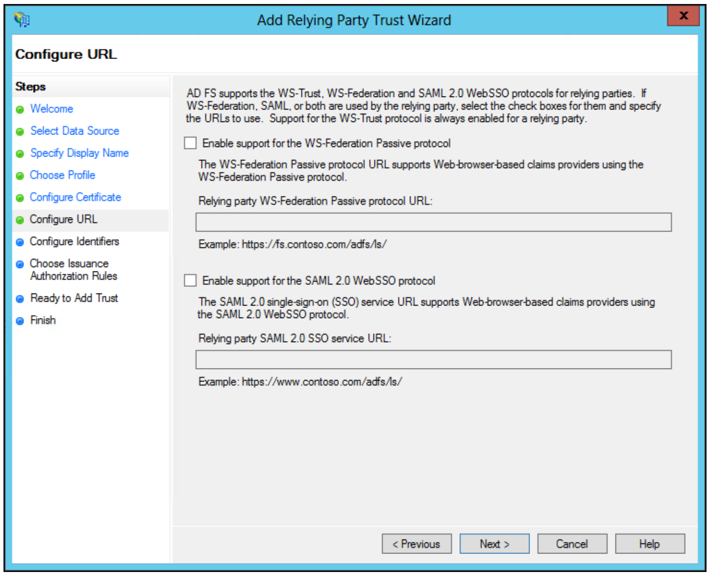
Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

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**.



Add Relying Party Trust Wizard

Configure URL

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

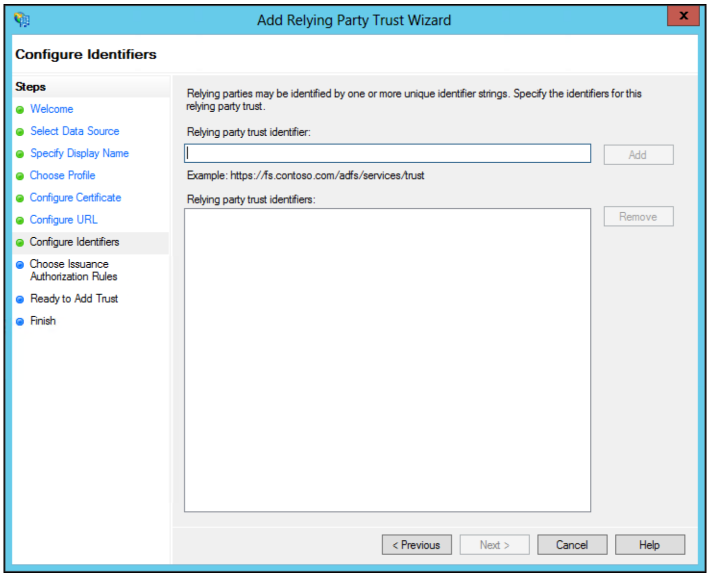
□ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

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 Anywhere Enterprise`.me/ServicesPortal/saml`
12. Click **Next**.



Add Relying Party Trust Wizard

Configure Identifiers

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

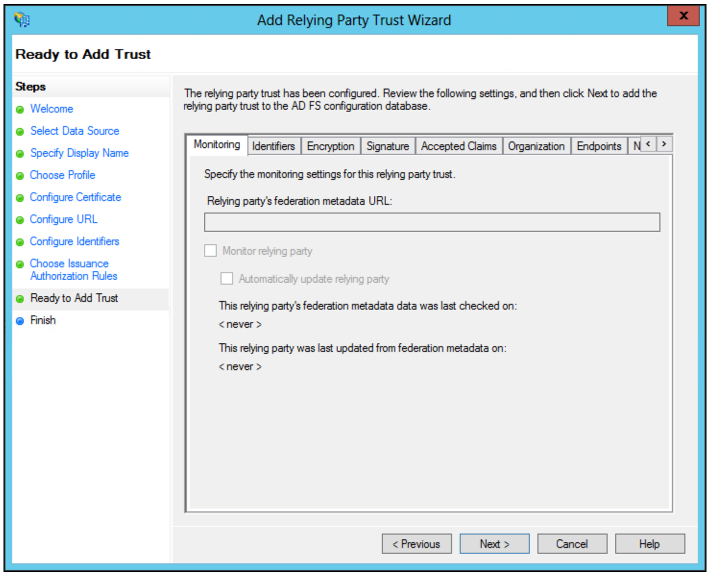
Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

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**.



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

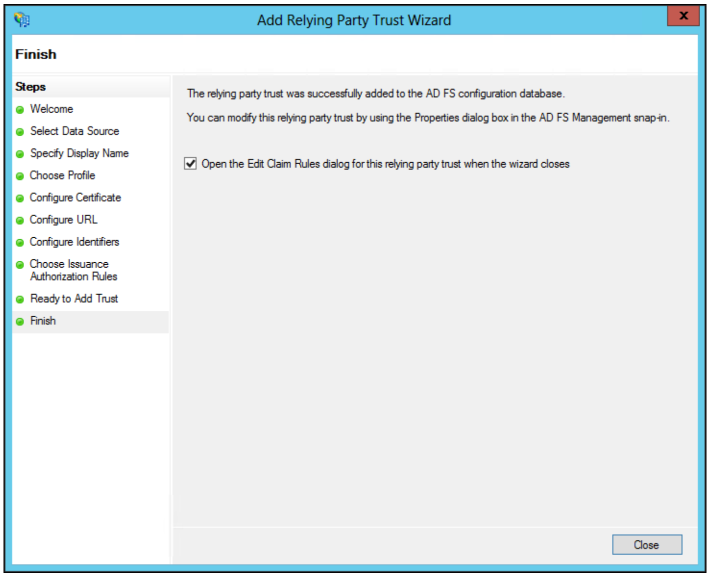
This relying party's federation metadata data was last checked on:
< never >

This relying party was last updated from federation metadata on:
< never >

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**.



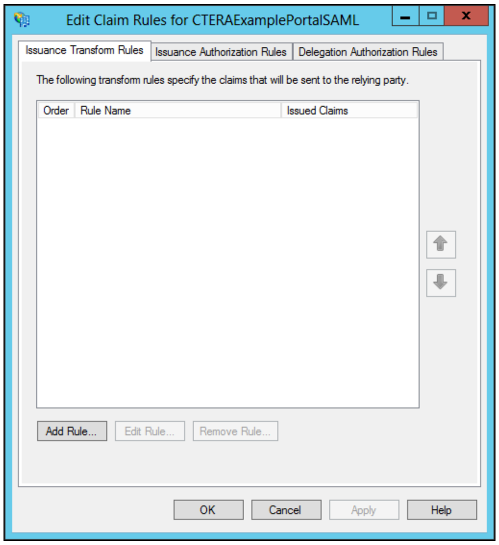
The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

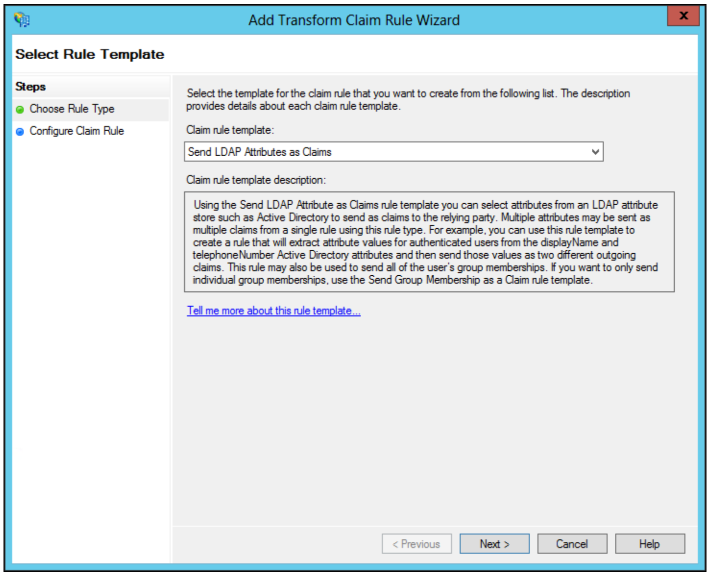
19. Check the **Open Edit Claim Rules dialog for this relying trust when the wizard closes** and click **Close**.

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



The following transform rules specify the claims that will be sent to the relying party.

20. Click **Add Rule**.



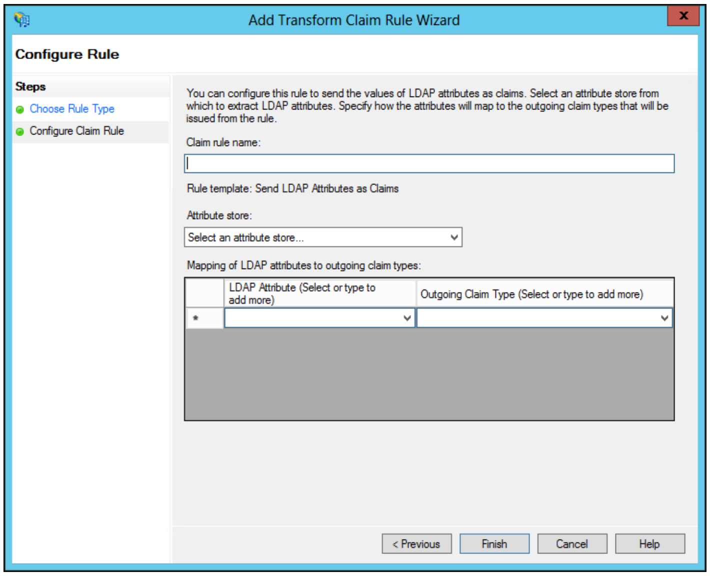
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

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



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

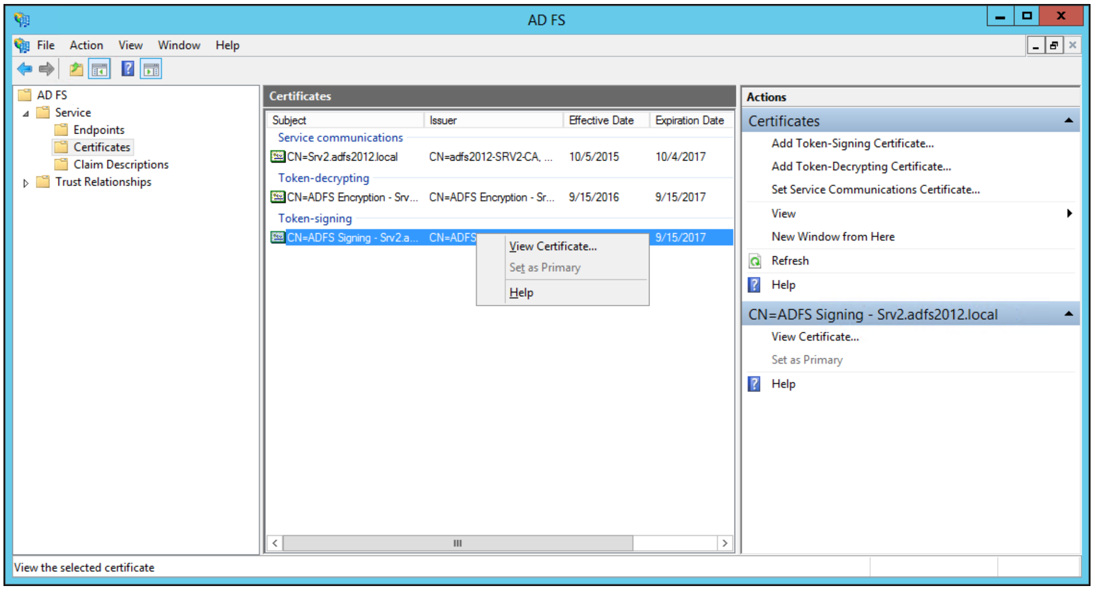
Select an attribute store...

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
*		

22. Enter the following:

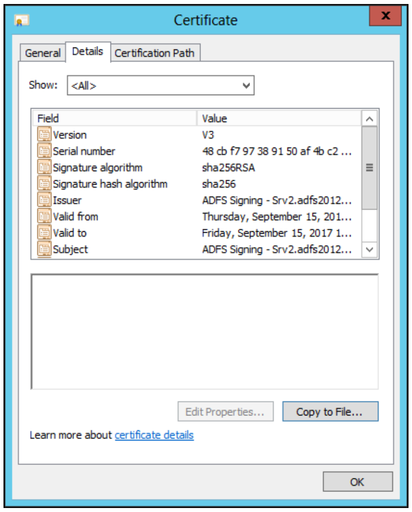
    Claim rule name – A name for the rule.
    Attribute store – Select the store from the list, for example, Active Directory.
    LDAP Attribute – Use **User-Principal-Name**.
    Outgoing Claim Type – Select **Name ID**.
23. Click **Finish**.
24. Click **OK**.
25. In the left pane navigation tree, select **Service > Certificates**, right-click the certificate under **Token-signing** and click **View Certificate**.



Subject	Issuer	Effective Date	Expiration Date
Service communications			
CN=Srv2.adfs2012.local	CN=adfs2012-SRV2-CA, ...	10/5/2015	10/4/2017
Token-decrypting			
CN=ADFS Encryption - Srv...	CN=ADFS Encryption - Sr...	9/15/2016	9/15/2017
Token-signing			
CN=ADFS Signing - Srv2.a...	CN=ADFS		9/15/2017

View Certificate...
Set as Primary
Help
Actions
Certificates
Add Token-Signing Certificate...
Add Token-Decrypting Certificate...
Set Service Communications Certificate...
View
New Window from Here
Refresh
Help
CN=ADFS Signing - Srv2.adfs2012.local
View Certificate...
Set as Primary
Help
View the selected certificate

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

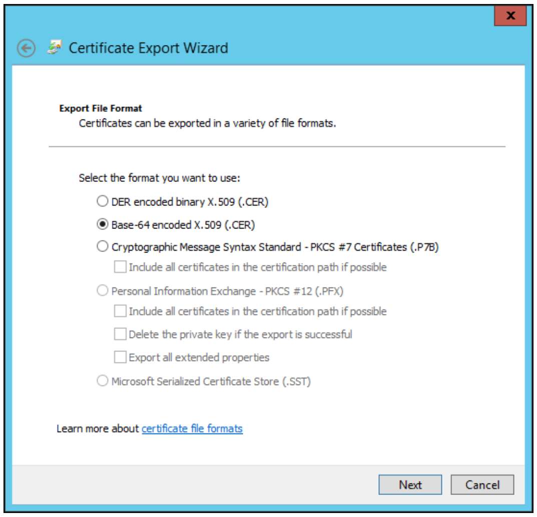


Show: <All>

Field	Value
Version	V3
Serial number	48 cb f7 97 38 91 50 af 4b c2 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - Srv2.adfs2012...
Valid from	Thursday, September 15, 201...
Valid to	Friday, September 15, 2017 1...
Subject	ADFS Signing - Srv2.adfs2012...

Learn more about certificate details

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



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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`.

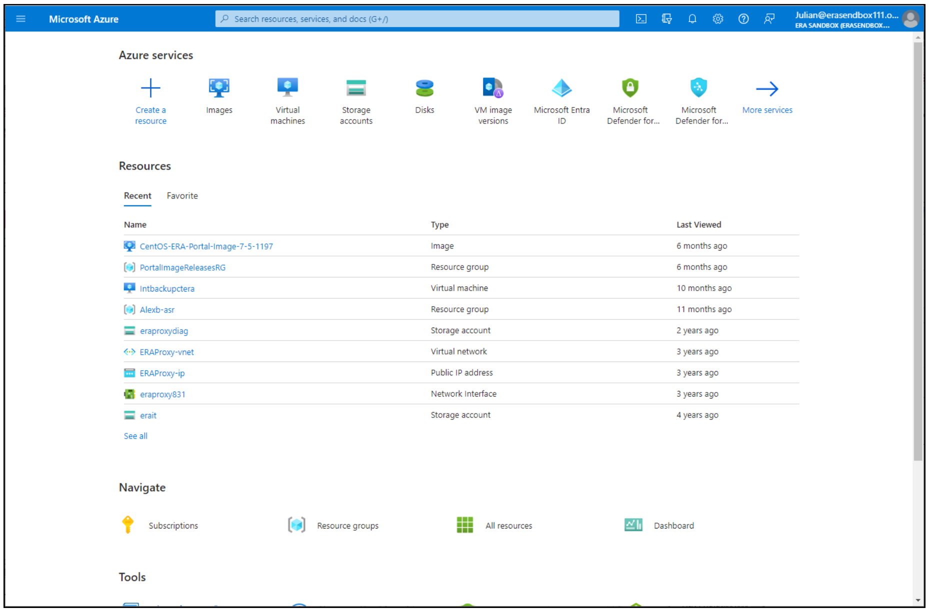
Configuring Microsoft Entra ID (Azure Active Directory) to Work with HCP Anywhere Enterprise Portal

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.

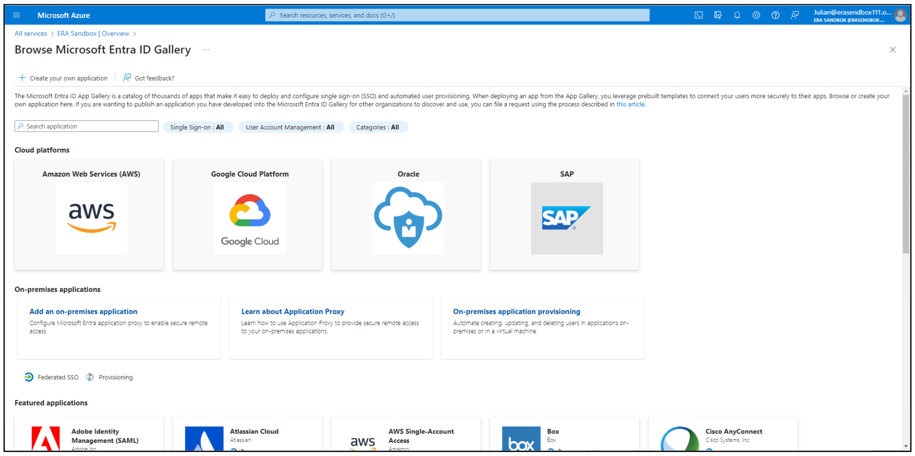


Name	Type	Last Viewed
CentOS-ERA-Portal-Image-7-5-1197	Image	6 months ago
PortalImageReleasesRG	Resource group	6 months ago
Intbackupctera	Virtual machine	10 months ago
Alexb-asr	Resource group	11 months ago
eraproxydiag	Storage account	2 years ago
ERAProxy-vnet	Virtual network	3 years ago
ERAProxy-ip	Public IP address	3 years ago
eraproxy831	Network Interface	3 years ago
erait	Storage account	4 years ago

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.


Microsoft Azure
Search resources, services, and docs (G+/)
Julian@erasendbox111.o...
ERA SANDBOX (ERASENDBOX...

All services > ERA Sandbox | Overview >

Browse Microsoft Entra ID Gallery ...

+ Create your own application | Got feedback?

The Microsoft Entra ID App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra ID Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Search application | Single Sign-on : **All** | User Account Management : **All** | Categories : **All**

Cloud platforms

Amazon Web Services (AWS) | Google Cloud Platform | Oracle | SAP

On-premises applications

Add an on-premises application
Configure Microsoft Entra application proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises application provisioning
Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.

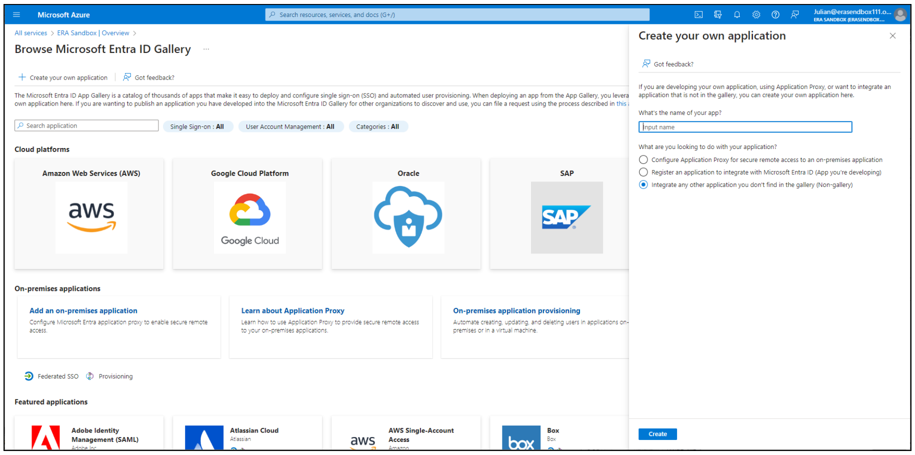
Federated SSO   Provisioning

Featured applications

Adobe Identity Management (SAML) – Adobe Inc
Atlassian Cloud – Atlassian
AWS Single-Account Access – Amazon
Box – Box
Cisco AnyConnect – Cisco Systems, Inc.

4. Click the **Create your own application** tab.

   The **Create your own application** blade is displayed.


Microsoft Azure
Search resources, services, and docs (G+/)
Julian@erasendbox111.o...
ERA SANDBOX (ERASENDBOX...

All services > ERA Sandbox | Overview >

Browse Microsoft Entra ID Gallery ...

+ Create your own application | Got feedback?

The Microsoft Entra ID App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you levera... own application here. If you are wanting to publish an application you have developed into the Microsoft Entra ID Gallery for other organizations to discover and use, you can file a request using the process described in this ...

Search application | Single Sign-on : All | User Account Management : All | Categories : All

Cloud platforms

Amazon Web Services (AWS) | Google Cloud Platform | Oracle | SAP

On-premises applications

Add an on-premises application
Configure Microsoft Entra application proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises application provisioning
Automate creating, updating, and deleting users in applications on-premises or in a virtual machine.

Federated SSO   Provisioning

Featured applications

Adobe Identity Management (SAML) – Adobe Inc
Atlassian Cloud – Atlassian
AWS Single-Account Access – Amazon
Box – Box

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

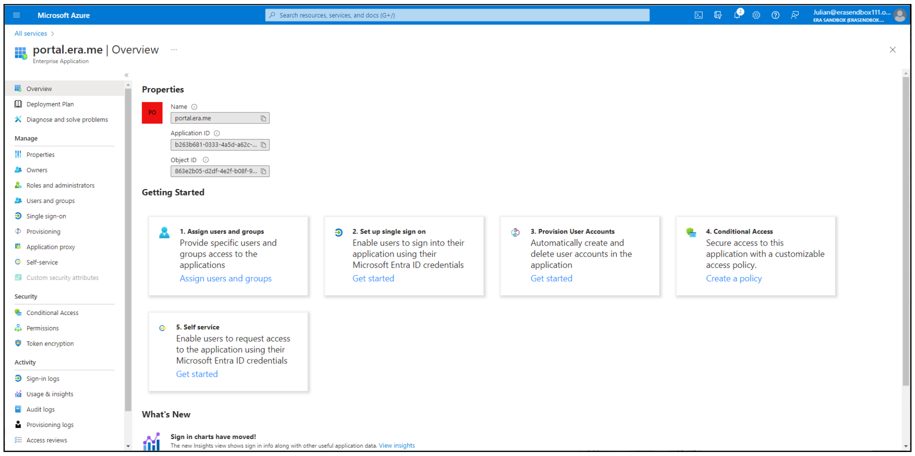
Input name

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Microsoft Entra ID (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

Create

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


Microsoft Azure
Search resources, services, and docs (G+/)
Julian@erasendbox111.o...
ERA SANDBOX (ERASENDBOX...

All services >

portal.era.me | Overview ...
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes

Security
Conditional Access
Permissions
Token encryption

Activity
Sign-in logs
Usage & insights
Audit logs
Provisioning logs
Access reviews

Properties

PO

Name: portal.era.me

Application ID: b263b681-0333-4a5d-a62c-...

Object ID: 863e2b05-d2df-4e2f-b08f-9...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra ID credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

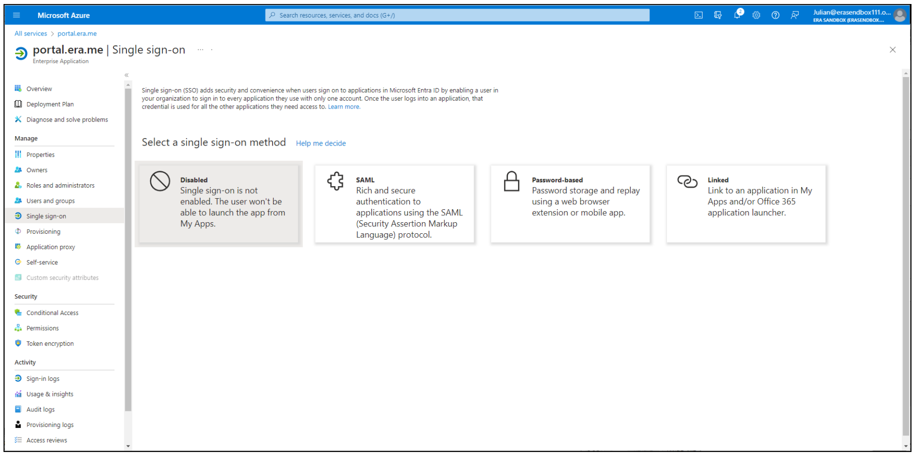
4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Microsoft Entra ID credentials
Get started

What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

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



Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

Select a single sign-on method Help me decide

Disabled Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

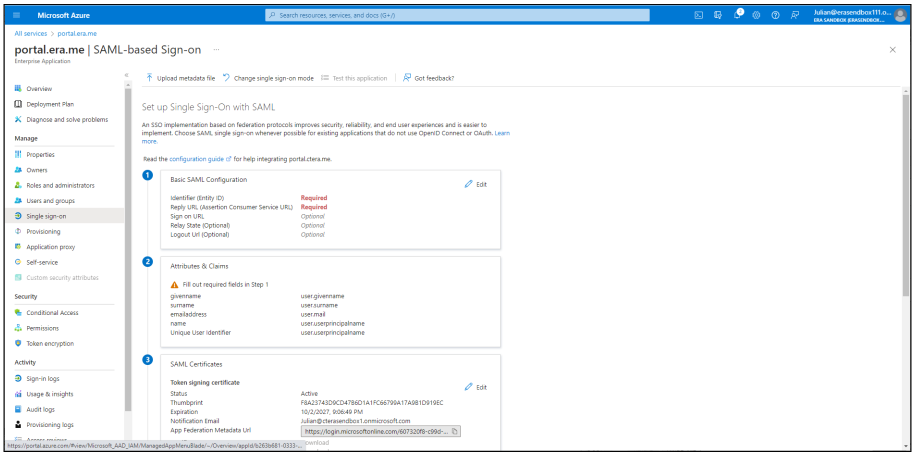
SAML Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based Password storage and replay using a web browser extension or mobile app.

Linked Link to an application in My Apps and/or Office 365 application launcher.

7. Click **SAML**.

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



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating portal.ctera.me.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

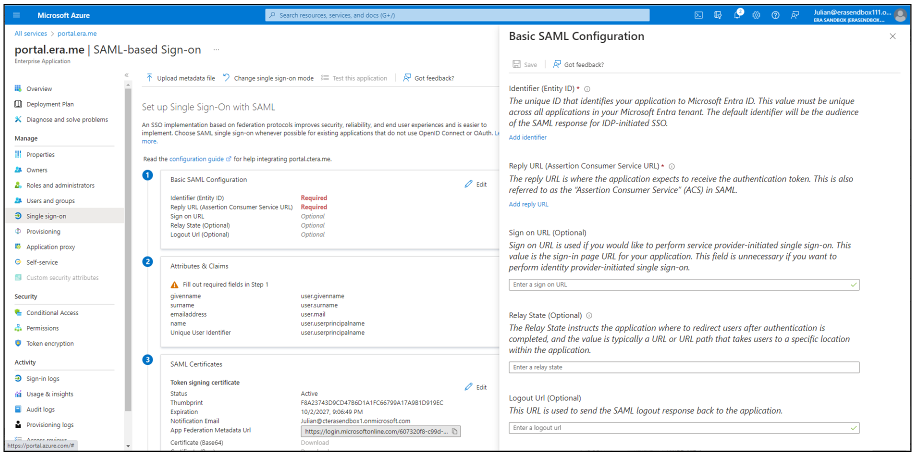
Token signing certificate

Status	Active
Thumbprint	F8A23743D9CD47B6D1A1FC66799A17A9B1D919EC
Expiration	10/2/2027, 9:06:49 PM
Notification Email	Julian@cterasendbox1.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/607320f8-c99d-...

https://portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~/Overview/appId/b263b681-0333-...

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

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


Microsoft Azure
Search resources, services, and docs (G+/)
Julian@erasendbox111.o...
ERA SANDBOX (ERASENDBOX...
All services > portal.era.me
portal.era.me | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Edit
Save
Got feedback?
Add identifier
Add reply URL
https://portal.azure.com/#

Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url

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.

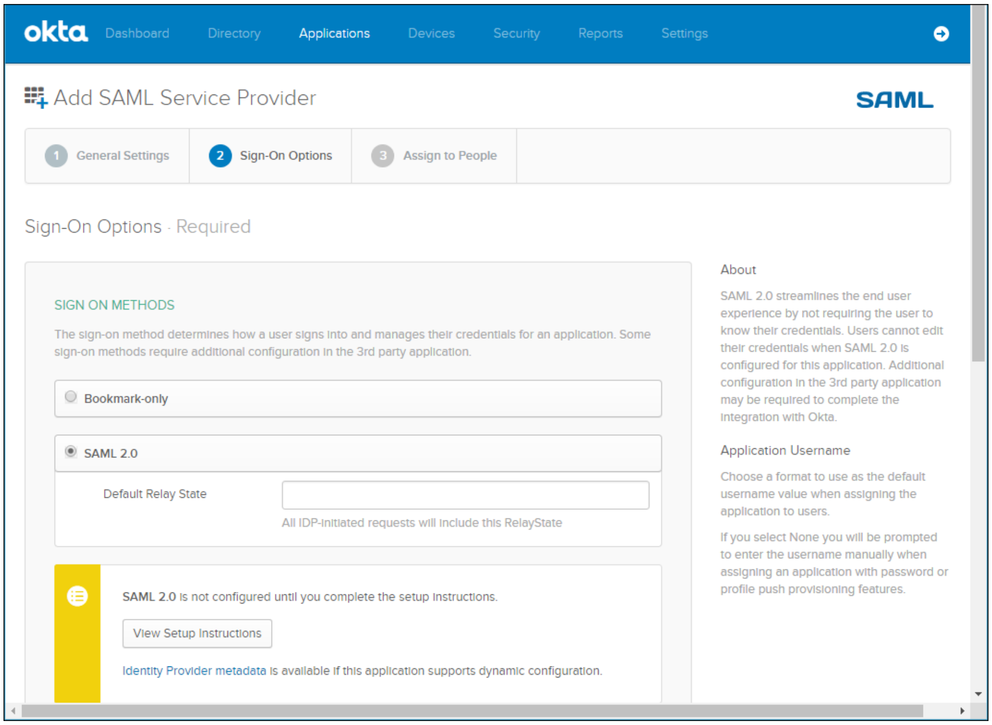
10. Enter the URL to access the HCP Anywhere Enterprise Portal login in the **Reply URL (Assertion Consumer Service URL)** box: `http://<teamportal>.<DNS_Suffix>/ServicesPortal/saml` where `<teamportal>` is the name of the HCP Anywhere Enterprise Portal, and `<DNS_Suffix>` is the DNS suffix for the HCP Anywhere Enterprise Portal installation.
11. Click **Download** for the **Certificate (Base64)**.

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**.



Add SAML Service Provider

1 General Settings | 2 Sign-On Options | 3 Assign to People

Sign-On Options · Required

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

○ Bookmark-only

● SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

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**.

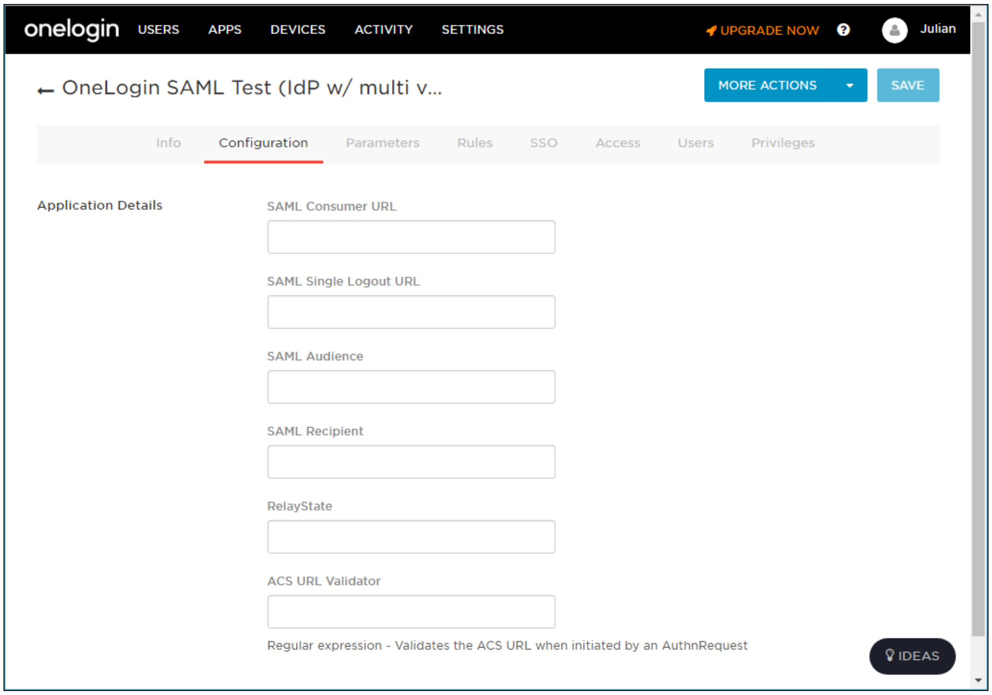
   The **Assertion Consumer Service URL** is the URL where SAML responses are posted, as follows: *https://fully_qualified_domain_name/ServicesPortal/saml*.
   For example, `https://myportal.example.com/ServicesPortal/saml`.
   You use the **Service Provider Entity Id** in the HCP Anywhere Enterprise Portal **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.



← OneLogin SAML Test (IdP w/ multi v...

Application Details

SAML Consumer URL

SAML Single Logout URL

SAML Audience

SAML Recipient

RelayState

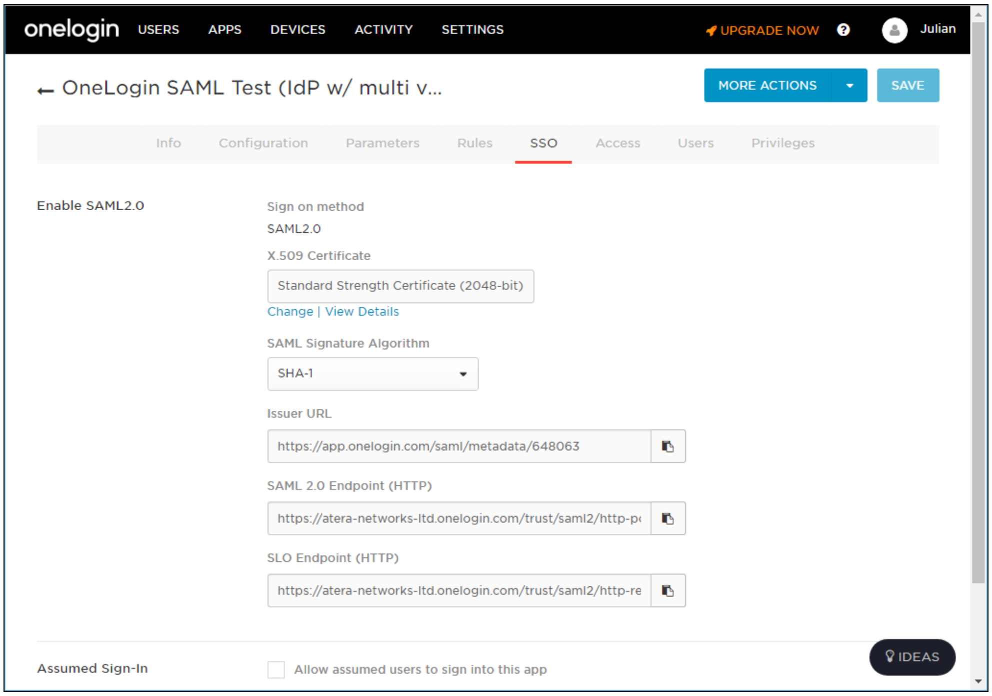
ACS URL Validator

Regular expression - Validates the ACS URL when initiated by an AuthnRequest

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.



← OneLogin SAML Test (IdP w/ multi v...

Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)

SAML Signature Algorithm
SHA-1

Issuer URL
https://app.onelogin.com/saml/metadata/648063

SAML 2.0 Endpoint (HTTP)
https://atera-networks-ltd.onelogin.com/trust/saml2/http-p

SLO Endpoint (HTTP)
https://atera-networks-ltd.onelogin.com/trust/saml2/http-re

Assumed Sign-In
□ Allow assumed users to sign into this app

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

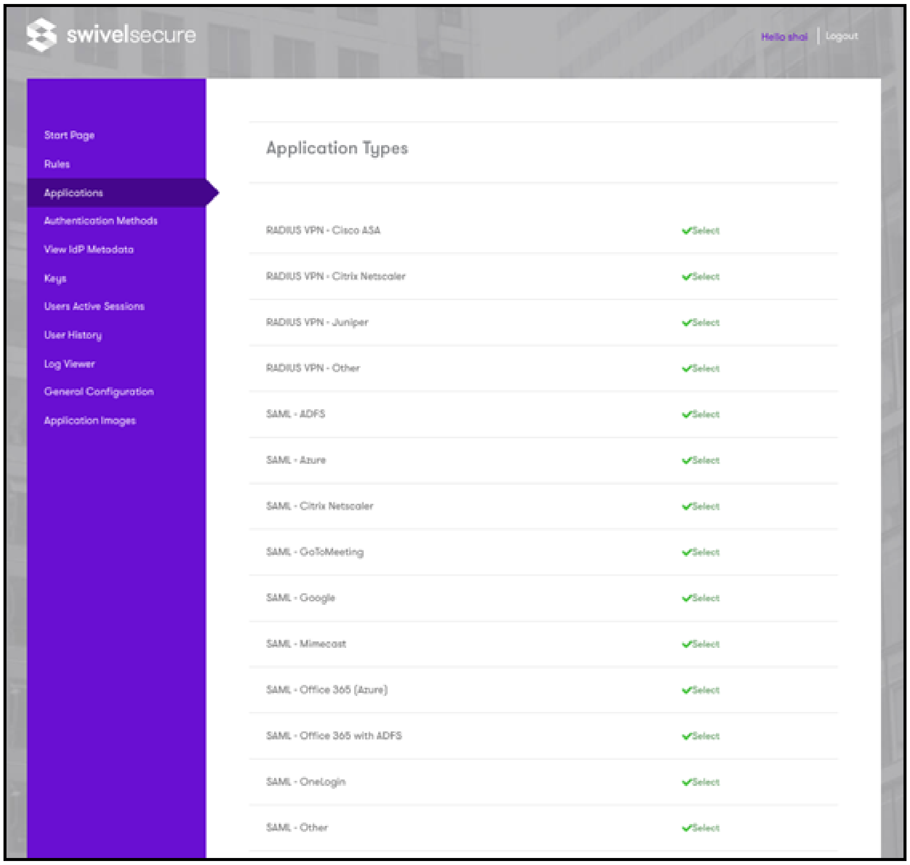
You set up SAML single sign-on support in Swivel AuthControl Sentry and gather the information you need to connect the HCP Anywhere Enterprise Portal to Swivel AuthControl Sentry.

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.

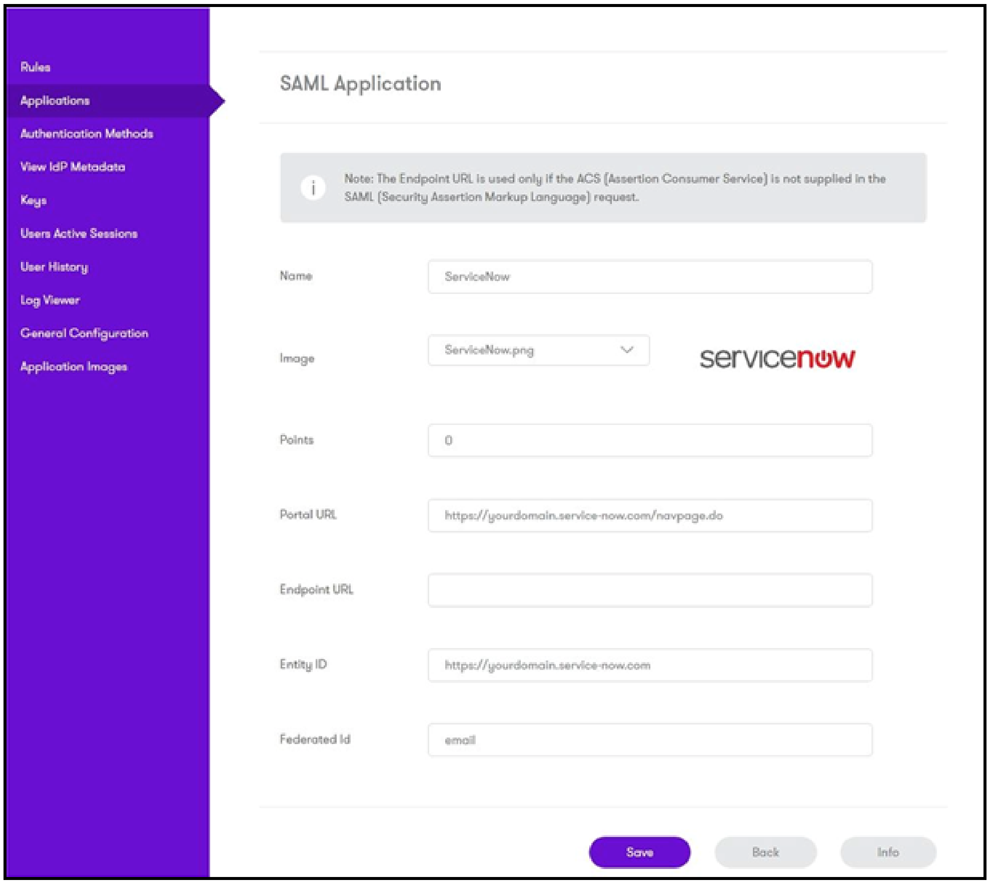
   The **Keys** screen is displayed.



Application Types

RADIUS VPN - Cisco ASA	✓Select
RADIUS VPN - Citrix Netscaler	✓Select
RADIUS VPN - Juniper	✓Select
RADIUS VPN - Other	✓Select
SAML - ADFS	✓Select
SAML - Azure	✓Select
SAML - Citrix Netscaler	✓Select
SAML - GoToMeeting	✓Select
SAML - Google	✓Select
SAML - Mimecast	✓Select
SAML - Office 365 (Azure)	✓Select
SAML - Office 365 with ADFS	✓Select
SAML - OneLogin	✓Select
SAML - Other	✓Select

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.



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name: ServiceNow

Image: ServiceNow.png

Points: 0

Portal URL: https://yourdomain.service-now.com/navpage.do

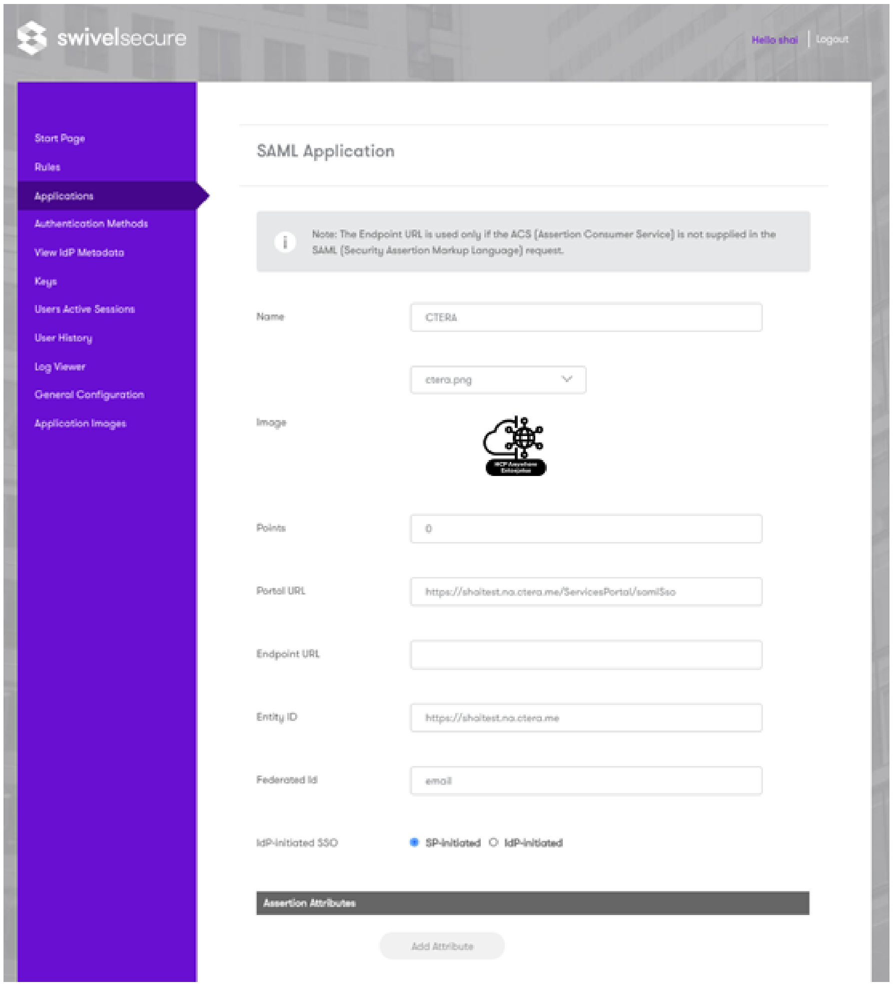
Endpoint URL:

Entity ID: https://yourdomain.service-now.com

Federated Id: email

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.



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name: CTERA

Image: ctera.png

Points: 0

Portal URL: https://shaitest.na.ctera.me/ServicesPortal/samlSso

Endpoint URL:

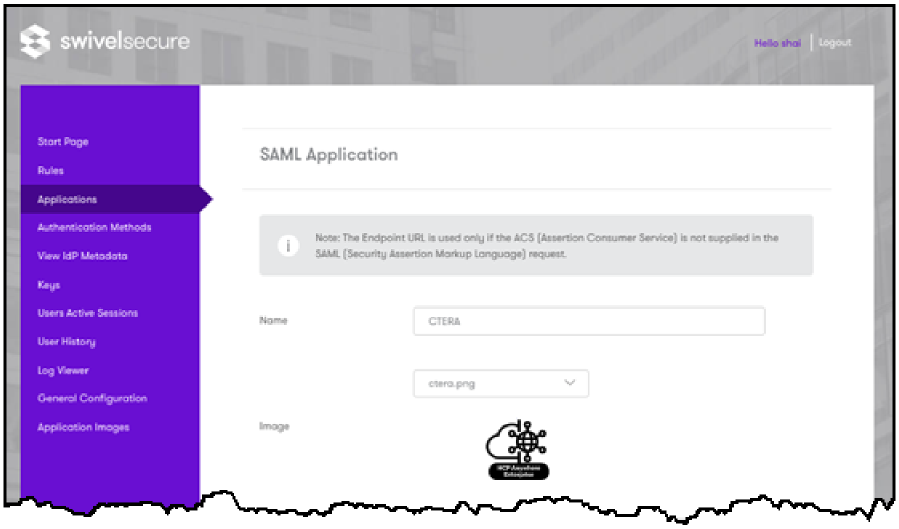
Entity ID: https://shaitest.na.ctera.me

Federated Id: email

IdP-initiated SSO: ● SP-initiated ○ IdP-initiated

Assertion Attributes

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



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name: CTERA

Image: ctera.png

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**.

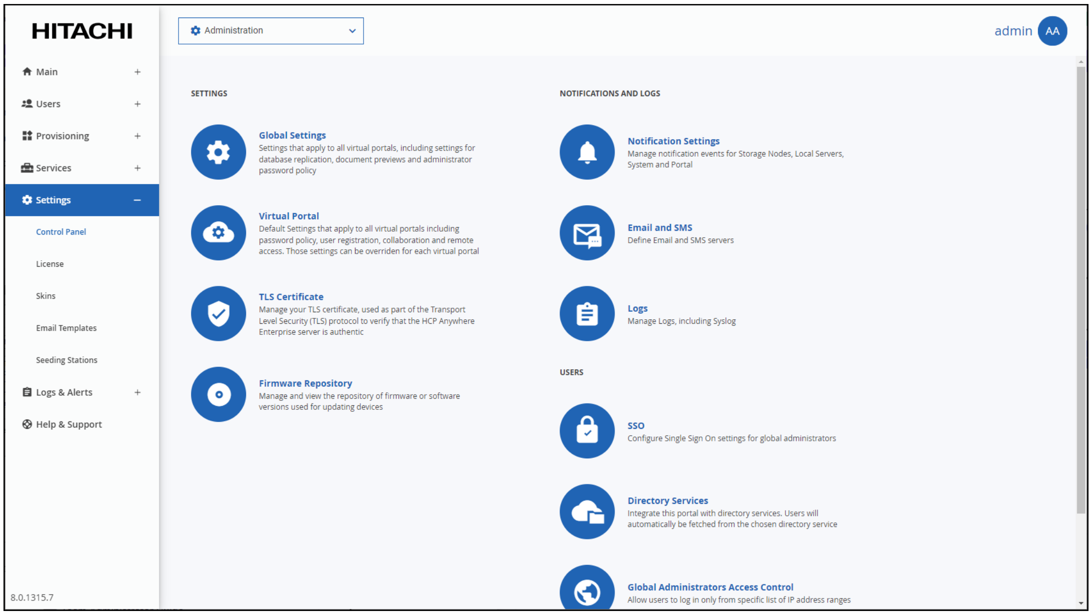
To verify that SSO has been set up in Swivel AuthControl Sentry:

- 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

To configure SAML single sign-on:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

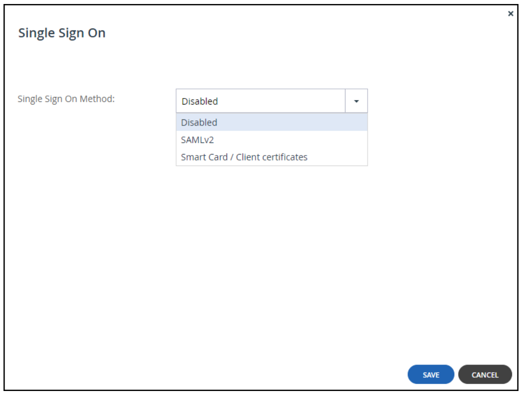
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

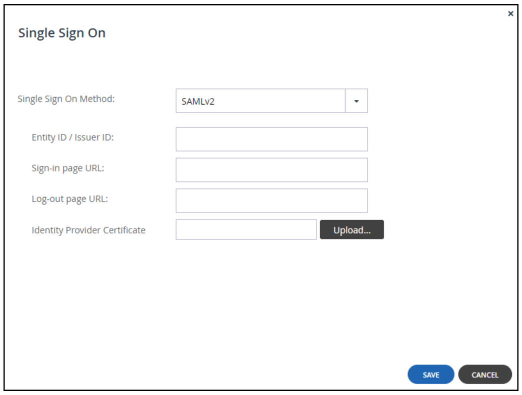
2. Select **SSO** under **USERS** in the **Control Panel** page.
   The **Single Sign On** window is displayed.



Single Sign On

Single Sign On Method: Disabled

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



Single Sign On

Single Sign On Method: SAMLv2

Entity ID / Issuer ID:

Sign-in page URL:

Log-out page URL:

Identity Provider Certificate

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 the procedure described in 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)** from the fourth part of the **SAML-based Sign-on** blade, in the procedure described in 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 entity ID that you choose when signing up for the Swivel AuthControl Sentry SAML Application, see the procedure described in 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** from the fourth part of the **SAML-based Sign-on** blade, in the procedure described in 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 portal. Without this URL configured, a logout will redirect to the sign-in page URL and log the user back into the 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, in the procedure described in 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 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, shown in step **11**, in the procedure described in 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, from the procedure described in 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 portal must be defined in the portal. The SAML response can be the user name or a unique customized filed, such as the user email and UPN (user principal name).

Bypassing SAML Authentication

As a global administrator, you may need to bypass authentication by SAML authentication in the following circumstances:

- When testing the integration of an SAML SSO provider.
- The SAML SSO provider’s login page is temporarily unavailable.

To bypass SAML authentication:

- Log in to the portal at the following URL: `http://`*`portal_address`*`/admin/bypass` where *portal_address* is the portal address.

Setting Up CAC (Common Access Card)

When a CAC, Common Access Card, is used, you can set the portal to allow access without the client CAC user entering a user name and password.

To configure the HCP Anywhere Enterprise Portal servers for CAC authentication:

1. Log in to the HCP Anywhere Enterprise Portal primary database server as root, using SSH.
2. Copy the root certificate file associated with the CAC certificate and any intermediate certificates in the chain to the /root/ path of the primary database server.
3. Create the truststore.

   a) In the primary database server enter the following:

   ```
   . $bindir/ctera-common.sh ; export _JAVA_OPTIONS
   ```

   b) Move to the `/usr/local/ctera/apache-tomcat/webapps/` directory and run the following keytool commands for the CAC certificate file and any intermediate certificates in the chain. For example, for a CAC certificate file named *RootCA1.cer* and an intermediate certificate named *IntermediateCA1.cer*, run the following two commands, changing the *`jdk1.8.0_201`* value to the JDK on the server (use the command `ls -d /usr/local/ctera/jdk*/bin` to find the current JDK bin directory):

```
/usr/local/ctera/jdk1.8.0_201/bin/keytool -import -keystore
truststore -file /root/RootCA1.cer -alias rootca1 -trustcacerts
-deststorepass $(grep -o -P "(?<=SERVER_KEY=).*"
/etc/ctera/portal.cfg)
/usr/local/ctera/jdk1.8.0_201/bin/keytool -import -keystore
truststore -file /root/IntermediateCA1.cer -alias intermediateca1
-trustcacerts -deststorepass $(grep -o -P "(?<=SERVER_KEY=).*"
/etc/ctera/portal.cfg)
```

Note: The alias name of each certificate in the keytool command must be unique.
You can display the certificates in the truststore with the following command:

```
keytool -list -v -keystore truststore -deststorepass $(grep -o
-P "(?<=SERVER_KEY=).*" /etc/ctera/portal.cfg)
```

c) Convert the truststore format to BCFKS format by running the following command, changing the *jdk* value to the JDK on the server:

```
keytool -importkeystore -srckeystore
/usr/local/ctera/apache-tomcat/webapps/truststore -srcstoretype
JKS -destkeystore
/usr/local/ctera/apache-tomcat/webapps/truststore.bcfks
-deststoretype BCFKS -srcprovidername "SUN" -providerclass
com.safelogic.cryptocomply.jcajce.provider.CryptoComplyFipsProvide
r  -providerpath
/usr/local/ctera/jdk1.8.0_201/jre/lib/ext/SafeLogic_CTERA.jar
-srcstorepass $(grep -o -P "(?<=SERVER_KEY=).*"
/etc/ctera/portal.cfg) -deststorepass $(grep -o -P
"(?<=SERVER_KEY=).*" /etc/ctera/portal.cfg)
```

You can display the entries in the new BCFKS keystore with the following command:

```
keytool -list -v -keystore truststore.bcfks -storetype BCFKS
-deststorepass $(grep -o -P "(?<=SERVER_KEY=).*"
/etc/ctera/portal.cfg)
```

The password is the SERVER_KEY, which is extracted automatically from `/etc/ctera/portal.cfg` and used in the following part of the above command `$(grep -o -P "(?<=SERVER_KEY=).*" /etc/ctera/portal.cfg)`.

d) Copy the truststore.bcfks file to the same path of the Replication DB server and all the portal servers, such as the application and preview servers. For example, using SCP, run the following command:

```
scp truststore.bcfks
root@portal_ip_address:/usr/local/ctera/apache-tomcat/webapps
```

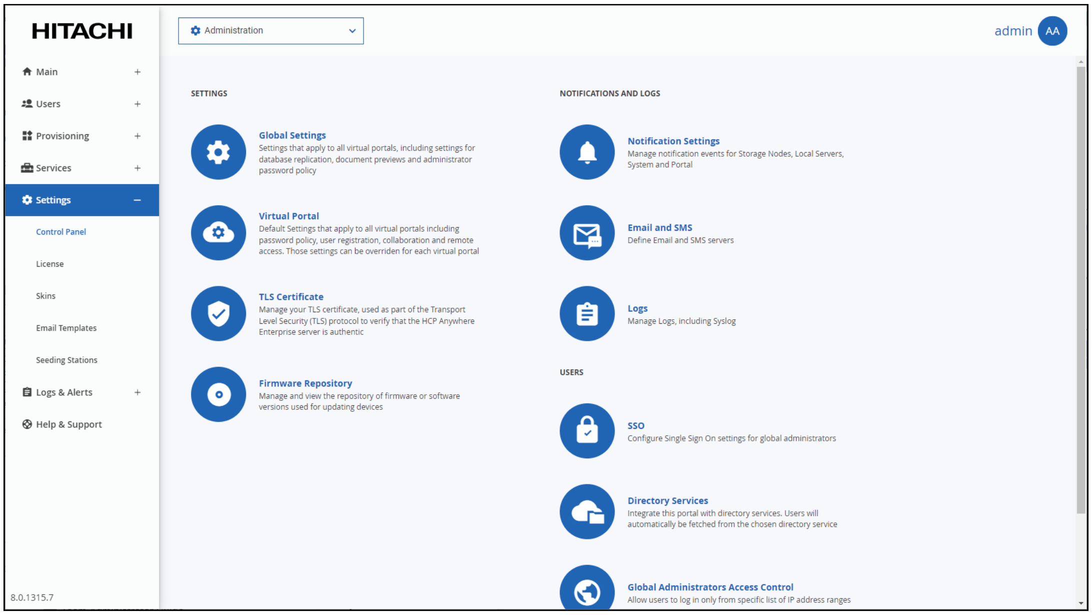
4. Enable FIPS by running the following in the command line:

```
set /settings/javaSecurityProviderMode FIPS
```

5. Restart the portal servers.

To configure CAC single sign-on in the portal user interface:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

USERS

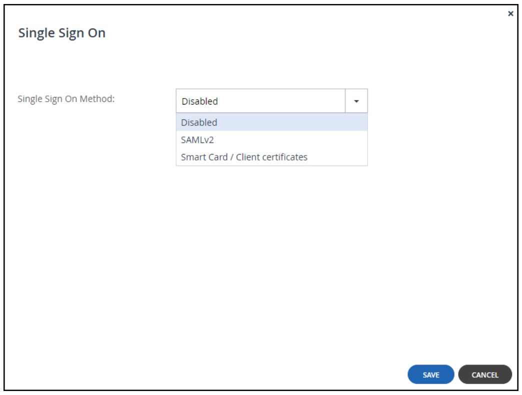
SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **SSO** under **USERS** in the **Control Panel** page.

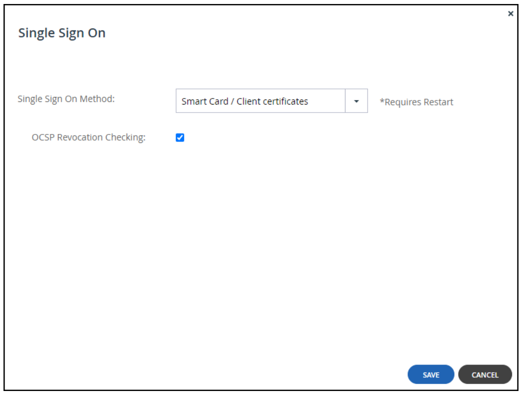
   The **Single Sign On** window is displayed.



Single Sign On Method: Disabled

3. Select **Smart Card / Client certificates** from the drop-down box.

   The **Single Sign On** window is redisplayed for CAC authentication.



Single Sign On Method: Smart Card / Client certificates

OCSP Revocation Checking: ☑

4. If an OCSP server is being used for certificate revocation, make sure **OCSP Revocation Checking** is checked.

   When checked, the answer from the OCSP server is used when attempting to log on.
5. Click **SAVE**.

The portal servers are restarted.

Users log on to their systems using CAC.

Chapter 9. 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 supports snapshots of the HCP Anywhere Enterprise Portal Cloud Drive.

The Snapshot Retention Policy

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 Managing Subscription Plans, in the **Snapshot Retention Policy** window.

Applying a Snapshot Retention Policy

The snapshot retention policy defined in the subscription plan can be applied globally as the default plan for team portals.

Snapshot Retention for the Cloud Drive Service

Each user account using the Cloud Drive service can be 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 and HCP Anywhere Enterprise

Drive Share (Agent) 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.

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 10. Managing Subscription Plans

Provisioning is the process of assigning services and quotas to users or team portals (tenants) in subscription plans.

HCP Anywhere Enterprise includes two levels of provisioning:

- **Portal-level provisioning**
  The HCP Anywhere Enterprise Portal owner provisions each team portal owner with services and quotas. For example, it is possible to limit a team portal to use a total of up to 100GB of storage space.
  Portal-level provisioning is performed by global administrators.
  The following provisioning methods are available for portal-level provisioning:
  - **Global plans**
    In order to obtain services, virtual portals are assigned to a global plan which defines a set of services that the portal will receive, and which will subsequently be used by the HCP Anywhere Enterprise Portal end users. Further, the plan can specify a maximum snapshot retention policy for the portal. See The Snapshot Retention Policy. The global plan is set for a team portal in **Main > Portals**. Click the team portal and then specify the global plan to use in the **Provisioning** option.
  - **Global add-ons**
    In addition to the global plan, one or more global add-ons can be added to HCP Anywhere Enterprise Portals. Each global add-on defines a set of services that HCP Anywhere Enterprise Portals will receive in addition to the services specified in the global plan. For example, an add-on may include an additional 10 GB of storage space for the number of devices specified in the global plan. Add-ons can be set to expire after a specified time period and can be stacked as desired. For example, a HCP Anywhere Enterprise Portal may have a subscription plan for 100 GB of storage, as well as two add-ons for 10GB of storage and one add-on for 5GB of storage. While the add-ons are valid, the HCP Anywhere Enterprise Portal will be entitled to allocate up to 125GB of cloud storage to end users.
- **End-user provisioning**
  The team portal owner provisions end users with services and quotas, such as storage space and the number of HCP Anywhere Enterprise Drive Share (Agents). In team portals, end-user provisioning is optional and is performed by team or global administrators.

You provision licenses to virtual portals, by assigning the virtual portals to global plans and add-ons.

When a team portal is assigned to a global plan or add-on, HCP Anywhere Enterprise Portal automatically creates a default subscription plan containing the licenses specified in the global plan and add-ons, and assigns all user accounts in the team portal to this plan. The global plan limits the total amount of resources used by end users. Portal Licenses are consumed immediately, when the team portal is provisioned. You can create alternate subscription plans and assign those to individual user accounts. Users in a team portal obtain services through their subscription plans for an open-ended period of time.

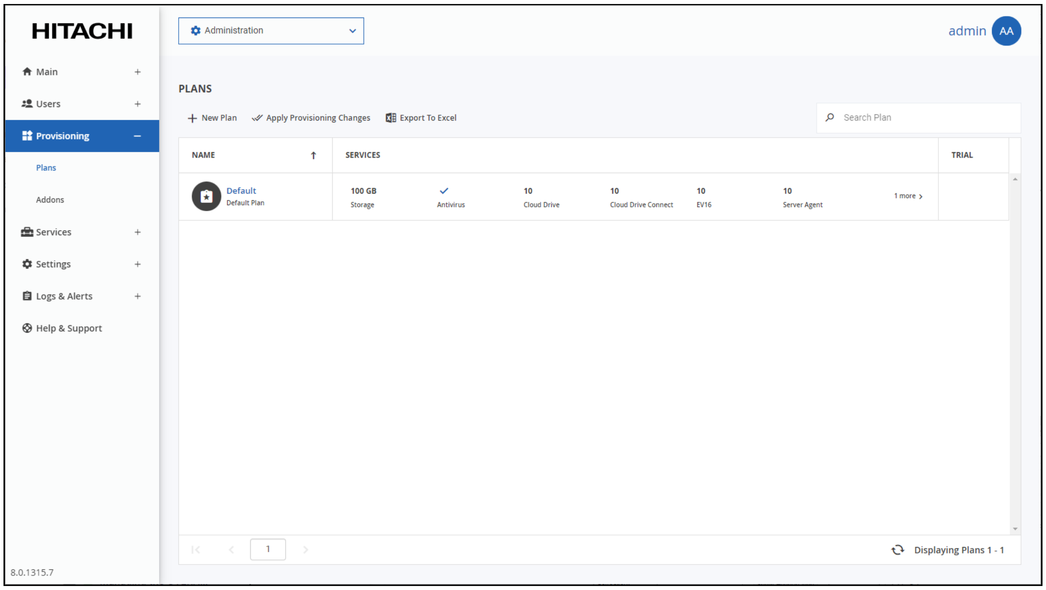
In this chapter

- [Deleting a Plan](#)
- [Setting or Removing the Default Plan](#)
- [Exporting Plan Details to Excel](#)

Viewing Subscription Plans

To view all plans:

- In the global administration view, select **Provisioning > Plans** in the navigation pane.
  The **PLANS** page is displayed.



NAME	SERVICES							TRIAL
Default Default Plan	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more ›	

Where:

NAME – The subscription plan's name.is displayed under the plan name for the default plan.

SERVICES – The services provisioned in the plan.

- **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 Drive Share (Agent) licenses

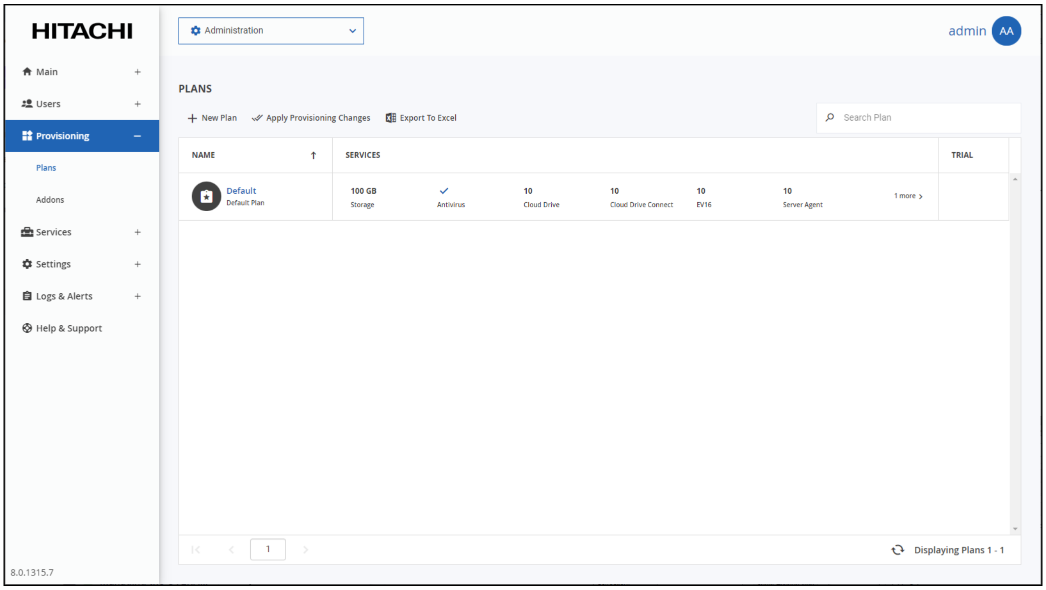
included in the plan.

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

Adding or Editing a Subscription Plan

To add or edit a subscription plan:

1. In the global administration view, select **Provisioning > Plans** in the navigation pane. The **PLANS** page is displayed.



NAME	SERVICES							TRIAL
Default Default Plan	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more ›	

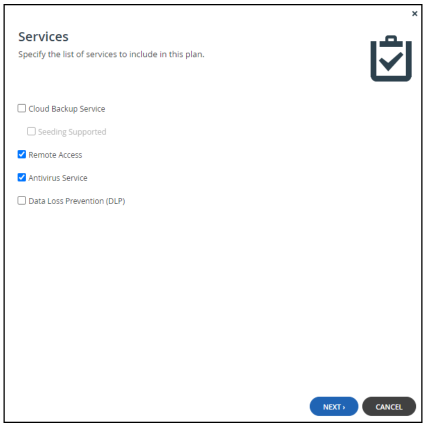
2. To add a new plan, click **New Plan**.

   Or,

   To edit an existing plan, click the plan's name**.**

   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.

   The plan wizard opens, displaying the **Services** window.



Services

Specify the list of services to include in this plan.

☐ Cloud Backup Service

☐ Seeding Supported

☑ Remote Access

☑ Antivirus Service

☐ Data Loss Prevention (DLP)

3. Choose which services to include in the plan:

   Cloud Backup Service – This feature is currently not supported.

   Seeding Supported – This feature is currently not supported.

   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.

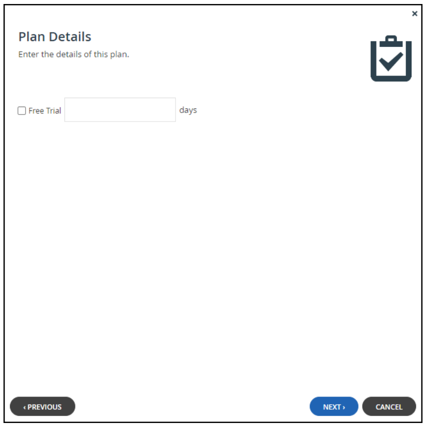
   None – Cloud drive services are not included in the plan.

   Antivirus Service – Include the Cloud Drive antivirus service in the plan. When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time. The Cloud Drive antivirus service requires an additional license.

   Data Loss Prevention (DLP) – Currently not supported.

4. Click **NEXT**.

   The **Plan Details** window is displayed.



Plan Details

Enter the details of this plan.

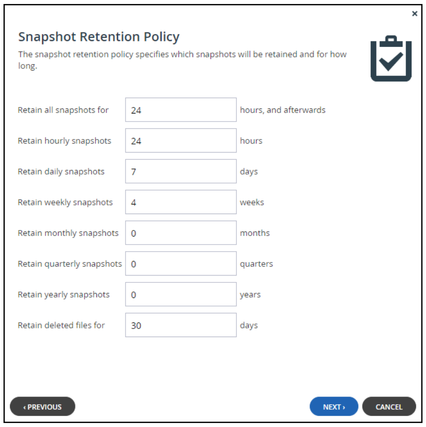
☐ Free Trial ______ days

5. Set the plan details.

   Free Trial – Include a free trial period in the plan. Enter the number of days that subscribers can receive the plan for free.

6. Click **NEXT**.

   The **Snapshot Retention Policy** window is displayed. This policy applies to Cloud Drive snapshots.



Snapshot Retention Policy

The snapshot retention policy specifies which snapshots will be retained and for how long.

Retain all snapshots for 24 hours, and afterwards

Retain hourly snapshots 24 hours

Retain daily snapshots 7 days

Retain weekly snapshots 4 weeks

Retain monthly snapshots 0 months

Retain quarterly snapshots 0 quarters

Retain yearly snapshots 0 years

Retain deleted files for 30 days

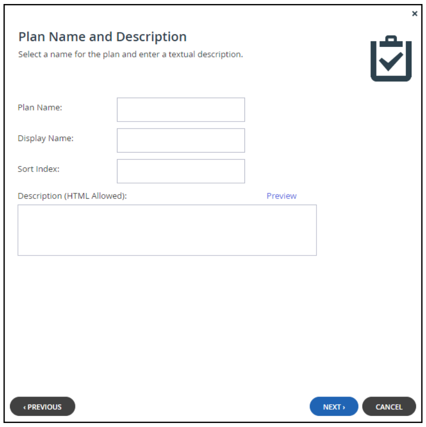
7. Set the snapshot retention policy.

   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 value is 1 day.

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

8. Click **NEXT**.

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



Plan Name and Description

Select a name for the plan and enter a textual description.

Plan Name:

Display Name:

Sort Index:

Description (HTML Allowed):

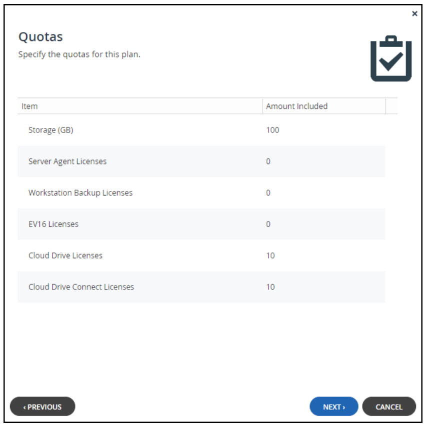
9. Specify the plan name and provide a description.

   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.

10. Click **NEXT**.

    The **Quotas** window is displayed.

    Quotas

    Specify the quotas for this plan.

Item	Amount Included
Storage (GB)	100
Server Agent Licenses	0
Workstation Backup Licenses	0
EV16 Licenses	0
Cloud Drive Licenses	10
Cloud Drive Connect Licenses	10

11. 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.

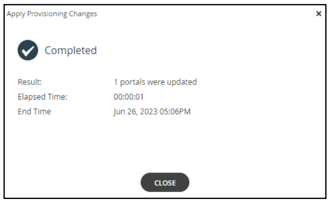
    Note: The quotas must not exceed the number specified in the license. An error message is displayed when you attempt to assign a user to a plan with a quota that exceeds the number specified in the license.

12. Click **NEXT**.

    The **Wizard Completed** screen is displayed.

13. 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**.



Apply Provisioning Changes

Completed

Result: 1 portals were updated
Elapsed Time: 00:00:01
End Time Jun 26, 2023 05:06PM

Deleting a Plan

You cannot delete the default plan, nor a plan that is already assigned.

To delete a plan:

1. In the global administration view, 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.

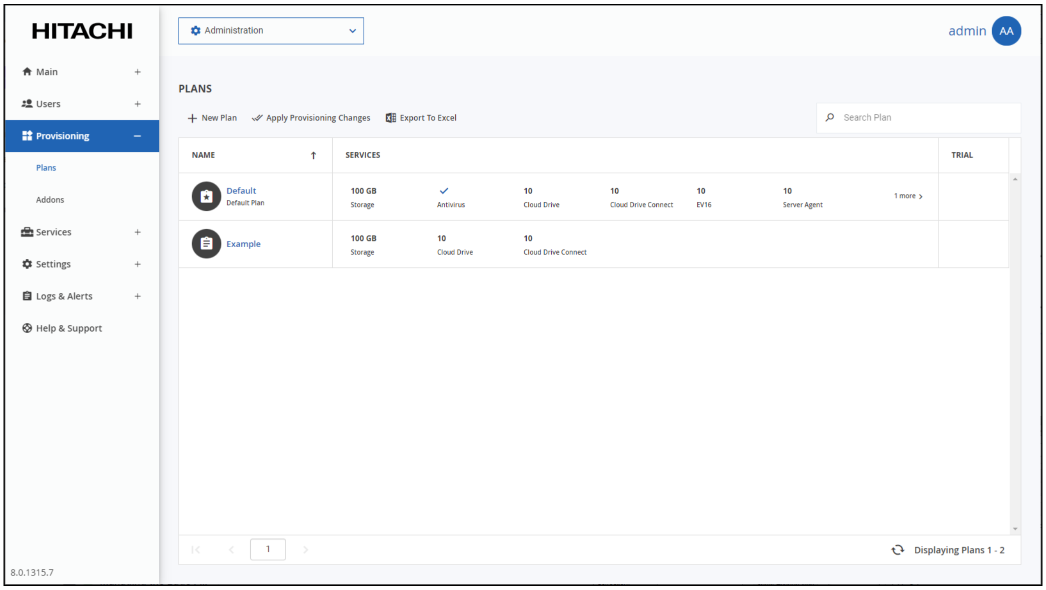
The subscription plan is deleted.

Setting or Removing the Default Plan

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

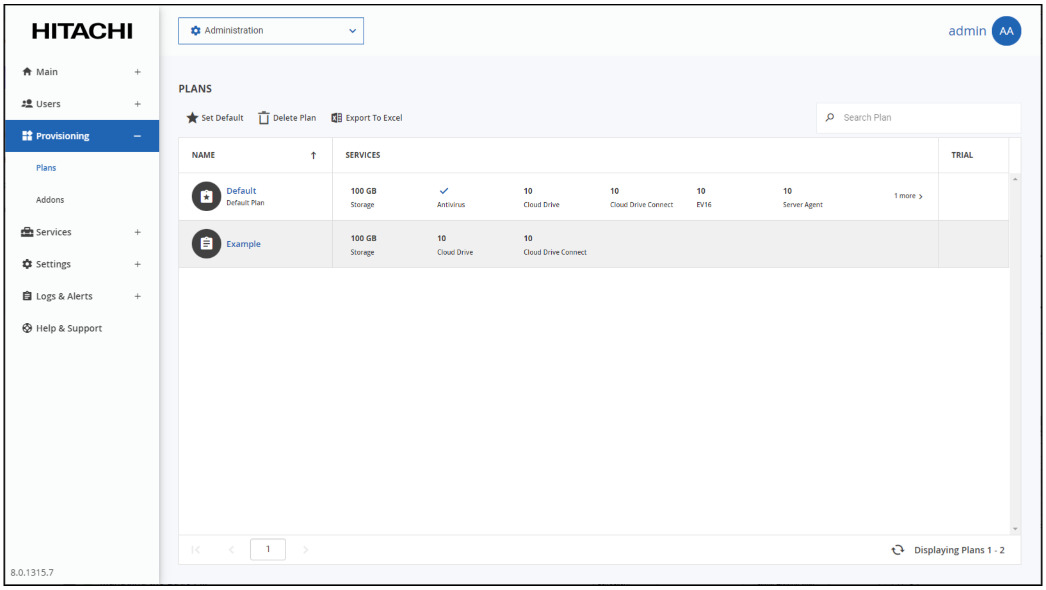
To set a plan as the default:

1. In the global administration view, select **Provisioning > Plans** in the navigation pane.
   The **PLANS** page is displayed.



NAME	SERVICES							TRIAL
Default Default Plan	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more	
Example	100 GB Storage	10 Cloud Drive	10 Cloud Drive Connect					

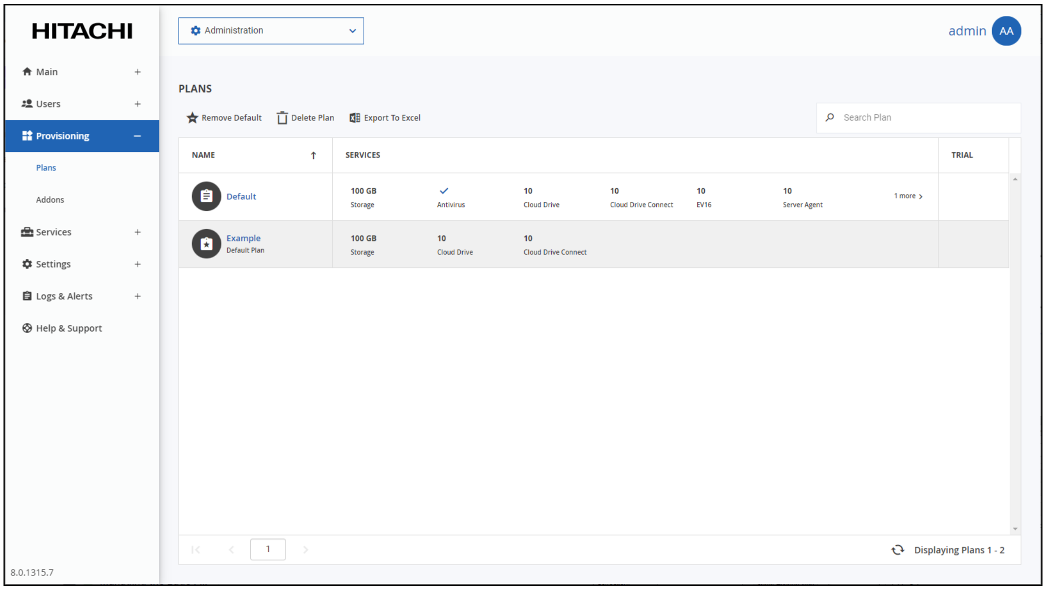
2. Select the row of the plan to make default.



NAME	SERVICES							TRIAL
Default Default Plan	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more ›	
Example	100 GB Storage	10 Cloud Drive	10 Cloud Drive Connect					

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.



NAME	SERVICES							TRIAL
Default	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more ›	
Example Default Plan	100 GB Storage	10 Cloud Drive	10 Cloud Drive Connect					

To remove a subscription plan from being the default:

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

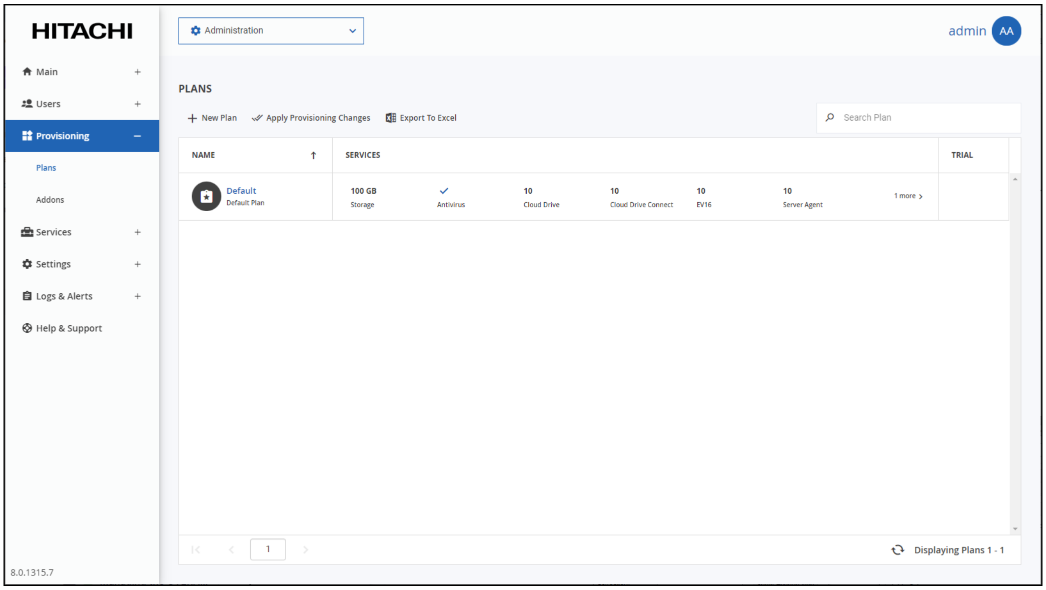
The subscription plan is no longer the default.

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. In the global administration view, select **Provisioning > Plans** in the navigation pane. The **PLANS** page is displayed.



NAME	SERVICES							TRIAL
Default Default Plan	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more ›	

2. Click **Export to Excel**.

The list of plans is exported to your computer.

Chapter 11. Managing Add-ons

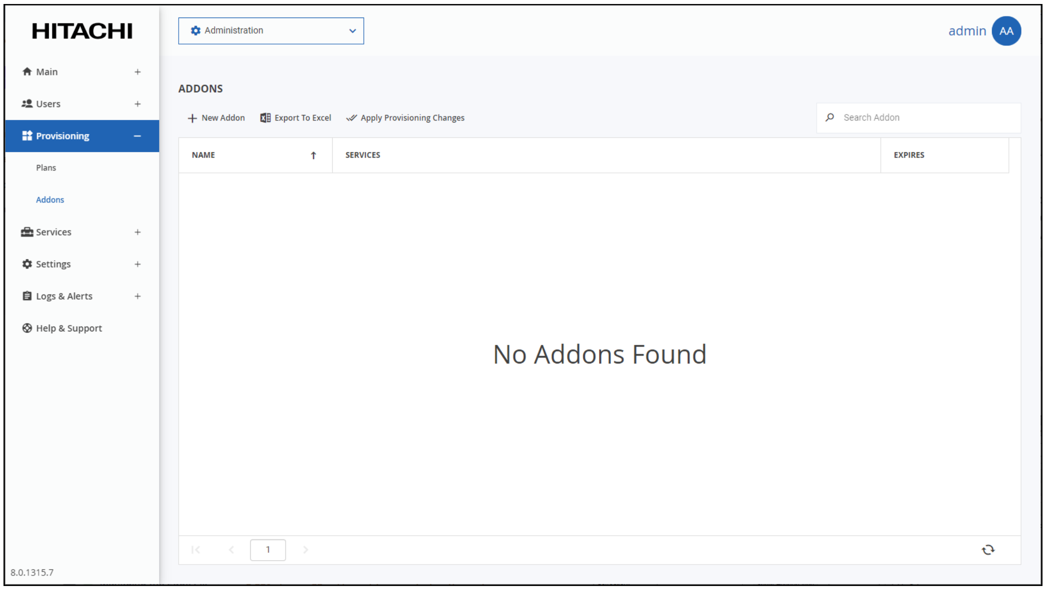
In a team portal, when the portal is subscribed to a *global add-on*, all users obtain additional services for a specified period of time.

In this chapter

Viewing Add-ons

To view all add-ons:

- In the global administration view, select **Provisioning > Addons** in the navigation pane.
  The **ADDONS** page is displayed.



No Addons Found

Where:
NAME – The add-on name. The add-on display name, displayed in the End User Portal and notifications, is displayed under the name.
SERVICES – The services that the add-on applies to.

- **Storage** – The amount of storage for the add-on.
- **Antivirus** – The add-on includes the antivirus service.
- **Cloud Drive** – The HCP Anywhere Enterprise Cloud Drive license is included in the add-on.
- **Cloud Drive Connect** – The HCP Anywhere Enterprise Cloud Drive Connect license is included in the add-on.
- **EV8** – The number of EV8 HCP Anywhere Enterprise Edge Filer licenses included in the add-on.

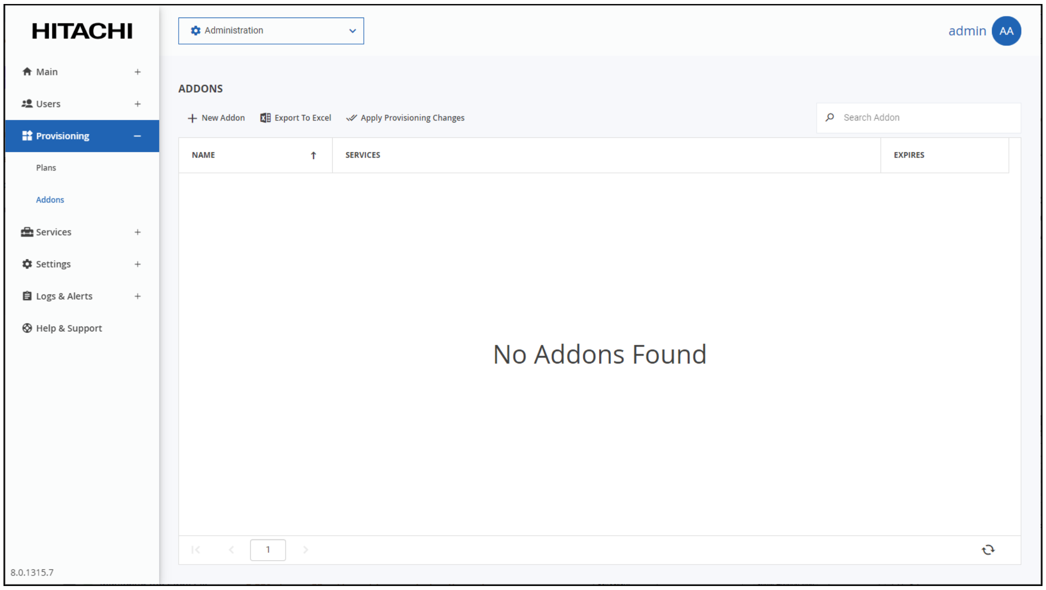
- **EV16** – The number of EV16 HCP Anywhere Enterprise Edge Filer licenses included in the add-on.
- **EV32** – The number of EV32 HCP Anywhere Enterprise Edge Filer licenses included in the add-on.
- **EV64** – The number of EV64 HCP Anywhere Enterprise Edge Filer licenses included in the add-on.
- **EV128** – The number of EV128 HCP Anywhere Enterprise Edge Filer licenses included in the add-on.
- **EV256** – The number of EV256 HCP Anywhere Enterprise Edge Filer licenses included in the add-on.
- **Server Agent** – The number of HCP Anywhere Enterprise Drive Share (Agent) licenses included in the add-on.
- **Workstation Backup** – Currently not supported.

EXPIRES – The number of days after adding this add-on, that the add-on will expire.

Adding, Editing, or Deleting Add-ons

To add or edit an add-on:

1. In the global administration view, select **Provisioning > Addons** in the navigation pane. The **ADDONS** page is displayed.



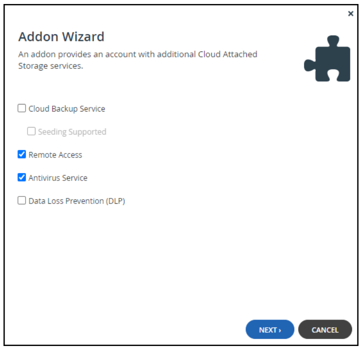
No Addons Found

2. To add a new add-on, click **New Addon**.

   Or,

   To edit an existing add-on, click the add-on name**.**

   The **Addon** wizard is displayed.



Addon Wizard

An addon provides an account with additional Cloud Attached Storage services.

☐ Cloud Backup Service

☐ Seeding Supported

☑ Remote Access

☑ Antivirus Service

☐ Data Loss Prevention (DLP)

3. Choose which services to include in the add-on:

Cloud Backup Service – This option is currently not supported.

Seeding Supported – This option is currently not supported.

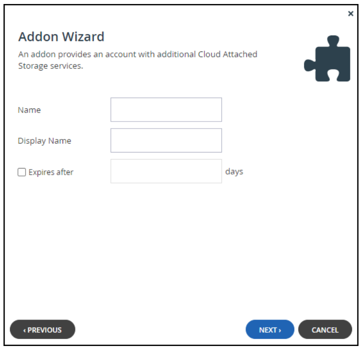
Remote Access – Include remote access in the subscription plan. Remote access includes both access to the device's management interface via the HCP Anywhere Enterprise Portal and a dedicated URL, access to the user's files via the HCP Anywhere Enterprise Portal and a dedicated URL.

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

Antivirus Service – Include the Cloud Drive antivirus service in the plan. When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time. The antivirus service requires an additional license. For details about the antivirus service, see Managing Antivirus Servers.

Data Loss Prevention (DLP) – This option is currently not supported.

4. Click **NEXT**.



Addon Wizard

An addon provides an account with additional Cloud Attached Storage services.

Name

Display Name

☐ Expires after days

5. Set the addon details.

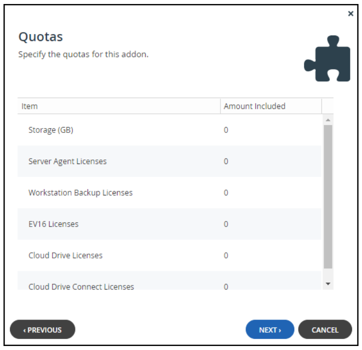
Name – A name for the add-on. Only letters and numbers can be used for the name.

Display Name – The name to use when displaying this add-on in the end user portal and notifications.

Expires after – The number of days after adding this add-on, that the add-on will expire.

6. Click **NEXT**.

The **Quotas** window is displayed.



Quotas

Specify the quotas for this addon.

Item	Amount Included
Storage (GB)	0
Server Agent Licenses	0
Workstation Backup Licenses	0
EV16 Licenses	0
Cloud Drive Licenses	0
Cloud Drive Connect Licenses	0

7. 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.

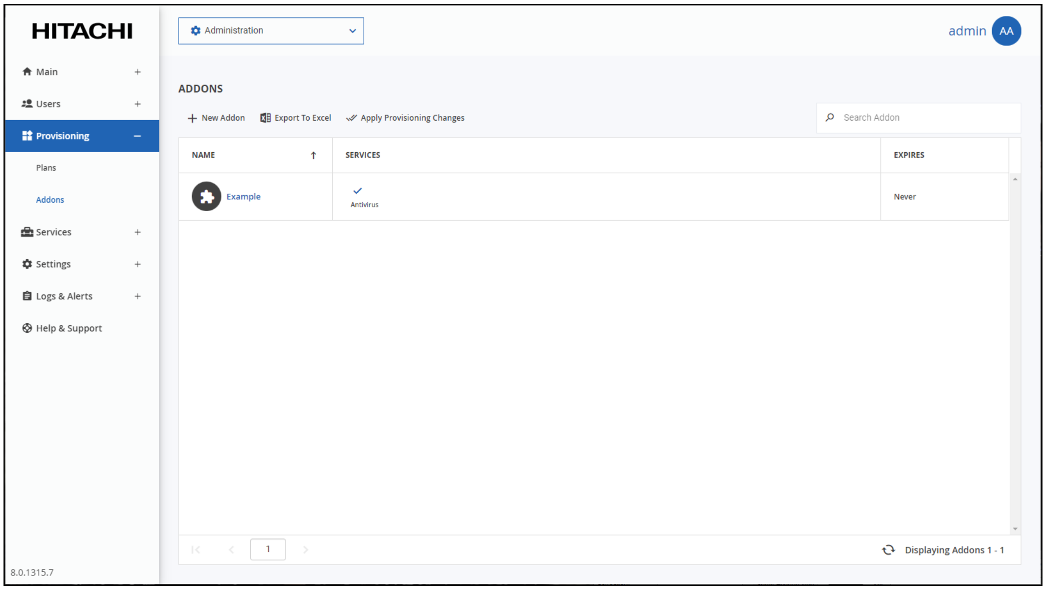
   Note: The quotas must not exceed the number specified in the license. An error message is displayed when you attempt to assign a user to a plan with a quota that exceeds the number specified in the license.

8. Click **NEXT**.

   The **Wizard Completed** screen is displayed.

9. Click **FINISH**.

   The **ADDONS** page is displayed with the add-on.

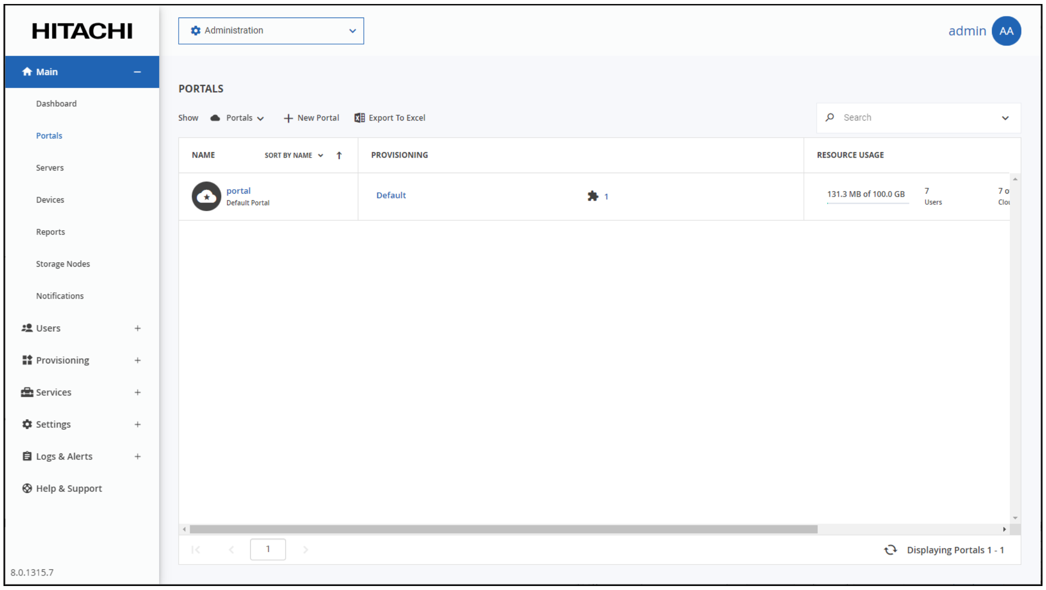


NAME	SERVICES	EXPIRES
Example	✓ Antivirus	Never

10. Assign the add-on to virtual portal, as described in Assigning Add-ons to Team Portals.

    The number of add-ons specified for a portal is displayed in the following:

    - In **Main > Portals**. Click the add-on icon, 🧩, to view the add-on details.

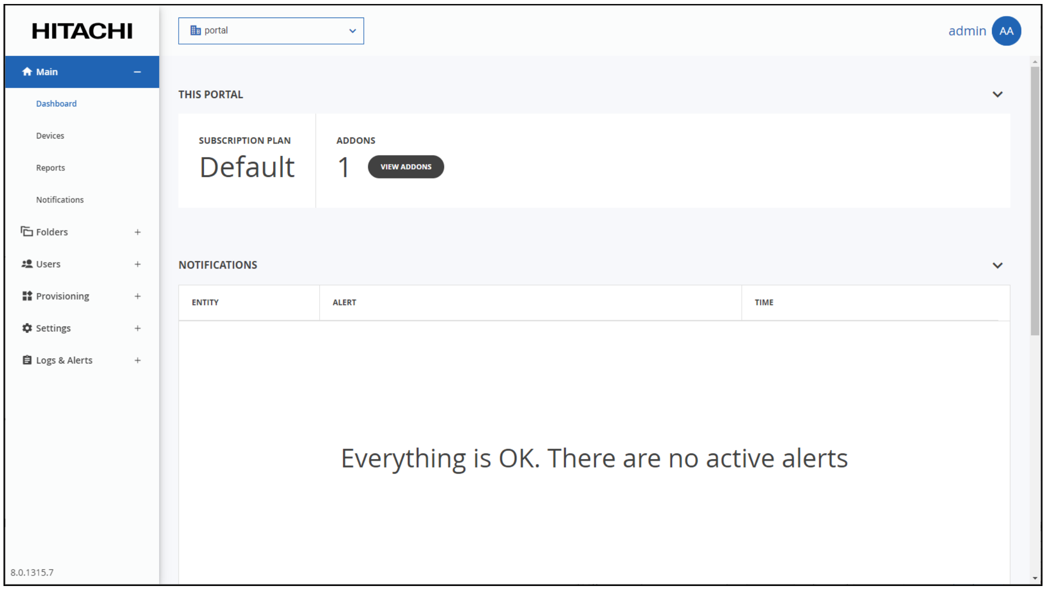


PORTALS

NAME	PROVISIONING		RESOURCE USAGE		
portal Default Portal	Default	1	131.3 MB of 100.0 GB	7 Users	7 o Clo

Displaying Portals 1 - 1

- In **Main > Dashboard**. Click **VIEW ADDONS** to view the add-on details.



THIS PORTAL

SUBSCRIPTION PLAN: Default

ADDONS: 1

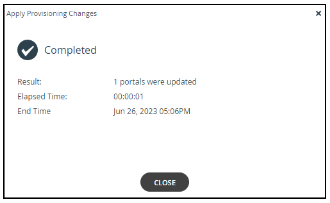
NOTIFICATIONS

ENTITY	ALERT	TIME

Everything is OK. There are no active alerts

If you edited an existing add-on, HCP Anywhere Enterprise Portal applies changed plans to all users every day at midnight.

You can use apply the plan changes immediately by clicking **Apply Provisioning Changes**. The **Apply Provisioning Changes** window is displayed and the changes are applied. After the changes have been applied click **CLOSE**.



Apply Provisioning Changes

Completed

Result:	1 portals were updated
Elapsed Time:	00:00:01
End Time	Jun 26, 2023 05:06PM

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**.

Deleting an Add-On

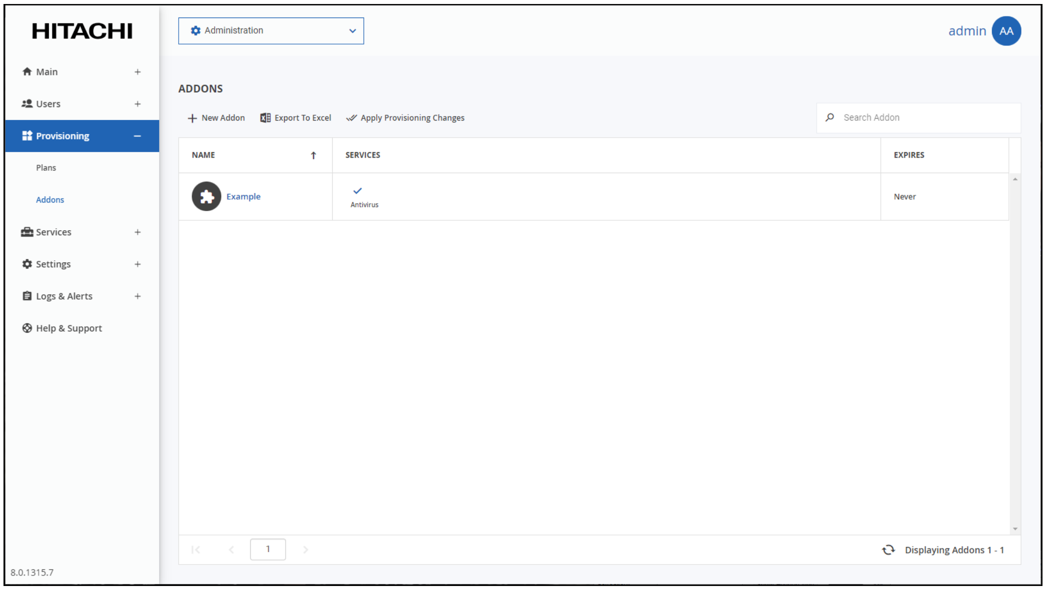
Before you can delete an add-on, you must delete the add-on from the portal provisioning:

1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.
2. Click the portal name that includes the add-on.
3. Click the **Provisioning** option.

   The **Provisioning** window is displayed.
4. Select the **Add-ons** tab.
5. In the add-on row in the list box, click 🗑.
6. Click **SAVE**.

To delete an Add-on:

1. In the global administration view, select **Provisioning > Addons** in the navigation pane.
   The **ADDONS** page is displayed.



ADDONS

NAME	SERVICES	EXPIRES
Example	✓ Antivirus	Never

2. Select the add-on row.
3. Click **Delete Addon**.

A confirmation window is displayed.

4. Click **DELETE** to confirm.

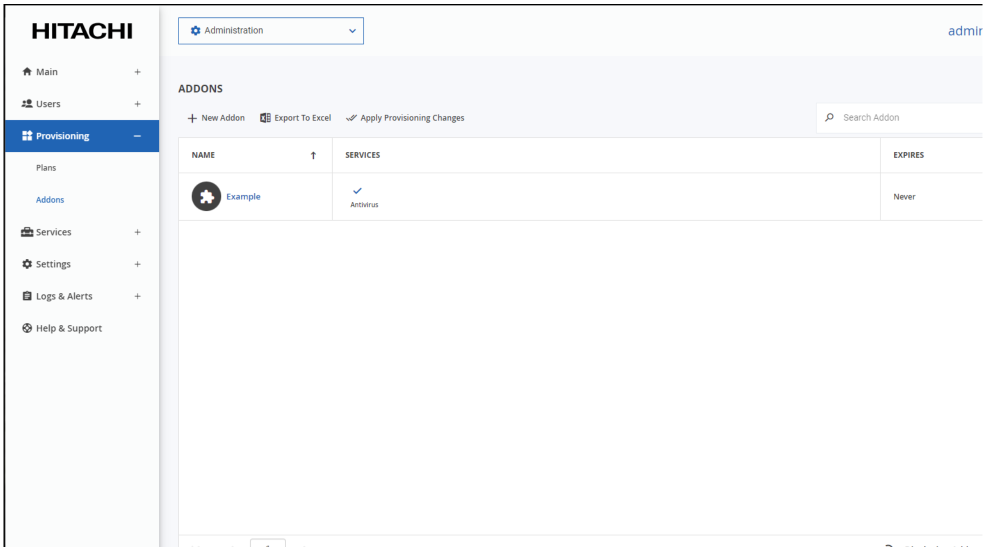
The add-on is deleted.

Exporting Add-On Details to Excel

You can export the list of add-ons and their details to a comma separated values (*.csv) Excel file.

To export the list of add-ons to an Excel file:

1. In the global administration view, select **Provisioning > Addons** in the navigation pane. The **ADDONS** page is displayed.



NAME	SERVICES	EXPIRES
Example	✓ Antivirus	Never

2. Click **Export to Excel**.

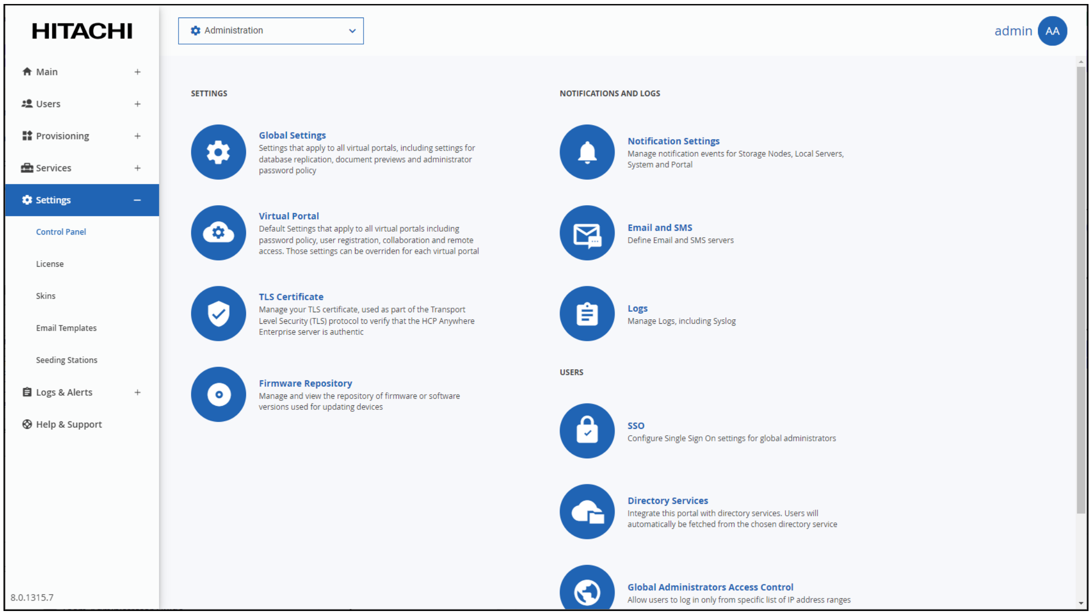
The add-on list is downloaded to your computer. The list includes the number of days before the add-on expires.

Chapter 12. Configuring Email and SMS Settings

You can configure global email and SMS settings that will be inherited by all servers. For information on overriding these settings on a per-server basis, see Editing Server Settings.

To configure email and SMS settings:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

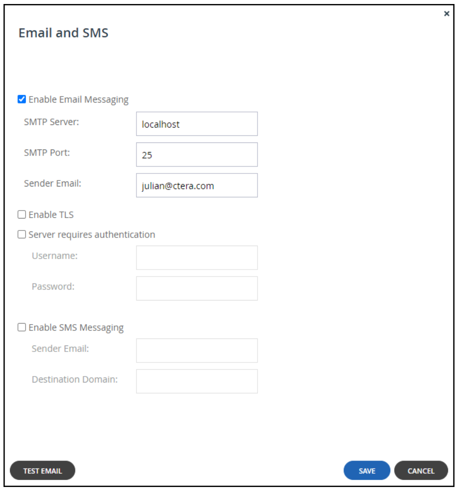
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Email and SMS** under **NOTIFICATIONS AND LOGS** in the **Control Panel** page.
   The **Email and SMS** window is displayed.



Email and SMS

☑ Enable Email Messaging

SMTP Server:	localhost
SMTP Port:	25
Sender Email:	julian@ctera.com

☐ Enable TLS

☐ Server requires authentication

Username:	
Password:	

☐ Enable SMS Messaging

Sender Email:	
Destination Domain:	

3. Complete the fields.

   Enable Email Messaging – Enable sending email messages from the HCP Anywhere Enterprise Portal to users. The **SMTP Server**, **SMTP Port**, and **Sender Email** fields are enabled.

SMTP Server – The outgoing mail server address for sending email messages from the HCP Anywhere Enterprise Portal to users.

SMTP Port – The port number for sending email messages from the HCP Anywhere Enterprise Portal to users.

Sender Email – The email address to use in the From field of notifications sent to global administrators by the global portal.

For example: `"Example Customer Service <support@example.com>"`.

Enable TLS – Use Transport Layer Security (TLS) encryption for sending email messages from the HCP Anywhere Enterprise Portal to users.

Server requires authentication – The SMTP server requires authentication. The **Username** and **Password** fields are enabled.

Username – The user name that the HCP Anywhere Enterprise Portal uses when authenticating to the SMTP server.

Password – The password that the HCP Anywhere Enterprise Portal uses when authenticating to the SMTP server.

Enable SMS Messaging – Enable sending passcodes via text message to protect access to guest invitations. To effectively enable SMS messaging, you must register with an SMS gateway and then enter the sender email and destination domain in the fields below.

SMS messaging must be enabled here in order for the **SMS** option to be displayed among the authentication options in the Collaboration section of the **Settings > Virtual Portal Settings** page.

Sender Email – The sender email address registered with the SMS gateway.

Destination Domain – The DNS suffix of the sender email.

4. Click **SAVE**.

To validate SMTP mail server settings:

1. Click **Test Email** to send a test email. Verify that you receive the test mail at the email address defined in your administrator user account.
2. If you changed the SMTP settings, restart the portal servers in order for the changes to take effect.

Chapter 13. Managing Team Portals

The HCP Anywhere Enterprise Portal can be divided into tenants, known as virtual portals, each of which manages a subset of devices and HCP Anywhere Enterprise Portal user accounts.

A Team portal is designed for the needs of a company or team with multiple members, and as such does not include support for reseller-oriented features. The users in the portal are the team members.

Team portals are managed by team administrators, who are team members with the Administrator role.

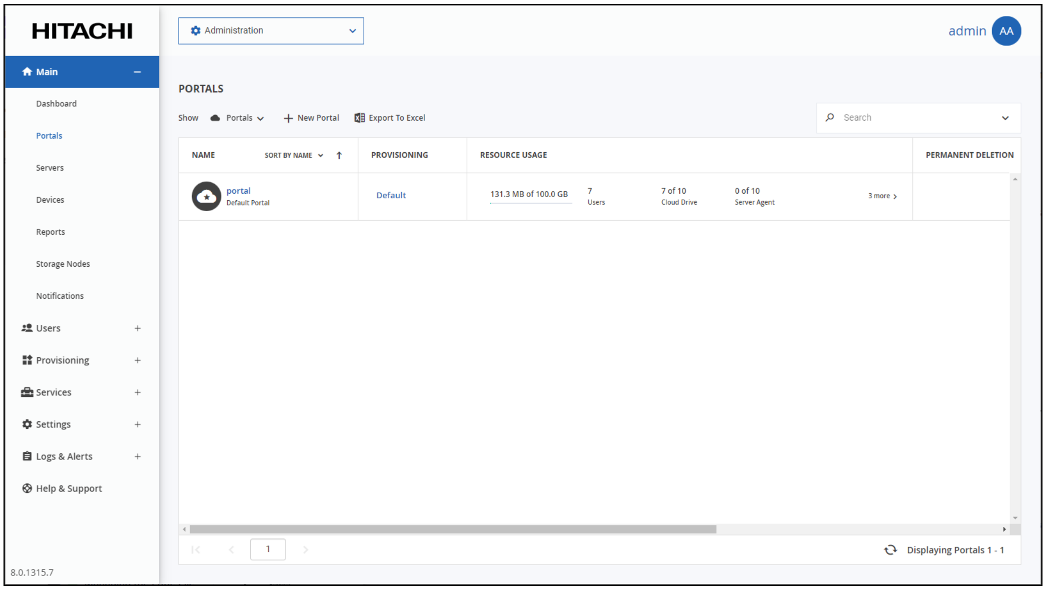
This chapter explains how to add, edit, and delete virtual portals, as well as log in to any virtual portal and manage its contents.

In this chapter

Viewing Virtual Portals

To view all virtual portals

- In the global administration view, select **Main > Portals** in the navigation pane.
  The **PORTALS** page opens, displaying all the virtual portals.



NAME	PROVISIONING	RESOURCE USAGE					PERMANENT DELETION
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 of 10 Cloud Drive	0 of 10 Server Agent	3 more ›	

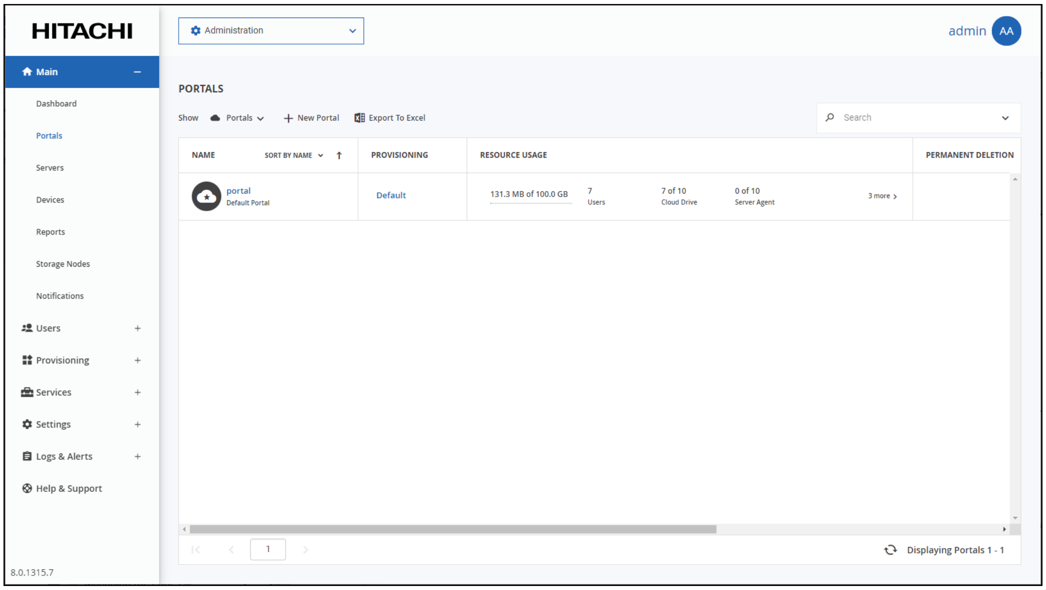
Team portals are indicated by the ▦ icon. The default portal is indicated by the ☁ icon.
The page includes the following columns:

Field	Description
NAME	The virtual portal name. To edit the virtual portal, click the name. For further details, see Adding, Editing, Deleting and Undeleting a Virtual Portal. If the portal is disabled, `Disabled` is displayed below the name.
PROVISIONING	The global plan to which this portal is assigned. To modify the plan, click the plan's name. For further details, see Adding or Editing a Subscription Plan. If the portal is assigned any add-ons, the 🧩 icon is displayed with the number of add-ons. To modify the list of add-ons, click on the number. For further details, see Adding, Editing, or Deleting Add-ons.
RESOURCE USAGE	The amount of storage currently in use by the virtual portal, out of the total provisioned amount. The number of devices: HCP Anywhere Enterprise Edge Filer (EV) licenses and HCP Anywhere Enterprise Drive Share (Agent) licenses, and Cloud Drive licenses in use by the portal, out of the total provisioned number is displayed.
BILLING ID	The virtual portal owner's billing ID.

Adding, Editing, Deleting and Undeleting a Virtual Portal

To add or edit a virtual portal:

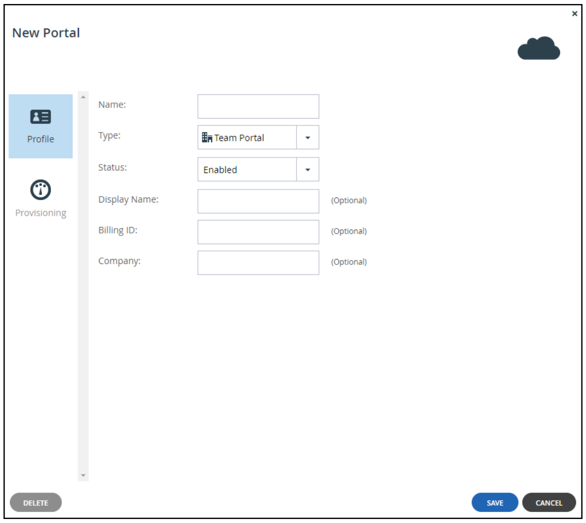
1. In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual portals.



NAME SORT BY NAME	PROVISIONING	RESOURCE USAGE					PERMANENT DELETION
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 of 10 Cloud Drive	0 of 10 Server Agent	3 more	

2. Either,

- Add a new virtual portal, click **New Portal**.
The **New Portal** window is displayed.



Name:		
Type:	Team Portal	
Status:	Enabled	
Display Name:		(Optional)
Billing ID:		(Optional)
Company:		(Optional)

Or,

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

3. Complete the fields.

Name – Type a unique name for the virtual portal.

Type – Select **Team Portal** (the default). This field is read-only, when editing an existing virtual portal.

Status – The status: either **Enabled** or **Disabled**. If you set the status to disabled:

- Users cannot log in to the portal, and devices cannot connect.
- Reports and email notifications are not sent from the portal.
- User self-registration is disabled.

Global administrators can still connect to disabled portals via the *global administration view*.

Display Name – Optional. The name displayed.

Billing ID – Optional. The virtual portal owner's billing ID. This enables integration of the portal with an external billing system.

Note: The Billing ID must be unique so that only this virtual portal is associated with it.

Company – Optional. The name of the company owning the portal.

Enable Resource Provisioning (Reseller portal only) – Deselect this box to allow a reseller unlimited quotas, subject only to the limits of the HCP Anywhere Enterprise Portal license. If you deselect the box, the **Provisioning** option is removed.

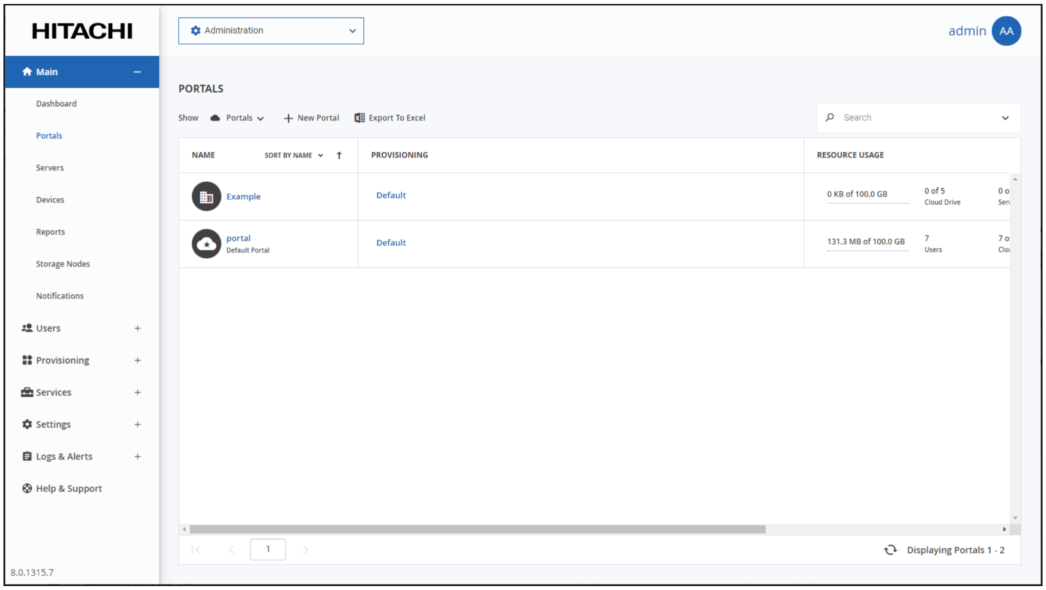
4. Assign a plan, as described in Assigning Global Plans to Team Portals.
5. Add global add-ons, as described in Assigning Add-ons to Team Portals.
6. Click **SAVE**.

Deleting and Undeleting Virtual Portals

Note: When a virtual portal is deleted, it is retained for the number of days specified in the **Retain deleted portals for** field in the global settings, where the retention period is defined. For details refer to Configuring Global Settings.
All the portal content and configuration is retained during this time and any unique values associated with the portal cannot be used for another portal. At the end of the retention period, the portal content is permanently deleted and unique values that were associated with the portal can be used for another portal. During the retention period the portal can be restored, as described in the procedure **To restore a deleted portal**, below.

To delete a virtual portal:

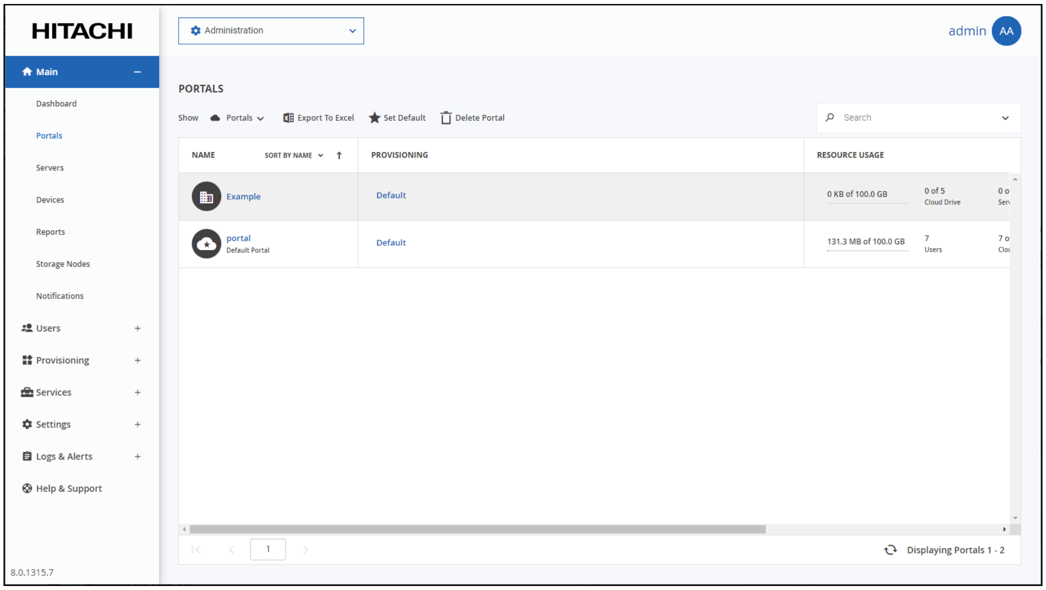
1. In the global administration view, select **Main > Portals** in the navigation pane.
The **PORTALS** page opens, displaying all the virtual portals.



PORTALS

NAME	PROVISIONING	RESOURCE USAGE		
Example	Default	0 KB of 100.0 GB	0 of 5 Cloud Drive	0 o Serv
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 o Clou

2. Select the row of the portal to delete and click **Delete Portal**.



NAME	PROVISIONING	RESOURCE USAGE		
Example	Default	0 KB of 100.0 GB	0 of 5 Cloud Drive	0 o Ser
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 o Clou

A confirmation window is displayed.

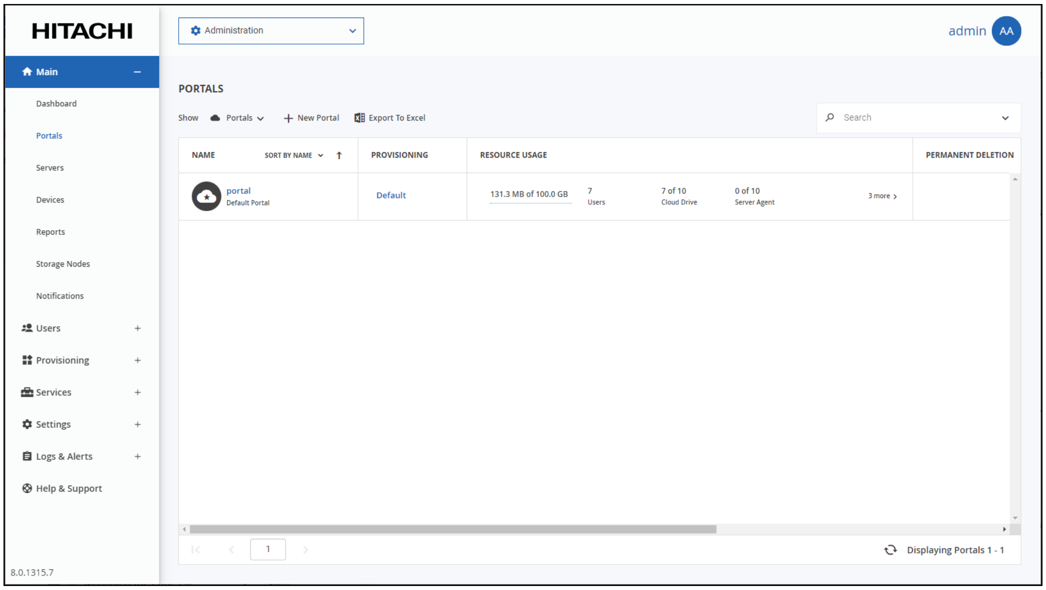
3. Click **DELETE**.

The portal is deleted.

To restore a deleted portal:

Note: A deleted portal can be restored after it is deleted for the number of days specified in the **Retain deleted portals for** field in the global settings, where th**e** retention period is defined. For details refer to Configuring Global Settings**.**

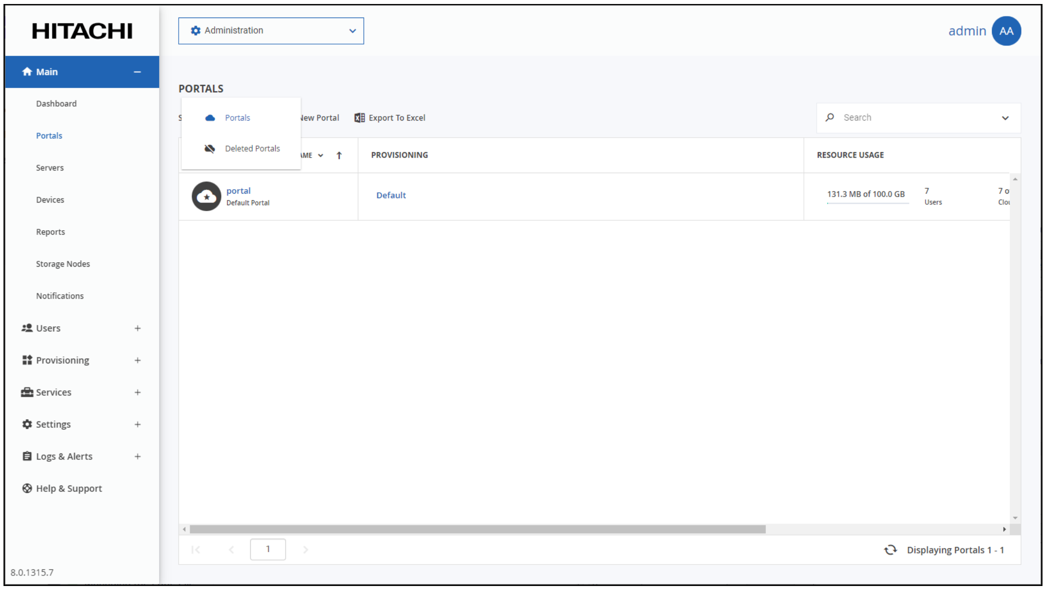
1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.



NAME	PROVISIONING	RESOURCE USAGE					PERMANENT DELETION
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 of 10 Cloud Drive	0 of 10 Server Agent	3 more ›	

2. Change the view to display the deleted portals by clicking **Show Portals** and selecting **Deleted**

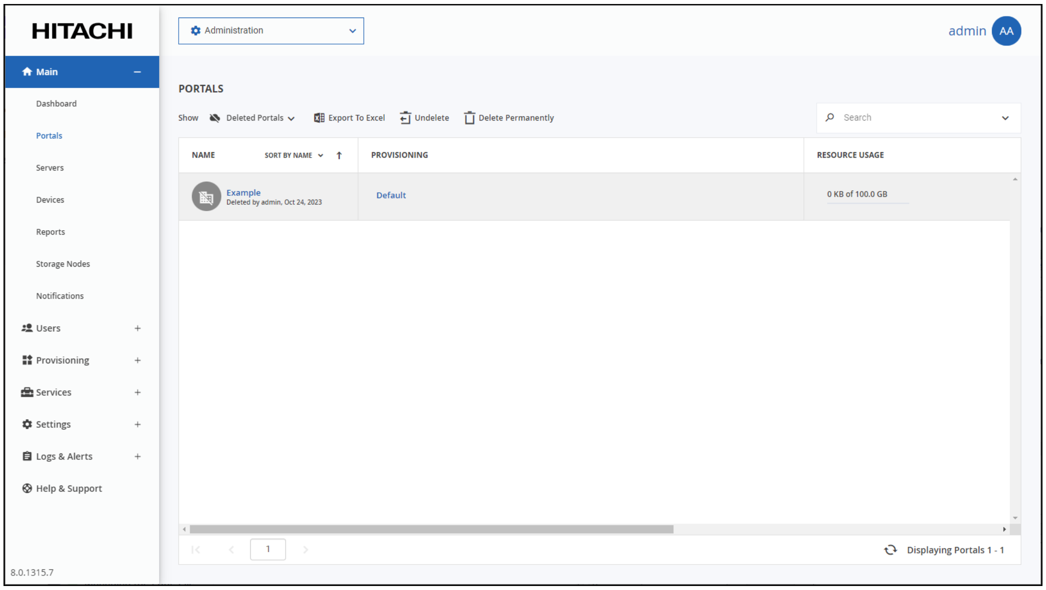
Portals.



The view changes to display deleted portals.

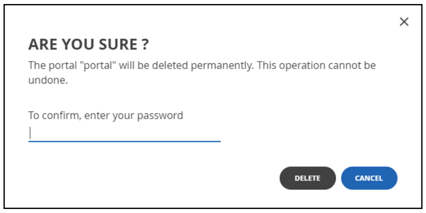
Note: Deleted portals in this list do not use any licenses or consume storage from storage quotas.

3. Select the row of the portal to recover and click **Undelete**.



The portal and portal content is restored.

Note: You can export the list of deleted portals with information such as the storage used by the portal, when it was deleted and licenses for the portal, by clicking **Export to Excel**. You can click **Delete Permanently** to immediately delete the portal and all the content. In this case, you are prompted to confirm that you want to permanently delete the portal by entering you administrator password.



ARE YOU SURE ?

The portal "portal" will be deleted permanently. This operation cannot be undone.

To confirm, enter your password

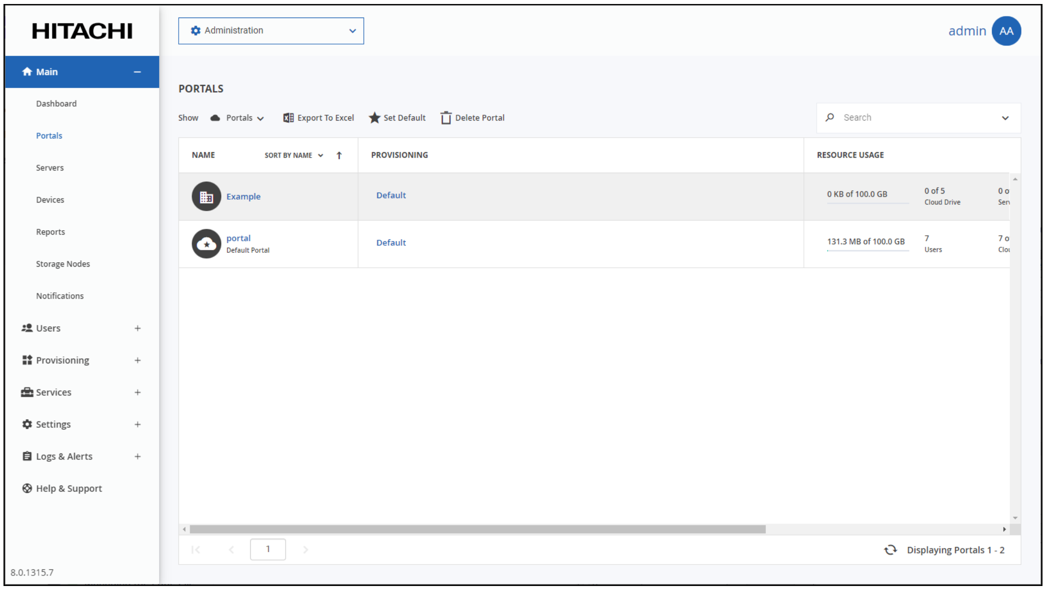
The audit log includes an entry for a portal that is deleted, undeleted or permanently deleted.

Setting the Default Virtual Portal

The default portal is is the portal that is displayed when end users or team or staff administrators access the portal using the portal IP address or DNS name.

To set a portal as the default:

1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.



NAME	PROVISIONING	RESOURCE USAGE		
Example	Default	0 KB of 100.0 GB	0 of 5 Cloud Drive	0 o Serv
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 o Clou

2. Select the row of the portal to make default and click **Set Default**.

The selected portal becomes the default portal.is displayed under the portal name and the portal icon changes to .

To remove a portal from being the default:

1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.
2. Select the default portal's row and click **Remove Default**.

The portal is no longer the default.

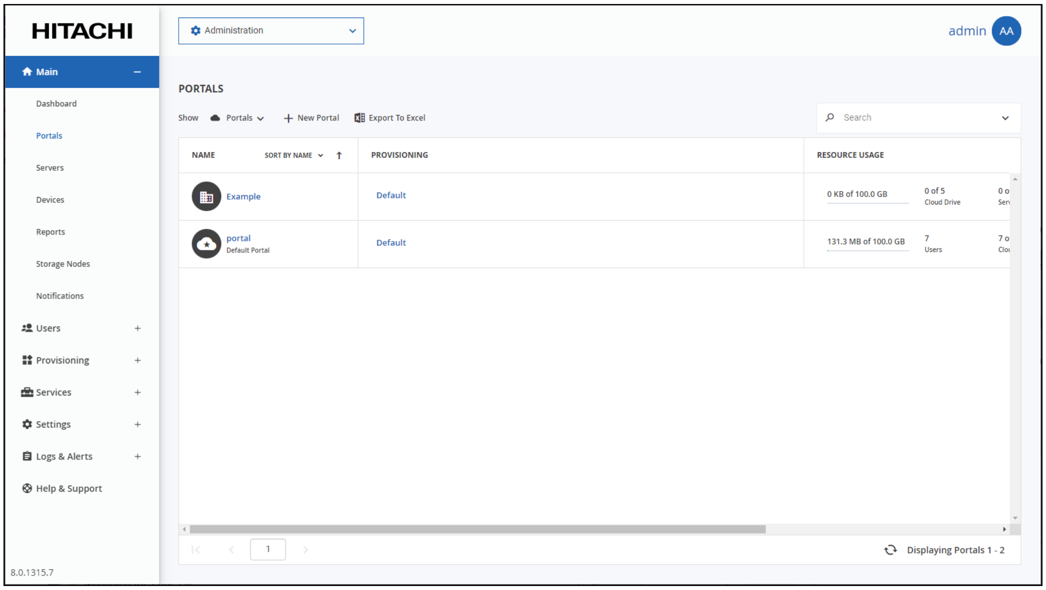
Provisioning the Team Portal: Global Plans and Add- ons

Assigning Global Plans to Team Portals

A global plan can be added to a team portal for every user in the team portal. Plans can be assigned to individual users in the team portal.

To assign a global plan to a virtual portal:

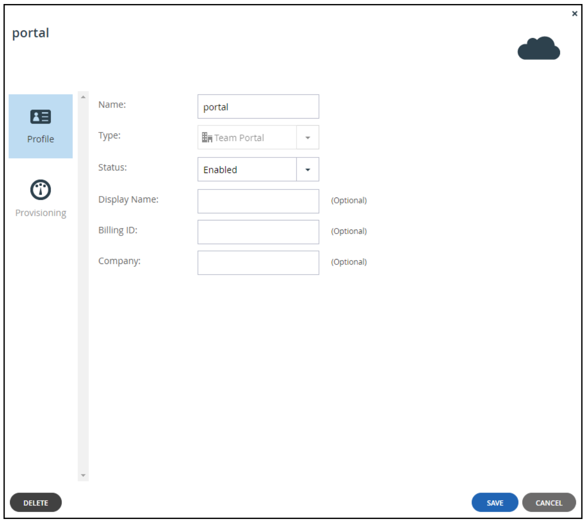
1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.



PORTALS

NAME	PROVISIONING	RESOURCE USAGE		
Example	Default	0 KB of 100.0 GB	0 of 5 Cloud Drive	0 o Serv
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 o Clo

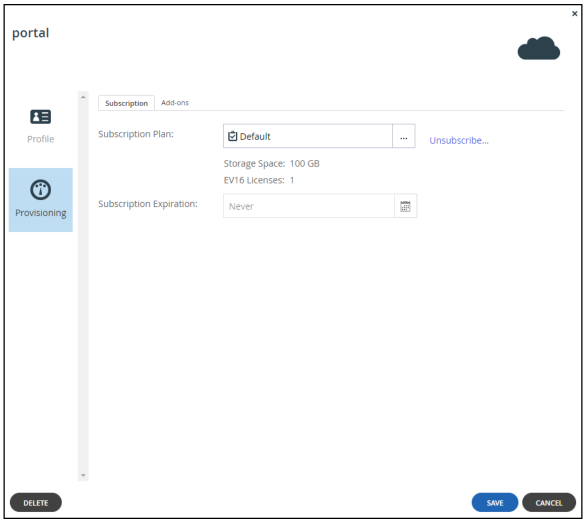
2. Click the portal name.



portal

Name:	portal	
Type:	Team Portal	
Status:	Enabled	
Display Name:		(Optional)
Billing ID:		(Optional)
Company:		(Optional)

3. Click the **Provisioning** option.
   The **Provisioning** window is displayed.



Subscription Plan: Default

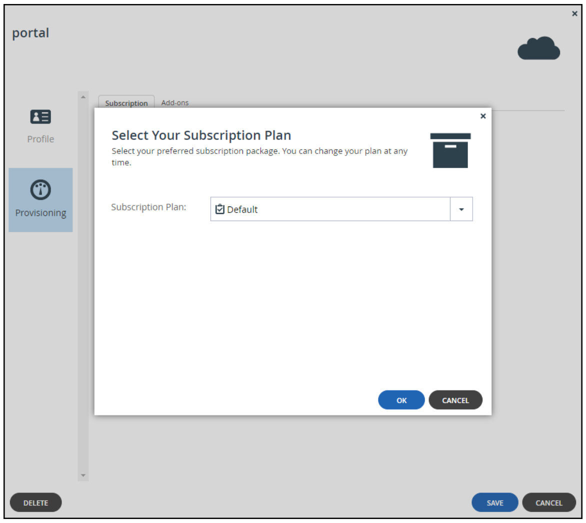
Storage Space: 100 GB

EV16 Licenses: 1

Subscription Expiration: Never

4. Click the **Subscription Plan** field.

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



Select Your Subscription Plan

Select your preferred subscription package. You can change your plan at any time.

Subscription Plan: Default

5. In the **Subscription Plan** drop-down list, select the global plan to assign the portal.
6. Click **OK**.
7. In the **Subscription Expiration** field, click 📅 to specify the date on which the portal's subscription to the selected plan will expire. This field is only enabled for plans that are defined as time limited trial plan.
8. Click **SAVE**.

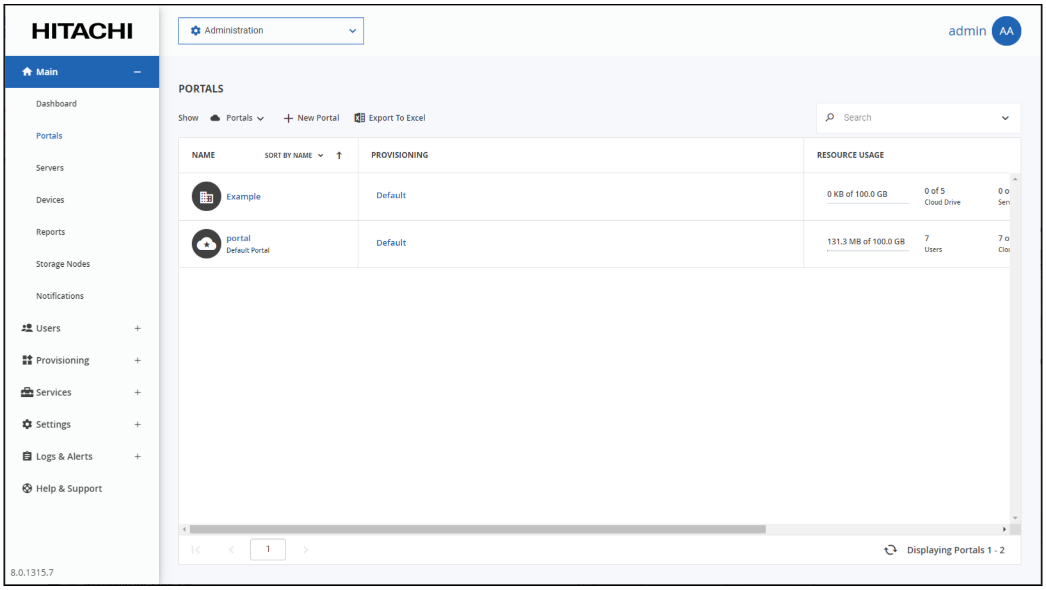
The team portal is assigned to the subscription plan.

Assigning Add-ons to Team Portals

An add-on can be added to a team portal as part of the provisioning for the team portal and the add-on is valid for every user in the team portal.

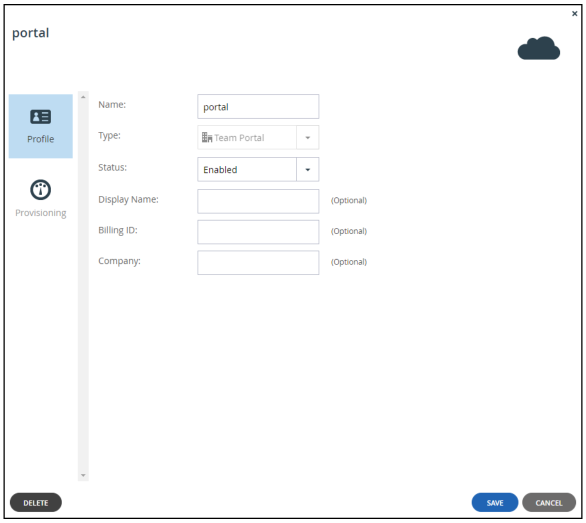
To assign global add-ons to a virtual portal:

1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.



NAME	PROVISIONING	RESOURCE USAGE		
Example	Default	0 KB of 100.0 GB	0 of 5 Cloud Drive	0 o Serv
portal Default Portal	Default	131.3 MB of 100.0 GB	7 Users	7 o Clo

2. Click the portal name.



Name: portal

Type: Team Portal

Status: Enabled

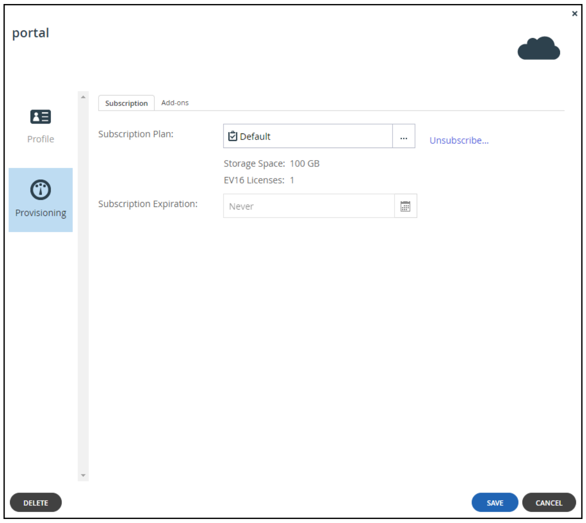
Display Name: (Optional)

Billing ID: (Optional)

Company: (Optional)

3. Click the **Provisioning** option.

   The **Provisioning** window is displayed.



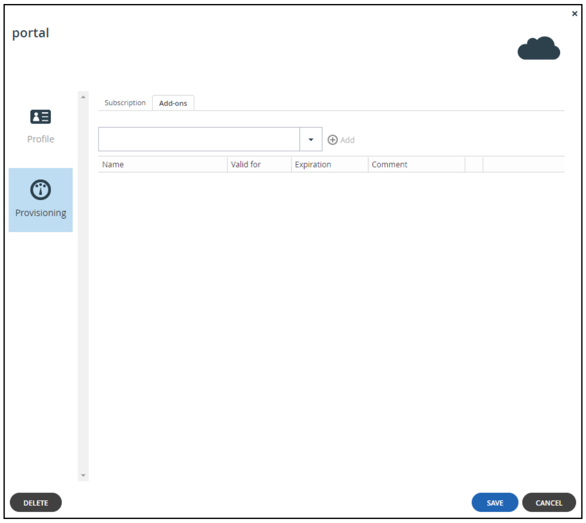
Subscription Plan: Default ... Unsubscribe...

Storage Space: 100 GB

EV16 Licenses: 1

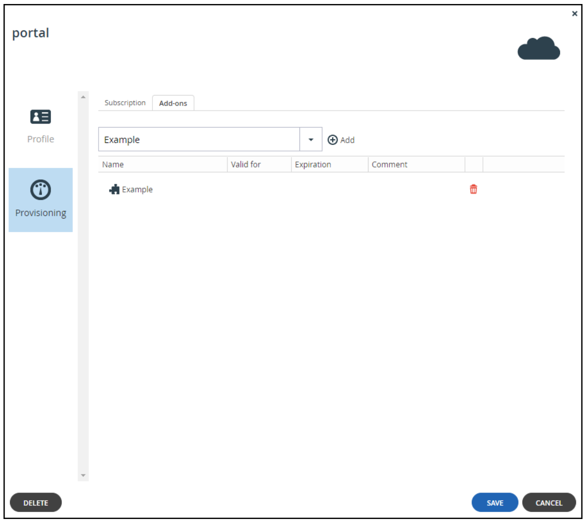
Subscription Expiration: Never

4. Select the **Add-ons** tab.

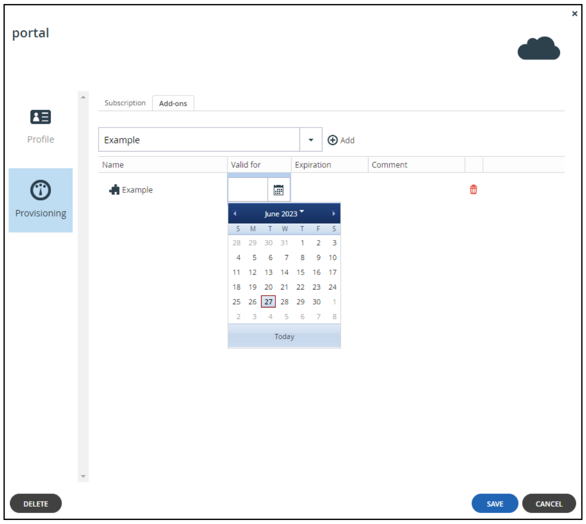


Name	Valid for	Expiration	Comment

5. Add an add-on for the team portal.
   a) In the drop-down list, select the add-on.
   b) Click **Add**.
   The add-on is displayed.



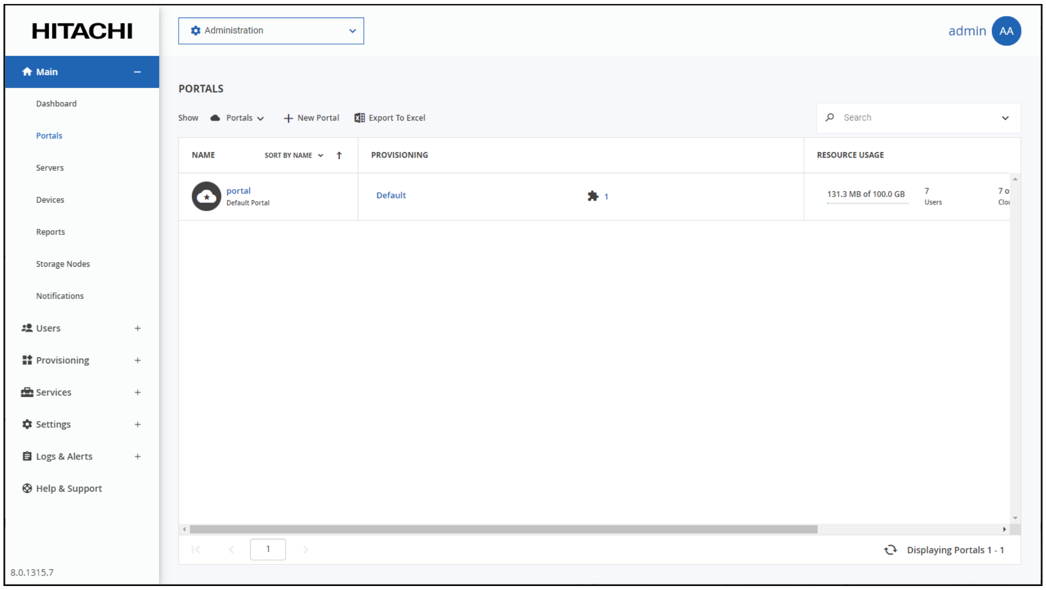
c) To select a new date until when the add-on is valid, in the add-on row, click in the **Valid for** column and then either clear the value, type a new value or click 📅 to display a calendar to select a new date when the add-on subscription should end.
The **Expiration** column is updated accordingly.



d) Optionally, enter a comment in the **Comment** column.

6. To remove an add-on from the team portal, in the add-on row in the list box, click 🗑.
   The add-on is removed.
7. Click **SAVE**.

The add-on, identified by the 🧩 icon, is assigned to the virtual portal.

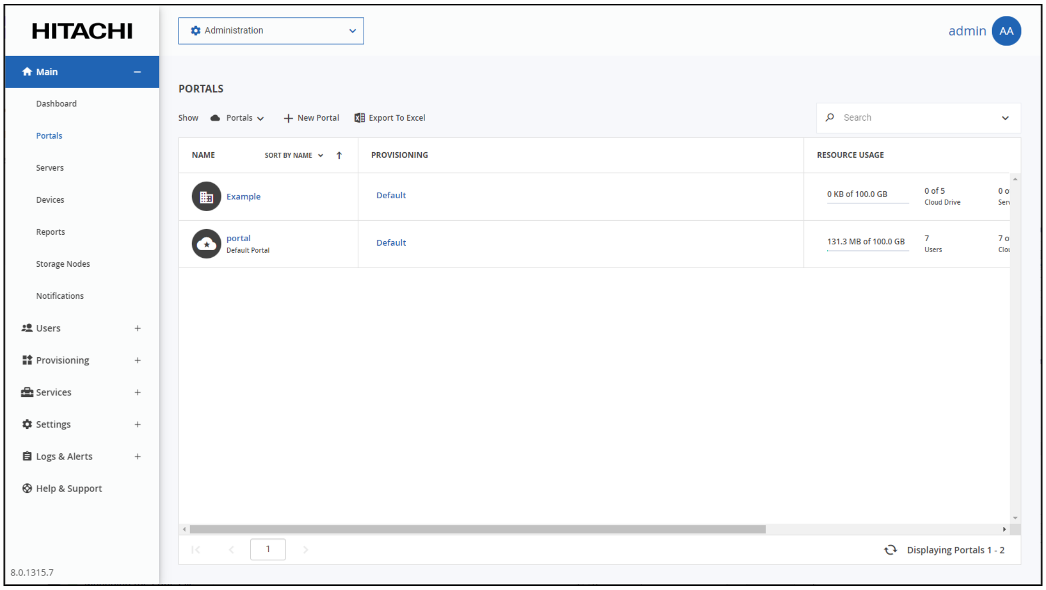


Exporting Virtual Portal Details to Excel

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

To export virtual portals to Excel:

1. In the global administration view, select **Main > Portals** in the navigation pane.
   The **PORTALS** page opens, displaying all the virtual portals.



2. Click **Export to Excel**.

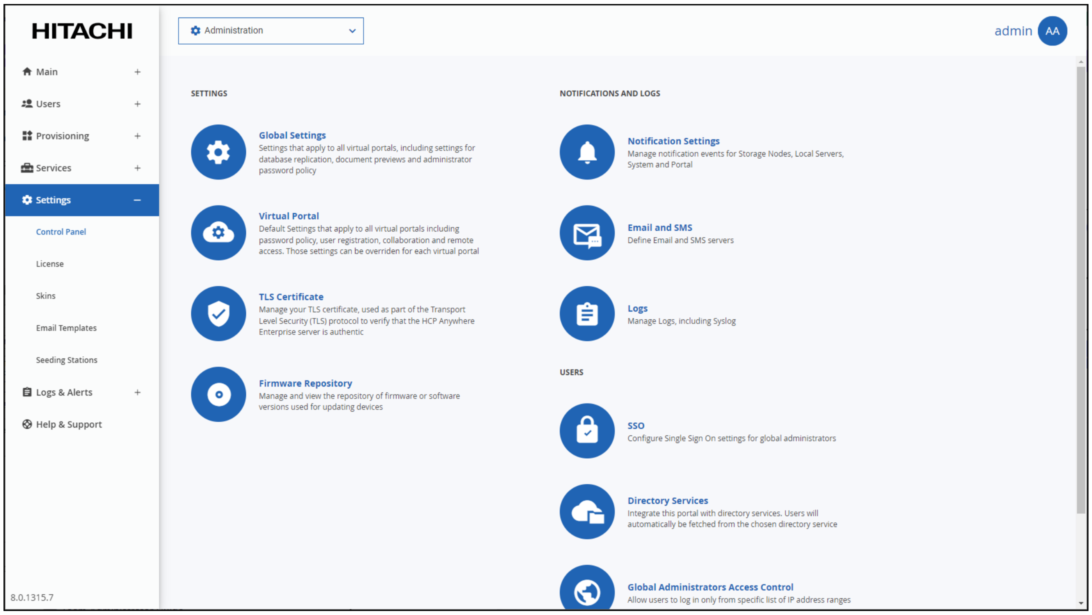
The list of team portals with their details exported to your computer. The details include the provisioned plan, user and storage quotas and actual usage and storage, for example the cloud drive quota and actual number used.

Configuring Team Portal Settings

Team portal settings are default settings that apply to all team portals. Default settings can be overridden for each team portal from that team portal's administration interface.

To set virtual portal settings:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

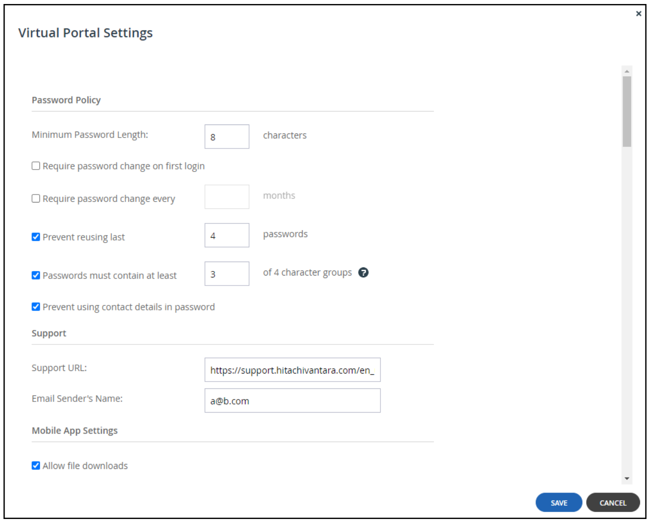
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Virtual Portal**, under **SETTINGS** in the **Control Panel** page.
   The **Virtual Portal Settings** window is displayed.



Virtual Portal Settings

Password Policy

Minimum Password Length: 8 characters

□ Require password change on first login

□ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Support

Support URL: https://support.hitachivantara.com/en_

Email Sender's Name: a@b.com

Mobile App Settings

☑ Allow file downloads

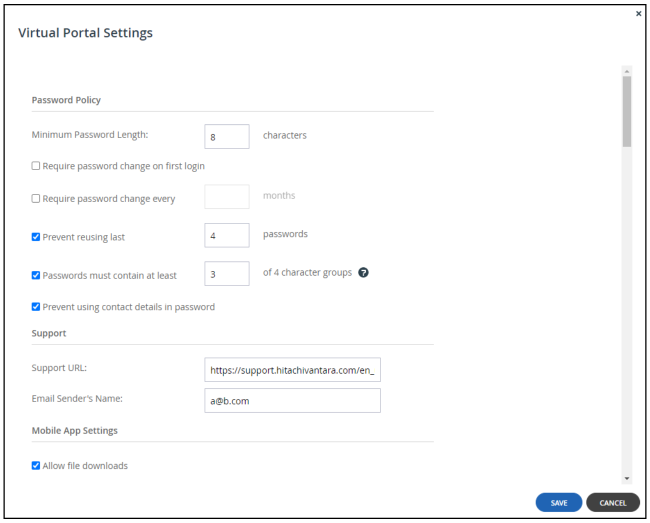
3. Change settings as required, as described below.
    - Password Policy
    - Support Settings
    - Mobile App Settings
    - General Settings
    - User Registration Settings
    - Reseller Portal Settings
    - Team Portal Settings
    - Default Settings for New Folder Groups
    - Default Settings for New User
    - Cloud Drive Settings
    - Public Links
    - Collaboration
    - External Collaboration
    - Office 365 Integration
    - Preview Only Mode
    - Remote Access Settings
    - Advanced
4. 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.



Virtual Portal Settings

Password Policy

Minimum Password Length: 8 characters

☐ Require password change on first login

☐ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Support

Support URL: https://support.hitachivantara.com/en_

Email Sender's Name: a@b.com

Mobile App Settings

☑ Allow file downloads

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

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.

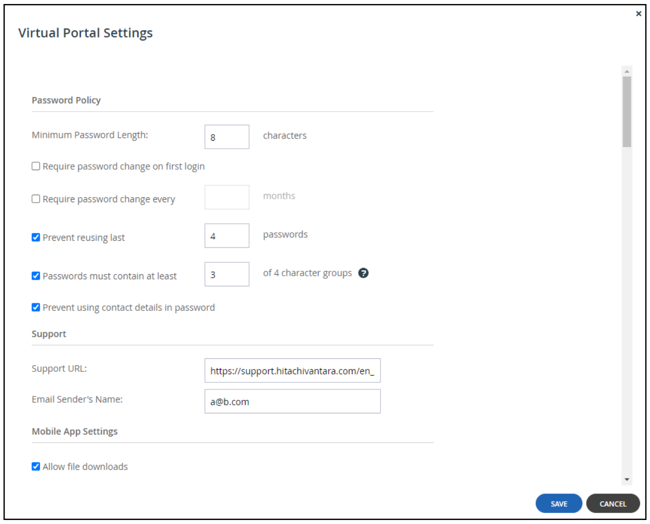
Prevent reusing last... passwords – Prevent users from reusing a specified number of their previous passwords when they change their password. Specify the number of previous passwords you want this to apply to.

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



Virtual Portal Settings

Password Policy

Minimum Password Length: 8 characters

☐ Require password change on first login

☐ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Support

Support URL: https://support.hitachivantara.com/en_

Email Sender's Name: a@b.com

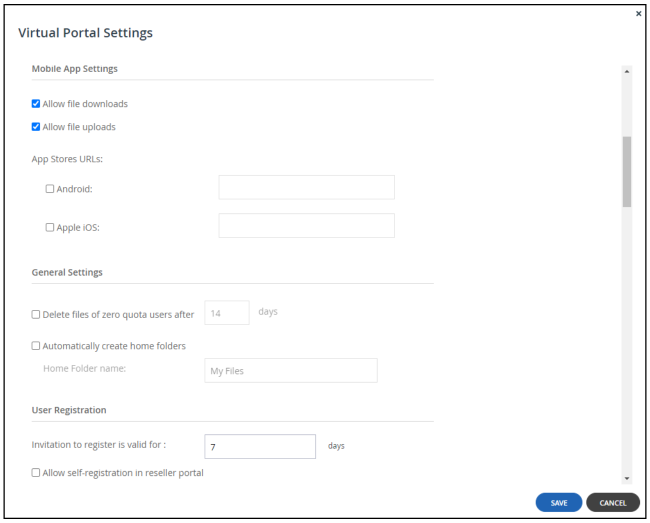
Mobile App Settings

☑ Allow file downloads

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 portal.

Mobile App Settings



Virtual Portal Settings

Mobile App Settings

☑ Allow file downloads

☑ Allow file uploads

App Stores URLs:

☐ Android:

☐ Apple iOS:

General Settings

☐ Delete files of zero quota users after 14 days

☐ Automatically create home folders

Home Folder name: My Files

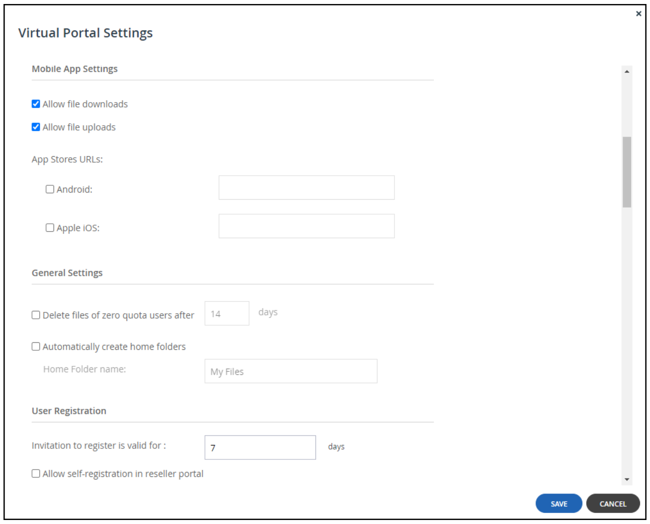
User Registration

Invitation to register is valid for : 7 days

☐ Allow self-registration in reseller portal

This feature is currently not supported.

General Settings



Virtual Portal Settings

Mobile App Settings

☑ Allow file downloads

☑ Allow file uploads

App Stores URLs:

□ Android:

□ Apple iOS:

General Settings

□ Delete files of zero quota users after 14 days

□ Automatically create home folders

Home Folder name: My Files

User Registration

Invitation to register is valid for : 7 days

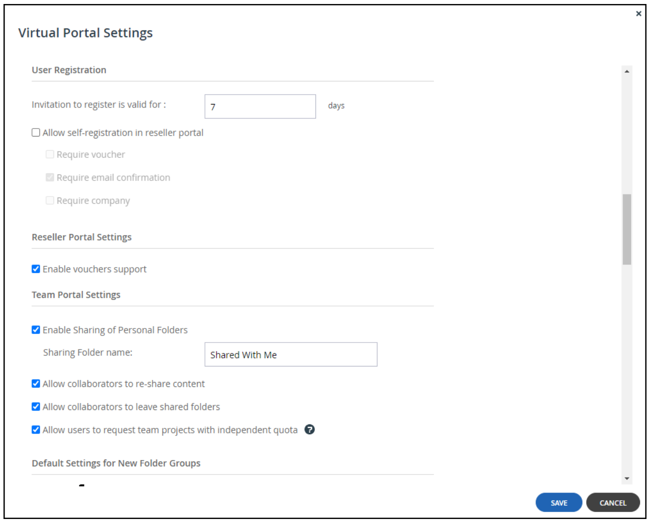
□ Allow self-registration in reseller portal

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



Virtual Portal Settings

User Registration

Invitation to register is valid for : 7 days

□ Allow self-registration in reseller portal

□ Require voucher

☑ Require email confirmation

□ Require company

Reseller Portal Settings

☑ Enable vouchers support

Team Portal Settings

☑ Enable Sharing of Personal Folders

Sharing Folder name: Shared With Me

☑ Allow collaborators to re-share content

☑ Allow collaborators to leave shared folders

☑ Allow users to request team projects with independent quota

Default Settings for New Folder Groups

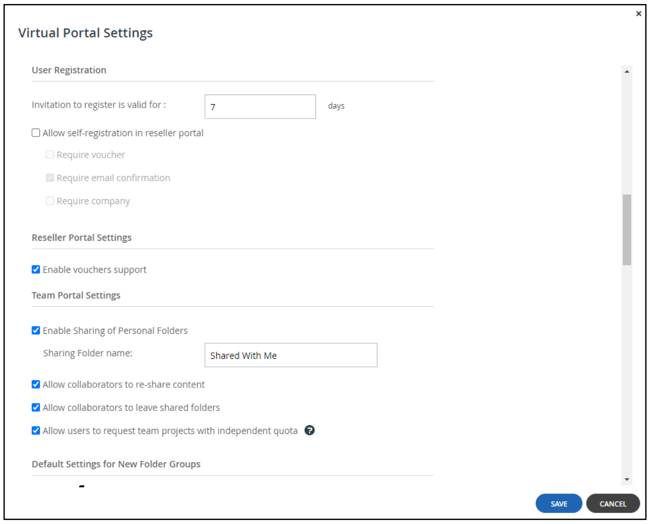
Invitation to register is valid for:... days – The validity period, in days, for registration invitations sent to users by team portal administrators. If a user has not registered for the service after the number of days specified in this field, the invitation expires.

Allow self-registration in reseller portal – This feature is currently not supported.

Reseller Portal Settings

This feature is currently not supported.

Team Portal Settings



Virtual Portal Settings

User Registration

Invitation to register is valid for : 7 days

□ Allow self-registration in reseller portal

□ Require voucher

☑ Require email confirmation

□ Require company

Reseller Portal Settings

☑ Enable vouchers support

Team Portal Settings

☑ Enable Sharing of Personal Folders

Sharing Folder name: Shared With Me

☑ Allow collaborators to re-share content

☑ Allow collaborators to leave shared folders

☑ Allow users to request team projects with independent quota

Default Settings for New Folder Groups

Enable Sharing of Personal Folders – Enable team portal members to share personal folders with other team portal members.

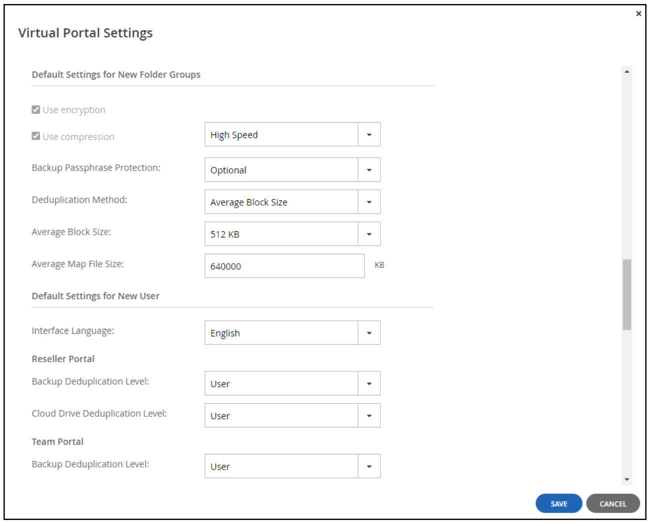
> **Sharing Folder name** – The name of the folder in each user's cloud drive folder hierarchy in which other users' personal folders that were shared with the user are displayed.

Allow collaborators to re-share content – Enable team portal 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 team portal 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 team portal members to request a team project, so that storage for the project does not use personal storage.

Default Settings for New Folder Groups


Virtual Portal Settings

Default Settings for New Folder Groups

☑ Use encryption

☑ Use compression: High Speed

Backup Passphrase Protection: Optional

Deduplication Method: Average Block Size

Average Block Size: 512 KB

Average Map File Size: 640000 KB

Default Settings for New User

Interface Language: English

Reseller Portal

Backup Deduplication Level: User

Cloud Drive Deduplication Level: User

Team Portal

Backup Deduplication Level: User

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.

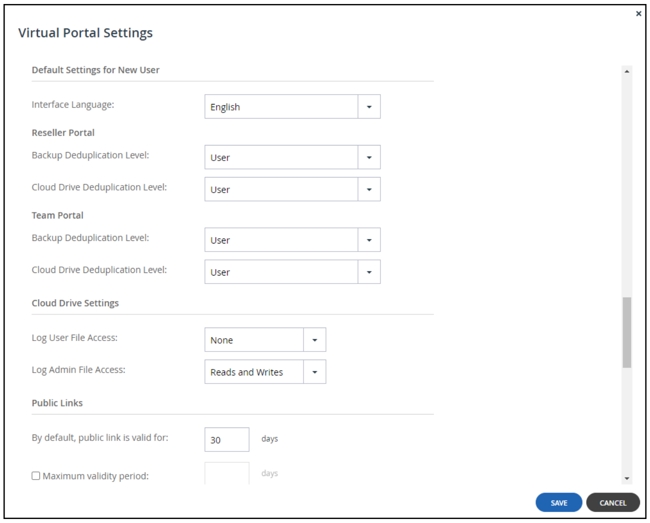
Backup Passphrase Protection – This feature is currently not supported.

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: **Average Block Size** or **Fixed Block Size**. Use **Fixed Block Size** if many of the folder groups include large files where deduplication is not common, such as media files. Hitachi Vantara also recommends using Fixed Block Size if direct mode is defined for the storage node, which enables files to be transferred to and from the HCP Anywhere Enterprise Edge Filer or HCP Anywhere Enterprise Drive Share (Agent) direct to storage, bypassing the portal. For details, refer to Adding and Editing Storage Nodes.

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. 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 portal can better identify finer-grained duplicate data. If direct mode is defined 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.

Default Settings for New User



Virtual Portal Settings

Default Settings for New User

Interface Language: English

Reseller Portal

Backup Deduplication Level: User

Cloud Drive Deduplication Level: User

Team Portal

Backup Deduplication Level: User

Cloud Drive Deduplication Level: User

Cloud Drive Settings

Log User File Access: None

Log Admin File Access: Reads and Writes

Public Links

By default, public link is valid for: 30 days

□ Maximum validity period: days

Interface Language – The default language for new users. This language can be overridden by end users in the End User Portal.

Reseller Portal

This feature is currently not supported.

Team Portal

Backup Deduplication Level – This feature is currently not supported.

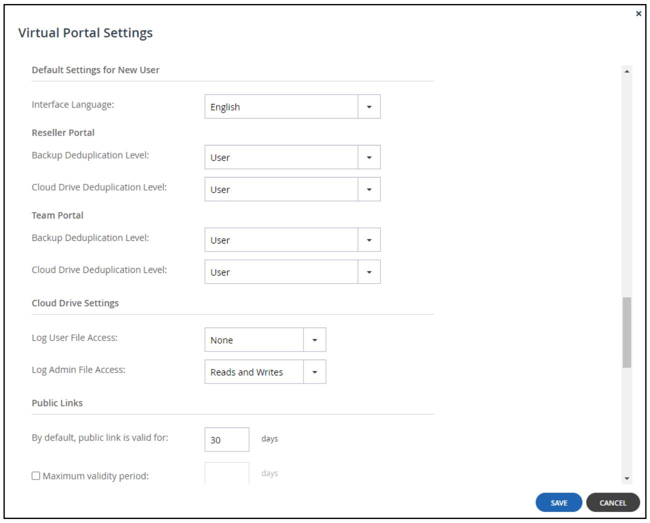
Cloud Drive Deduplication Level – The default deduplication level to use for cloud folders, for all new users in team portals. Deduplication is performed on the device before the data is uploaded to the portal:

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 portal, containing all of the cloud folders in the team 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



Virtual Portal Settings

Default Settings for New User

Interface Language: English

Reseller Portal

Backup Deduplication Level: User

Cloud Drive Deduplication Level: User

Team Portal

Backup Deduplication Level: User

Cloud Drive Deduplication Level: User

Cloud Drive Settings

Log User File Access: None

Log Admin File Access: Reads and Writes

Public Links

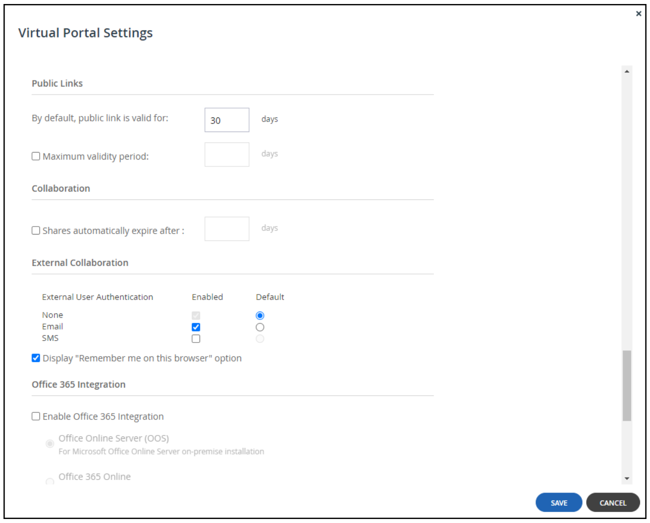
By default, public link is valid for: 30 days

□ Maximum validity period: days

Cloud Drive Logging Level – The logging level for the Cloud Drive; for user, **Log User File Access**, and admin, **Log Admin File Access**:

None
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



Virtual Portal Settings

Public Links

By default, public link is valid for: 30 days

□ Maximum validity period: days

Collaboration

□ Shares automatically expire after : days

External Collaboration

External User Authentication	Enabled	Default
None	☑	●
Email	☑	○
SMS	□	○

☑ Display "Remember me on this browser" option

Office 365 Integration

□ Enable Office 365 Integration

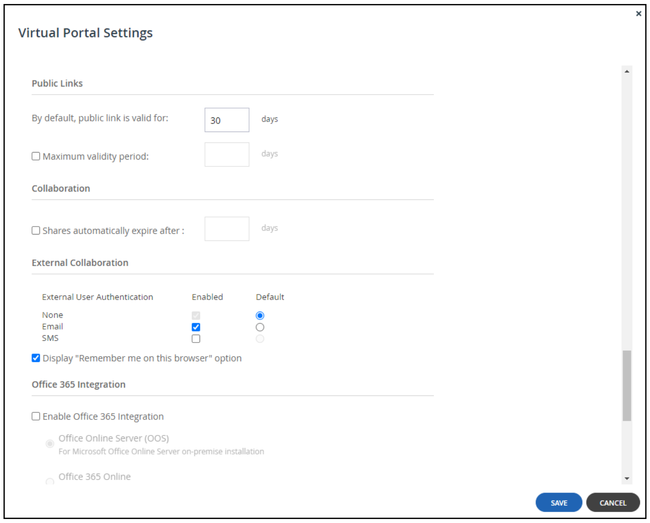
● Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online

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.

Collaboration



Virtual Portal Settings

Public Links

By default, public link is valid for: 30 days

□ Maximum validity period: days

Collaboration

□ Shares automatically expire after : days

External Collaboration

External User Authentication	Enabled	Default
None	□	●
Email	☑	○
SMS	□	○

☑ Display "Remember me on this browser" option

Office 365 Integration

□ Enable Office 365 Integration

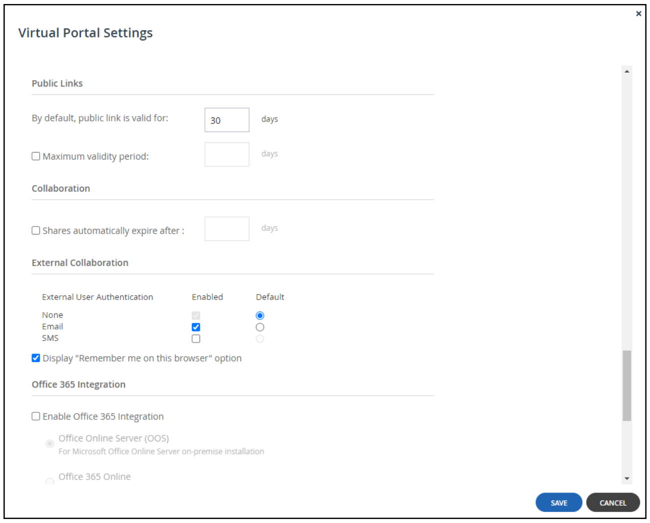
○ Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online

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



Virtual Portal Settings

Public Links

By default, public link is valid for: 30 days

□ Maximum validity period: days

Collaboration

□ Shares automatically expire after : days

External Collaboration

External User Authentication	Enabled	Default
None	□	●
Email	☑	○
SMS	□	○

☑ Display "Remember me on this browser" option

Office 365 Integration

□ Enable Office 365 Integration

○ Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online

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.

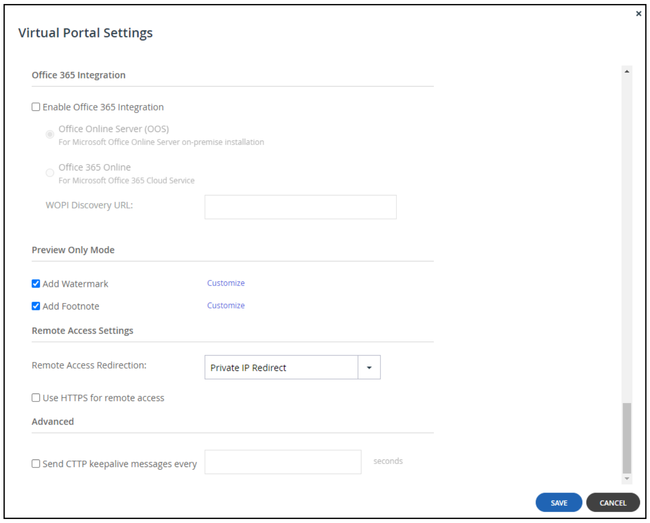
Email – The invitation recipient receives a time limited authenticated link to the file or folder. On every access, a new 6 digit passcode challenge is sent to the recipient by email. The recipient must enter the passcode before accessing the file or folder. This ensures that the invitation is not usable 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 portal Cloud Drive. The plug-in syncs attached files to the portal Cloud Dive and inserts public links to the files into the email body.

SMS – 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 text message. 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.

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



Virtual Portal Settings

Office 365 Integration

□ Enable Office 365 Integration

● Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online
For Microsoft Office 365 Cloud Service

WOPI Discovery URL:

Preview Only Mode

☑ Add Watermark — Customize

☑ Add Footnote — Customize

Remote Access Settings

Remote Access Redirection: Private IP Redirect

□ Use HTTPS for remote access

Advanced

□ Send CTTP keepalive messages every ___ seconds

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, Hitachi Vantara 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, Hitachi Vantara 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 support is enabled.
  You can verify that TLS 1.2 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 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.

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 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

portals can use the same WOPI URL.

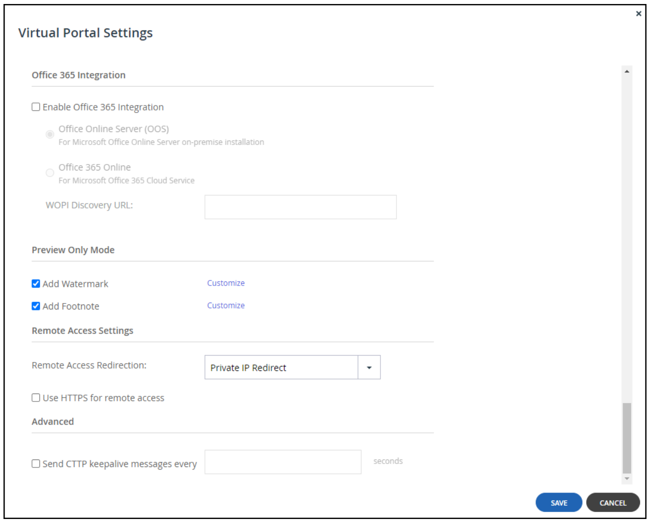
Troubleshooting

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



Virtual Portal Settings

Office 365 Integration

□ Enable Office 365 Integration

● Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online
For Microsoft Office 365 Cloud Service

WOPI Discovery URL:

Preview Only Mode

☑ Add Watermark — Customize

☑ Add Footnote — Customize

Remote Access Settings

Remote Access Redirection: Private IP Redirect

□ Use HTTPS for remote access

Advanced

□ Send CTTP keepalive messages every seconds

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

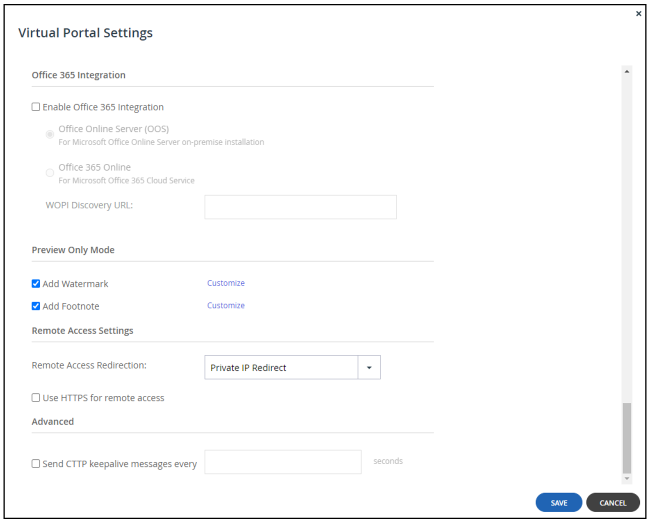
Text – The text to be displayed at the bottom of each page of a file restricted to previewing only. The following variables are supported in the text field: ${recipient}, ${date} and ${company}.

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



Virtual Portal Settings

Office 365 Integration

☐ Enable Office 365 Integration

● Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online
For Microsoft Office 365 Cloud Service

WOPI Discovery URL:

Preview Only Mode

☑ Add Watermark Customize

☑ Add Footnote Customize

Remote Access Settings

Remote Access Redirection: Private IP Redirect

☐ Use HTTPS for remote access

Advanced

☐ Send CTTP keepalive messages every seconds

Remote access must be configured **On** in the HCP Anywhere Enterprise Edge Filer in **Cloud Services > Remote Access**, in the **Configuration** view. 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 disabled
Remote access is currently not available for this device.
```

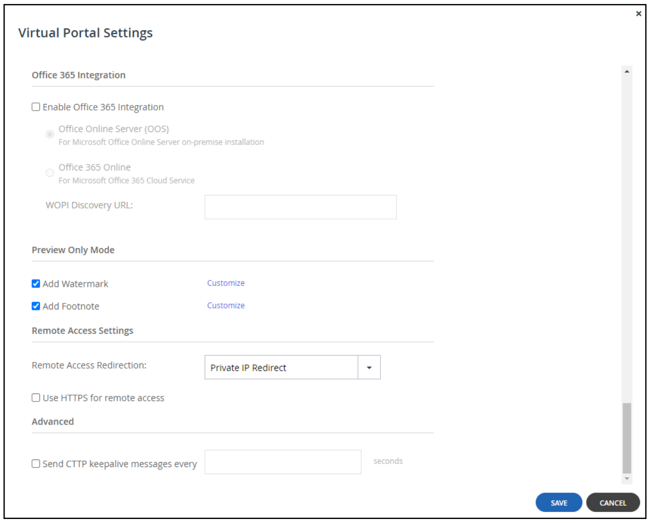
Remote Access Redirection – Whether Web clients attempting to remotely access a HCP Anywhere Enterprise Edge Filer are redirected to communicate directly with the HCP Anywhere Enterprise Edge Filer, instead of relaying communications through the HCP Anywhere Enterprise Portal:

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 EnterprisePortal.

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 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



Virtual Portal Settings

Office 365 Integration

□ Enable Office 365 Integration

● Office Online Server (OOS)
For Microsoft Office Online Server on-premise installation

○ Office 365 Online
For Microsoft Office 365 Cloud Service

WOPI Discovery URL:

Preview Only Mode

☑ Add Watermark Customize

☑ Add Footnote Customize

Remote Access Settings

Remote Access Redirection: Private IP Redirect

□ Use HTTPS for remote access

Advanced

□ Send CTTP keepalive messages every seconds

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 device 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.

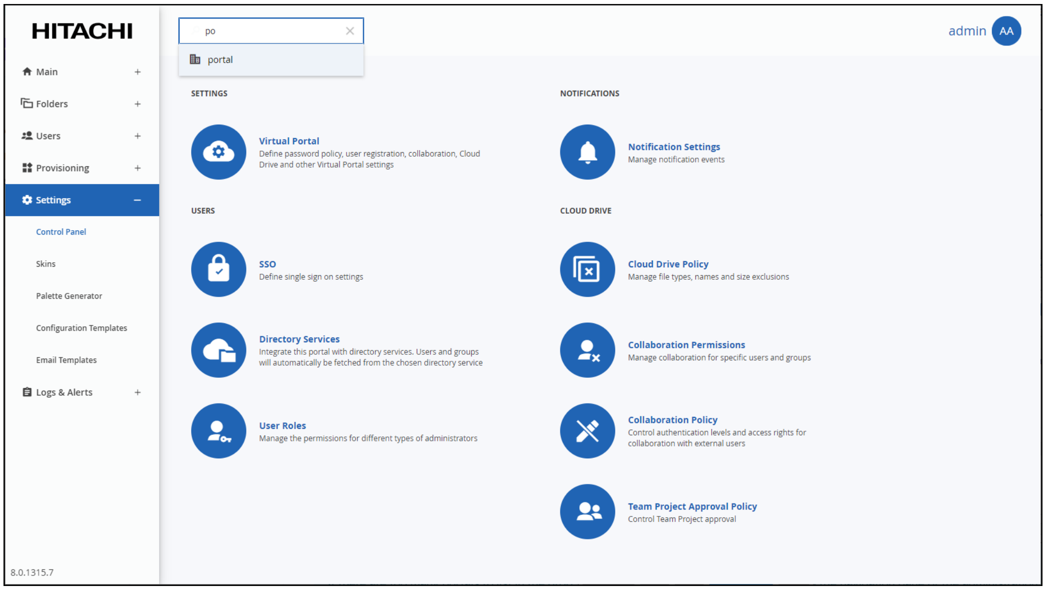
CTTP is the HCP Anywhere Enterprise Transport Protocol used between HCP Anywhere Enterprise Edge Filers and HCP Anywhere Enterprise Drive Share (Agents) and the HCP Anywhere Enterprise Portal. This protocol has been designed to be a secure, WAN optimized transport protocol.

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

Overriding Global Settings for a Specific Team Portal

To override the global virtual portal settings for a specific virtual portal:

1. Open the HCP Anywhere Enterprise Portal drop-down list in the top bar.
2. Select the virtual portal you want to manage. You can start typing the name of the portal in the drop-down to filter the names displayed in the drop-down.



SETTINGS

Virtual Portal Define password policy, user registration, collaboration, Cloud Drive and other Virtual Portal settings

USERS

SSO Define single sign on settings

Directory Services Integrate this portal with directory services. Users and groups will automatically be fetched from the chosen directory service

User Roles Manage the permissions for different types of administrators

NOTIFICATIONS

Notification Settings Manage notification events

CLOUD DRIVE

Cloud Drive Policy Manage file types, names and size exclusions

Collaboration Permissions Manage collaboration for specific users and groups

Collaboration Policy Control authentication levels and access rights for collaboration with external users

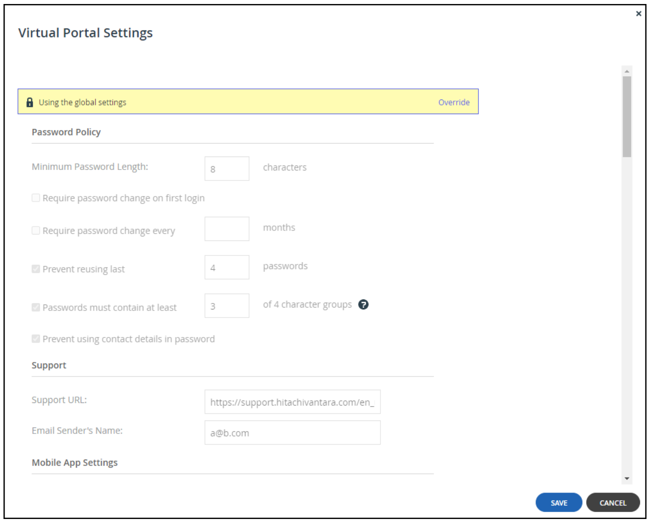
Team Project Approval Policy Control Team Project approval

Note: If there are too many portals to list in the drop-down, you can also choose **Main > Portals** in the navigation pane of the administration view and scroll to the portal you want.

Click the ↗ icon in the **NAME** column to open the administration view for the portal.

3. Select **Settings** in the navigation pane.
4. Select **Virtual Portal**, under **SETTINGS** in the **Control Panel** content page.

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



Virtual Portal Settings

Using the global settings — Override

Password Policy

Minimum Password Length: 8 characters

□ Require password change on first login

□ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

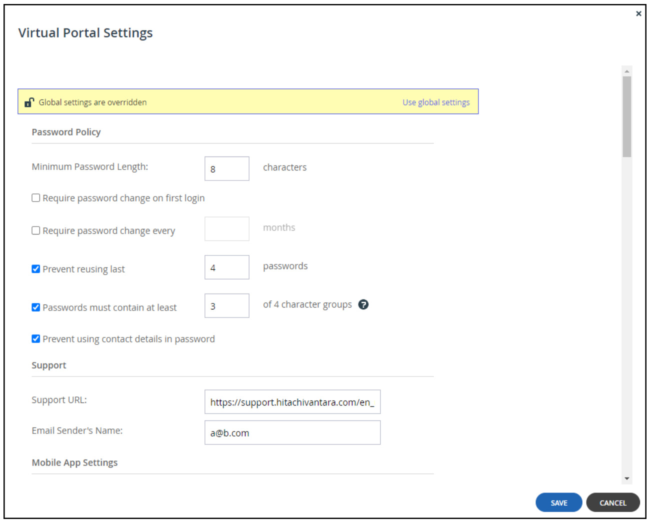
Support

Support URL: https://support.hitachivantara.com/en_

Email Sender's Name: a@b.com

Mobile App Settings

5. Click **Override** to enable changing the default settings for the virtual portal.


Virtual Portal Settings

Global settings are overridden — Use global settings

Password Policy

Minimum Password Length: 8 characters

☐ Require password change on first login

☐ Require password change every months

☑ Prevent reusing last 4 passwords

☑ Passwords must contain at least 3 of 4 character groups

☑ Prevent using contact details in password

Support

Support URL: https://support.hitachivantara.com/en_

Email Sender's Name: a@b.com

Mobile App Settings

Note: To revert to global settings, click **Use global settings**.

6. Make the required specific changes to the portal's settings.
7. Click **SAVE**.

Customizing the Portal Look and Feel

If you want to change the portal look and feel you can do the following:

- Change the color scheme for an individual team or reseller portal.
- Customize the portal skin by changing objects in the default skin. Customizing a skin should only be performed with Hitachi Vantara support. After a skin has been customized you can upload it to the portal and set it as the default skin.

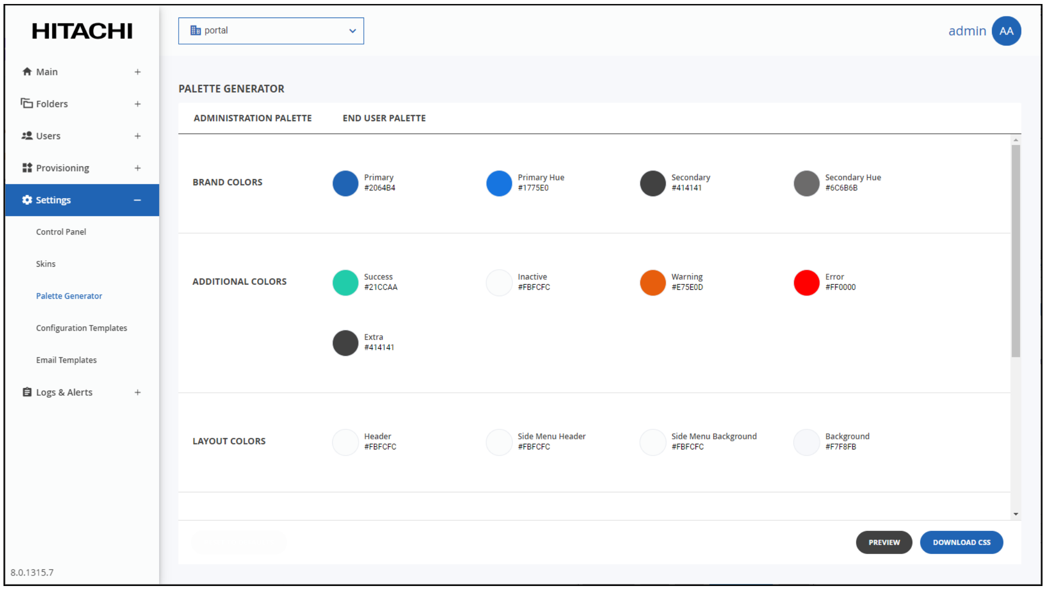
Managing the Portal Colors

You can define the portal colors for both the administration and end user views for a specific team or reseller portal in the view for that portal. You can change the color scheme for both the portal administrator view and end user view.

Note: You cannot define the portal colors for a virtual portal in the virtual portal administration.

To define the portal color scheme:

1. For a specific virtual portal, in the view for that team portal, select **Settings > Palette Generator** in the navigation pane.
The **Palette Generator** page is displayed.



BRAND COLORS
Primary #2064B4
Primary Hue #1775E0
Secondary #414141
Secondary Hue #6C6B6B

ADDITIONAL COLORS
Success #21CCAA
Inactive #FBFCFC
Warning #E75E0D
Error #FF0000
Extra #414141

LAYOUT COLORS
Header #FBFCFC
Side Menu Header #FBFCFC
Side Menu Background #FBFCFC
Background #F7F8FB

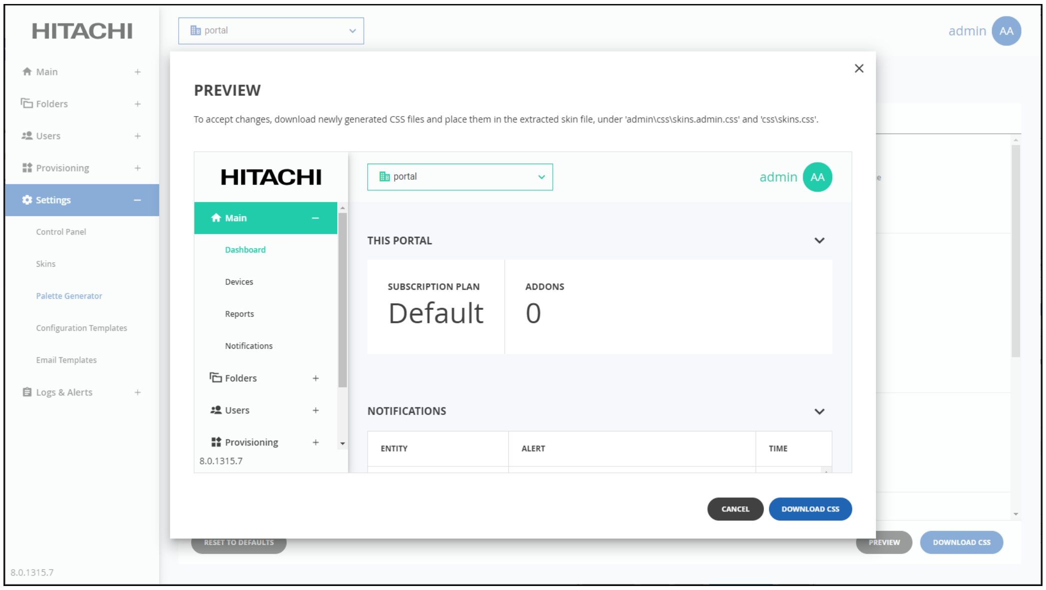
The color scheme is separated into the following areas:

- The brand colors, which determine such things as the color for the main menu items in the navigation menu, as well as action icons and buttons.
- The additional colors, which determine such things as message colors.
- Layout colors, which determine such things as the general page layout.
- Grid colors, which determine such things as table colors.
- Text colors, which determine such things as the text colors.

Clicking an item in one of these areas displays the current color in an editable format and to what the item applies to.

2. Choose the view to change: **ADMINISTRATION PALETTE** or **END USER PALETTE**.
3. Click the item to change the color and enter the HTML color code you want for that item.
4. Click **PREVIEW** to preview the new color scheme.

   For example, setting the primary color to #21CCAA changes the portal color scheme to the following:



To accept changes, download newly generated CSS files and place them in the extracted skin file, under 'admin\css\skins.admin.css' and 'css\skins.css'.

Click **CANCEL** in the preview and then If you do not like the changes, **RESET TO DEFAULTS** in the **Palette Generator** page to undone all your changes.

5. Once you are satisfied with the color scheme, click **DOWNLOAD CSS**.

   Two files are downloaded: *skins.css* and *skins.admin.css*.
6. Use these files as part of the skin for your portal, as described in Managing a Skin.

Managing a Skin

You can upload a default skin for all the portals in the global administrator view or for a specific team portal in the view for that portal.

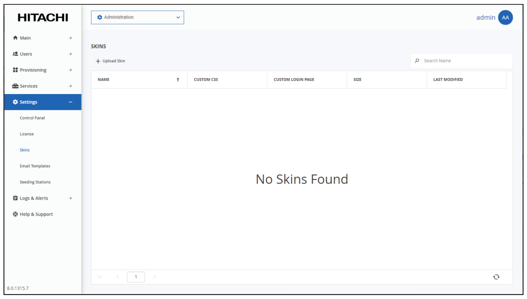
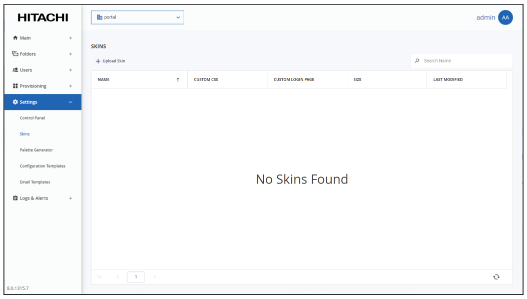
Note: You can get a basic skin from Hitachi Vantara support. The skin file has an extension **.skin**.

To change a skin to include a new color scheme:

1. Create CSS files with the desired color scheme as described in Managing the Portal Colors.
2. Change the extension of the **.skin** file you want to use to **.zip**.
3. Add the files, that were downloaded when you created the desired color scheme, to the css folder in the zip.
4. Change the ZIP file's extension to **.skin**.
5. Upload the skin file to the portal and set it as the default, as described in To upload a skin to the portal:.

To upload a skin to the portal:

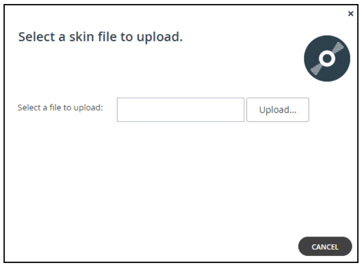
1. For all portals, in the global administration view or for a specific team portal, in the view for the virtual portal, select **Settings > Skins** in the navigation pane.

All team portals (global administration view)	Specific team portal (team portal view)
 HITACHI Administration admin AA Main Users Provisioning Services Settings Control Panel License Skins Email Templates Seeding Stations Logs & Alerts Help & Support 8.0.1315.7 SKINS Upload Skin Search Name NAME CUSTOM CSS CUSTOM LOGIN PAGE SIZE LAST MODIFIED 1 No Skins Found	 HITACHI portal admin AA Main Folders Users Provisioning Settings Control Panel Skins Palette Generator Configuration Templates Email Templates Logs & Alerts 8.0.1315.7 SKINS Upload Skin Search Name NAME CUSTOM CSS CUSTOM LOGIN PAGE SIZE LAST MODIFIED 1 No Skins Found

   The **SKINS** page is displayed.

2. Click **Upload Skin** to upload the new skin.

   The **Select a skin file to upload** window is displayed.



Select a skin file to upload.

Select a file to upload:

3. Click **Upload** and browse to the skin received from Hitachi Vantara support.
4. Select the skin and click **Open**.

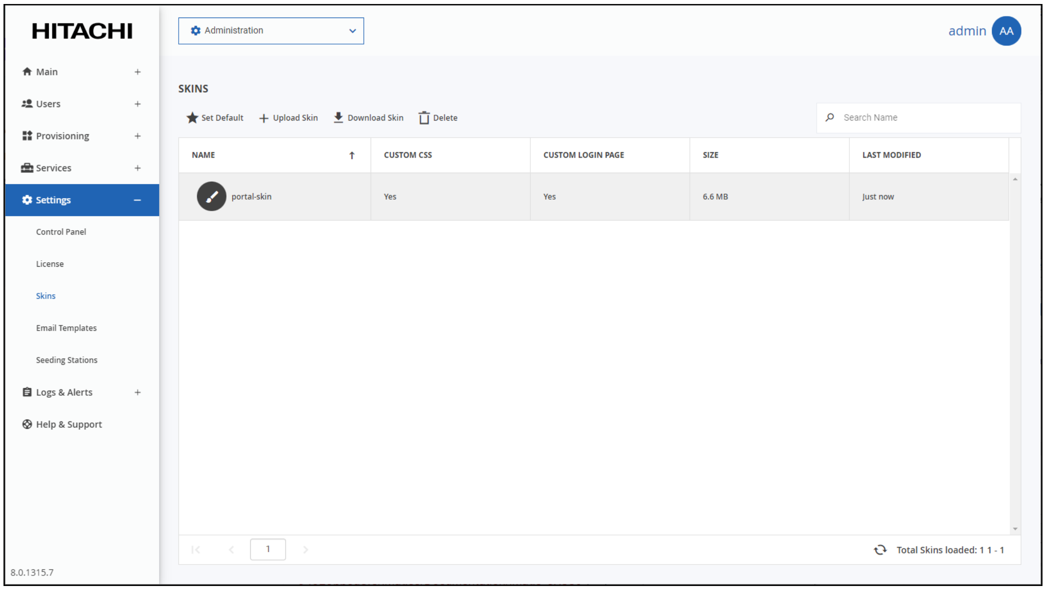
   The selected skin is uploaded.

5. Click **FINISH**.

Note: You can also download a skin from the portal to make changes. Hitachi Vantara recommends only doing this in coordination with Hitachi Vantara support.

To make a skin the default skin:

1. For all HCP Anywhere Enterprise Portals in the global administration view, or for a specific team portal, in the view for the team portal: Select **Settings > Skins** in the navigation pane.
   The **SKINS** page opens, displaying all the available skins.



NAME	CUSTOM CSS	CUSTOM LOGIN PAGE	SIZE	LAST MODIFIED
portal-skin	Yes	Yes	6.6 MB	Just now

2. Select the skin to use as the default and click **Set Default**.

   The selected skin becomes the default skin. `Default Skin` is displayed under the skin name and the icon changes from 🖌 to ★.
3. Refresh the HCP Anywhere Enterprise Portal.

   The default skin cannot be deleted.

To remove a skin from being the default:

1. For all portals, in the global administration view or for a specific team portal, in the view for the team portal, select **Settings > Skins** in the navigation pane.
   The **SKINS** page opens, displaying all the available skins.
2. Select the row of the default skin and click **Remove Default**.

   The icon changes from ★ to 🖌.
3. Refresh the HCP Anywhere Enterprise Portal.

   The skin is no longer used as the default skin.

To delete a skin that is not the default skin:

1. For all portals, in the global administration view or for a specific team portal, in the view for the team portal, select **Settings > Skins** in the navigation pane.
   The **SKINS** page opens, displaying all the available skins.
2. Select the skin to delete and click **Delete**.

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

   The skin is deleted.

Chapter 14. Managing Devices

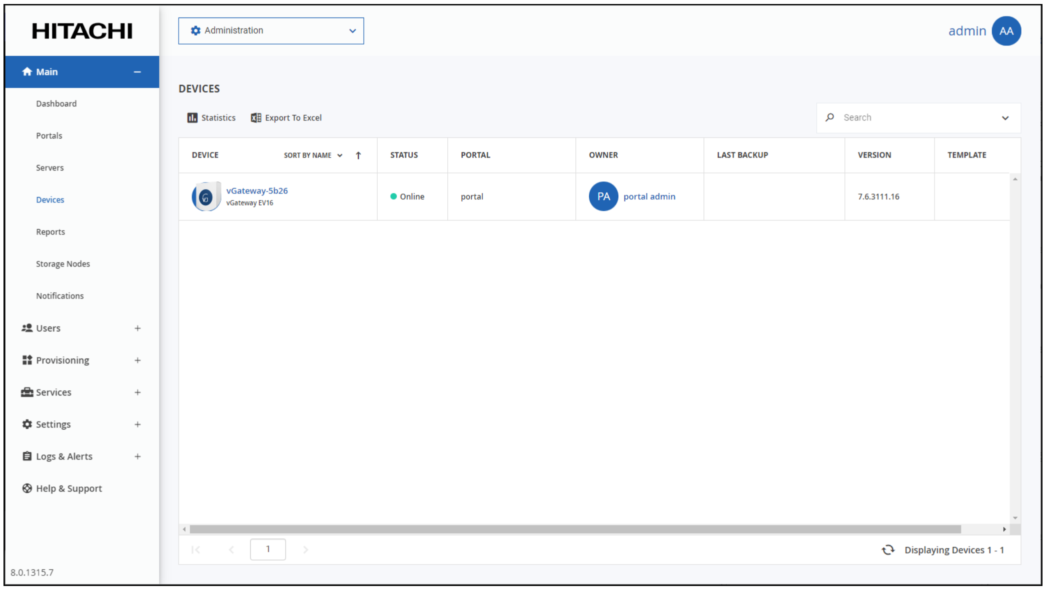
A *device* refers to a HCP Anywhere Enterprise Edge Filer, HCP Anywhere Enterprise Drive Share (Agent), or HCP Anywhere Enterprise Drive Connect, connected to the HCP Anywhere Enterprise Portal. Devices are automatically added to the HCP Anywhere Enterprise Portal, when their owners connect the device to the HCP Anywhere Enterprise Portal.

In this chapter

Viewing All Devices

To view all devices connected to all virtual portals:

- In the global administration view, select **Main > Devices** in the navigation pane.
  The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICES

DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	Online	portal	PA portal admin		7.6.3111.16	

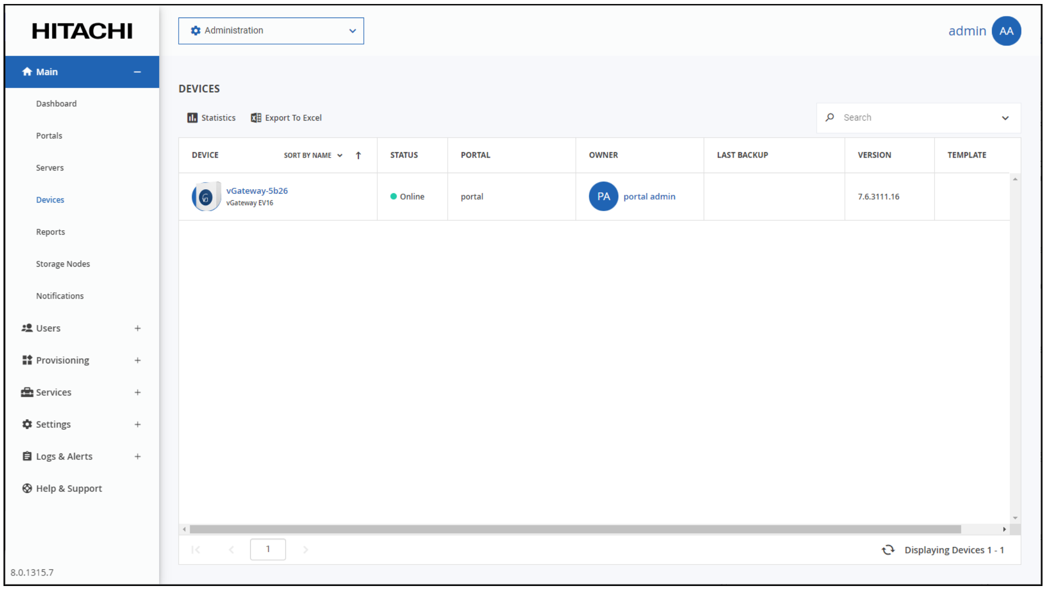
The page includes the following columns:

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**.
PORTAL	The name of the portal hosting the device.
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.

Viewing Individual Device Details

To view individual device details:

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.

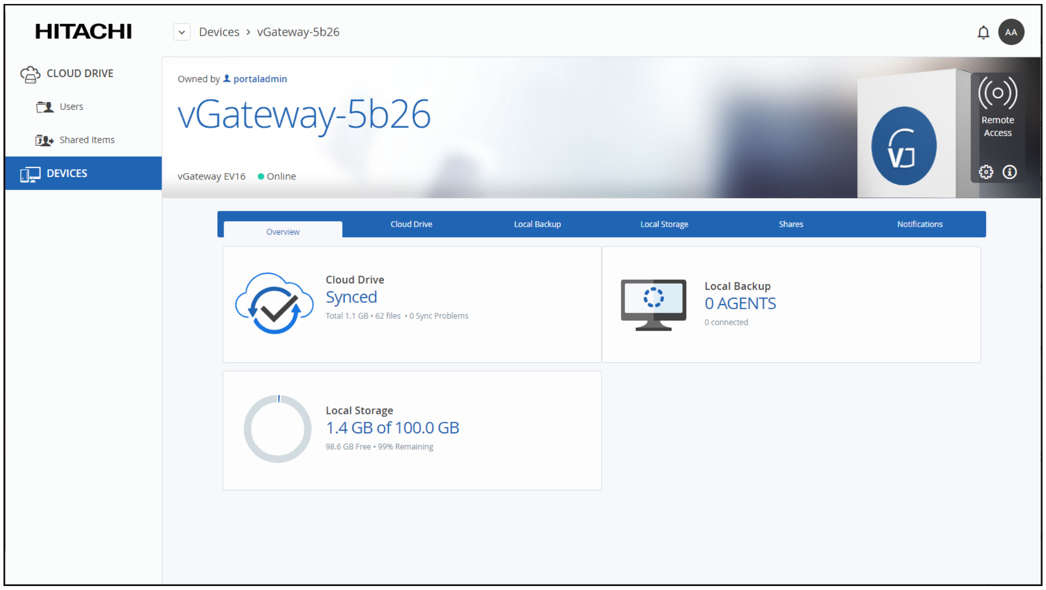


DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	Online	portal	PA portal admin		7.6.3111.16	

2. Click the device name.

   A warning is displayed that you will be redirected to the portal view for the selected device.
3. Click **CONFIRM**.

   The device details are displayed in a new browser window.



Owned by portaladmin

vGateway-5b26

vGateway EV16 ● Online

Cloud Drive
Synced
Total 1.1 GB • 62 files • 0 Sync Problems

Local Backup
0 AGENTS
0 connected

Local Storage
1.4 GB of 100.0 GB
98.6 GB Free • 99% Remaining

The details can be different for each device as well as the details for each type of device and whether the device is connected to the portal or not.

From this window:

- Click **Remote Access** to access the device over the Internet for administration or to access files. The portal administrator must enable **Remote Access**.

  Note: For a PC, the HCP Anywhere Enterprise Drive Share (Agent) must be installed on the PC and connected to the HCP Anywhere Enterprise Portal. For a HCP Anywhere Enterprise Edge Filer, the device must be 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 that is online:
  - The license is displayed and if required, can be changed.
  - You can download a report to send to Hitachi Vantara support for troubleshooting the edge filer.

The device details are divided over a number of tabs.

- The HCP Anywhere Enterprise Drive Share (Agent) details include the following tabs:
  Overview – An overview of backup and cloud sync between the HCP Anywhere Enterprise Drive Share (Agent) and the HCP Anywhere Enterprise Portal.
  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 Drive Share (Agent) statistics, by clicking **Statistics**.
  Notifications – A list of notifications for this device.
  The color of the exclamation mark to the left of each notification indicates the severity.
  Blue – Information

Orange – Warning

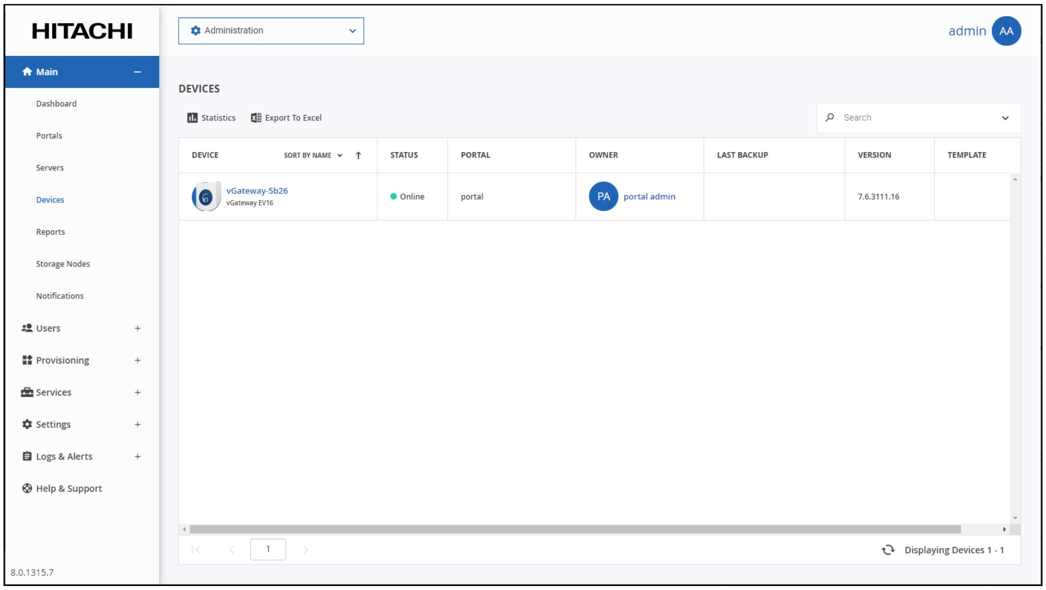
- The HCP Anywhere Enterprise Edge Filer details include the following tabs:
  Overview – Details of the device, including an overview of the following:
  The cloud drive status
  Local storage
  Cloud Drive – File sync details. You can also sync a folder, as described in Syncing Content to the HCP Anywhere Enterprise Portal Global File System and view HCP Anywhere Enterprise Edge Filer statistics, by clicking **Statistics**.
  Local Storage – Details about the HCP Anywhere Enterprise Edge Filer volumes and arrays storage utilization.
  Shares – Manage the edge filer shares from the portal.
  Notifications – A list of notifications for this HCP Anywhere Enterprise Edge Filer.
  The color of the exclamation mark to the left of each notification indicates the severity.
  Blue – Information
  Orange – Warning

Deleting a Device

Deleting a device from the HCP Anywhere Enterprise Portal, removes the device from the user account. When the number of registered devices is near the provisioned number that is allowed, you should remove unwanted devices.

To remove a device:

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	● Online	portal	PA portal admin		7.6.3111.16	

2. Select the row of the device to delete and click **Delete**.
   A confirmation window is displayed.
3. Click **DELETE**.

The device is disconnected and it is is removed from the number of devices licensed for the HCP Anywhere Enterprise Portal.

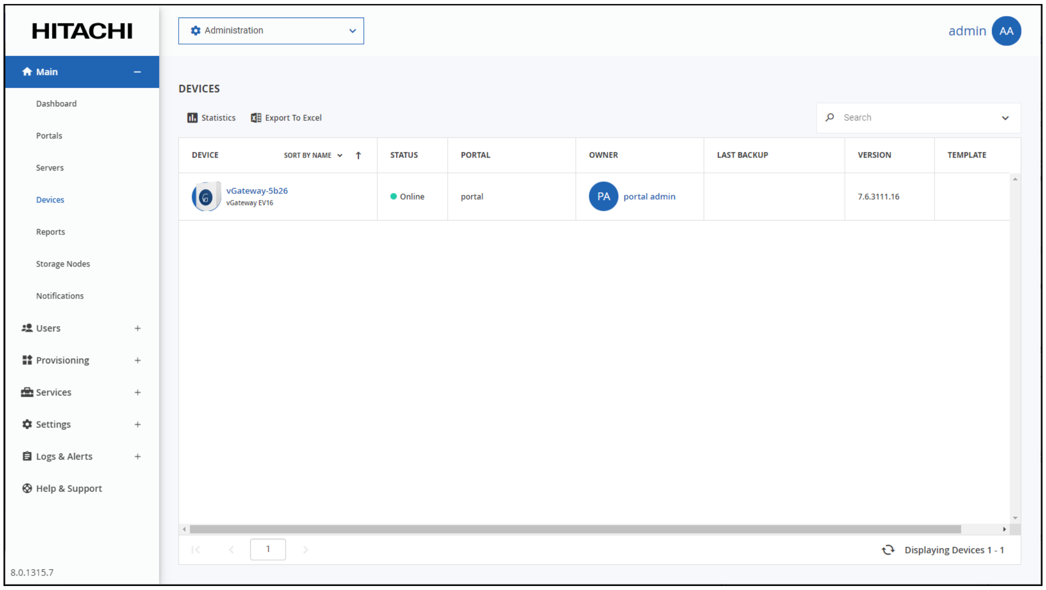
Managing Individual Device Details

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, for example backup details.
- Advanced settings, including:
  - The MAC address
  - The software version.
  - The configuration template, the default template or another templates defined in the portal.
  - You can restart devices and delete devices from the portal, for example inactive devices that are using a license can be deleted to free up a license.
  - Disconnecting a device from the portal.

To manage individual device details:

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.

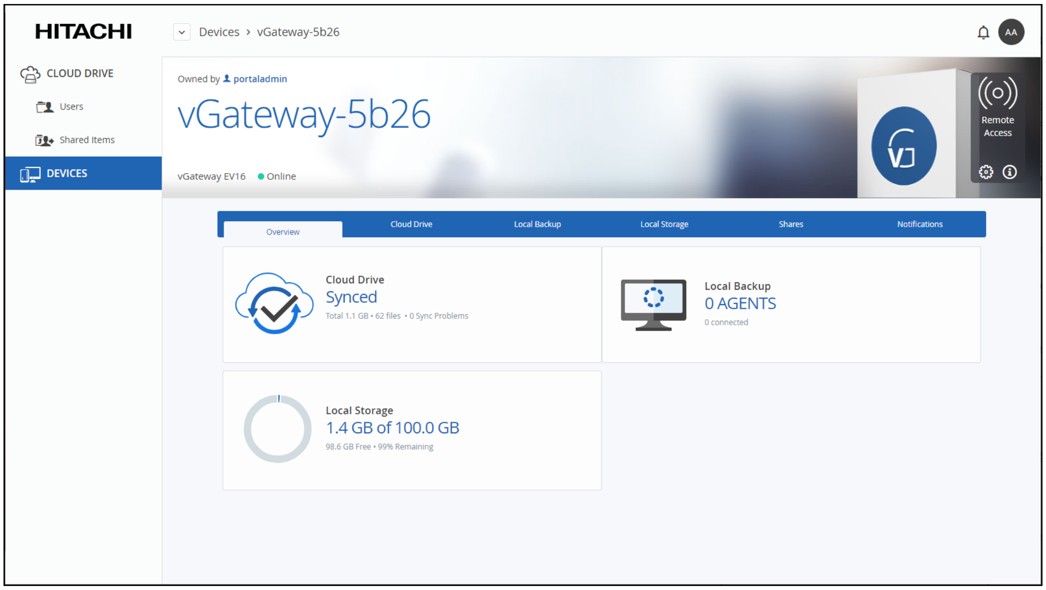


DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	● Online	portal	PA portal admin		7.6.3111.16	

2. Click the device name.

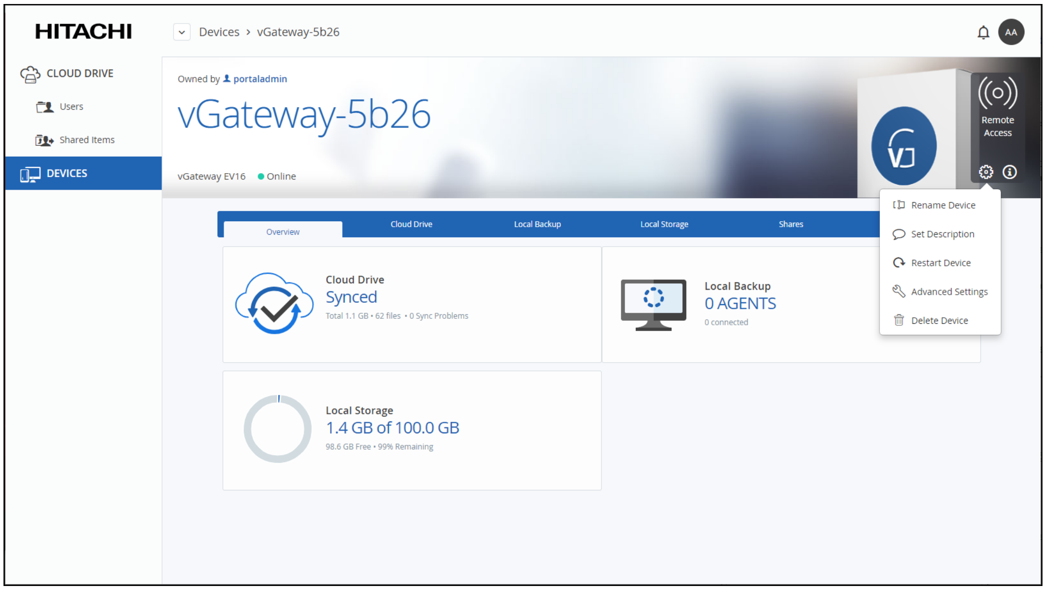
   A warning is displayed that you will be redirected to the portal view for the selected device.
3. Click **CONFIRM**.

   The device details are displayed in a new browser window.



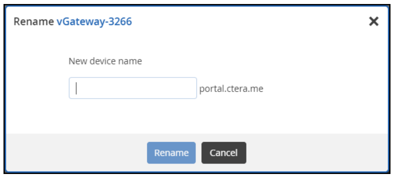
The details are different for each type of device and whether the device is currently connected to the portal.

4. Click the ⚙ icon and select the option required for the device.



Note: The list of available options is dependent on the device. For example, mobile devices do not have the devices do not have the **Advanced Settings** option and only connected devices have a **Restart Device** option.

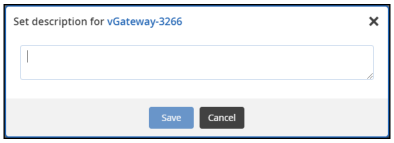
When **Rename Device** is selected, the **Rename** window is displayed.


Rename vGateway-3266

Enter the new device name and click **Rename**. The device is offline for a few seconds as the name change is applied.

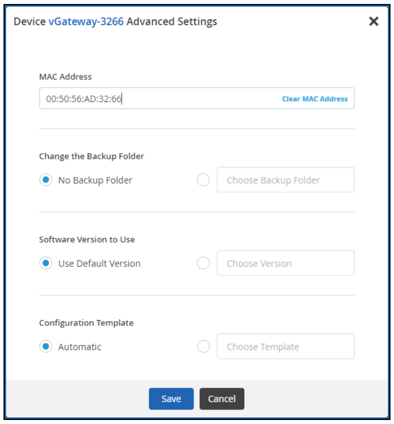
When **Restart Device** is selected, the **Restart Device** window is displayed prompting the restart. Click **Restart** to restart the device.

When **Set Description** is selected, the **Set Description** window is displayed.


Set description for vGateway-3266

Enter any information you want to describe the device and click **Save**.

When **Advanced Settings** is selected, the **Device Advanced Settings** window is displayed.


Device vGateway-3266 Advanced Settings

MAC Address: 00:50:56:AD:32:66

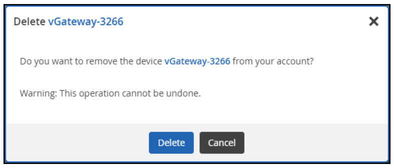
Change the Backup Folder: ● No Backup Folder ○ Choose Backup Folder

Software Version to Use: ● Use Default Version ○ Choose Version

Configuration Template: ● Automatic ○ Choose Template

Enter the configuration you want for the device and click **Save**.

When **Delete Device** is selected, the **Delete *device name*** window is displayed.


Delete vGateway-3266

Do you want to remove the device vGateway-3266 from your account?

Warning: This operation cannot be undone.

Click **Delete** to disconnect the device from the portal and remove it, along with deleting any backups, from the number of devices licensed for the portal.

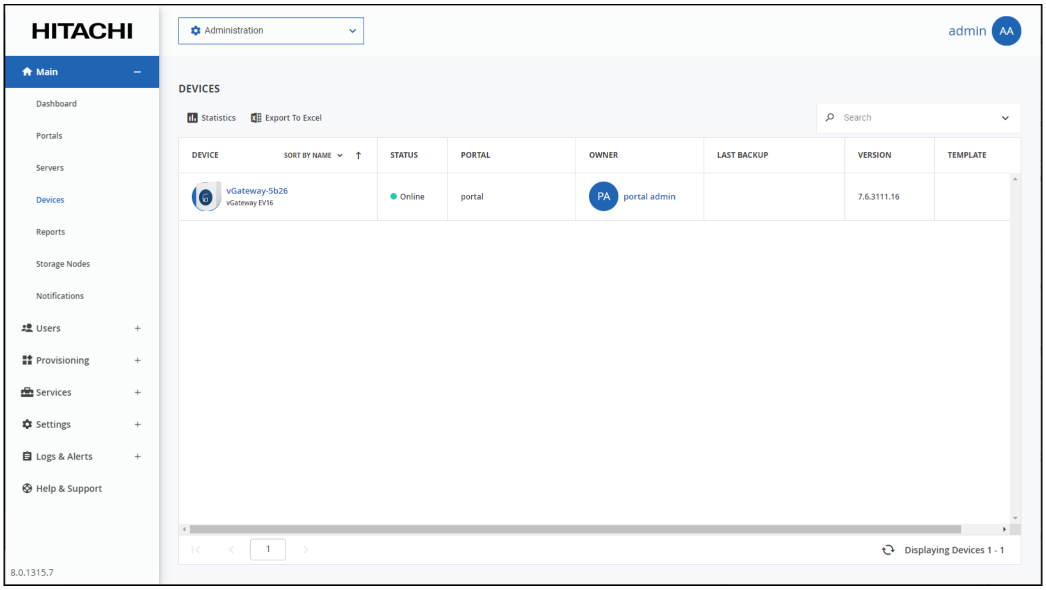
Syncing Content to the HCP Anywhere Enterprise Portal Global File System

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.

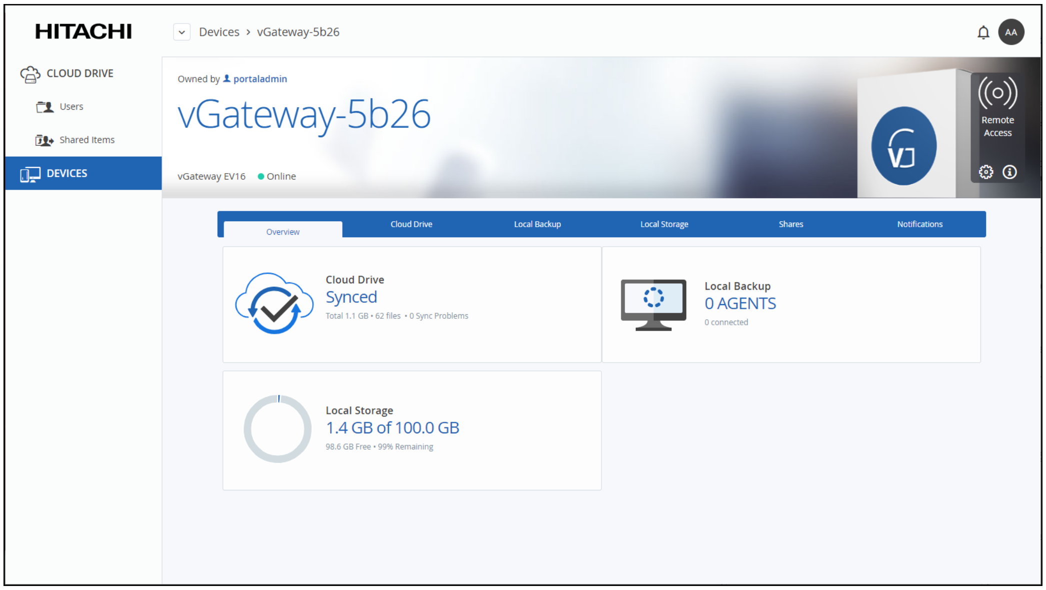
To sync content from the HCP Anywhere Enterprise Portal global file system:

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	● Online	portal	PA portal admin		7.6.3111.16	

2. Click the device name.
   A warning is displayed that you will be redirected to the portal view for the selected device.
3. Click **CONFIRM**.
   The device details are displayed in a new browser window.



Owned by portaladmin

vGateway-5b26

vGateway EV16 ● Online

Cloud Drive
Synced
Total 1.1 GB • 62 files • 0 Sync Problems

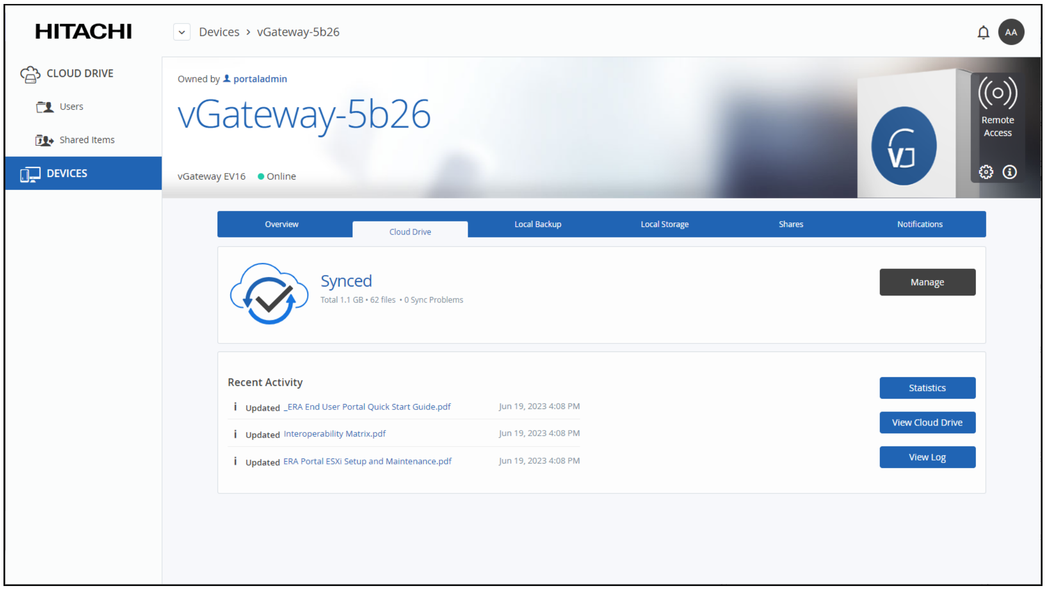
Local Backup
0 AGENTS
0 connected

Local Storage
1.4 GB of 100.0 GB
98.6 GB Free • 99% Remaining

The details are different for each type of device and whether the device is currently connected to the portal.

4. Click the **Cloud Drive** tab.

   The cloud drive details for the device are displayed.



Owned by portaladmin

vGateway-5b26

vGateway EV16 ● Online

Synced
Total 1.1 GB • 62 files • 0 Sync Problems

Recent Activity

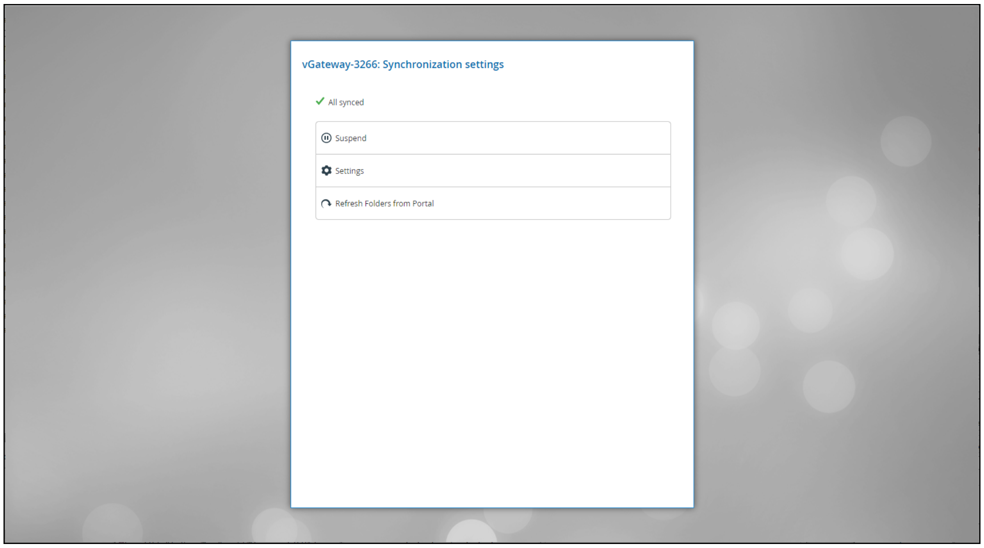
i Updated	_ERA End User Portal Quick Start Guide.pdf	Jun 19, 2023 4:08 PM
i Updated	Interoperability Matrix.pdf	Jun 19, 2023 4:08 PM
i Updated	ERA Portal ESXi Setup and Maintenance.pdf	Jun 19, 2023 4:08 PM

5. To suspend syncing, click ⏸.

   To resume syncing after it was suspended, click ⏯.

6. Click Manage to manage the sync settings.

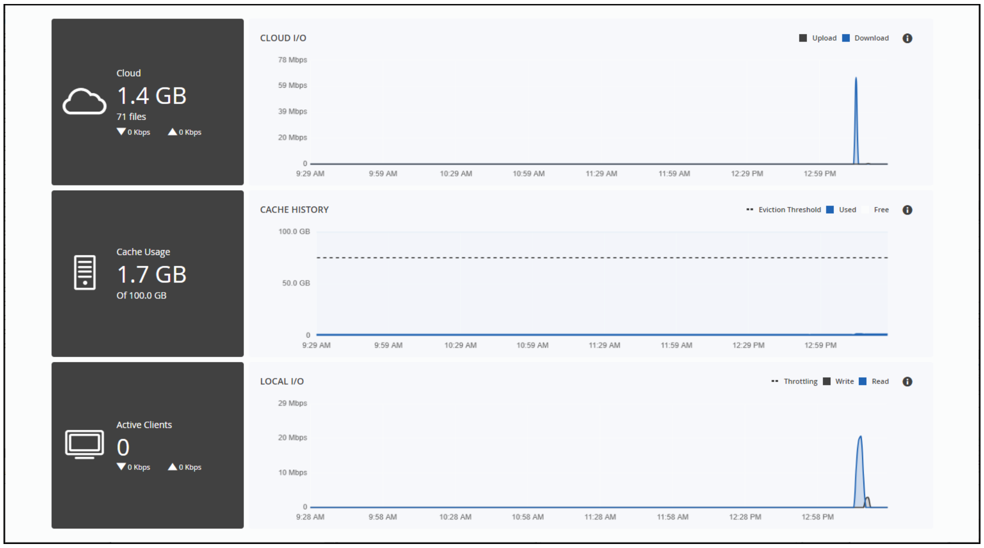
   The settings window is displayed in a new browser window.



vGateway-3266: Synchronization settings
✓ All synced
Suspend
Settings
Refresh Folders from Portal

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*.

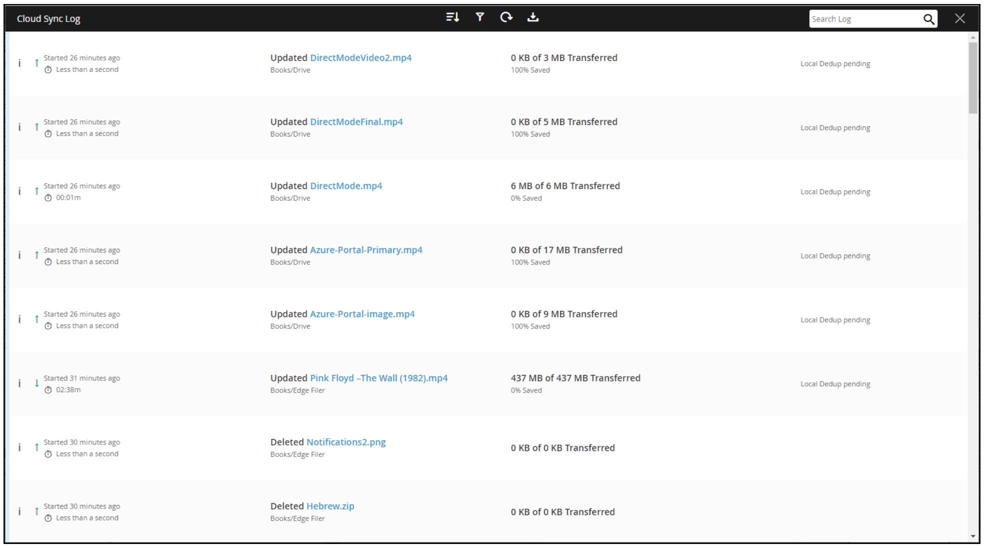
You can view device statistics by clicking Statistics.
The statistics window is displayed in a new browser window.



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.



Cloud Sync Log

Search Log

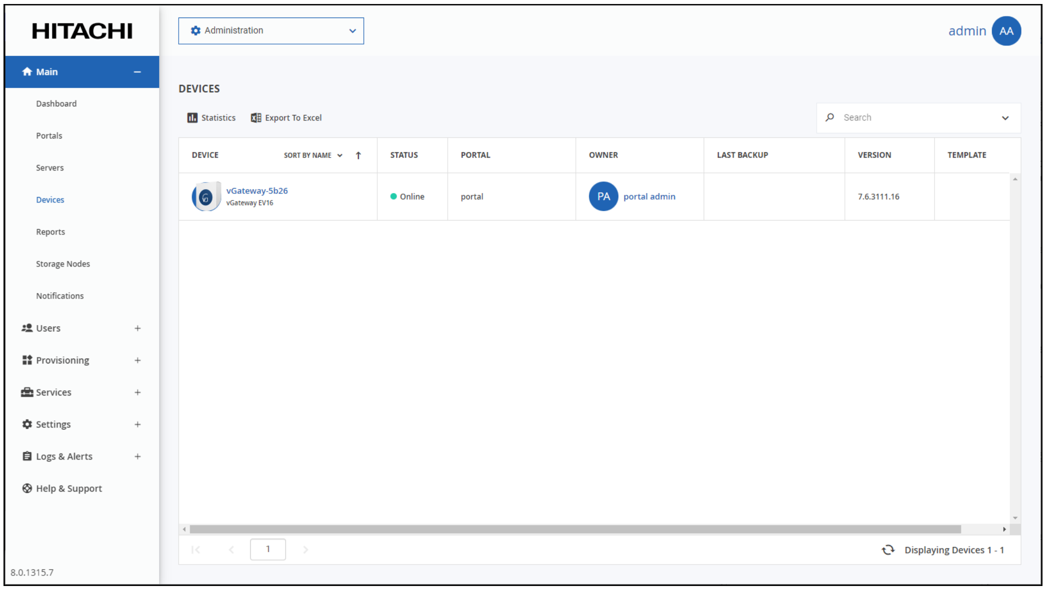
```
i ↑ Started 26 minutes ago      Updated DirectModeVideo2.mp4            0 KB of 3 MB Transferred        Local Dedup pending
    Less than a second          Books/Drive                             100% Saved
i ↑ Started 26 minutes ago      Updated DirectModeFinal.mp4             0 KB of 5 MB Transferred        Local Dedup pending
    Less than a second          Books/Drive                             100% Saved
i ↑ Started 26 minutes ago      Updated DirectMode.mp4                  6 MB of 6 MB Transferred        Local Dedup pending
    00:01m                      Books/Drive                             0% Saved
i ↑ Started 26 minutes ago      Updated Azure-Portal-Primary.mp4        0 KB of 17 MB Transferred       Local Dedup pending
    Less than a second          Books/Drive                             100% Saved
i ↑ Started 26 minutes ago      Updated Azure-Portal-image.mp4          0 KB of 9 MB Transferred        Local Dedup pending
    Less than a second          Books/Drive                             100% Saved
i ↓ Started 31 minutes ago      Updated Pink Floyd –The Wall (1982).mp4 437 MB of 437 MB Transferred    Local Dedup pending
    02:38m                      Books/Edge Filer                        0% Saved
i ↑ Started 30 minutes ago      Deleted Notifications2.png              0 KB of 0 KB Transferred
    Less than a second          Books/Edge Filer
i ↑ Started 30 minutes ago      Deleted Hebrew.zip                      0 KB of 0 KB Transferred
    Less than a second          Books/Edge Filer
```

Note: The information is the same as when choosing **Cloud Sync Log** under **Logs & Alerts** in the navigation pane, but the presentation is different.

Managing the HCP Anywhere Enterprise Edge Filer Shares

Manage the edge filer from the portal has been changed to match the edge filer procedure.

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICES

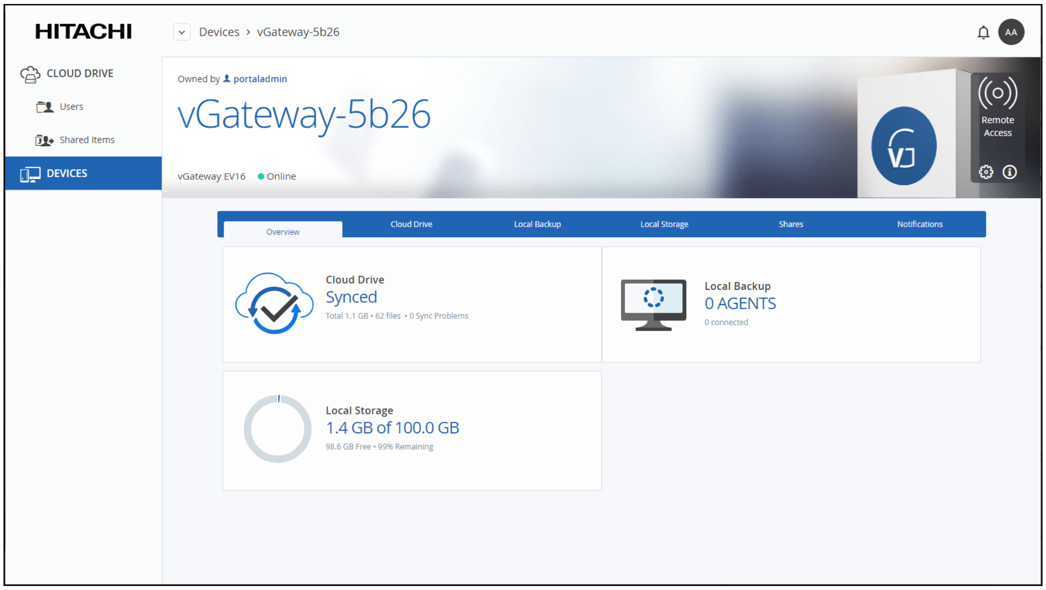
DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	● Online	portal	PA portal admin		7.6.3111.16	

2. Click the device name.

A warning is displayed that you will be redirected to the portal view for the selected device.

3. Click **CONFIRM**.

   The device details are displayed in a new browser window.



Cloud Drive
Synced
Total 1.1 GB • 62 files • 0 Sync Problems

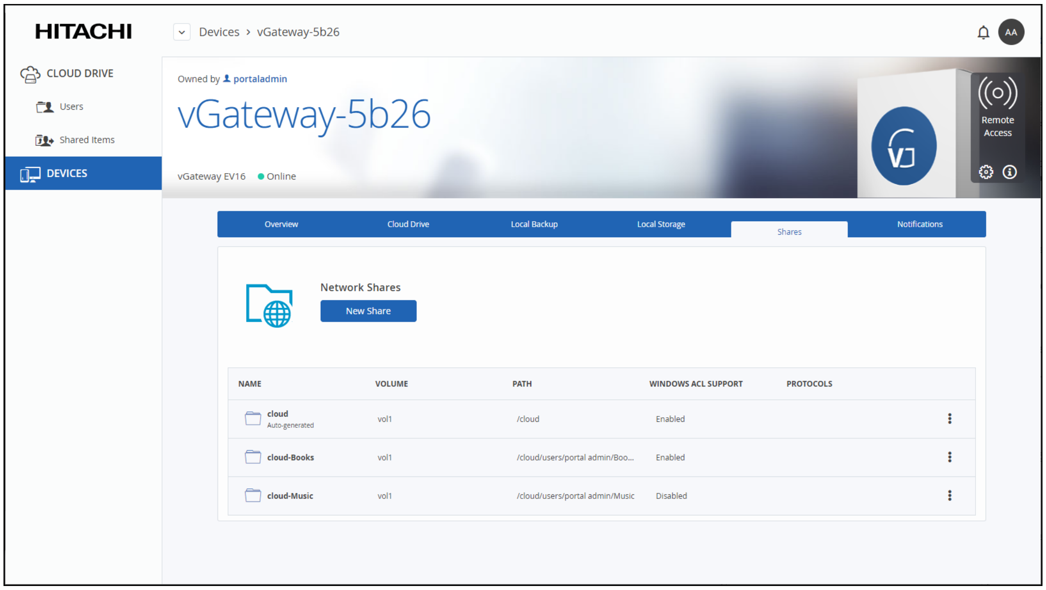
Local Backup
0 AGENTS
0 connected

Local Storage
1.4 GB of 100.0 GB
98.6 GB Free • 99% Remaining

The details are different for each type of device and whether the device is currently connected to the portal.

4. Click the **Shares** tab.

   The share details for the device are displayed.



NAME	VOLUME	PATH	WINDOWS ACL SUPPORT	PROTOCOLS
cloud Auto-generated	vol1	/cloud	Enabled	
cloud-Books	vol1	/cloud/users/portal admin/Boo...	Enabled	
cloud-Music	vol1	/cloud/users/portal admin/Music	Disabled	

5. 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*.

6. Select the volume, folder, or subfolder on which you want to define the share.

   Note: Subfolders, nested shares, are **not** available for Cloud Backup.

   - 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:

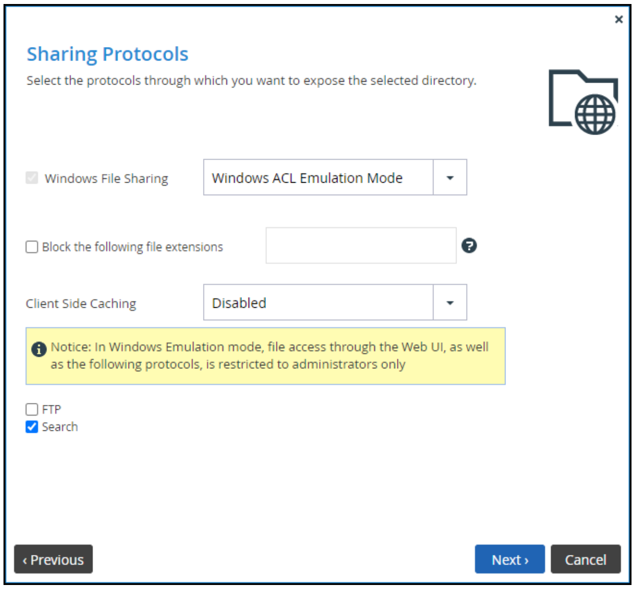
     ```
     /Cloud
     /WIN-File-Server
       /Share1
       /Share2
     /My Files
     /Shared with me
     ```

     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
     ```

7. Click **Next** and then assign the network share a name.
8. Click **Next** to choose through which sharing protocols to expose this share.

   The **Sharing Protocols** window is displayed.



Sharing Protocols

Select the protocols through which you want to expose the selected directory.

☑ Windows File Sharing: Windows ACL Emulation Mode

□ Block the following file extensions

Client Side Caching: Disabled

Notice: In Windows Emulation mode, file access through the Web UI, as well as the following protocols, is restricted to administrators only

□ FTP

☑ Search

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.

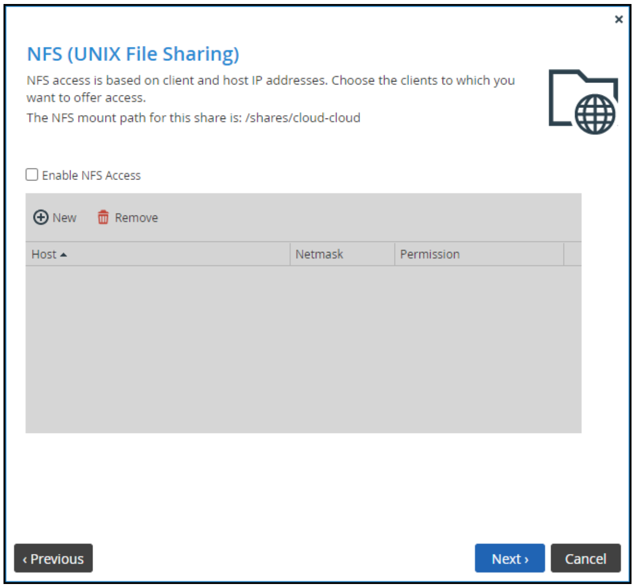
Manual caching for documents – Users must cache files manually.
Automatic caching for documents – A copy of the files is cached automatically.
Disabled – The client computer cannot cache files locally and the updated copy must be retrieved from the file server.

9. 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.

10. Click **Next**.

    The **NFS (UNIX File Sharing)** window is displayed.

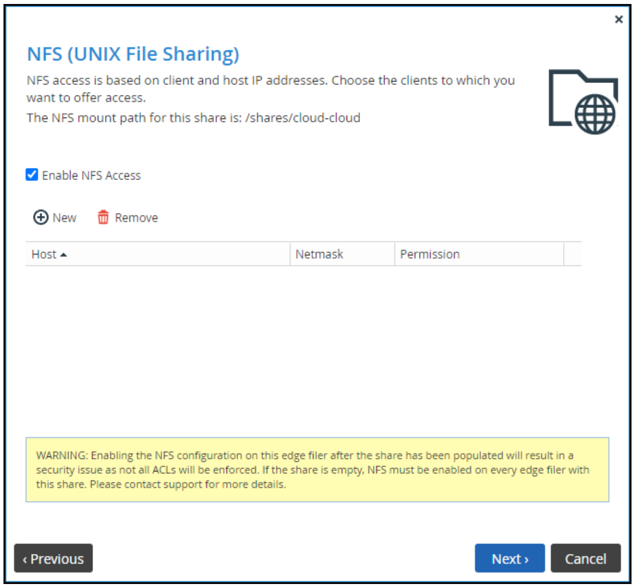


NFS (UNIX File Sharing)

NFS access is based on client and host IP addresses. Choose the clients to which you want to offer access.
The NFS mount path for this share is: /shares/cloud-cloud

☐ Enable NFS Access

11. Check the **Enable NFS Access** option to enable NFS clients to access the share.



NFS (UNIX File Sharing)

NFS access is based on client and host IP addresses. Choose the clients to which you want to offer access.

The NFS mount path for this share is: /shares/cloud-cloud

☑ Enable NFS Access

Host ▲	Netmask	Permission

WARNING: Enabling the NFS configuration on this edge filer after the share has been populated will result in a security issue as not all ACLs will be enforced. If the share is empty, NFS must be enabled on every edge filer with this share. Please contact support for more details.

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. For full details, refer to the *Hitachi Content Platform Anywhere Enterprise Portal Team Administration Guide*.

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.

12. 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.

13. Click **Next** and then **Finish** to complete the wizard.

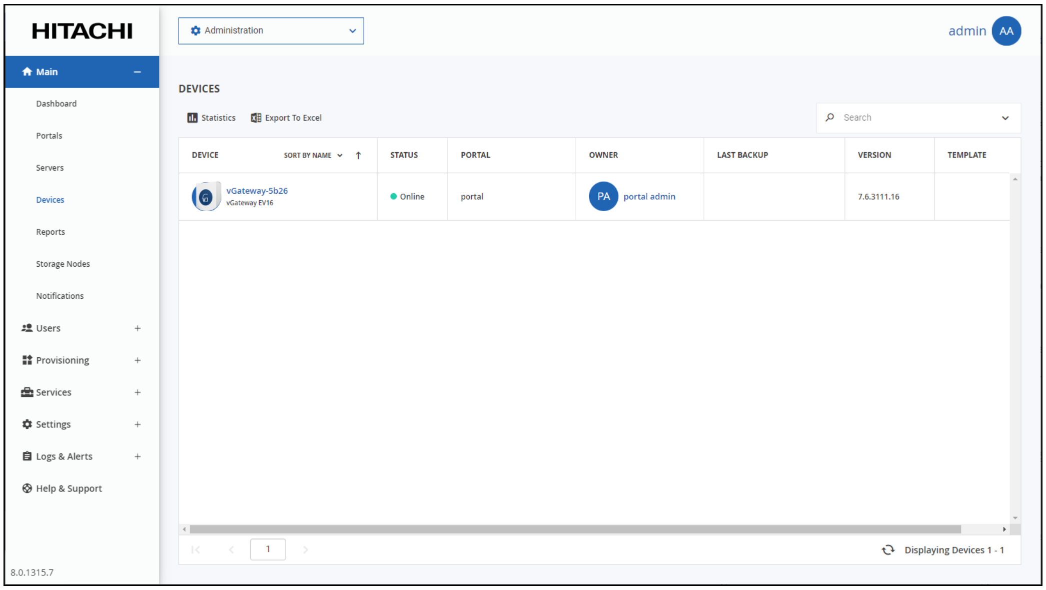
Click ⋮ next to the share to edit it or remove it.

Generating a Device Statistics Report

Administrators can generate a statistics report about all the devices registered to the portal.

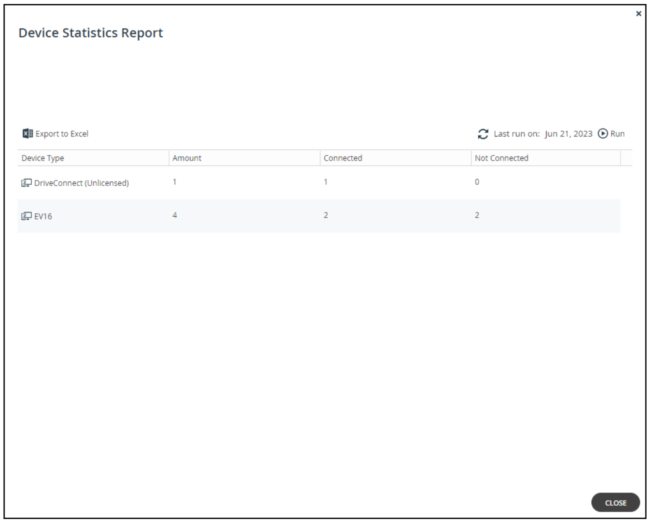
To generate a statistics report:

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	Online	portal	PA portal admin		7.6.3111.16	

2. Click **Statistics**.
   The **Device Statistics Report** window is displayed.



Device Statistics Report

Device Type	Amount	Connected	Not Connected
DriveConnect (Unlicensed)	1	1	0
EV16	4	2	2

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 for each virtual portal, the list of devices types with the total number of registered devices of each type and then the number of these devices currently connected or not connected to the portal. After each team portal, the report includes the total numbers or all the device types for that 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. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.
2. Click **Statistics**.

   The **Device Statistics Report** window is displayed.
3. Click **Export to Excel**.

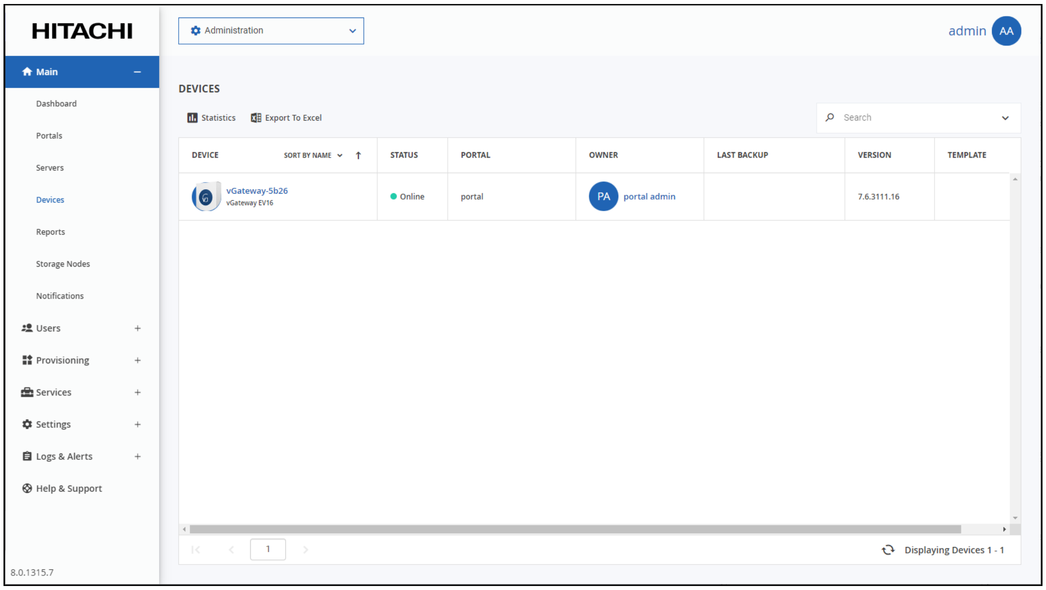
The report is exported to your computer. The report includes the name of the team portal for each device type.

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. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	Online	portal	PA portal admin		7.6.3111.16	

2. Click **Export to Excel**.

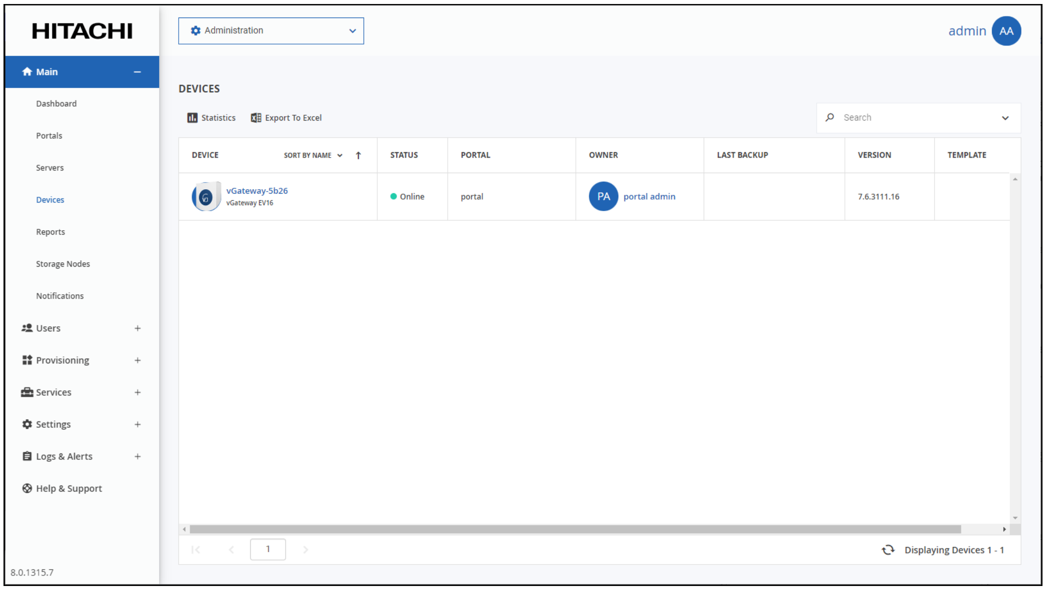
The list of devices is exported to your computer. The report includes the type of device, version and any description set for the device.

Changing an Edge Filer license

If you have changed the license for a HCP Anywhere Enterprise Edge Filer that is connected to the HCP Anywhere Enterprise Portal, for example from EV16 to EV32, you update the license details for the HCP Anywhere Enterprise Edge Filer in the HCP Anywhere Enterprise Portal.

To change an edge filer license:

1. In the global administration view, select **Main > Devices** in the navigation pane.
   The **DEVICES** page opens, displaying all the devices registered to all the team portals.



DEVICE	STATUS	PORTAL	OWNER	LAST BACKUP	VERSION	TEMPLATE
vGateway-5b26 vGateway EV16	Online	portal	PA portal admin		7.6.3111.16	

2. Click the device name.

   A warning is displayed that you will be redirected to the HCP Anywhere Enterprise Portal view for the selected device.
3. Click **CONFIRM**.

   The device details are displayed in a new browser window.
4. Click the ⓘ icon and in the License entry, click **Change**.

   The edge filer license is displayed.
5. Select the new license and click **Save**.

Remote Wiping Mobile Devices

This feature is currently not supported.

Chapter 15. Managing HCP Anywhere Enterprise Portal Notifications and Email Templates

As an administrator, you can receive and view notifications about all portals and users as follows:

- On the **Notifications** dashboard of the global administration interface **(Main > Notifications**). Here, you receive all types of notifications that are enabled on the Notification Settings page (**Settings > Notification Settings**).
- In the main dashboard of the global administration interface. This page displays a summary of the ten highest priority notifications.
- By email. Notifications are sent to administrators by email.

Notifications enable you to track error and warning conditions. For instance, one can use the notification dashboard to track failed backup jobs.

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.

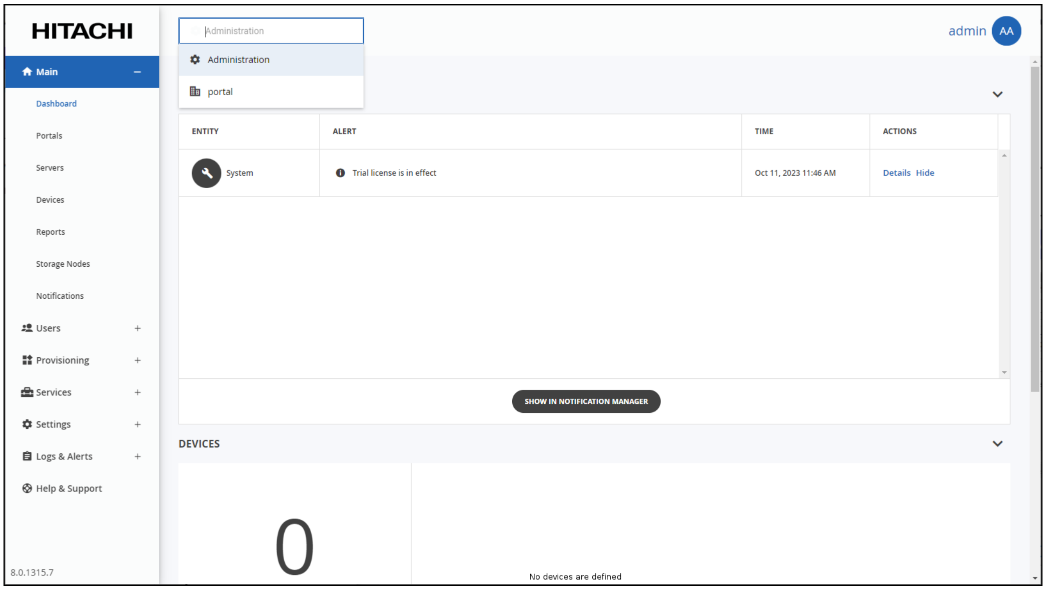
In this chapter

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 Main Dashboard

The dashboard displays a summary of the highest priority active notifications.



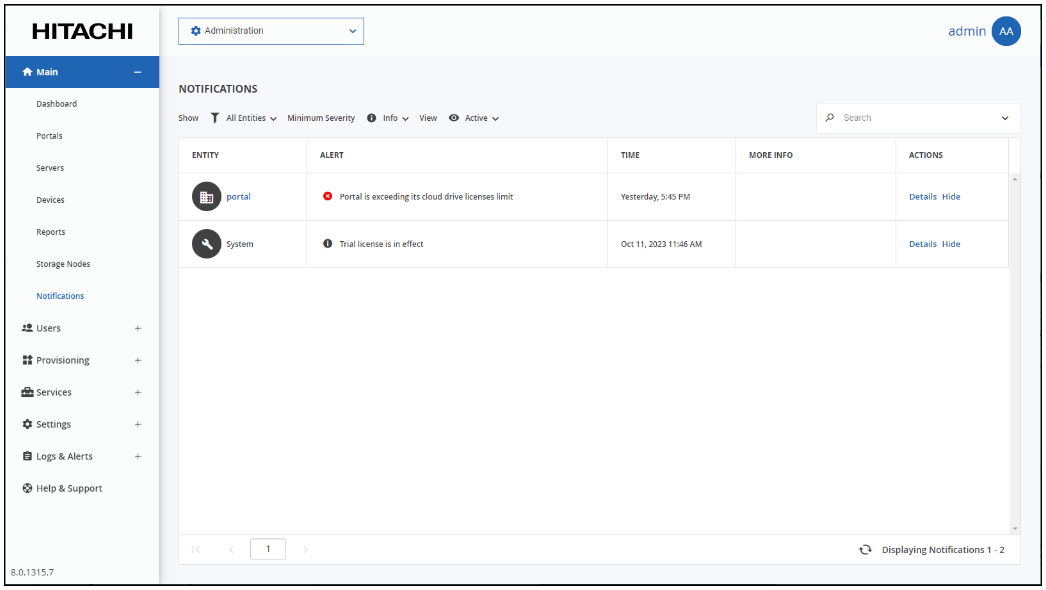
ENTITY	ALERT	TIME	ACTIONS
System	Trial license is in effect	Oct 11, 2023 11:46 AM	Details Hide

If there are notifications you can go directly to the **NOTIFICATIONS** page by clicking **SHOW IN NOTIFICATION MANAGER**, which is displayed at the bottom of the **NOTIFICATIONS** area when there are notifications displayed.

Viewing Notifications in the Notification Page

To view notifications via the notification page:

1. In the global administration view, select **Main > Notifications** in the navigation pane.
   The **NOTIFICATIONS** page is displayed.



ENTITY	ALERT	TIME	MORE INFO	ACTIONS
portal	Portal is exceeding its cloud drive licenses limit	Yesterday, 5:45 PM		Details Hide
System	Trial license is in effect	Oct 11, 2023 11:46 AM		Details Hide

   ENTITY – The entity issuing the notification.
   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 system, storage nodes, and portals.
   - **System** – Notifications from the system.
   - **Storage Node** – Notifications from the storage nodes.
   - **Portal** – Notifications from the HCP Anywhere Enterprise Portal.

   Minimum Severity – Filter notifications dependent on the notification severity: **Info**, **Warning**, or **Error**.
   View – Filter notifications by whether they are active or not. Non-active notifications are marked as hidden.

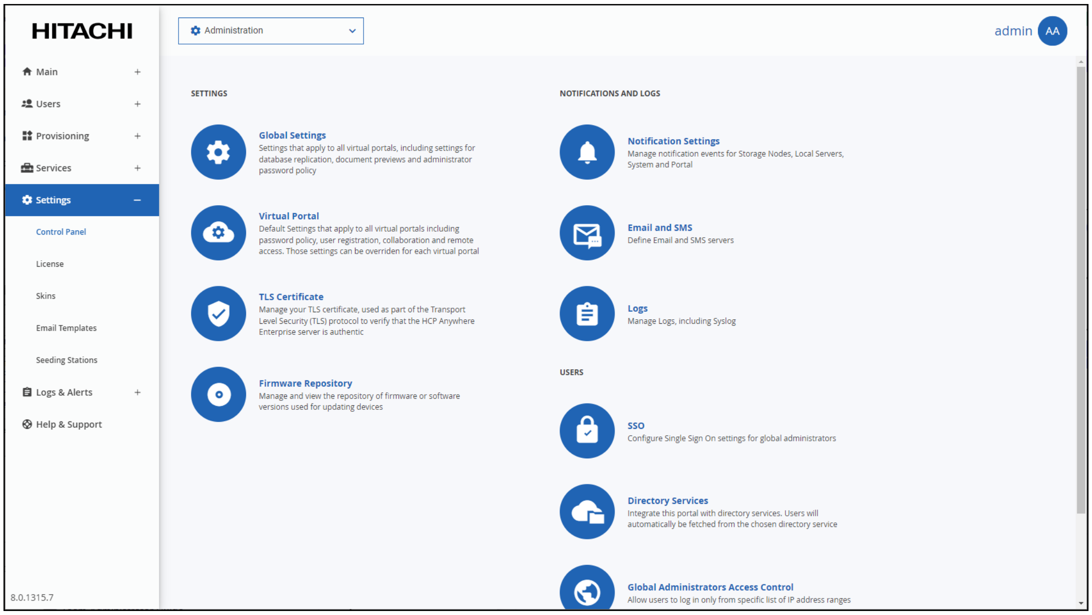
3. You can search the list of alerts, searching everything or by entity or by the **MORE INFO** or **ALERT** columns.

4. You can unhide a 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. In the global administration view, select **Settings** in the navigation pane.
The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

USERS

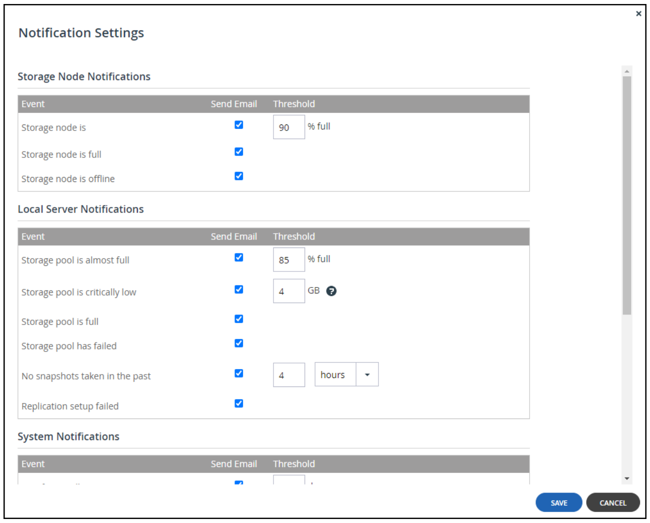
SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Notification Settings**, under **NOTIFICATIONS AND LOGS** in the **Control Panel** content page.

The **Notification Settings** window is displayed.



Notification Settings

Storage Node Notifications

Event	Send Email	Threshold
Storage node is	☑	90 % full
Storage node is full	☑	
Storage node is offline	☑	

Local Server Notifications

Event	Send Email	Threshold
Storage pool is almost full	☑	85 % full
Storage pool is critically low	☑	4 GB
Storage pool is full	☑	
Storage pool has failed	☑	
No snapshots taken in the past	☑	4 hours
Replication setup failed	☑	

System Notifications

Event	Send Email	Threshold

3. Select the notifications which you want to be informed about via email.

The following notifications can be set:

- Storage node notifications:
  The storage node is a specified percentage full.

The storage node is 100% full.
The storage node is offline.

- Local server notifications:
  The storage pool is a specified percentage full.
  The storage pool is almost full, under a specified number of gigabytes.
  The storage pool is full.
  The storage pool has failed.
  Snapshots of the storage pool have not been taken for a specified number of hours or days.
  The storage pool replication failed.
- System notifications:
  The portal certificate has a specified number of days remaining before it expires.
  The catalog database is down.
  The server is offline.
- Portal notifications:
  The portal trial is about to expire.
  The number of devices used exceeds the quota.
  The amount of storage used exceeds the quota.
  The amount of storage used is over a specified percentage of the quota.
  An addon is about to expire.
  An addon has expired.

4. Click **SAVE**.

Email Notification Templates

There are email notification templates for the following:

- Email notification templates for the global administration portal.
  These notifications are sent to global administrators. They are customizable.
- Default email notification templates for all virtual portals.
  These notifications are sent to virtual portal administrators and end users.

The email notifications are in HTML format.

Available Email Notification Templates

The following email templates are provided.

Template Name	Description
Alert Notification	An alert is sent to portal administrators when a log is generated, if an applicable email alert is configured.
Antivirus Server Is Offline	A notification to global administrators to inform them that an antivirus server is not responding and therefore, clients may be unable to download files.
Audit Log Failure	A notification to global 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.

Template Name	Description
Backup Completed With Errors Or Warnings	This feature is currently not supported.
Backup Did Not Complete On Schedule	This feature is currently not supported.
Catalog Database is Down	A notification to global administrators to inform them that the HCP Anywhere Enterprise Portal catalog database is not responding and clients will not be able to access their files and a list of the affected virtual portals.
Certificate Does Not Match The DNS Suffix	A notification to portal administrators to inform them that the HCP Anywhere Enterprise Portal's security certificate does not match the configured DNS suffix.
Certificate Is Not Installed	A notification to portal administrators to inform them that a security certificate is not installed on the HCP Anywhere Enterprise Portal.
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.
Database Tables Were Not Vacuumed	A notification to portal administrators that the portal is unlicensed and explaining how to get a license for the portal.
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	This feature is currently not supported.
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.
DLP Server Is Offline	This feature is currently not supported.
Edge Filer Syslog Warning	A notification to global administrators to inform them that one of the edge filer Syslog servers has exceeded the defined Lag threshold.
Edge Filers Syslog Connector unavailable	A notification to global administrators to inform them that the edge filer Syslog connector is not available.
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.

Template Name	Description
Email Verification Code For Action	A notification to an administrator in the process of permanently deleting a folders and files. The administrator must enter the passcode before the process can continue.
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.
Invitation To Collaborate	A guest invitation to access shared files or folders.
Invitation To Register	An invitation to an external user to register.
Invoice Notification	A notification to users with their invoice.
Key management service unavailable	A notification to global administrators that the specified KMIP Server is not functioning.
Malware Blocked	A notification to end users to tell them that malware was detected and blocked in a file they recently uploaded.
Messaging provisioning has failed	A notification to global administrators that the HCP Anywhere Enterprise messaging service provisioning has failed.
Messaging replication has failed	A notification to global administrators that the HCP Anywhere Enterprise messaging service replication has failed.
Messaging service has errors	A notification to global administrators with the list of the messaging servers with errors and what each error is.
Messaging service has failed	A notification to global administrators with the list of the failed messaging servers and the reason each one has failed.
Messaging status stale	A notification to global administrators with the list of the messaging servers that have stalled and the date each one was last updated.
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.
No License Installed	A notification informing users that their portal is unlicensed and asking them to contact Hitachi Vantara to purchase a license.

Template Name	Description
No Storage Nodes Defined	A notification to global administrators to alert them that no storage nodes are defined in their portal, and therefore cloud storage services cannot be provided.
One Of The Certificates Has Expired	A notification to global administrators to inform them that a certificate of their HCP Anywhere Enterprise Portal expired on a certain date and requesting them to log into the Global Administration View to upload a renewed certificate.
One Of The Certificates Is About To Expire	A notification to global administrators when a HCP Anywhere Enterprise Portal SSL certificate will expire in 30 days.
One Or More Addon Has Expired	A notification to portal administrators to inform them that one or more add-ons has expired, listing the details of the expired add-ons.
One Or More Addon Is About To Expire	A notification to end users when one or more add-on(s) to which they are subscribed will expire in a certain number of days. The number of days is configured locally. See Configuring Email Notifications.
One Or More Portal Addon Has Expired	A notification to portal administrators to inform them that one or more portal add-ons have expired.
One Or More Portal Addon Is About To Expire	A notification to portal administrators when one or more add-on(s) to which their portal is subscribed will expire in a certain number of days. The number of days is configured locally. See Configuring Email Notifications.
Password Recovery Notification	A notification to end users when a request is made to reset their password.
Portal Administrator Report	A monthly report sent to portal administrators.
Portal Has Reached The License Limit	A notification to global administrators, when one of the limits specified in the installed HCP Anywhere Enterprise Portal license installed on the global portal, is reached.
Portal Is Disabled	A notification to end users to inform them that their portal has been disabled by a global administrator.
Portal Is Exceeding Its License	A notification to portal administrators when the portal is exceeding any of its license quotas.
Portal Is Near Quota Limitation	A notification to portal administrators when the amount of cloud storage space used reaches or exceeds 90%.
Portal Is Over Quota Limitation	A notification to portal administrators when their cloud storage space is full.
Portal Is Unlicensed	A notification to global administrators when the portal is not licensed.
Portal License Exceeded	A notification to portal administrators when the portal license has been exceeded.
Portal License Is About To Expire	A notification to portal administrators when one of the portal's license keys will expire in 7 days.

Template Name	Description
Portal Plan Is About To Expire	A notification to the portal administrator when the portal's plan is soon to expire.
Preview Server Has Failed	A notification to the global administrators warning that a preview server has unexpectedly shut down and users may be unable to preview files.
Registration Confirmation	A notification to end users after they register with the HCP Anywhere Enterprise Portal, and before their account is activated.
Replication Has Errors	A notification to global administrators to alert them the a database replication has errors.
Replication Setup Failed	A notification to global administrators to alert them the a database replication has failed to start.
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.
Server Is Offline	A notification to global administrators to inform the administrator that a specific HCP Anywhere Enterprise Portal server is not responding to connection requests from clients for more than a certain time period.
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.
Storage License Exceeded	A notification to global administrators to say that the HCP Anywhere Enterprise Portal is exceeding the licensed storage space.
Storage Node Full	A notification to global administrators when a storage node is full.
Storage Node Has Failed	A notification to global administrators when a storage node has failed.
Storage Node Migration Completed Successfully	A notification to global administrators to say that the migration of a storage node was completed successfully.
Storage Node Migration Completed With Errors	A notification to global administrators to say that storage node migration completed with errors, detailing the errors.
Storage Node Migration Stopped Due To Error	A notification to global administrators to say that migration of a storage node stopped due to a specific error.
Storage Node Nearly Full	A notification to global administrators when a storage node is over 90% full.

Template Name	Description
Storage Pool Failed	A notification to global administrators when a storage pool has failed.
Storage Pool Has Critically Low Space - Working In Degraded Mode	A notification to global administrators when a storage node is over 95% full.
Storage Pool Is Almost Full	A notification to global administrators when a storage pool is over 90% full.
Storage Pool Is Full	A notification to global administrators when a storage pool is full.
Storage Pool Snapshots Are Overdue	A notification to global administrators when storage pool snapshots have not been taken for more than 4 hours.
Successful User Registration	A notification to a end users informing them that a user they invited has successfully completed the registration process to.
System Administrator Report	A monthly report sent to global administrators.
Team Project Request	A notification to portal administrators that an end user has requested a team project be created.
Team Project Request Approved	A notification to portal administrators that a team project request has been approved.
Team Project Request Rejected	A notification to portal administrators that a team project request has been rejected.
Test email	A test notification sent to global administrators.
The Installed SAML Certificate Is About To Expire	A notification to portal administrators that a SAML certificate is invalid or expired, and that users will not be able to connect to the HCP Anywhere Enterprise Portal using SAML authentication.
The Installed SAML Certificate Is Invalid Or Expired	A notification to portal administrators that the HCP Anywhere Enterprise Portal’s SAML certificate is invalid or expired.
There are blocks that can not be deleted from storage	A notification to global administrators that some blocks cannot be deleted.
Trial Is About To Expire	A notification to end users when their trial subscription will expire in a certain number of days. The number of days is configured locally. See Configuring Email Notifications.
Trial License Has Ended	A notification to portal administrators that the portal's trial license has expired and they need to purchase a license.
Trial License Is In Effect	A notification that the portal is using a trial license that is limited.
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.

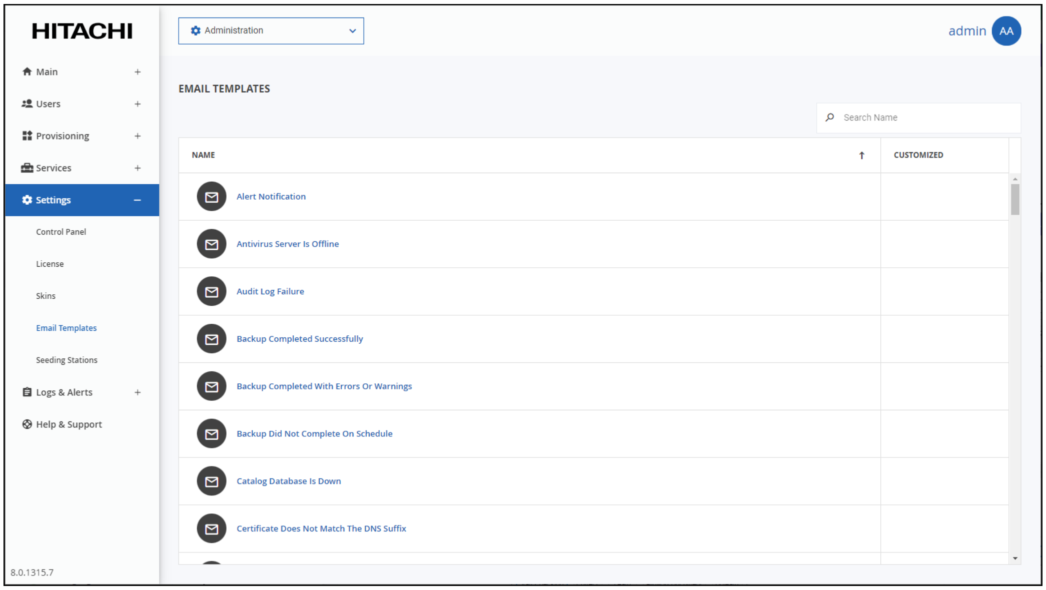
Template Name	Description
User Is Over Agents Limitation	A notification to end users when they have exceeded the licensed number of HCP Anywhere Enterprise Drive Share (Agents).
User Is Over Quota Limitation	A notification to end users when their cloud storage space is full.
User Report	A monthly report sent to end users, which includes the following information: Account information Storage statistics Usage report Details of all the user's devices Information on the status of the user's cloud backups
Vouchers Issued	This feature is currently not supported.

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. In the global administration view, 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.



EMAIL TEMPLATES

NAME	CUSTOMIZED
Alert Notification	
Antivirus Server Is Offline	
Audit Log Failure	
Backup Completed Successfully	
Backup Completed With Errors Or Warnings	
Backup Did Not Complete On Schedule	
Catalog Database Is Down	
Certificate Does Not Match The DNS Suffix	

2. Click the email template to edit.

   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**.
8. 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.
9. To edit a PDF attachment, In the **PDF File** tab, modify the template.
10. To preview changes to the PDF, click **PREVIEW**.

    The PDF is downloaded to your computer. where you can open an review the content.
11. To undo unsaved changes, click **REVERT**.
12. Click **SAVE**.
13. Click **CLOSE**.

Chapter 16. Managing Antivirus Servers

Antivirus software is used to prevent malware from infecting files in the organization. HCP Anywhere Enterprise Portal integrates with antivirus vendors through the ICAP protocol to ensure data protection.

To implement antivirus scanning of portal files, you require an antivirus license from Hitachi Vantara. Using HCP Anywhere Enterprise Portal subscription plans, you can activate or deactivate the antivirus feature for specific virtual portals.

When antivirus is activated, a background scan of the portal global file system is initiated. In addition, files are scanned for malware automatically and transparently, before they are downloaded from the portal.

Note: When the browser used is Google Chrome, you are notified that a download failed. With other browsers, the download is unsuccessful without a notification.

After the initial background scan, 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.
- Backup folders that are not passphrase protected.
- Cloud drive folders.

If an infected file is found, the infected file is quarantined so that you 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 your 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`

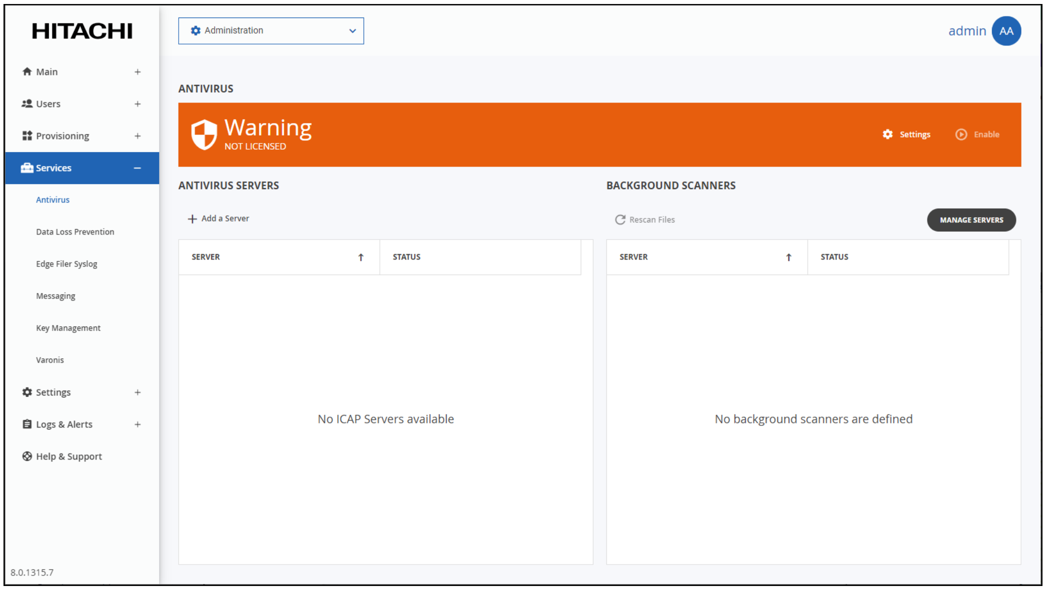
Administrators can view files that are quarantined by the antivirus servers, the Cloud Drive location and the user who downloaded the files.

In this chapter

Setting up Antivirus File Scanning

After adding the antivirus license, you add an antivirus server to the portal and then include antivirus scanning in a plan at the global level. Any HCP Anywhere Enterprise Portal assigned to this plan includes antivirus scanning.

When the HCP Anywhere Enterprise Portal is not licensed, the following screen is displayed.



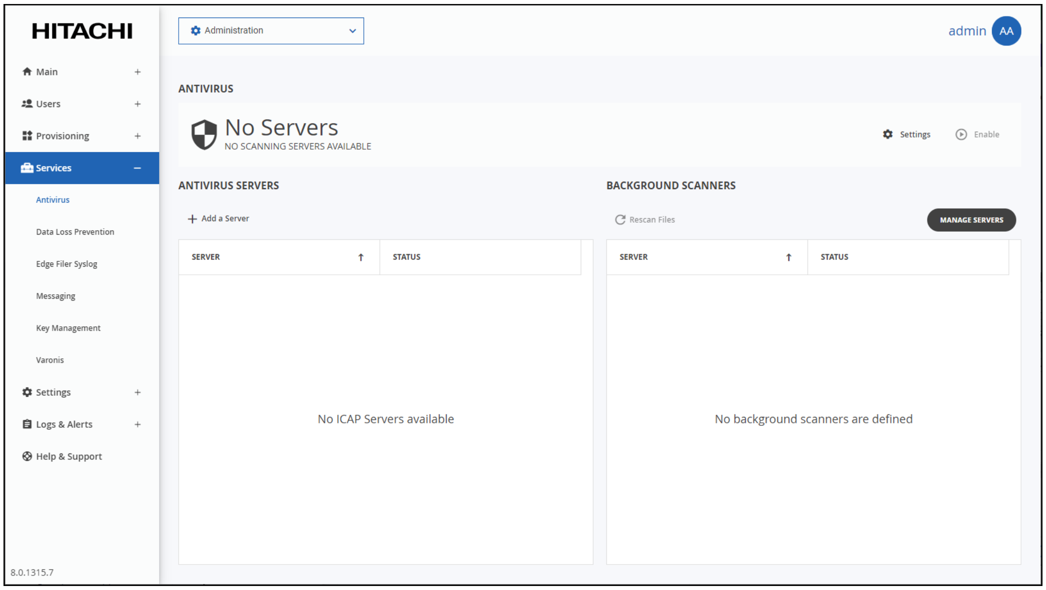
Warning
NOT LICENSED

No ICAP Servers available

No background scanners are defined

To add or edit an antivirus server:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.



No Servers
NO SCANNING SERVERS AVAILABLE

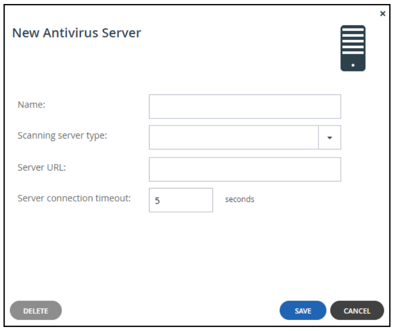
No ICAP Servers available

No background scanners are defined

The **Antivirus Status** bar at the top of the page shows the current status:
Active/RUNNING OK – Antivirus is running on at least one server.
No Servers/NO SCANNING SERVERS ABVAILABLE – There are no antivirus servers defined.
Failed/NO SCANNING SERVERS ABVAILABLE – The antivirus server is not running.
Disabled/NOT RUNNING – Antivirus scanning has been suspended.

2. To add a new server, click **Add a Server**.

   The **New Antivirus Server** window is displayed.



New Antivirus Server

Name:

Scanning server type:

Server URL:

Server connection timeout: 5 seconds

Or,
To edit an existing antivirus server, click the server’s name**.**
The antivirus server window is displayed with the server as the window title.

3. Specify the details:

   Name – A name for the server.
   Scanning server type – Select a supported antivirus:
   - McAfee Web Gateway
   - Symantec Protection Engine

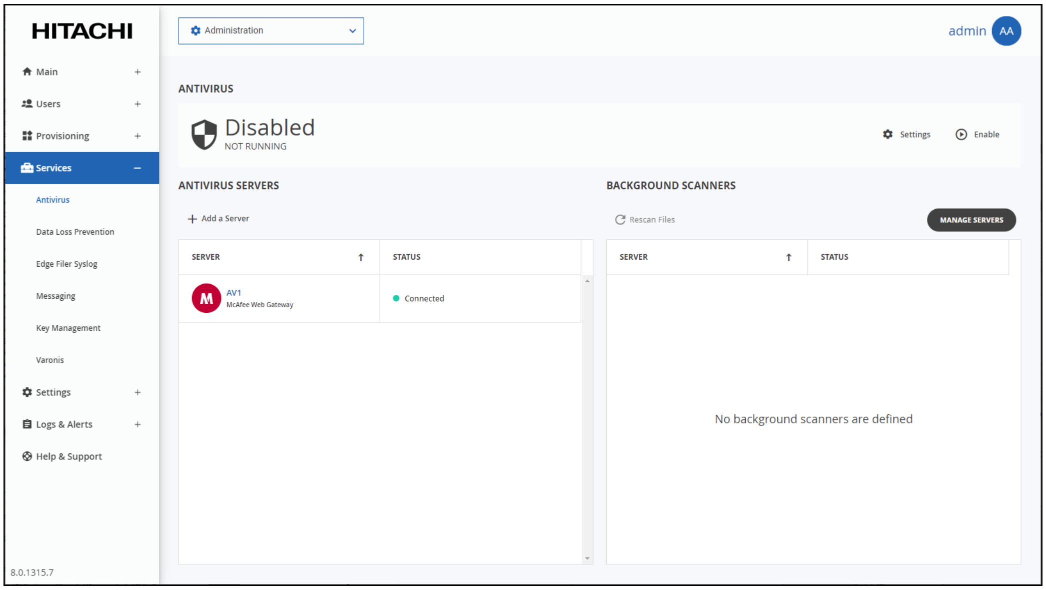
- ESET Gateway Security
- Sophos AV
- McAfee VirusScan Enterprise for Storage
- Trend Micro InterScan

Server URL – The URL of the server, including the ICAP port and the name of the service. The default ICAP port is 1344. The antivirus service name is configurable in the antivirus server software. Assuming the default ICAP port and default antivirus service name:
For all the scanning server types except for ESET, the URL is `http://`*`IP`*`:1344/avscan`
For ESET the URL is `http://`*`IP`*`:1344/av_scan`

Server connection timeout – The server's connection timeout, in seconds.

4. Click **SAVE**.

   The sever is added.



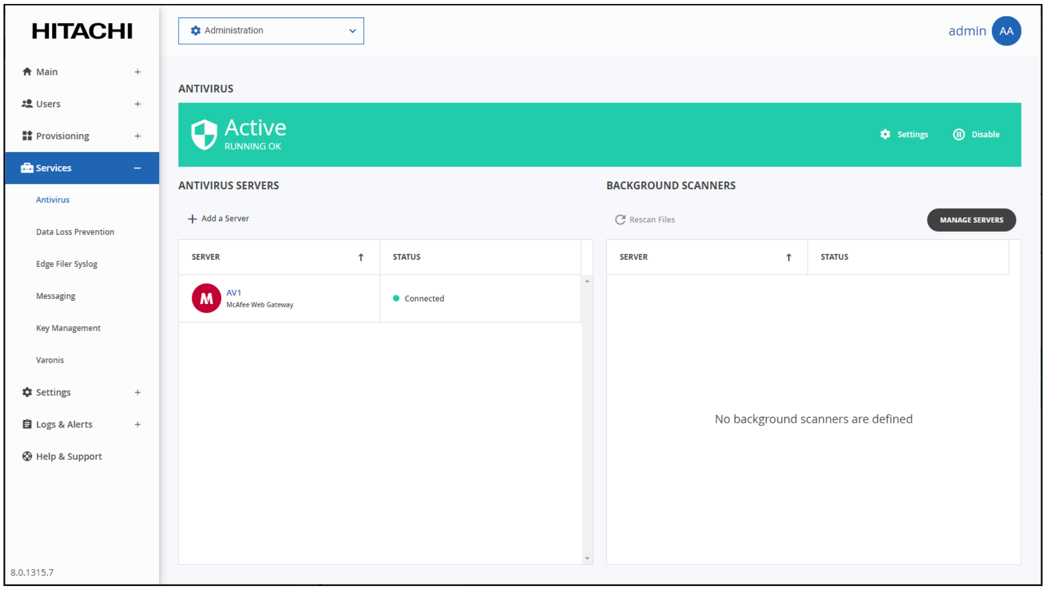
Disabled
NOT RUNNING

SERVER	STATUS
AV1 McAfee Web Gateway	Connected

SERVER	STATUS

No background scanners are defined

5. Click **Enable** to start the service.
6. The **ANTIVIRUS** page is redisplayed showing that the service is **Active**.



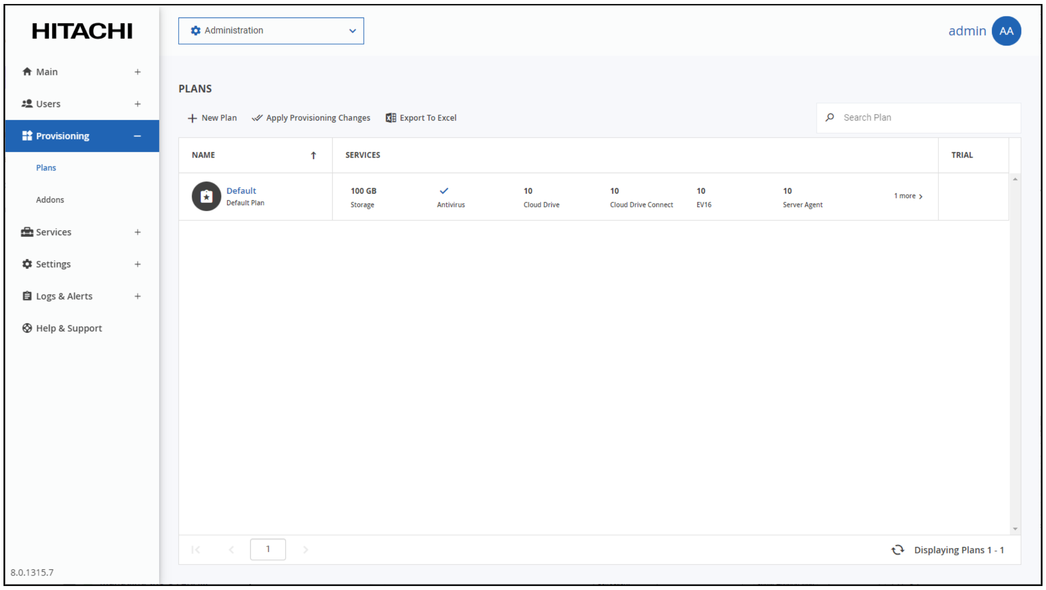
SERVER	STATUS
AV1 McAfee Web Gateway	Connected

SERVER	STATUS

No background scanners are defined

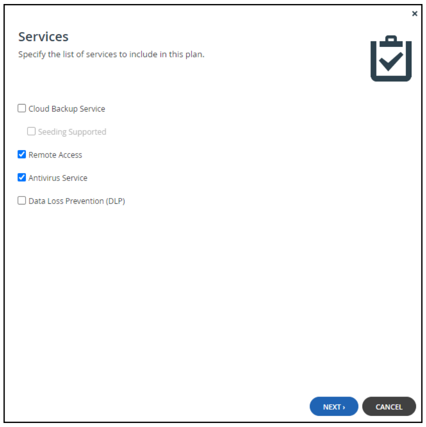
To set up antivirus scanning in a plan:

1. In the global administration view, select **Provisioning > Plans** in the navigation pane. The **PLANS** page is displayed.



NAME	SERVICES							TRIAL
Default Default Plan	100 GB Storage	✓ Antivirus	10 Cloud Drive	10 Cloud Drive Connect	10 EV16	10 Server Agent	1 more ›	

2. Click the plan to activate antivirus scanning.
   The plan wizard opens, displaying the **Services** window.



Services

Specify the list of services to include in this plan.

☐ Cloud Backup Service

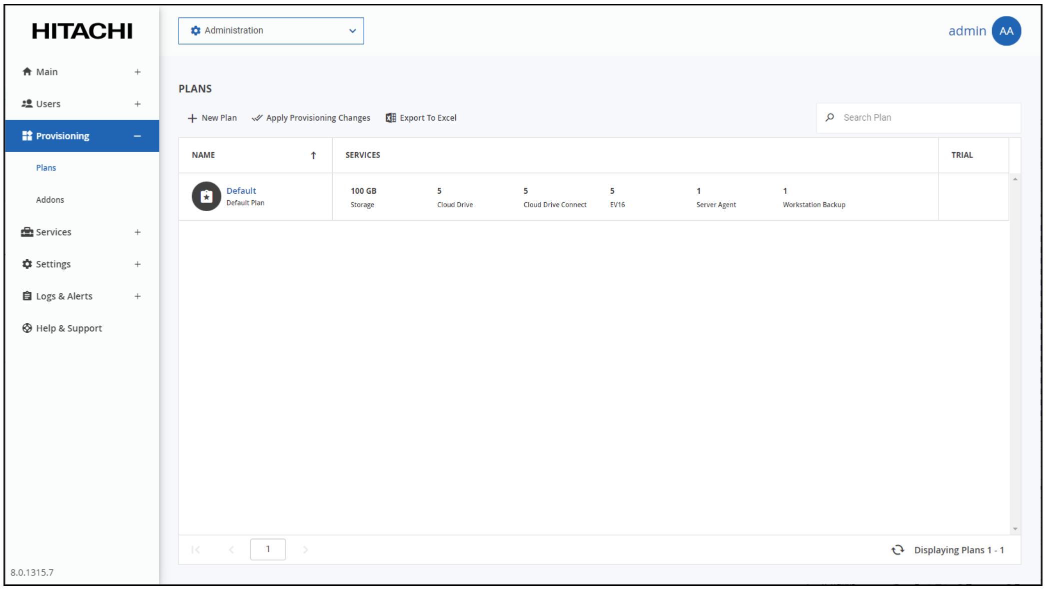
☐ Seeding Supported

☑ Remote Access

☑ Antivirus Service

☐ Data Loss Prevention (DLP)

3. Check **Antivirus Service** to activate the antivirus feature and continue with the wizard to completion.



PLANS

NAME	SERVICES	TRIAL
Default Default Plan	100 GB Storage 5 Cloud Drive 5 Cloud Drive Connect 5 EV16 1 Server Agent 1 Workstation Backup	

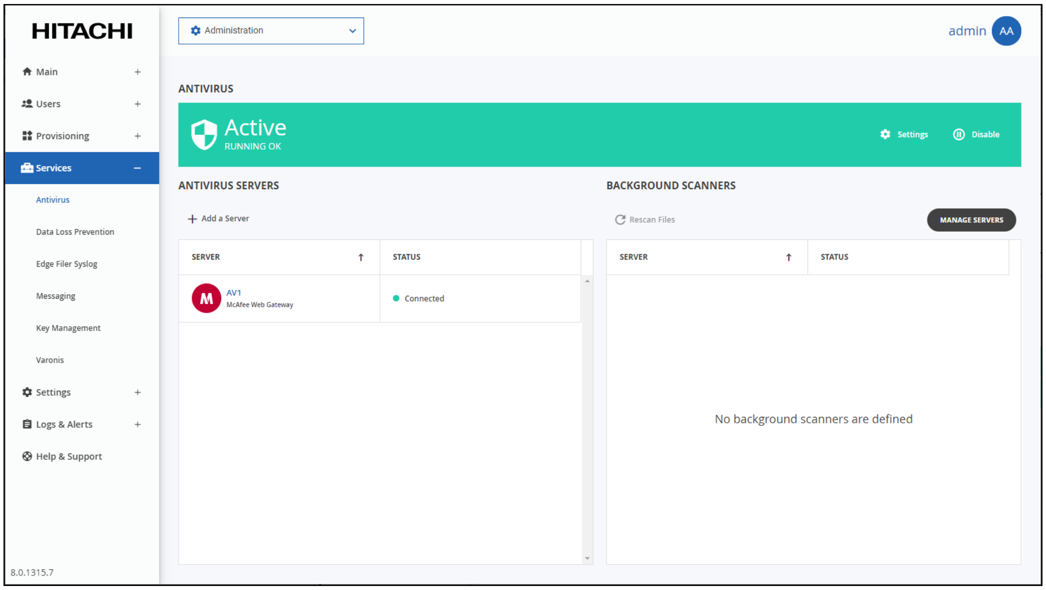
When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time.

Managing Antivirus Servers

You can specify how infected files are handled and suspend antivirus scanning.

To configure how infected files are handled:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane. The **ANTIVIRUS** page is displayed.



ANTIVIRUS

Active
RUNNING OK

ANTIVIRUS SERVERS

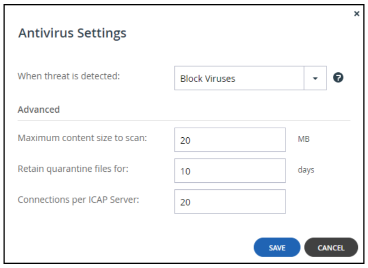
SERVER	STATUS
AV1 McAfee Web Gateway	Connected

BACKGROUND SCANNERS

SERVER	STATUS

No background scanners are defined

2. Click **Settings** to configure antivirus scanning.
   The **Antivirus Settings** window is displayed.



Antivirus Settings

When threat is detected: Block Viruses

Advanced

Maximum content size to scan: 20 MB

Retain quarantine files for: 10 days

Connections per ICAP Server: 20

When a threat is detected – Specify how to handle infected files:

Log Only – An email is sent to the portal listing the file that might be infected and the file is copied to quarantine. It is still possible to download or preview the infected file.

Block Viruses – The infected file is not downloaded and it is quarantined.

Maximum content size to scan – The maximum size of a file to be scanned.

Retain quarantine files for – The number of days that files are kept in quarantine before being removed.

Connections per ICAP Server– The number of connections available for use by the portal for the ICAP server.

To suspend or resume antivirus scanning for all servers:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. In the status bar, click **Suspend** to suspend antivirus scanning or **Resume** to resume antivirus scanning for all servers.

To suspend or resume antivirus scanning for a specific server:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. Select the server row in the list of **ANTIVIRUS SERVERS**.
3. Click **Suspend** to suspend antivirus scanning or **Resume** to resume antivirus scanning for the server.

   The status for resumed servers is `Connected` and for suspended servers it is `Disabled`.

Deleting an Antivirus Server

To delete an antivirus server:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. Either,
   a) Select the antivirus server to delete and click **Delete**.
   A confirmation window is displayed.
   b) Click **DELETE SERVER** to confirm.
   Or,
   a) Click the antivirus server's name in the list of **ANTIVIRUS SERVERS**.
   The antivirus server window is displayed with the server name as the window title.
   b) Click **DELETE**.
   A confirmation window is displayed.
   c) Click **YES** to confirm.

Background Scanning and Rescanning Files

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.
- Backup folders that are not passphrase protected.

The background scan runs constantly, scanning new files. If there are no new files to scan, the scan stops for 30 seconds before checking again for new files to scan.

If you need to run a scan on all the portal files, for example, when the antivirus software signatures database is updated with new viruses, you can initiate the scan. This scan checks all the files, both new files and files that were previously scanned.

It is recommended to manually rescan all the files after unquarantining files.

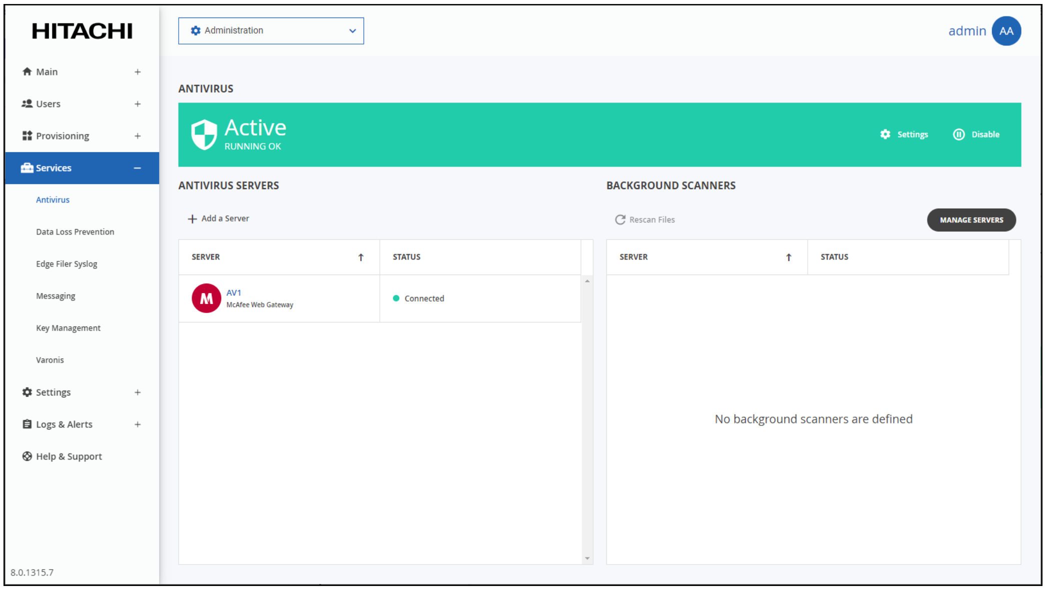
Note: The scan can take a long time, depending on the amount of data in your portal.

The following conditions apply to rescanning files:

- If a background scan has a file to scan when a rescan is initiated, the background scan completes before the rescan proceeds and files scanned during the background scan are not rescanned.
- Renaming a folder is treated as if the folder and the files in the folder are new. During a background scan the files in the folder are scanned first.

To activate background scanning:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane. The **ANTIVIRUS** page is displayed.



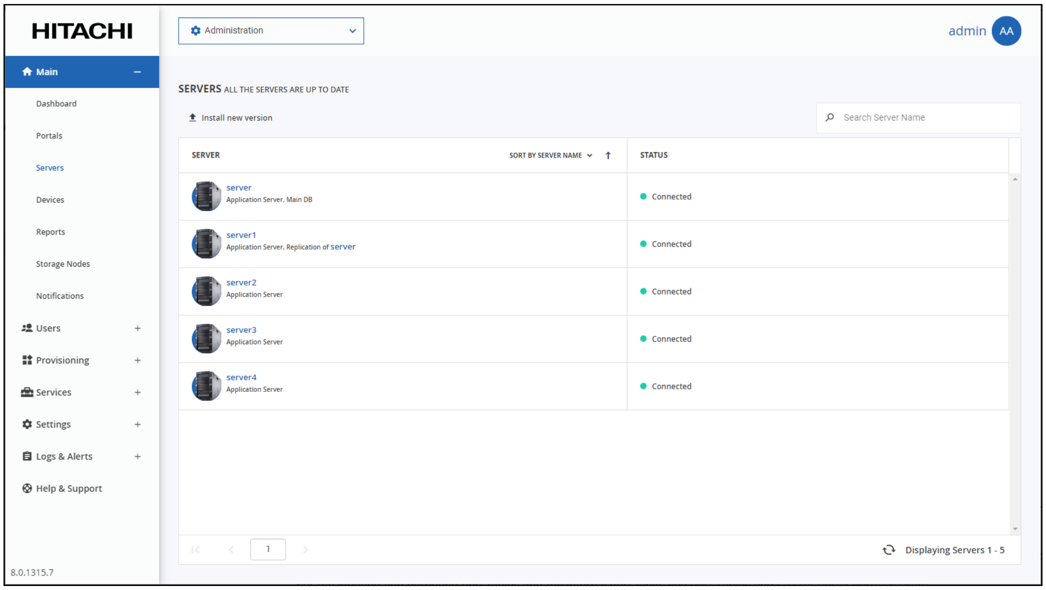
SERVER	STATUS
M AV1 McAfee Web Gateway	Connected

SERVER	STATUS

No background scanners are defined

2. Click the **MANAGE SERVERS**.

   The **SERVERS** page is displayed.



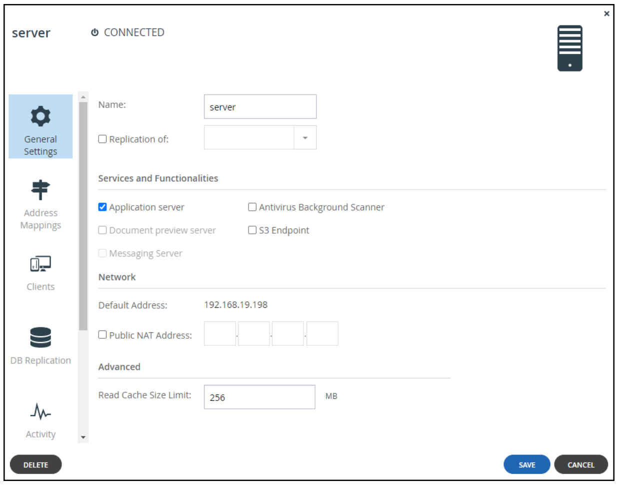
SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Note: You can access this page directly by selecting **Main > Servers** in the navigation pane.

3. Click the server to use to scan in background.

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



server CONNECTED

Name: server

□ Replication of:

Services and Functionalities

☑ Application server
□ Antivirus Background Scanner
□ Document preview server
□ S3 Endpoint
□ Messaging Server

Network

Default Address: 192.168.19.198

□ Public NAT Address:

Advanced

Read Cache Size Limit: 256 MB

4. Check **Antivirus Background Scanner**.

To rescan files:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.
2. Click **Rescan Files**.

   A confirmation windows is displayed.
3. Click **RESCAN NOW**.

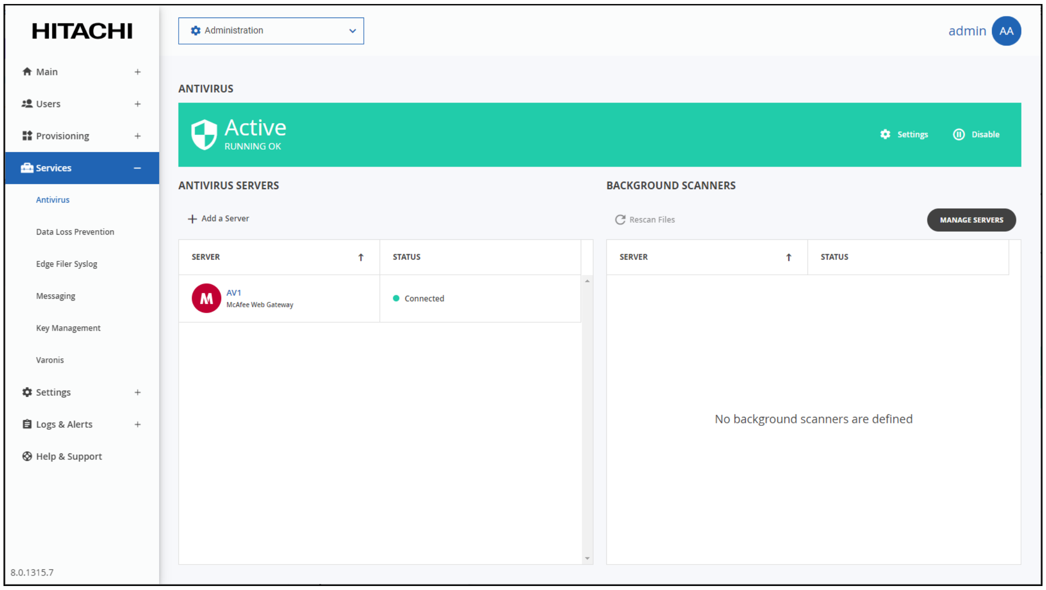
Files are scanned for viruses.

Monitoring Antivirus Scanning

You can monitor the antivirus scanning activity as well as the antivirus tasks.

To monitor antivirus scanning:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane. The **ANTIVIRUS** page is displayed.

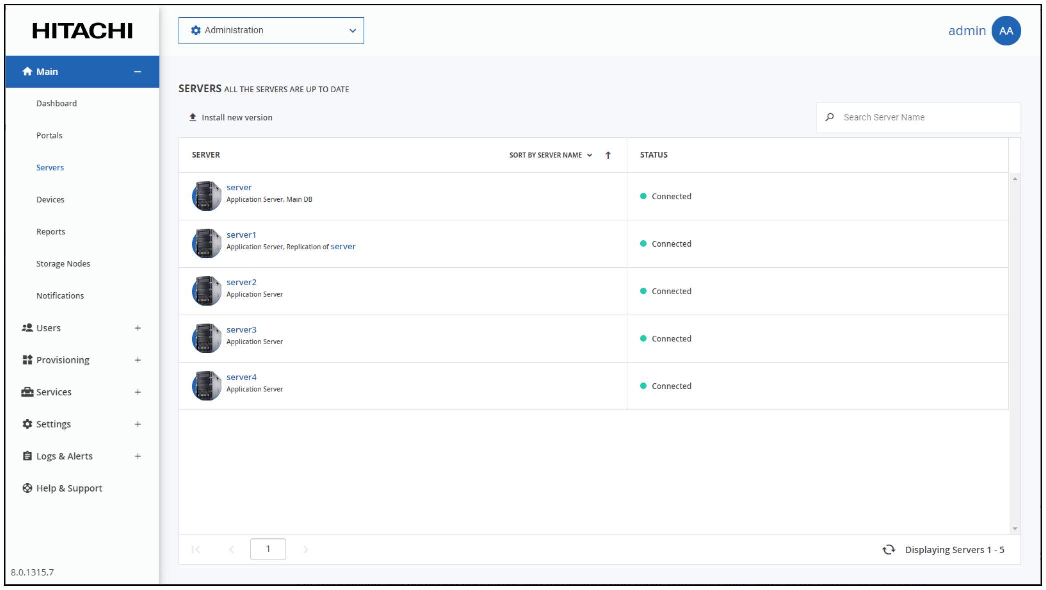


SERVER	STATUS
AV1 McAfee Web Gateway	Connected

SERVER	STATUS

No background scanners are defined

2. Click the **MANAGE SERVERS**.
   The **SERVERS** page is displayed.

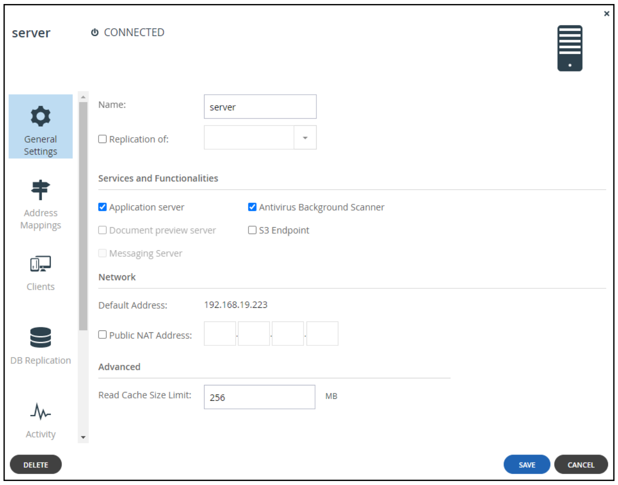


SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Note: You can access this page directly by selecting **Main > Servers** in the navigation pane.

3. Click the server to monitor.

Or, if antivirus background scanning has been defined, as described in Background Scanning and Rescanning Files, click the server under **BACKGROUND SCANNERS**.
The server window is displayed with the server name as the window title.



Name: server

□ Replication of:

Services and Functionalities

☑ Application server ☑ Antivirus Background Scanner

□ Document preview server □ S3 Endpoint

□ Messaging Server

Network

Default Address: 192.168.19.223

□ Public NAT Address:

Advanced

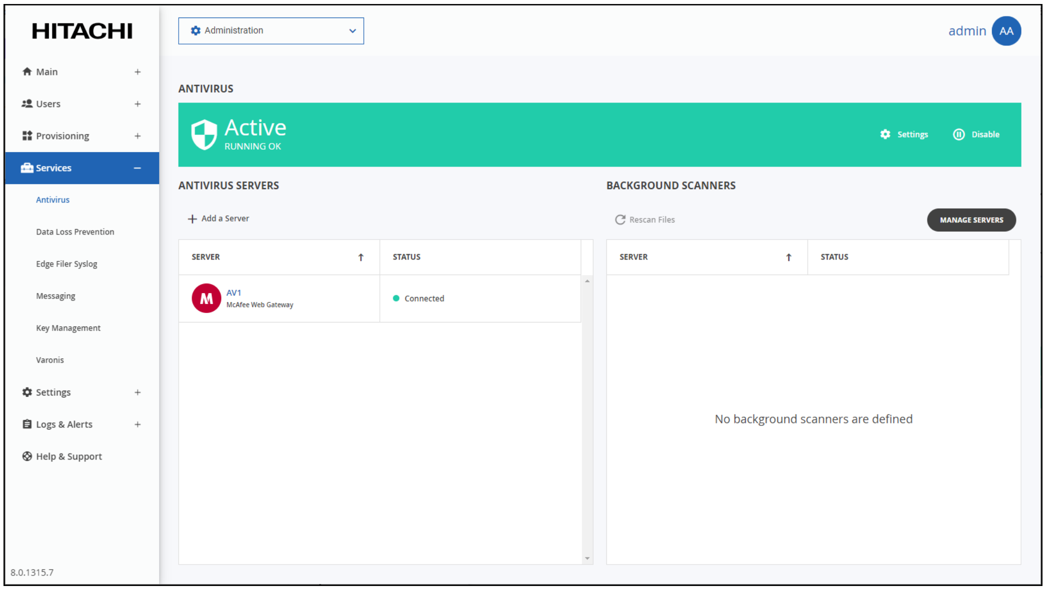
Read Cache Size Limit: 256 MB

4. In the navigation pane, scroll to **Activity**.

   The activity graphs are displayed. Scroll to the antivirus graphs to monitor antivirus activity.

To monitor antivirus tasks:

1. In the global administration view, select **Settings > Antivirus** in the navigation pane.
   The **ANTIVIRUS** page is displayed.



ANTIVIRUS

Active
RUNNING OK

ANTIVIRUS SERVERS

SERVER	STATUS
AV1 McAfee Web Gateway	Connected

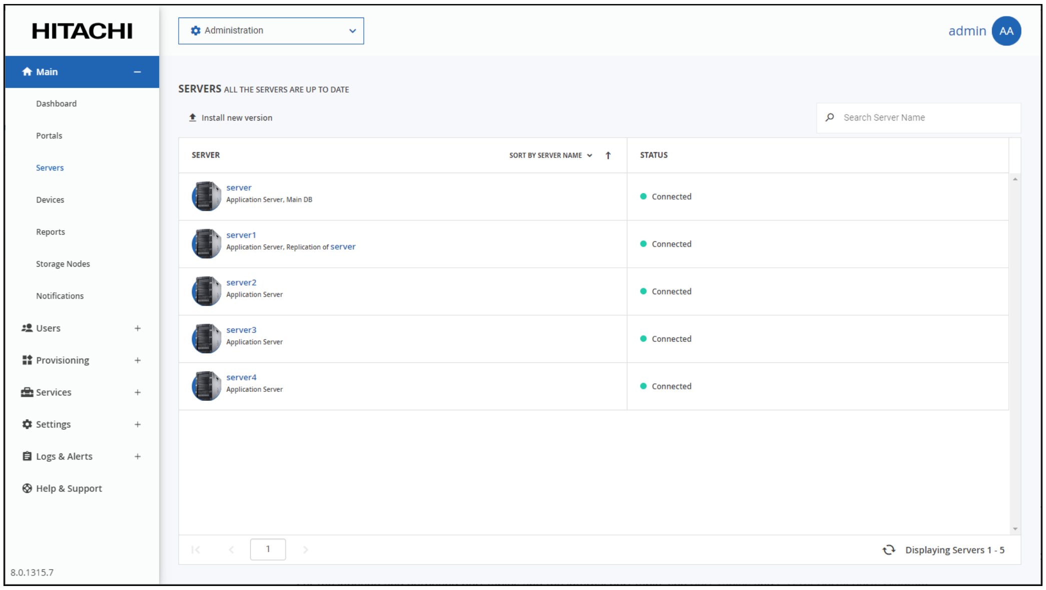
BACKGROUND SCANNERS

SERVER	STATUS

No background scanners are defined

2. Click the **MANAGE SERVERS**.

   The **SERVERS** page is displayed.



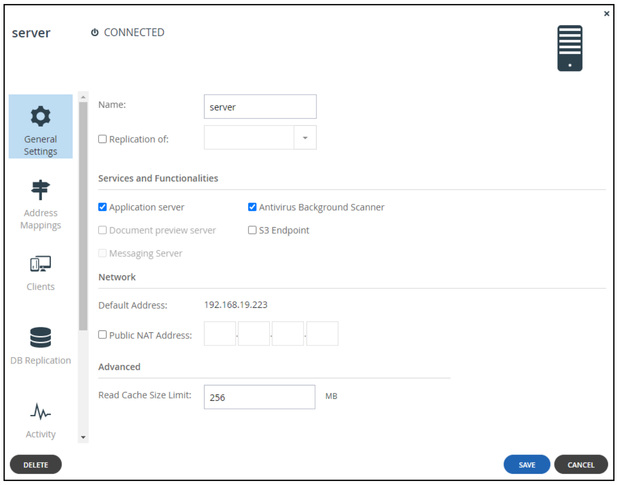
SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Note: You can access this page directly by selecting **Main > Servers** in the navigation pane.

3. Click the server to monitor.

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



server ⏻ CONNECTED

Name: server

□ Replication of:

Services and Functionalities

☑ Application server ☑ Antivirus Background Scanner

□ Document preview server □ S3 Endpoint

□ Messaging Server

Network

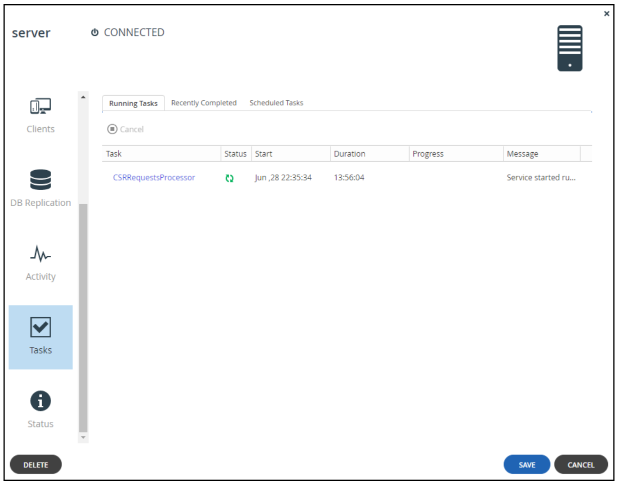
Default Address: 192.168.19.223

□ Public NAT Address:

Advanced

Read Cache Size Limit: 256 MB

4. In the navigation pane, scroll to **Tasks**.



Task	Status	Start	Duration	Progress	Message
CSRRequestsProcessor	↻	Jun ,28 22:35:34	13:56:04		Service started ru...

The tasks are displayed in the following tabs:

- Running Tasks
- Recently Completed
- Scheduled Tasks

Chapter 17. Managing the Data Loss Prevention (DLP) Service

This feature is currently not supported.

Chapter 18. Managing the HCP Anywhere Enterprise Messaging Service

The HCP Anywhere Enterprise Messaging Service enables sending notifications from the HCP Anywhere Enterprise Portal to various consumers, for example the Varonis Data Security Platform and the HCP Anywhere Enterprise Edge Filer Syslog service, which are connectors running on top of the HCP Anywhere Enterprise Messaging Service. Some features, such as managing local quotas on HCP Anywhere Enterprise Edge Filers also require the HCP Anywhere Enterprise Messaging Service.

Notifications are sent asynchronously in the background and are created in real-time from portal events.

In this chapter

HCP Anywhere Enterprise Messaging Service Requirements

The HCP Anywhere Enterprise Messaging Service must be installed on HCP Anywhere Enterprise Portal application servers and not on preview servers.

For production environments that use the messaging service, the HCP Anywhere Enterprise Portal must include three application servers defined as messaging servers, that are neither the main database server nor the replication server. For each messaging server you must **add** an extra 16GB RAM to the server RAM and a minimum of 250GB storage.

Note: The additional RAM and storage requirements for the HCP Anywhere Enterprise Messaging service must be applied to the server disk and not to the data disk.

For a POC, small, or test environment, with a single server deployment, the requirement is a 64-bit virtual machine with 4 vCPU, 32GB RAM, 250GB SSD storage.

Note: In a test deployment with messaging, you specify the primary database server as the messaging server. If you defined more than one server for the test deployment, you cannot set the primary database server as a messaging server.

Hitachi Vantara recommends contacting support to ensure correct sizing.

To move from a small POC environment to a production environment, see Moving From a Single Server Environment to a Multiple Server Environment.

Enabling the HCP Anywhere Enterprise Messaging Service

Before you can set up the HCP Anywhere Enterprise Messaging Service in the user interface, you must first initialize the messaging components by running the following CLI:

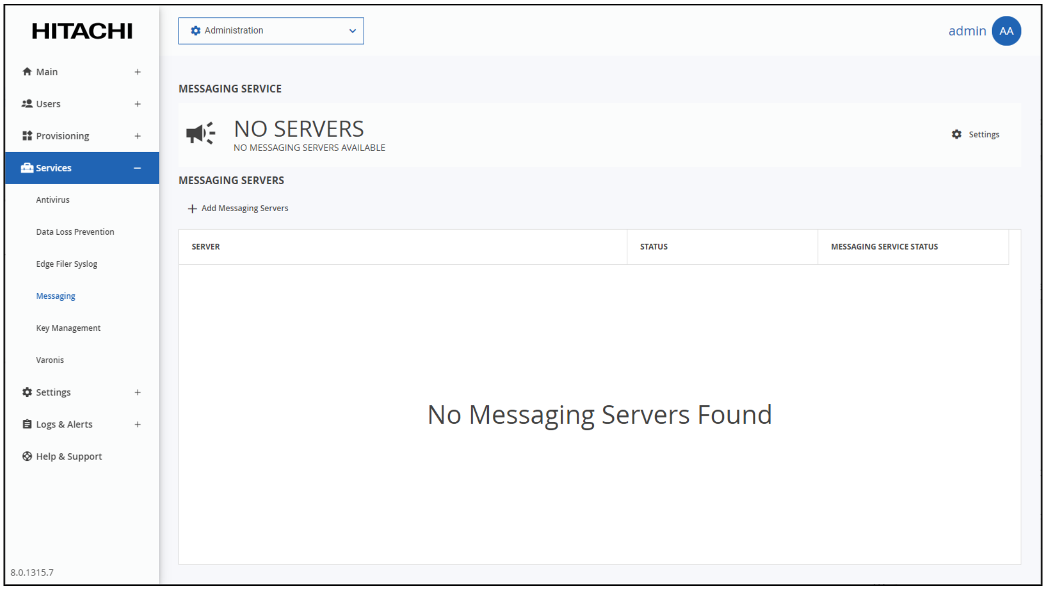
```
set /settings/platformServicesSetting/enabled true
```

Initializing the messaging components takes a few minutes.

Setting Up the HCP Anywhere Enterprise Messaging Service

To set up the HCP Anywhere Enterprise Messaging Service:

1. In the global administration view, select **Services > Messaging** in the navigation pane.
   The **MESSAGING SERVICE** page is displayed.



MESSAGING SERVICE

NO SERVERS
NO MESSAGING SERVERS AVAILABLE

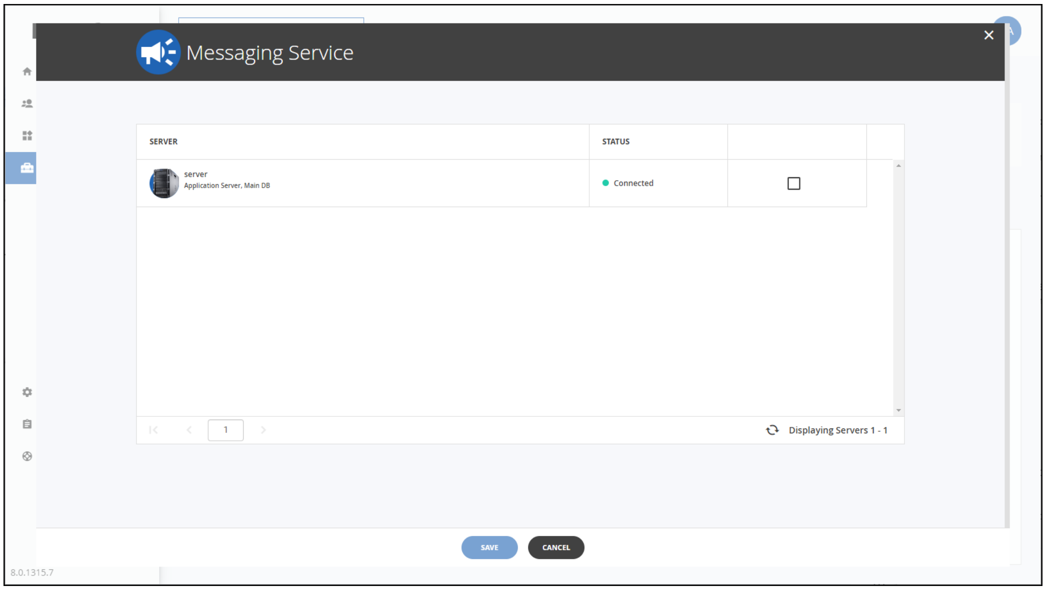
MESSAGING SERVERS

SERVER	STATUS	MESSAGING SERVICE STATUS

No Messaging Servers Found

2. To add a new messaging server, click **Add Messaging Servers**.
   The **Messaging Service** window is displayed, showing all the HCP Anywhere Enterprise Portal Servers.

In a test environment with one server:

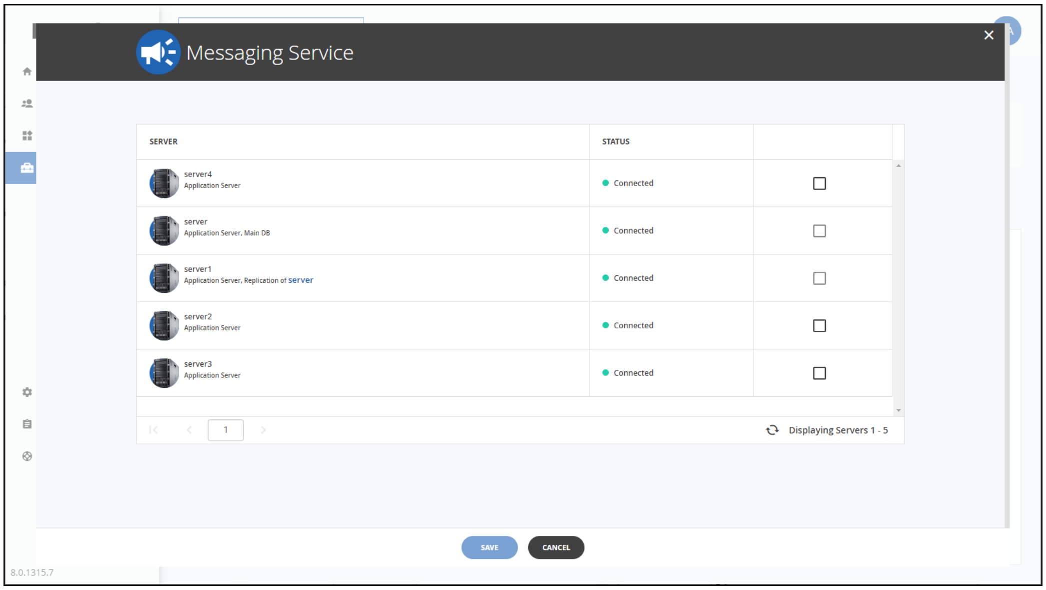


Messaging Service

SERVER	STATUS	
server Application Server, Main DB	● Connected	□

Displaying Servers 1 - 1

In a production environment with at least five servers:



Messaging Service

SERVER	STATUS	
server4 Application Server	● Connected	□
server Application Server, Main DB	● Connected	□
server1 Application Server, Replication of server	● Connected	□
server2 Application Server	● Connected	□
server3 Application Server	● Connected	□

Displaying Servers 1 - 5

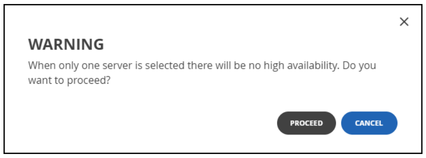
3. Check the servers you want to use as messaging servers.

   In a production environment, you must select three servers to be messaging servers. HCP Anywhere Enterprise allows a single messaging server in a small or test environment where the main database server is the only server. Otherwise you have to assign three, and only three, servers as messaging servers.

   Note: Unless the main database server is the only server, if you try to check the main database server, the replication server, or a preview server, a message is displayed.

4. Click **SAVE**.

   Note: If you only selected one server to be a messaging server, a warning is displayed.

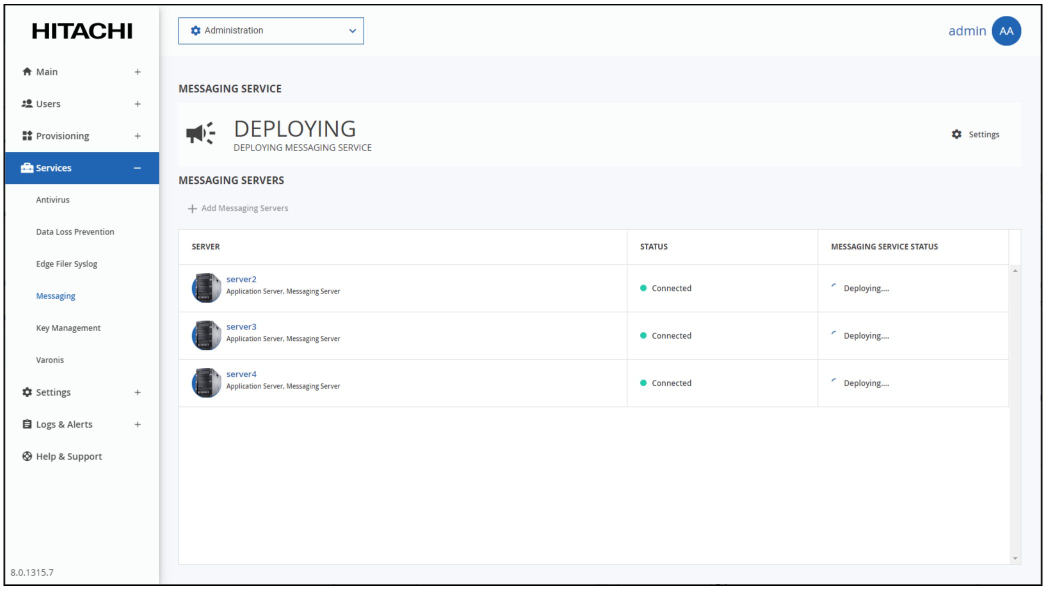


WARNING

When only one server is selected there will be no high availability. Do you want to proceed?

If the messaging components are not initialized, a message is displayed.

The selected servers are added as messaging servers.



MESSAGING SERVICE

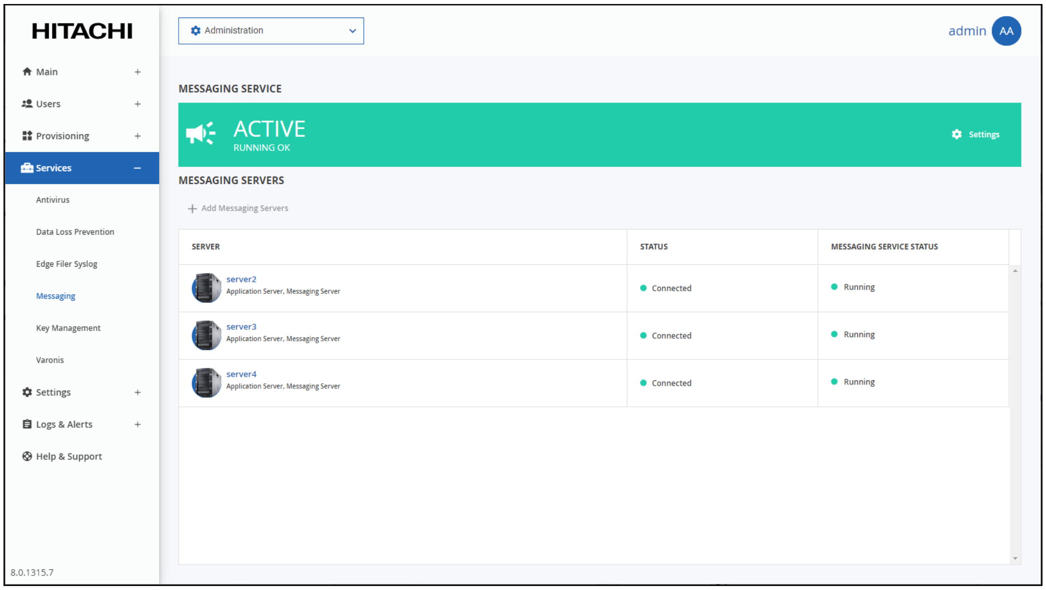
DEPLOYING

DEPLOYING MESSAGING SERVICE

MESSAGING SERVERS

SERVER	STATUS	MESSAGING SERVICE STATUS
server2 Application Server, Messaging Server	● Connected	Deploying....
server3 Application Server, Messaging Server	● Connected	Deploying....
server4 Application Server, Messaging Server	● Connected	Deploying....

Deploying the servers for the messaging service takes a few minutes, after which the status changes to **STARTING**. After the messaging service starts running, the status changes to **ACTIVE**.



MESSAGING SERVICE

ACTIVE

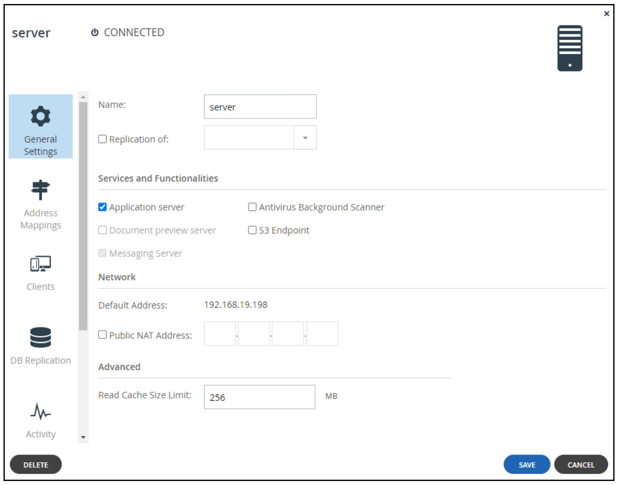
RUNNING OK

MESSAGING SERVERS

SERVER	STATUS	MESSAGING SERVICE STATUS
server2 Application Server, Messaging Server	● Connected	● Running
server3 Application Server, Messaging Server	● Connected	● Running
server4 Application Server, Messaging Server	● Connected	● Running

Note: The process of deploying and starting the messaging service takes a few minutes. You cannot start to configure any other service that requires the messaging service, such as Varonis, until the messaging service is running.

Clicking a server displays the server window with the server name as the window title. The **Messaging Server** box is checked.



server   CONNECTED

Name: server

☐ Replication of:

Services and Functionalities

☑ Application server   ☐ Antivirus Background Scanner

☐ Document preview server   ☐ S3 Endpoint

☑ Messaging Server

Network

Default Address: 192.168.19.198

☐ Public NAT Address:

Advanced

Read Cache Size Limit: 256 MB

You cannot uncheck this service.

Messaging Service Statuses

The messaging service is in one of the following statuses:

- **NO SERVERS: NO MESSAGING SERVERS AVAILABLE** – No servers have been defined as messaging servers.
- **DEPLOYING: DEPLOYING MESSAGING SERVICE** – The servers defined as messaging servers are being deployed. This status is displayed after defining messaging servers and takes a few minutes for the service to be deployed on the servers.
- **STARTING: COLLECTING MESSAGING SERVICE STATUS** – After the messaging service has been deployed, the portal starts to gather information before the service becomes active.
- **ACTIVE: RUNNING OK** – The messaging service is up and running.
- **WARNING: SOMETHING WRONG WITH SOME OF THE SERVERS** – At least one messaging server is working but one or more messaging servers have problems. The messaging service is still running but the problematic messaging servers need attention.
- **ERROR: MESSAGING SERVICE HAS FAILED** – The messaging service is not working.
- **ERROR: COULDN'T FETCH MESSAGING SERVICE STATUS** – The collection of the messaging service status failed.
- **READ-ONLY MODE: NOT ENOUGH AVAILABLE STORAGE ON THE MESSAGING SERVER** – The available storage for the messaging service logs has dropped to 4GB or less. The messaging server is in read-only mode until more space is freed up. Message retention in the logs can be set to help prevent this status. For details, see HCP Anywhere Enterprise Messaging Service Logs.

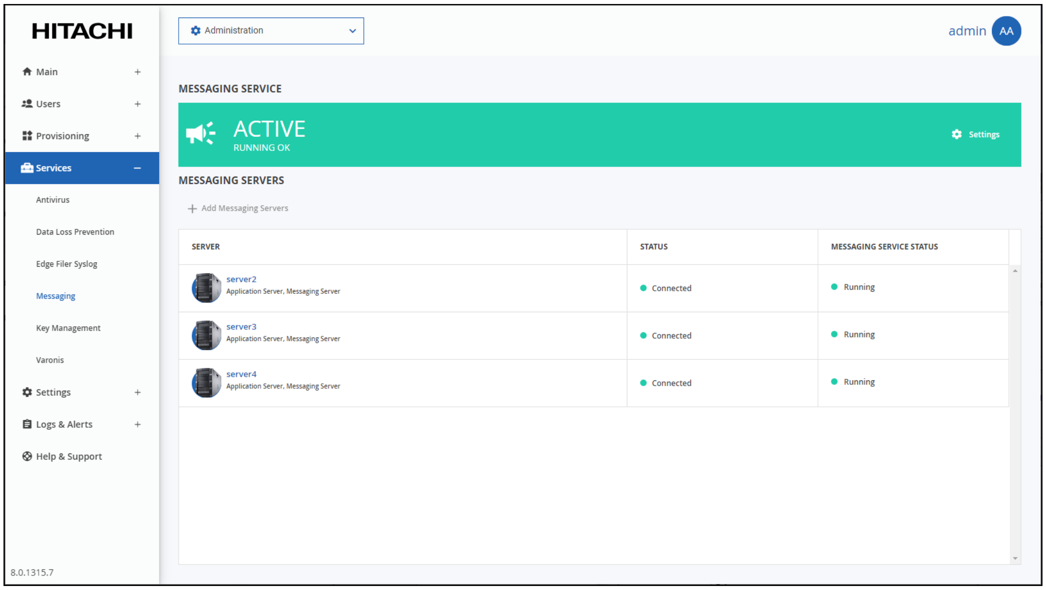
HCP Anywhere Enterprise Messaging Service Logs

All HCP Anywhere Enterprise services that require the HCP Anywhere Enterprise Messaging service, for example the Varonis log, write to the same volume.

In order that the logs do not grow too large, which can cause storage issues, you can set how long messages in the logs are retained.

To set the messaging service logs retention:

1. In the global administration view, select **Services > Messaging** in the navigation pane.
   The **MESSAGING SERVICE** page is displayed.



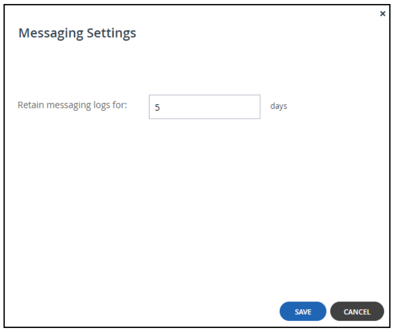
MESSAGING SERVICE

ACTIVE
RUNNING OK

MESSAGING SERVERS

SERVER	STATUS	MESSAGING SERVICE STATUS
server2 Application Server, Messaging Server	● Connected	● Running
server3 Application Server, Messaging Server	● Connected	● Running
server4 Application Server, Messaging Server	● Connected	● Running

2. Click **Settings** in the status bar and click **Configure Service**.
   The **Message Settings** window is displayed.



Messaging Settings

Retain messaging logs for: 5 days

3. Set the number of days messages should be retained.
4. Click **SAVE**.

Replacing a Messaging Server

You can replace a messaging server with another server.

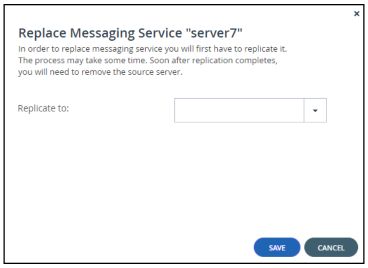
Note: When three servers are specified as messaging servers, you cannot add another server, but only replace an existing messaging server.

To replace a messaging server:

1. In the global administration view, select **Services > Messaging** in the navigation pane. The **MESSAGING SERVICE** page is displayed.
2. Select the row for the messaging server to replace.

   Note: The **Replace Messaging Server** option is only available if there is a server that can be used as a replacement.
3. Click **Replace Messaging Server**.

   The **Replace Messaging Server *serverName*** window is displayed.

   Replace Messaging Service "server7"

   In order to replace messaging service you will first have to replicate it. The process may take some time. Soon after replication completes, you will need to remove the source server.

   Replicate to:

4. Select the replacement server from the **Replicate to** list box.
5. Click **SAVE**.

   The server is replaced. This can take a few minutes.
6. Click **Remove Service** from the original server and then click **REMOVE** in the confirmation window that is displayed.

The server is removed from the list of servers.

Messaging Service Errors

The status in the **MESSAGING SERVICE** page changes to an error if all the messaging servers are down but only to a warning if at least one messaging server is still running.

Problems with the HCP Anywhere Enterprise Messaging Service are displayed, with the reason, either as part of the status bar message or the **MESSAGING SERVICE STATUS** field.

The **ERROR** banner can also provide information. For example, when there is not enough available storage on the messaging server the banner status is **READ-ONLY MODE** instead of **ERROR**:

When more than one messaging server is deployed, high availability (HA) is employed. As long as the status one of them is **ACTIVE**, the HCP Anywhere Enterprise Messaging Service continues to function properly.

Moving From a Single Server Environment to a Multiple Server Environment

In production with the HCP Anywhere Enterprise messaging service, the minimal production installation comprises of five servers: Two database servers (primary and secondary), and three application servers that also function as messaging servers. Therefore, to move from a single server test environment to a multiple server production environment requires adding at least four servers: one for replicating the primary database server and three as messaging servers.

Note: The servers for messaging require 4 vCPU, 32GB RAM, 250GB data pool (Magnetic) each. For details, refer to requirements in the installation guide for the environment.

To move to a production environment:

1. Add the additional servers, defining one server as a replication server, as described in the installation guide for the environment.
2. Configure two servers as messaging servers.

   Note: When setting up the messaging service, as described in Setting Up the HCP Anywhere Enterprise Messaging Service, you have to add two servers so that the total messaging servers are three. You cannot add one server at a time to the existing messaging server.
3. Replace the messaging service from the original primary database server with the third application server, as described in Replacing a Messaging Server.

Note: All existing messaging data from the single messaging server is erased.

Chapter 19. Managing the Key Management Service

Enterprises running services and applications that need to perform cryptographic operations, can delegate the key management task to an external provider using the Key Management Interoperability Protocol (KMIP). KMIP simplifies the way you manage cryptographic keys, eliminating the need for redundant, incompatible key management processes.

In HCP Anywhere Enterprise Portal, each folder group has an AES-256 data encryption key used for data-at-rest encryption of all the blocks in this folder group. The data encryption keys for each folder group are stored in the HCP Anywhere Enterprise Portal metadata database. When Key Management is enabled, each data encryption key in the database is stored encrypted and this encryption is performed with a separate key encryption key (KEK) that is obtained from the Key Management Server. The key encryption key is never stored persistently outside of the key management server, and can be rotated periodically on a configurable schedule by the Key Management Server.

HCP Anywhere Enterprise Portal integrates with *Thales CipherTrust Manager* for the Key Management Server.

Note: A license from Hitachi Vantara is required to use the Key Management service.

In this chapter

- Setting up Key Management for a HCP Anywhere Enterprise Portal
- Changing a Key Management Certificate
- Deleting a Key Management Server
- Removing the Key Management Service

Setting up Key Management for a HCP Anywhere Enterprise Portal

Setting up key management involves the following steps:

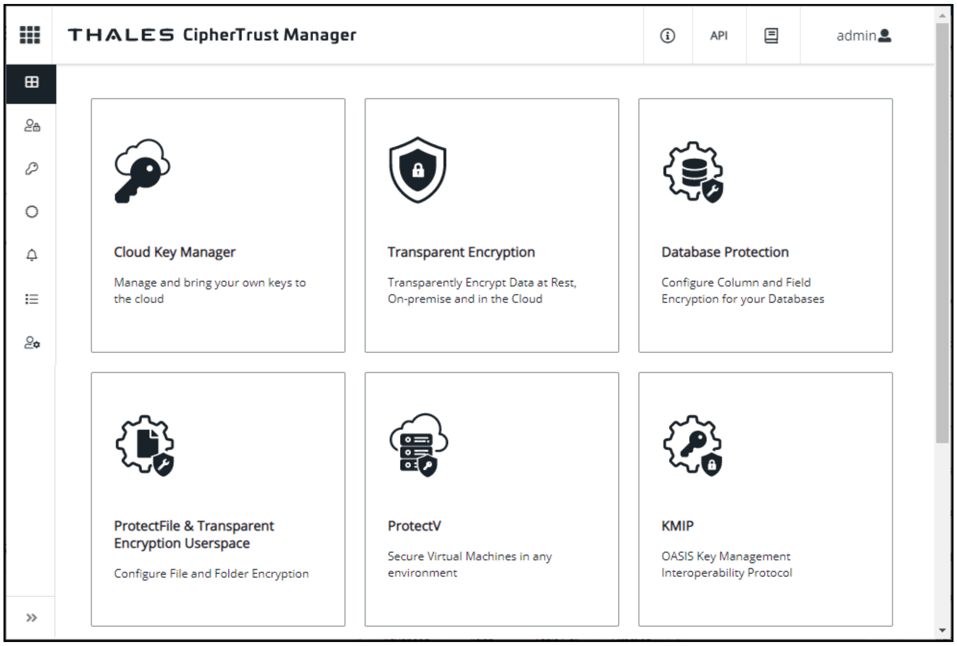
- Generating Keys for the Key Management Service
- Setting Up the HCP Anywhere Enterprise Portal Key Management Service
- Managing Key Management Servers in HCP Anywhere Enterprise Portal

Generating Keys for the Key Management Service

The server and client keys are generated in Thales CipherTrust Manager. The procedures described below use a local server certificate. If you want to use an external server certificate, replace **Local** with **External** in the procedures.

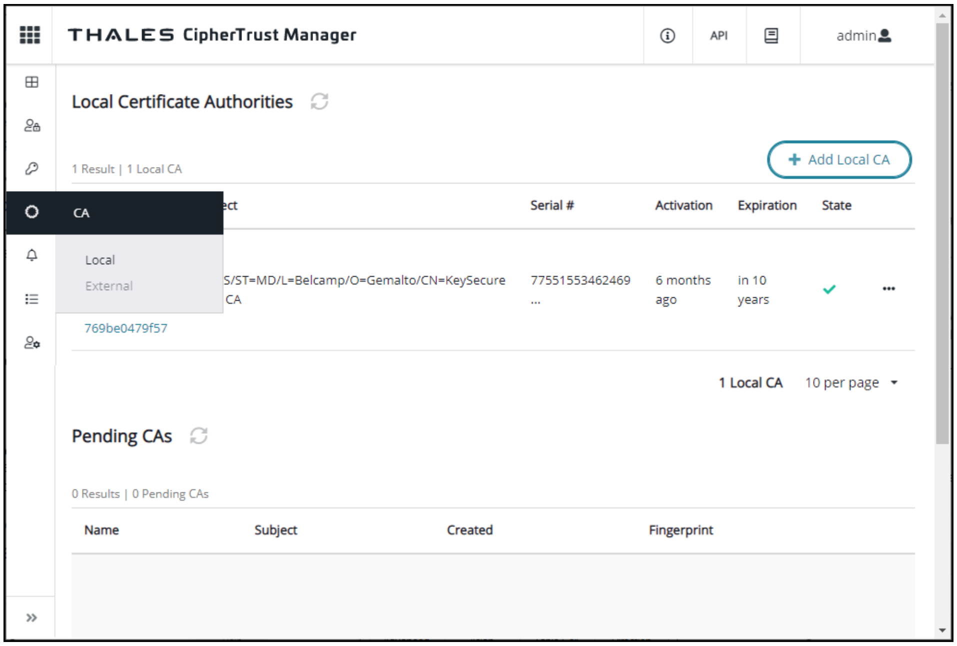
To add the server certificate to Thales CipherTrust Manager:

1. Access the Thales CipherTrust Manager as an administrator.



THALES CipherTrust Manager
API
admin
Cloud Key Manager
Manage and bring your own keys to the cloud
Transparent Encryption
Transparently Encrypt Data at Rest, On-premise and in the Cloud
Database Protection
Configure Column and Field Encryption for your Databases
ProtectFile & Transparent Encryption Userspace
Configure File and Folder Encryption
ProtectV
Secure Virtual Machines in any environment
KMIP
OASIS Key Management Interoperability Protocol

2. Click the **CA > Local** in the navigation pane.
   The **Local Certificate Authorities** page is displayed.



1 Result | 1 Local CA

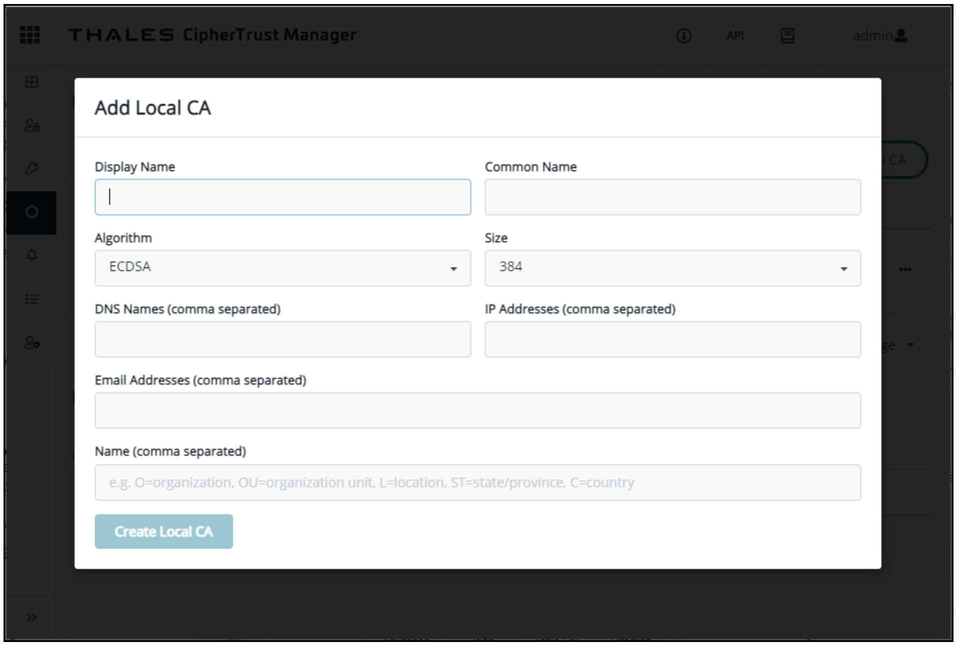
...ect	Serial #	Activation	Expiration	State
S/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure CA 769be0479f57	77551553462469 ...	6 months ago	in 10 years	✓

1 Local CA

0 Results | 0 Pending CAs

Name	Subject	Created	Fingerprint

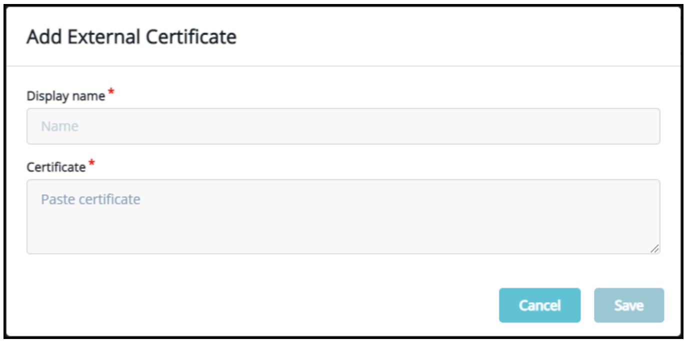
3. Click the **Add Local CA**.
   The **Add Local CA** window is displayed.


THALES CipherTrust Manager
API
admin
Add Local CA
Display Name
Common Name
DNS Names (comma separated)
IP Addresses (comma separated)
Email Addresses (comma separated)
Name (comma separated)
e.g. O=organization, OU=organization unit, L=location, ST=state/province, C=country
Create Local CA

Algorithm: ECDSA

Size: 384

Note: If using an external certificate, you copy and paste the certificate in the following window and click **Save**:



Add External Certificate

Display name *

Name

Certificate *

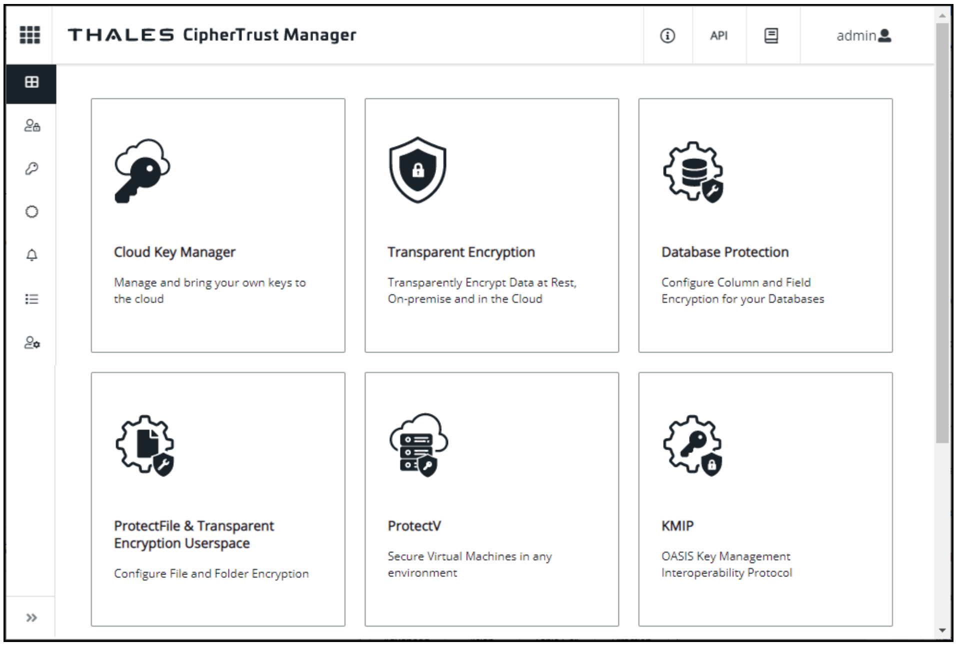
Paste certificate

4. Enter the information for the certificate and click **Create Local CA**.

   The **Local Certificate Authorities** page is redisplayed, showing the local server certificate.
5. Click the ellipsis (. . .) on the right of the certificate and then click **Download**.

To generate the client private key and certificate:

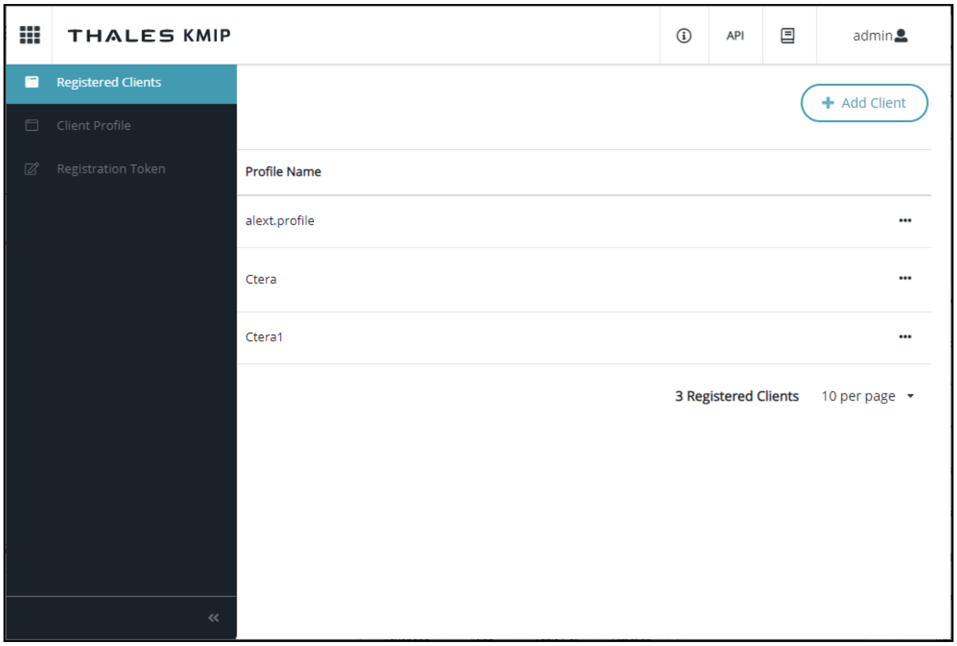
1. Access the Thales CipherTrust Manager as an administrator.



THALES CipherTrust Manager
API
admin
Cloud Key Manager
Manage and bring your own keys to the cloud
Transparent Encryption
Transparently Encrypt Data at Rest, On-premise and in the Cloud
Database Protection
Configure Column and Field Encryption for your Databases
ProtectFile & Transparent Encryption Userspace
Configure File and Folder Encryption
ProtectV
Secure Virtual Machines in any environment
KMIP
OASIS Key Management Interoperability Protocol

2. Click the **KMIP** product.

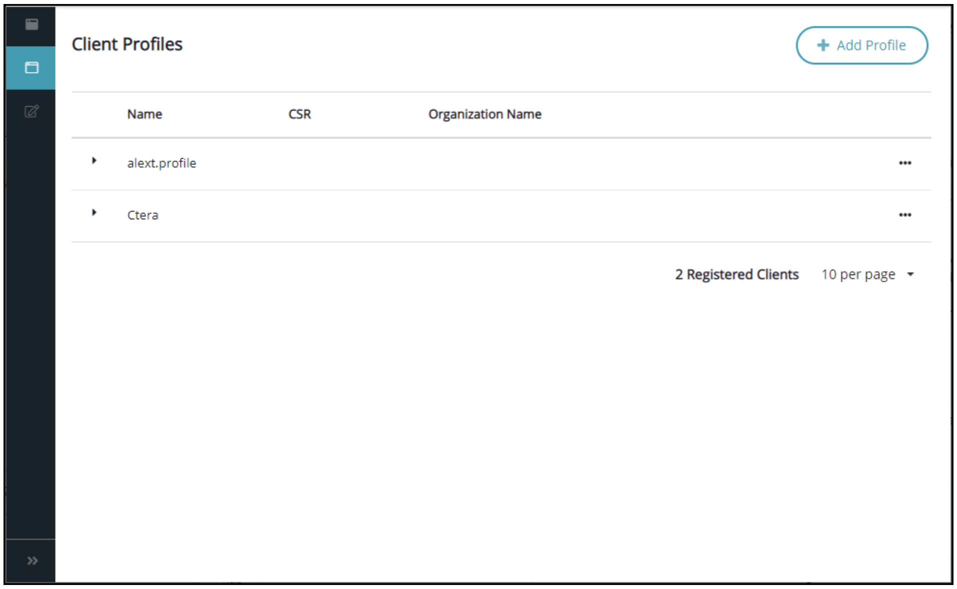
   The **Registered Clients** page is displayed.



Profile Name
alext.profile
Ctera
Ctera1

3 Registered Clients 10 per page

3. Click the **Client Profile** in the navigation pane.
   The **Client Profiles** page is displayed.

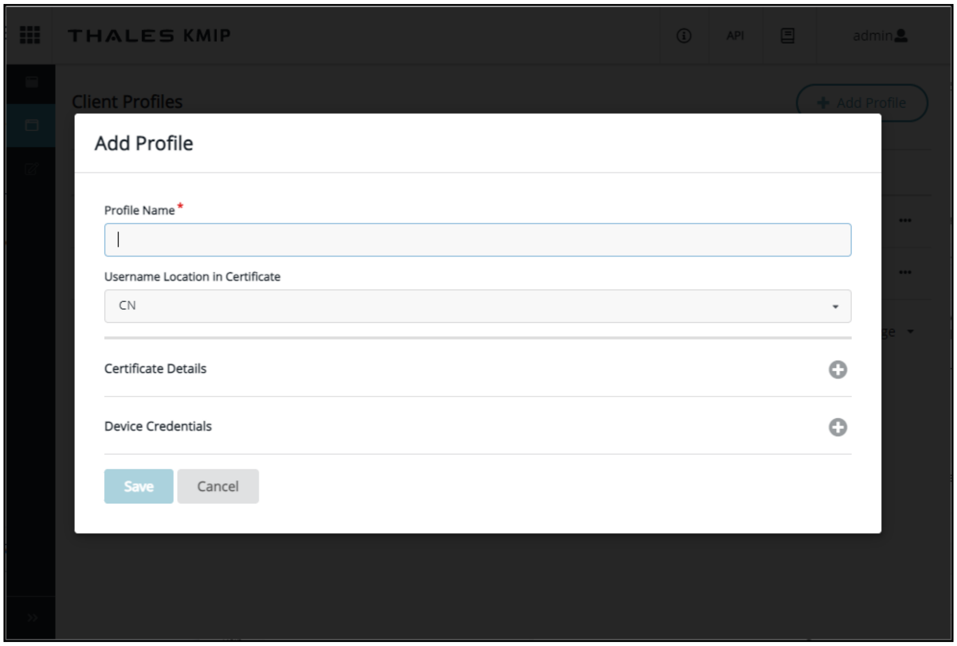


Client Profiles

Name	CSR	Organization Name
alext.profile		
Ctera		

2 Registered Clients 10 per page

4. Click the **Add Profile**.
   The **Add Profile** window is displayed.



Add Profile

Profile Name*

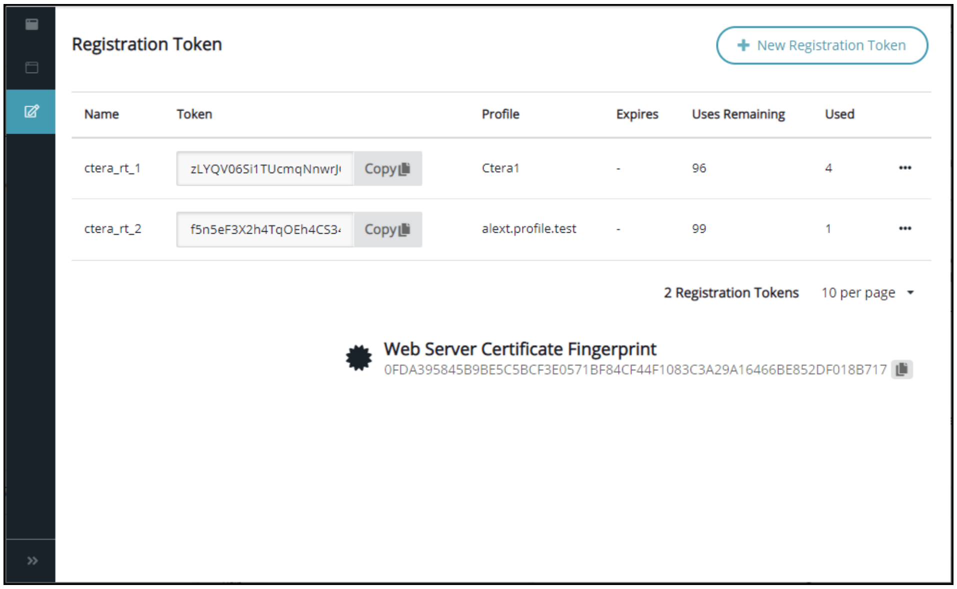
Username Location in Certificate: CN

Certificate Details

Device Credentials

5. Enter a **Profile Name** and click **Save**.
6. Click **Registration Token** in the navigation pane.

   The **Registration Token** page is displayed.



Registration Token

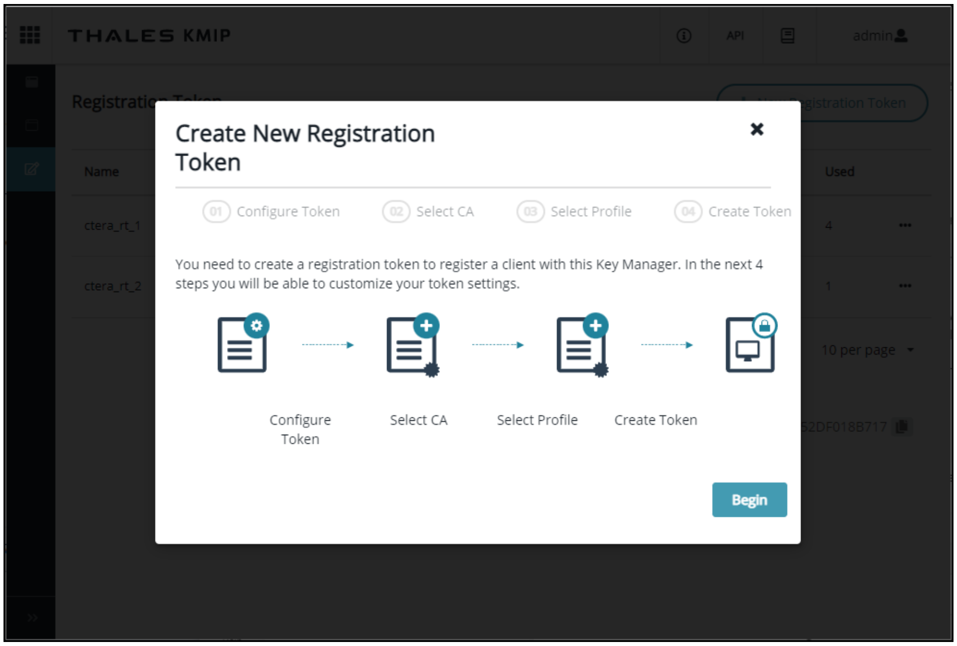
Name	Token	Profile	Expires	Uses Remaining	Used
ctera_rt_1	zLYQV06Si1TUcmqNnwrJ	Ctera1	-	96	4
ctera_rt_2	f5n5eF3X2h4TqOEh4CS3	alext.profile.test	-	99	1

2 Registration Tokens 10 per page

Web Server Certificate Fingerprint
0FDA395845B9BE5C5BCF3E0571BF84CF44F1083C3A29A16466BE852DF018B717

7. Click New **Registration Token**.

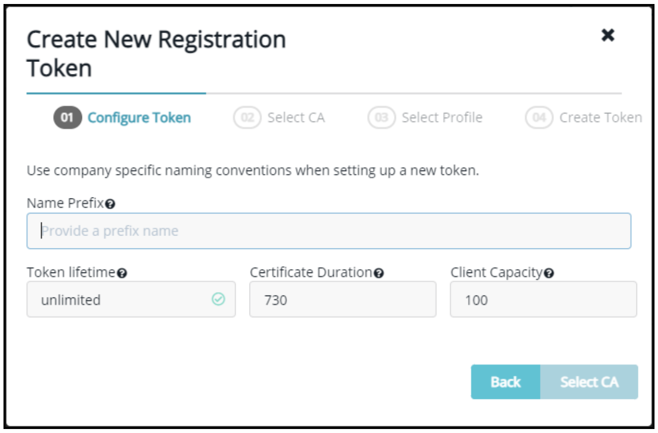
   The **Create New Registration Token** window is displayed.



Create New Registration Token

You need to create a registration token to register a client with this Key Manager. In the next 4 steps you will be able to customize your token settings.

8. Click **Begin**.



Create New Registration Token

Use company specific naming conventions when setting up a new token.

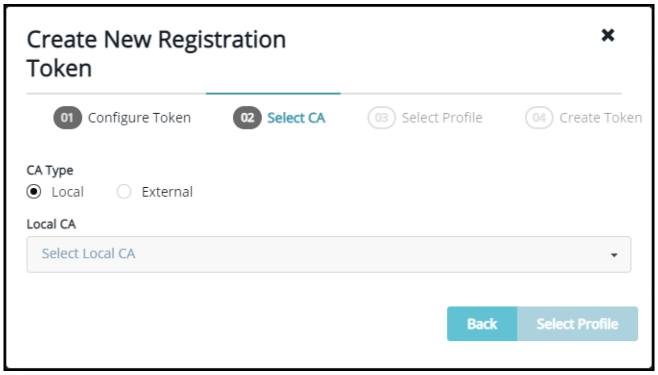
Name Prefix: Provide a prefix name

Token lifetime: unlimited

Certificate Duration: 730

Client Capacity: 100

9. Provide a **Name prefix** for the token and click **Select CA**.



Create New Registration Token

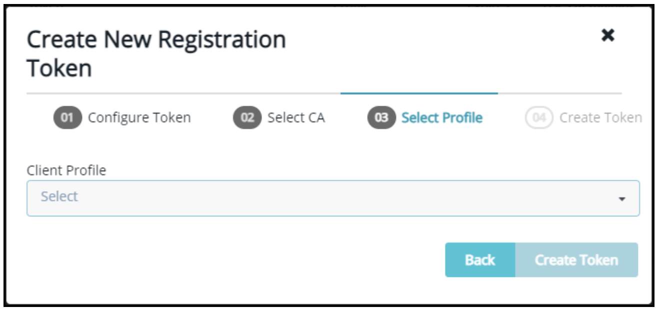
CA Type
● Local ○ External

Local CA: Select Local CA

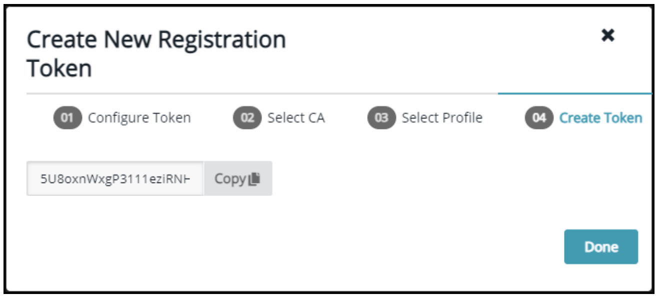
10. Choose **Local CA** and select the CA from the drop-down list. This is the certificate added to

Thales CipherTrust Manager in step 5 in the To add the server certificate to Thales CipherTrust Manager: procedure.

11. Click **Select Profile**.



12. Choose either the **Client Profile** from the drop-down list and click **Create Token**.



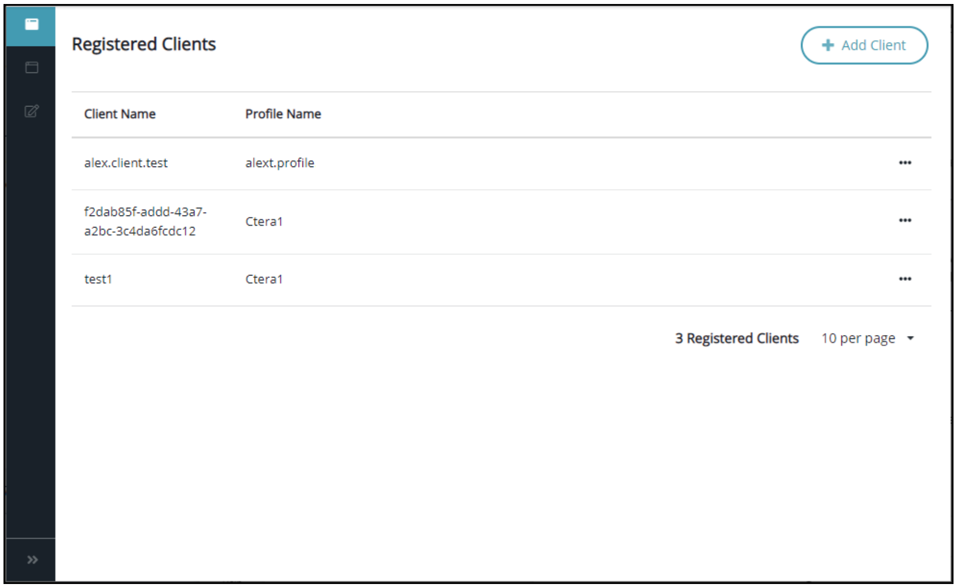
5U8oxnWxgP3111eziRNH

13. Copy the token and click **Done**.

    The **Registration Token** page is redisplayed, showing the token that was created.

14. Click **Registered Clients** in the navigation pane.

    The **Registered Clients** page is displayed.

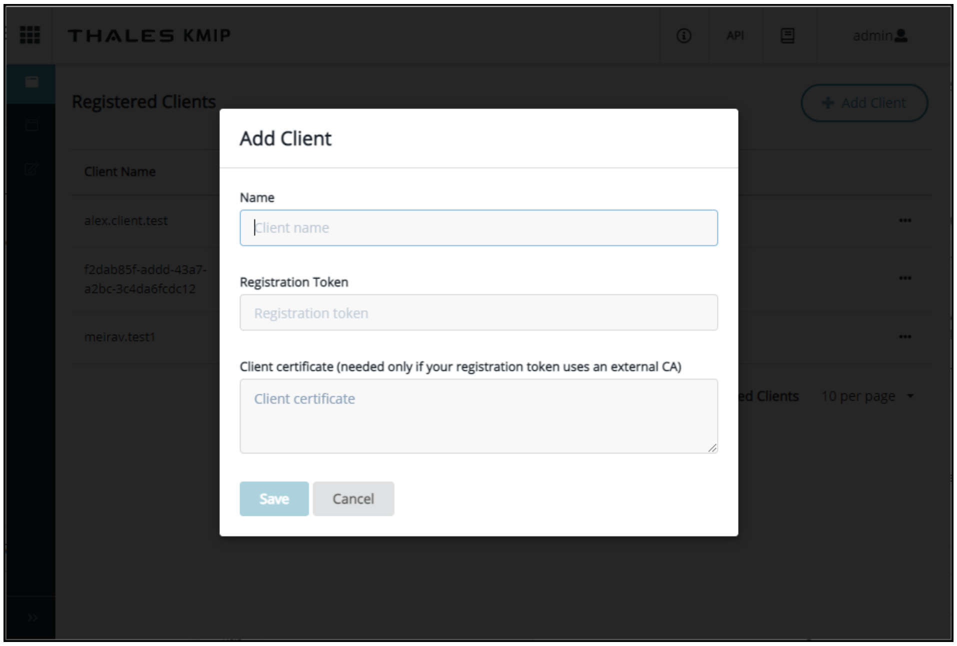


Client Name	Profile Name	
alex.client.test	alext.profile	•••
f2dab85f-addd-43a7-a2bc-3c4da6fcdc12	Ctera1	•••
test1	Ctera1	•••

3 Registered Clients 10 per page

15. Click **Add Client**.

    The **Add Client** window is displayed.



Add Client

Name

Client name

Registration Token

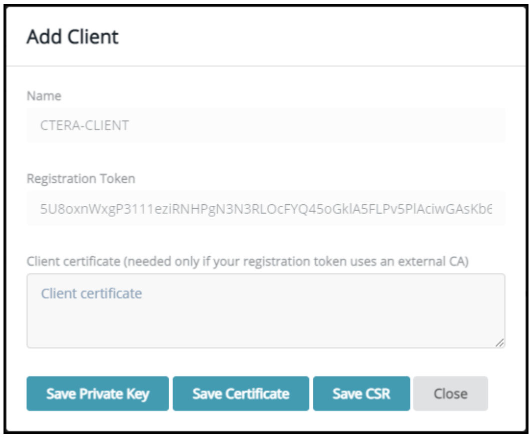
Registration token

Client certificate (needed only if your registration token uses an external CA)

Client certificate

16. Enter a **Name** and the **Registration Token**, copied in step 13 and, if required, the **Client certificate** and click **Save**.

    The **Add Client** window is displayed with buttons to download the client private key and certificate and a CSR.



Add Client

Name

CTERA-CLIENT

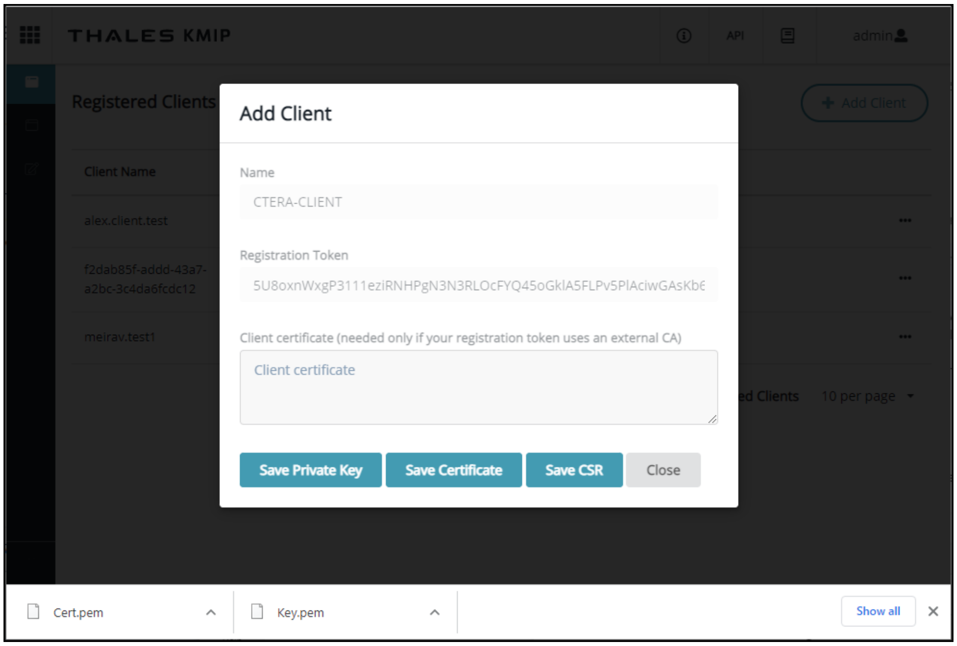
Registration Token

5U8oxnWxgP3111eziRNHPgN3N3RLOcFYQ45oGklA5FLPv5PlAciwGAsKb6

Client certificate (needed only if your registration token uses an external CA)

Client certificate

17. Click the **Save Private key** and **Save Certificate** buttons to download the private key and client certificate.



Add Client

Name: CTERA-CLIENT

Registration Token: 5U8oxnWxgP3111eziRNHPgN3N3RLOcFYQ45oGklA5FLPv5PlAciwGAsKb6

Client certificate (needed only if your registration token uses an external CA): Client certificate

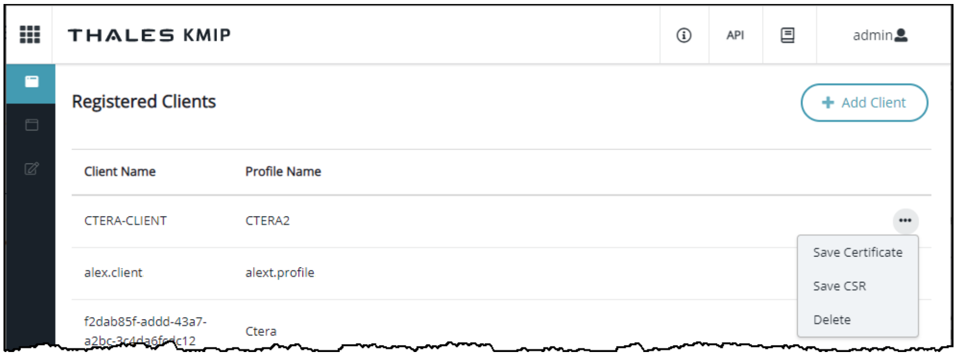
Client Name
alex.client.test
f2dab85f-addd-43a7-a2bc-3c4da6fcdc12
meirav.test1

Cert.pem

Key.pem

Warning: **If you do not download the private key, you cannot get it later and will not be able to set up key management in HCP Anywhere Enterprise Portal with the this key and certificate.**

Note: You can download the certificate later.



Registered Clients

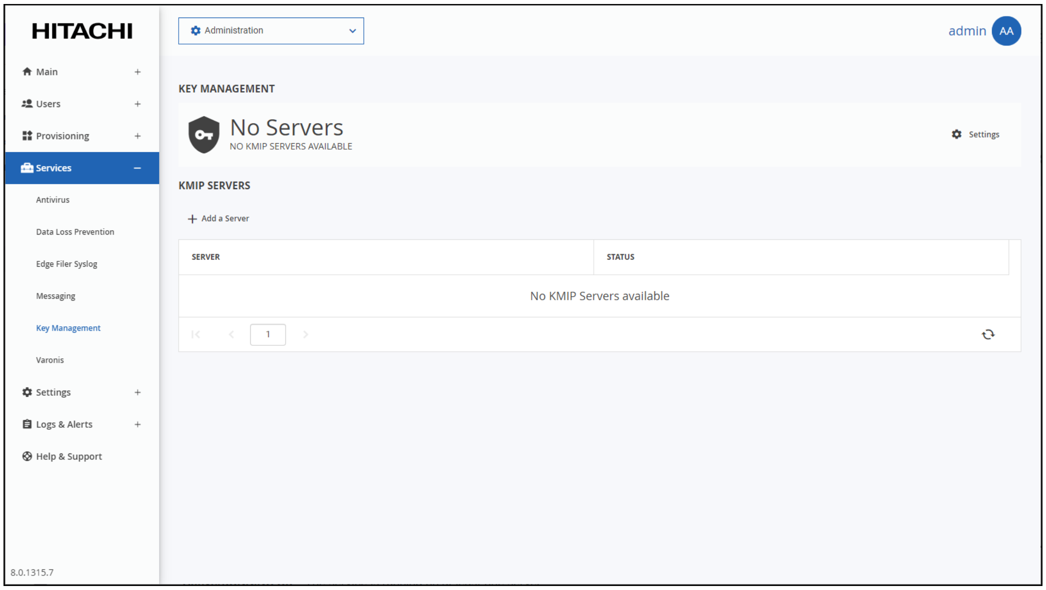
Client Name	Profile Name
CTERA-CLIENT	CTERA2
alex.client	alext.profile
f2dab85f-addd-43a7-a2bc-3c4da6fcdc12	Ctera

Setting Up the HCP Anywhere Enterprise Portal Key Management Service

You can specify key management server settings and authentication specifications.

To set up key management:

1. In the global administration view, select **Services > Key Management** in the navigation pane. The **KEY MANAGEMENT** page is displayed.



KEY MANAGEMENT

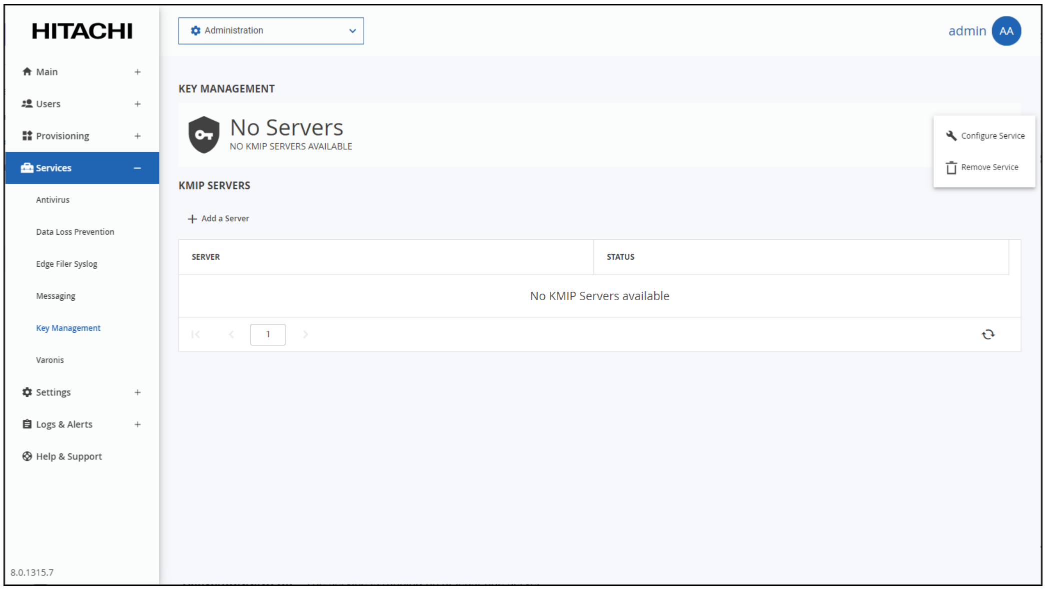
No Servers
NO KMIP SERVERS AVAILABLE

KMIP SERVERS

SERVER	STATUS
No KMIP Servers available	

The **Status** bar at the top of the page shows the current status:
Active/RUNNING OK – The server is running on at least one server.
Disabled/NOT RUNNING – The HCP Anywhere Enterprise Portal is not licensed for key management.
Error/ALL KEY MANAGEMENT SERVERS ARE OFFLINE – There is an error with the key management service.
Failed/INTERNAL ERROR – There is a error with the key management service.
No Servers/NOT RUNNING – A key management server has not been defined. To set up a server, see Setting up Key Management for a HCP Anywhere Enterprise Portal.
Warning – There is a problem with the key management service. The status message is one of the following:
    REMOVING THE SERVICE...
    FAILED TO REMOVE SERVICE
    SOME KEY MANAGEMENT SERVERS ARE OFFLINE
    KEY MANAGEMENT SERVICE IS IN WARNING STATE

2. Click **Settings** in the **KEY MANAGEMENT** bar to configure the key management settings.



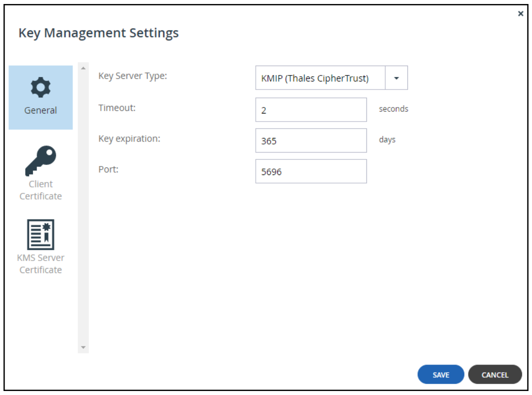
No Servers

NO KMIP SERVERS AVAILABLE

No KMIP Servers available

3. Click **Configure Service**.

   The **Key Management Settings** window is displayed.



Key Management Settings

Key Server Type: KMIP (Thales CipherTrust)

Timeout: 2 seconds

Key expiration: 365 days

Port: 5696

Key Server Type – The type of key manager server. Currently, only *Thales CipherTrust* is supported.

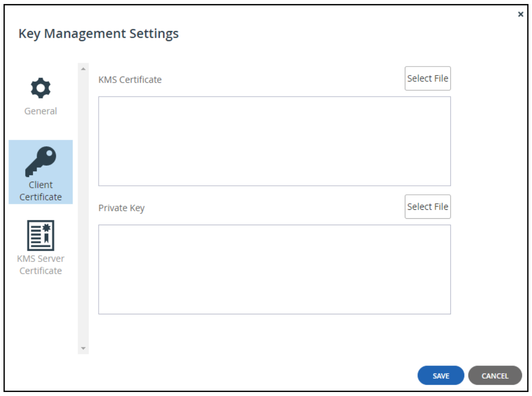
Timeout – The amount of time to wait for a reply from the key management server before the operation times out.

Key expiration – The amount of time the before the key encryption keys become invalid.

Note: Keys are automatically rotated before they expire.

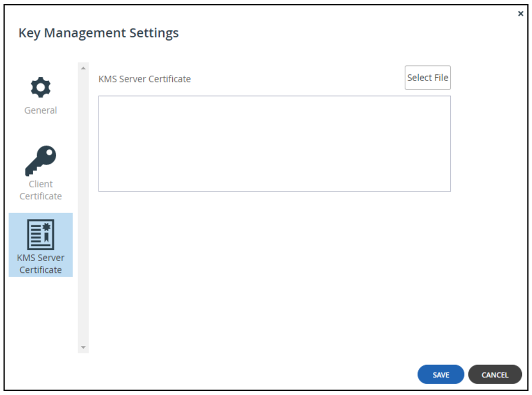
Port – The port used by the key management server.

4. Click **Client Certificate** to upload the client certificate.



5. Click **Select File** to select the .pem file KMS client certificate to use, from step **17** in the To generate the client private key and certificate: procedure.

   Note: Only pem files are allowed.
6. Click **Select File** to select the private key, from step **17** in the To generate the client private key and certificate: procedure. The private key must match the KMS certificate.
7. Click **KMS Server Certificate** to upload the server certificate.



8. Click **Select File** to select the .pem file KMS server certificate to use, from step **5** in the To add the server certificate to Thales CipherTrust Manager: procedure.

   Note: Only pem files are allowed. The certificate must match the client certificate.
9. Click **SAVE**.

If there is a problem with the certificate, for example the client and server certificates do not match, an error is displayed, with additional information written to the log.

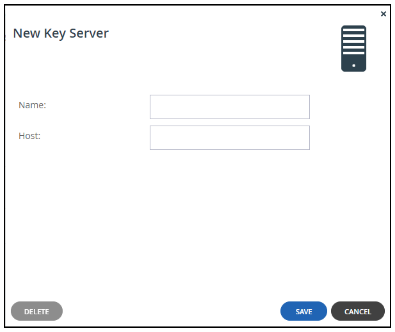
Managing Key Management Servers in HCP Anywhere Enterprise Portal

You can use more than one key management server. Hitachi Vantara recommends using more than one key management server for high availability. All the key management servers are expected to be members of a synchronized cluster. All the key management servers use the same client certificate and private key and server certificate and **not** a separate set per server.

To add or edit a key management server:

1. In the global administration view, select **Services > Key Management** in the navigation pane. The **KEY MANAGEMENT** page is displayed.
2. To add a new key management server, click **Add a Server**.

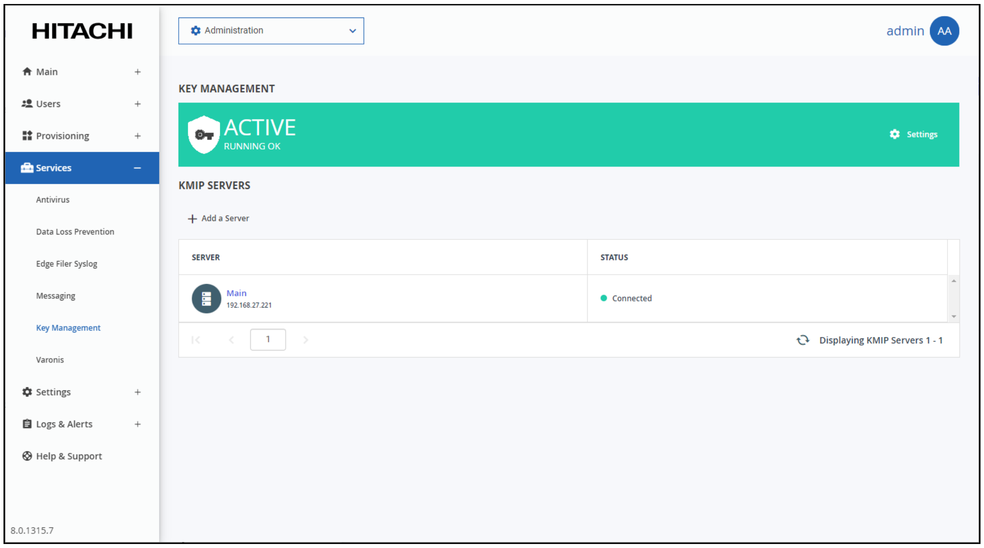
   The **New Key Server** window is displayed.



   Or,
   To edit an existing key management server, click the server's name**.**
   The key server window is displayed with the server as the window title.
3. Specify the details:

   Host – The IP address or DNS name of the server.
   Name – A display name for the server.
4. Click **SAVE**.

The server is added to the list of key management servers.



SERVER	STATUS
Main 192.168.27.221	● Connected

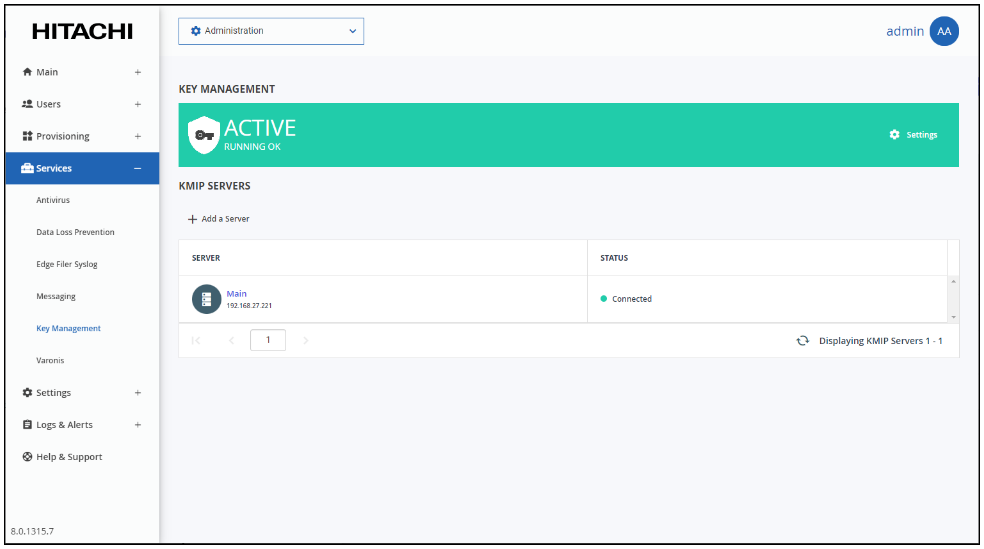
Any new folder group uses managed keys to access the folder group content. All existing folder groups are transitioned to use managed keys by a task that runs in the background.

Each folder group has a key in the key management server. After a file is accessed in the folder group for the first time, the key is saved in a cache in the HCP Anywhere Enterprise Portal. As long as the key is in the cache, access to the files in the folder group is quicker, and access is still possible, even if he key management server is not running.

Changing a Key Management Certificate

To change a key management certificate:

1. In the global administration view, select **Services > Key Management** in the navigation pane. The **KEY MANAGEMENT** page is displayed.



KEY MANAGEMENT

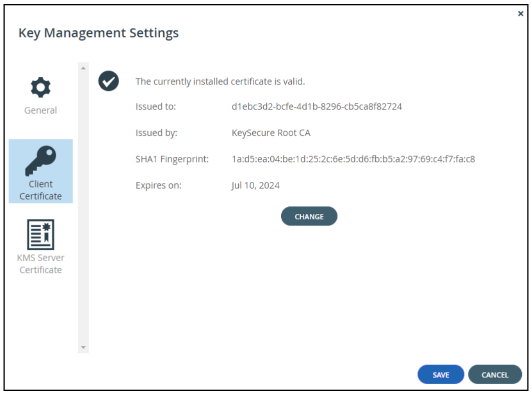
ACTIVE
RUNNING OK

KMIP SERVERS

SERVER	STATUS
Main 192.168.27.221	● Connected

2. Click **Settings** in the status bar at the top of the page to configure the key management settings and select **Configure Service** from the menu.

   The **Key Management Settings** window is displayed.

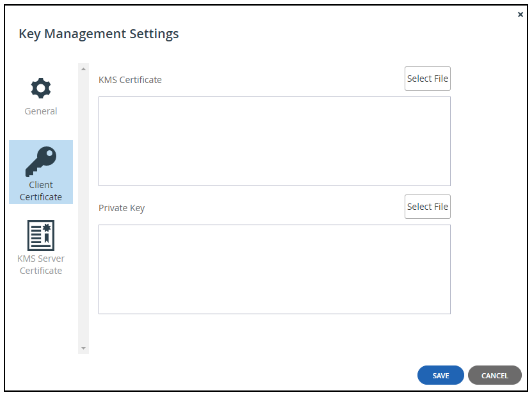


Key Management Settings

The currently installed certificate is valid.

Issued to:	d1ebc3d2-bcfe-4d1b-8296-cb5ca8f82724
Issued by:	KeySecure Root CA
SHA1 Fingerprint:	1a:d5:ea:04:be:1d:25:2c:6e:5d:d6:fb:b5:a2:97:69:c4:f7:fa:c8
Expires on:	Jul 10, 2024

3. Click **Client Certificate**.
4. Click **CHANGE** to change the .pem file used.

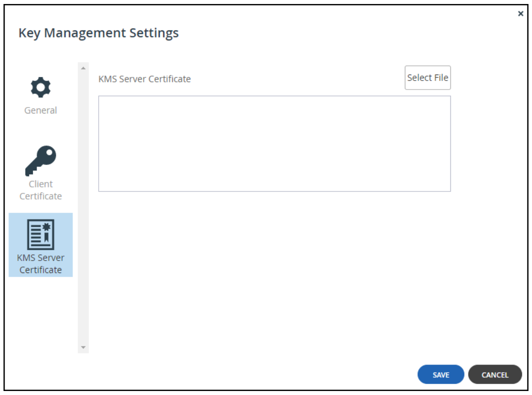


Note: The certificate is not displayed.

5. Click **Select File** to select the .pem file KMS client certificate to use.

   Note: Only pem files are allowed.

6. Click **Select File** to select a private key. The private key must match the KMS certificate.
7. Click **KMS Server Certificate** to change the server certificate.



8. Click **Select File** to select the .pem file KMS server certificate to use.

   Note: Only pem files are allowed. The certificate must match the client certificate.

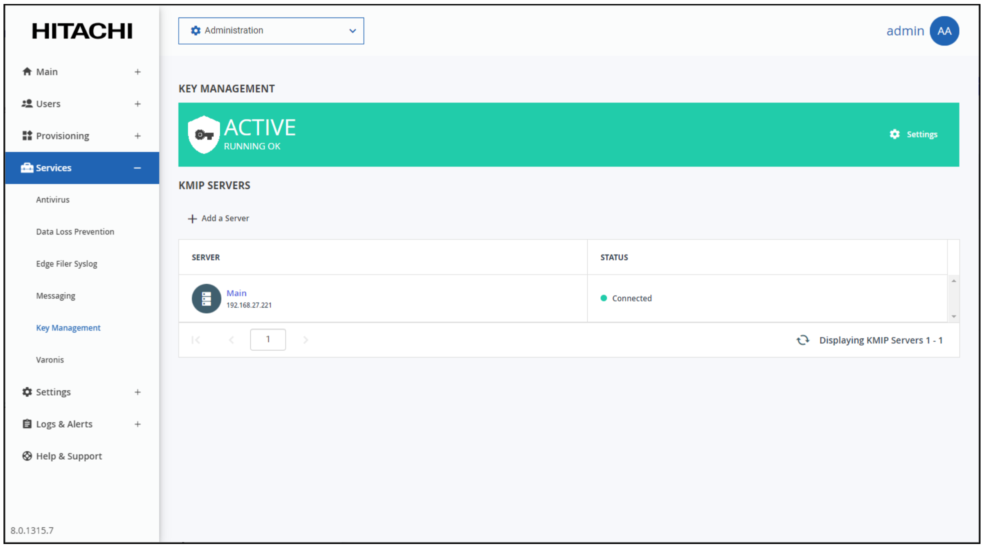
9. Click **SAVE**.

Deleting a Key Management Server

The *Thales CipherTrust Manager* Key Management Server must be running in order to delete the server from the HCP Anywhere Enterprise Portal.

To delete a key management server:

1. In the global administration view, select **Services > Key Management** in the navigation pane.
   The **KEY MANAGEMENT** page is displayed.



SERVER	STATUS
Main 192.168.27.221	● Connected

2. Either,
   - **a)** Select the key management server to delete and click **Delete**.
     A confirmation window is displayed.
   - **b)** Click **DELETE** to confirm.

   Or,
   - **a)** Click the key management server’s name in the list.
     The key management server window is displayed with the server as the window title.
   - **b)** Click **DELETE**.
     A confirmation window is displayed.
   - **c)** Click **YES** to confirm.

The server is deleted.

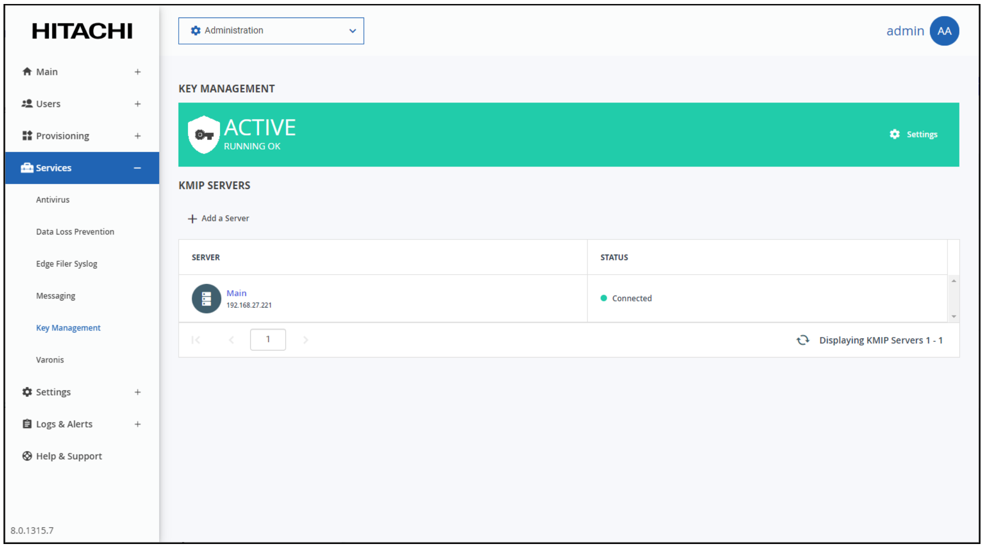
When there are more than one key management servers defined, you can delete them all and the last remaining server cannot be deleted unless you first remove the key management service from the HCP Anywhere Enterprise Portal, described in Removing the Key Management Service.

Removing the Key Management Service

The *Thales CipherTrust Manager* Key Management Server must be running in order to remove the service from the HCP Anywhere Enterprise Portal.

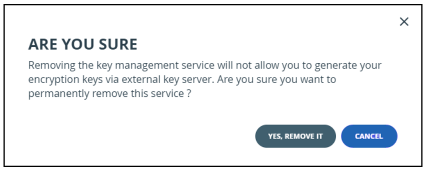
To remove the key management service:

1. In the global administration view, select **Services > Key Management** in the navigation pane. The **KEY MANAGEMENT** page is displayed.



2. Click **Settings** in the status bar at the top of the page to configure the key management settings and select **Remove Service** from the menu.

   A confirmation window is displayed.



ARE YOU SURE

Removing the key management service will not allow you to generate your encryption keys via external key server. Are you sure you want to permanently remove this service ?

3. Click **YES, REMOVE IT**.

All the folder groups are transitioned to unmanaged keys in the background. Upon completion, the key management servers and certificates are removed.

Chapter 20. Managing the HCP Anywhere Enterprise Edge Filer Syslog Service

The HCP Anywhere Enterprise Enterprise File Services Platform powers a global file system connecting remote sites and users. Each remote site includes logs to facilitate managing the site and HCP Anywhere Enterprise Portal acts as a centralized hub to collect logs from all your edge filers and send these logs to one or more syslog servers.

The protocol used to send logs from an edge filer to the HCP Anywhere Enterprise Portal ensures messages are not lost. By using the Edge Filer Syslog service:

- You can manage multiple edge filer logs to Syslog.
- You ensure that logs are never lost. For example, when an edge filer connects directly to Syslog, if the WAN connection goes down to a Syslog server in the cloud, logs will be lost. Using the Edge Filer Syslog server, the logs are not lost and when the WAN connection is re-established, sending logs resumes from with no loss.
- You can use multiple Syslog destinations by defining more than one Syslog server.

In the case of a warning or error with the connection between the HCP Anywhere Enterprise Portal and the Syslog server, email alerts are sent to the administrator. These alerts can be modified. For details of the Edge Filer Syslog email templates, see Managing HCP Anywhere Enterprise Portal Notifications and Email Templatess.

In this chapter

Edge Filer Syslog service tasks can be performed in the global administration view only.

The Edge Filer Syslog Service Requirements

To set up HCP Anywhere Enterprise with the Edge Filer Syslog service you must first set up the HCP Anywhere Enterprise Messaging Service, described in Setting Up the HCP Anywhere Enterprise Messaging Service.

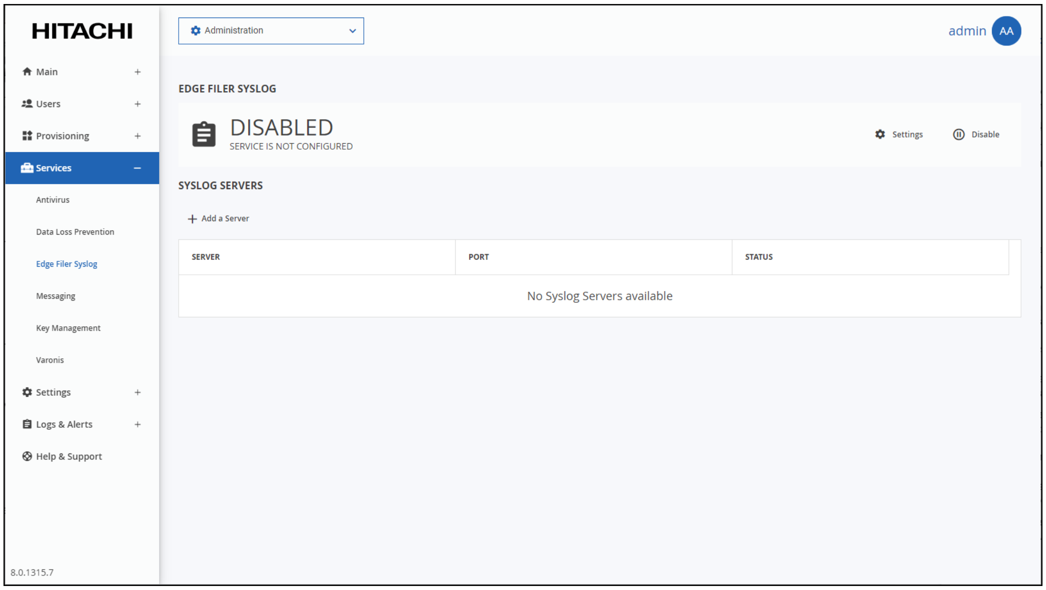
Warning: You must not start setting up the Edge Filer Syslog service until the messaging service setup has completed.

Setting up the **Edge Filer Syslog** service does not impact the portal syslog behavior, described in HCP Anywhere Enterprise Portal Logs.

Setting Up the Edge Filer Syslog Service

To set up the the Edge Filer Syslog service:

1. In the global administration view, select **Services > Edge Filer Syslog** in the navigation pane.
   The **EDGE FILER SYSLOG** page is displayed.



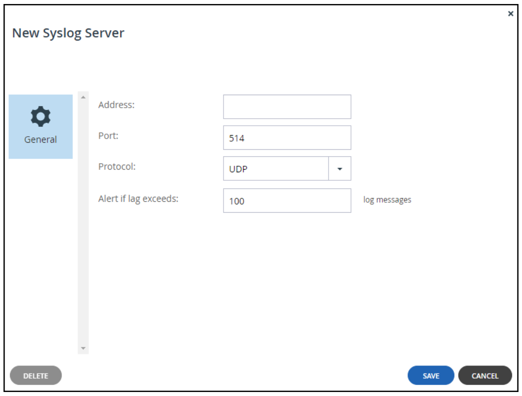
EDGE FILER SYSLOG

DISABLED
SERVICE IS NOT CONFIGURED

SYSLOG SERVERS

SERVER	PORT	STATUS
No Syslog Servers available		

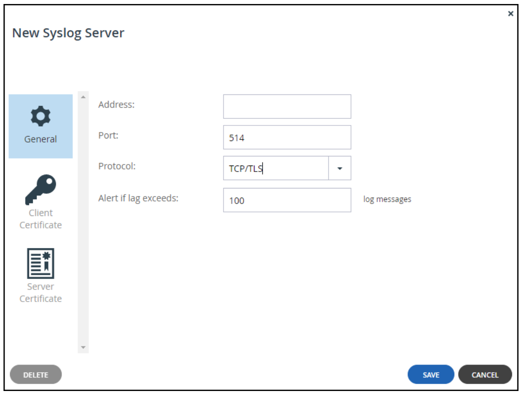
2. Click **Add a Server** to define the Syslog Server:
   The **New Syslog Server** window is displayed.



New Syslog Server

Address:
Port: 514
Protocol: UDP
Alert if lag exceeds: 100 log messages

Address – The address of the Syslog server.
Port – The syslog server's port number. The default port used by a syslog server when **Protocol Type** is `UDP` is 514. The default port used by a syslog server when **Protocol Type** is `TCP/TLS` is 6514.
Protocol – The protocol to use for sending logs to the syslog server: `UDP` or `TCP/TLS`.
If `TCP/TLS` is chosen the **New Syslog Server** window changes:


New Syslog Server

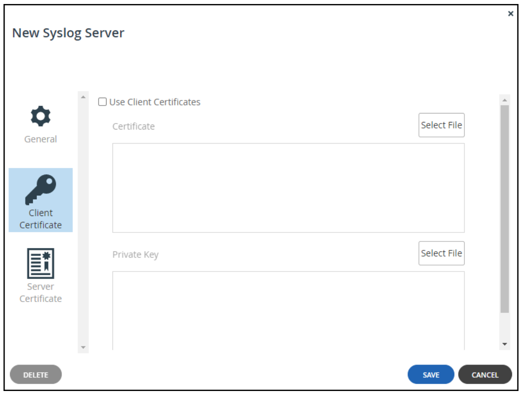
Address:

Port: 514

Protocol: TCP/TLS

Alert if lag exceeds: 100 log messages

a) Click **Client Certificate** to upload the client certificate.


New Syslog Server

☐ Use Client Certificates

Certificate

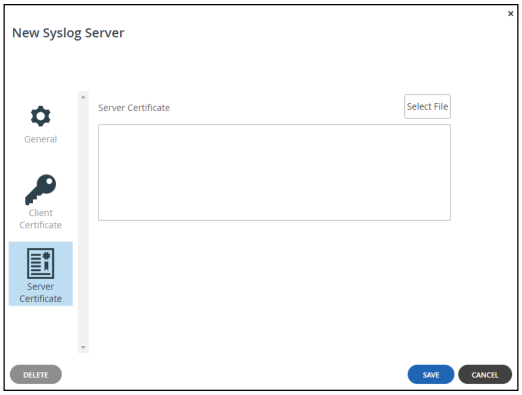
Private Key

b) Click **Select File** to select the .pem file client certificate to use.

Note: Only pem files are allowed.

c) Click **Select File** to select the private key. The private key must match the certificate.

d) Click **Server Certificate** to upload the server certificate.


New Syslog Server

Server Certificate

e) Click **Select File** to select the .pem file server certificate to use.

Note: Only pem files are allowed. The certificate must match the client certificate.

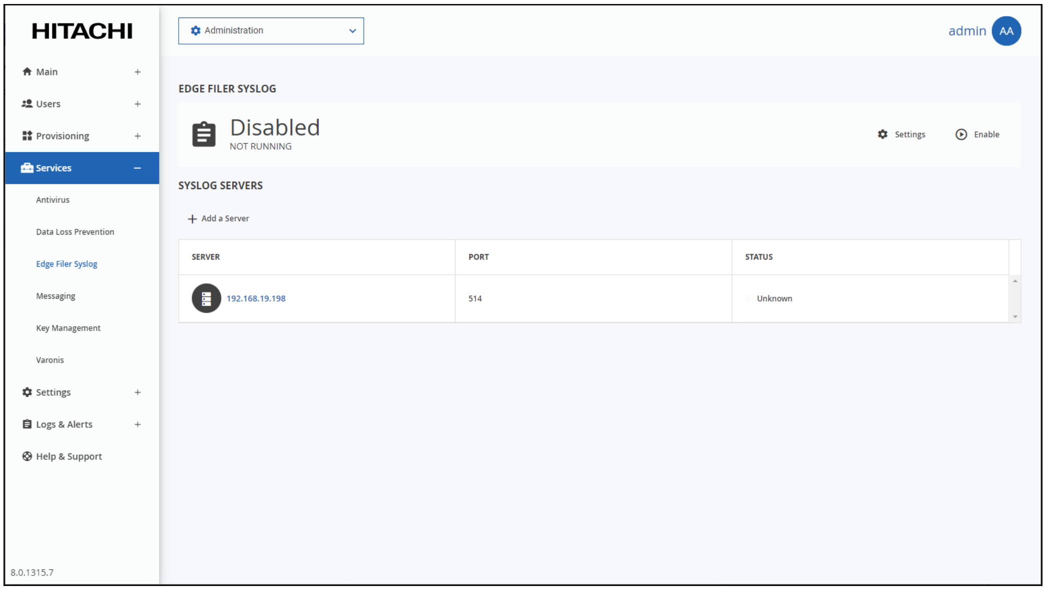
f) Click **SAVE**.

If there is a problem with the TCP connection or with the TLS certificate, for example the client and server certificates do not match or a certificated has expired, an error is displayed, with additional information written to the system log.

Alert if lag exceeds – The number of messages that are not sent to the Syslog server before an alert is issued,

3. Click **SAVE**.

   The server is added to the list of servers.



EDGE FILER SYSLOG

Disabled
NOT RUNNING

Settings Enable

SYSLOG SERVERS

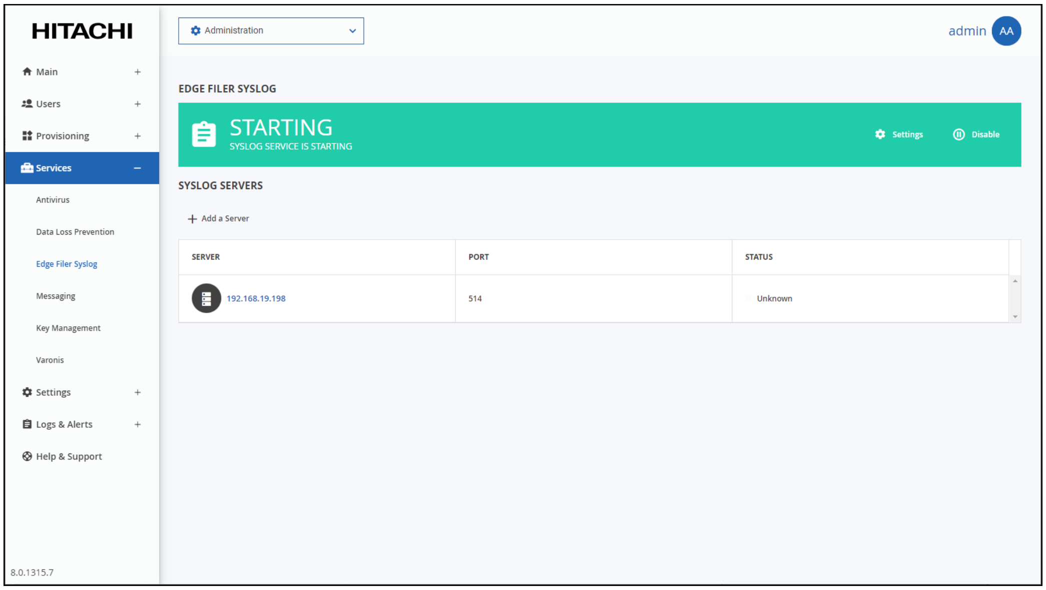
+ Add a Server

SERVER	PORT	STATUS
192.168.19.198	514	Unknown

The **STATUS** field is `Unknown` if the UDP protocol is used and either `Connected` or `Not Connected` if the TCP protocol is used.

4. Click **Enable** in the status bar.

   The **Edge Filer Syslog** service starts.



EDGE FILER SYSLOG

STARTING
SYSLOG SERVICE IS STARTING

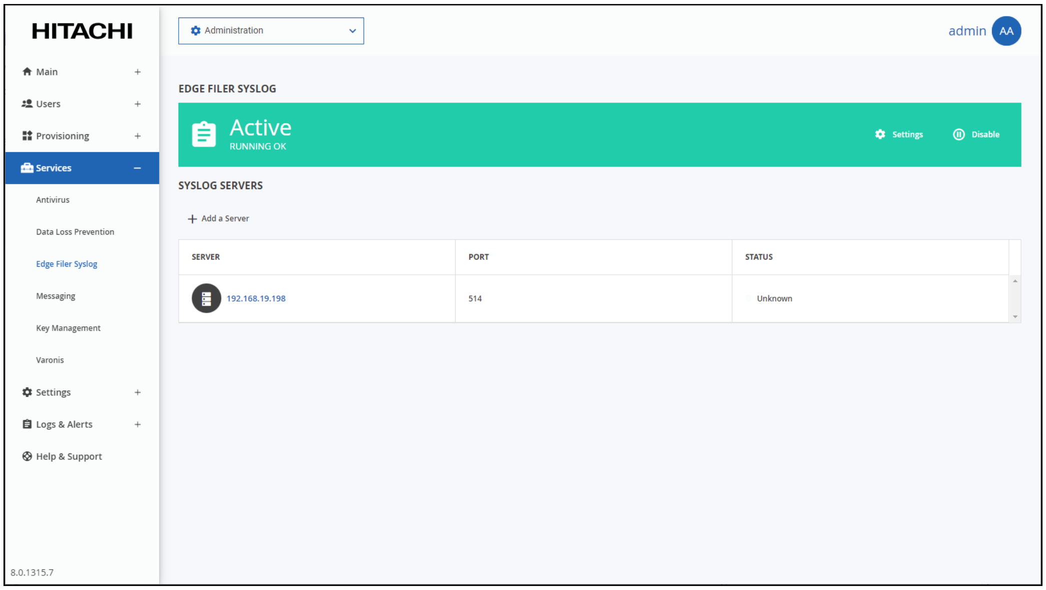
Settings Disable

SYSLOG SERVERS

+ Add a Server

SERVER	PORT	STATUS
192.168.19.198	514	Unknown

When the service has finished starting the status changes to **Active** and **RUNNING OK**.



SERVER	PORT	STATUS
192.168.19.198	514	Unknown

5. Enable CIFS/SMB audit logs on every HCP Anywhere Enterprise Edge Filer you want to use with the **Edge Filer Syslog** service

Disabling or Removing the Edge Filer Syslog Service

You can disable the Edge Filer Syslog service or remove it.

To disable the Edge Filer Syslog service:

1. In the global administration view, select **Services > Edge Filer Syslog** in the navigation pane. The **EDGE FILER SYSLOG** page is displayed.
2. Click **Disable** in the status bar.

   Note: You cannot disable the **Edge Filer Syslog** service while it is starting up.

The **Edge Filer Syslog** service is disabled.

To remove the Edge Filer Syslog service:

1. In the global administration view, select **Services > Edge Filer Syslog** in the navigation pane. The **EDGE FILER SYSLOG** page is displayed.
2. Click **Settings** in the status bar and then click **Remove Service**.

   A confirmation window is displayed.
3. Click **YES, REMOVE IT**.

The Syslog servers are removed and the **Edge Filer Syslog** service is disabled.

Chapter 21. Integrating HCP Anywhere Enterprise with Varonis Data Security Platform

HCP Anywhere Enterprise enables centralized data access from any edge location or device without compromising performance or security. In a distributed enterprise with an increasingly remote workforce, the need to ensure unstructured file data is private and secure is paramount for success. Files can contain sensitive enterprise data, such as intellectual property or customer information, and they must be protected from theft, leakage, and loss.

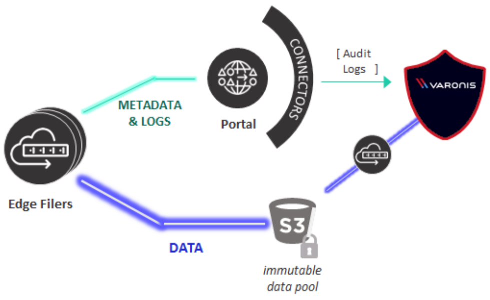
The Varonis Data Security Platform secures data from unauthorized access and cyber-threats by locating where sensitive and regulated information lives across on-premises and cloud datastores limiting access to data and analyzing activity for abnormal behavior or indications of compromise. Varonis correlates data activity from HCP Anywhere Enterprise into context with additional information such as data classification, authentication events, and network activity to provide a complete audit trail of user activity.

The integration between HCP Anywhere Enterprise and the Varonis Data Security Platform enables:

- Central feed of file operations from all devices
- Scans global file system to map files and permissions and identify sensitive data
- Alerts on compliance violations

Note: A license from Hitachi Vantara is required to use the Varonis service.
The Varonis version must be 8.6.32.x or higher.

As organizations begin to adopt more rigorous and modern security protocols like Zero Trust, they can utilize HCP Anywhere Enterprise and Varonis in tandem to help reach a mature Zero Trust environment. The Zero Trust security model states that all users, devices, applications, and networks should be inherently untrusted. With HCP Anywhere Enterprise, each direct request is approved and digitally signed by a centralized security authority. Edge devices never possess credentials for object storage, and they cannot corrupt your critical data even if they are compromised. Varonis adds an extra layer of security to the HCP Anywhere Enterprise global file system. The Varonis Data Security Platform rapidly detects and responds to threats by comparing data activity with baseline behavioral profiles created using machine learning algorithms. These algorithms automatically detect abnormal user behaviors and trigger automated responses that stop attackers in their tracks and mitigate any potential damage.



Varonis maps out your HCP Anywhere Enterprise environment's entire permission structure to understand where sensitive data lives within your environment, revealing where data is overexposed and at risk. Varonis grants complete control over access to your data and gives administrators the ability to control file access at a granular level, helping minimize exposure, reduce the attack surface, and protect sensitive data from potential threats. Additionally, HCP Anywhere Enterprise provides the ability to migrate and support previously defined Windows NT Access control lists (ACLs) and enforces them at both the filer and browser levels.

In this chapter

Varonis Integration Requirements

HCP Anywhere Enterprise Portal requires the following port open on all portal servers for monitoring with the Varonis Data Security Platform:

Port	Protocol	Direction
5671	TCP	Outbound

Note: Access to the Varonis Data Security Platform **must** be via IPv4.

To integrate HCP Anywhere Enterprise with Varonis you must first set up the HCP Anywhere Enterprise Messaging Service, described in Setting Up the HCP Anywhere Enterprise Messaging Service.

Warning: You must not start setting up the Varonis integration until the messaging service setup has completed.

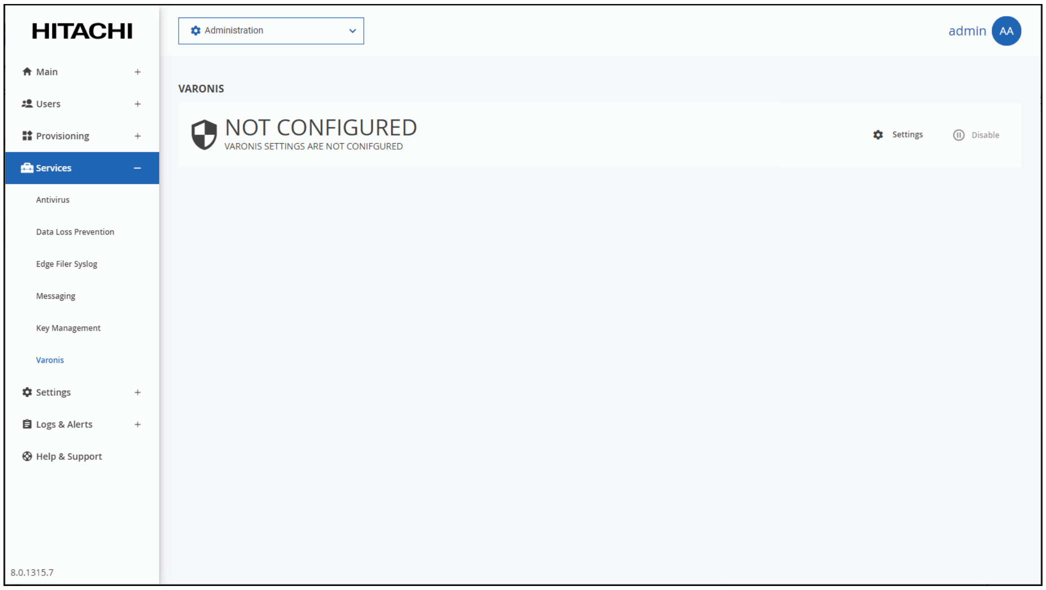
The HCP Anywhere Enterprise Edge Filer administrator must be an administrator in Active Directory and not the local administrator defined when the edge filer was initially configured. This administrator must also belong to the **Administrators** user group, which is a default edge filer user groups.

On each edge filer the audit logs of the SMB file access operations performed on the edge filer must be configured to ensure compliance with enterprise policies and regulations, as described in the *HCP Anywhere Enterprise Edge Filer Administration Guide*.

Setting Up the Integration Between HCP Anywhere Enterprise and Varonis

To set up the Varonis Integration:

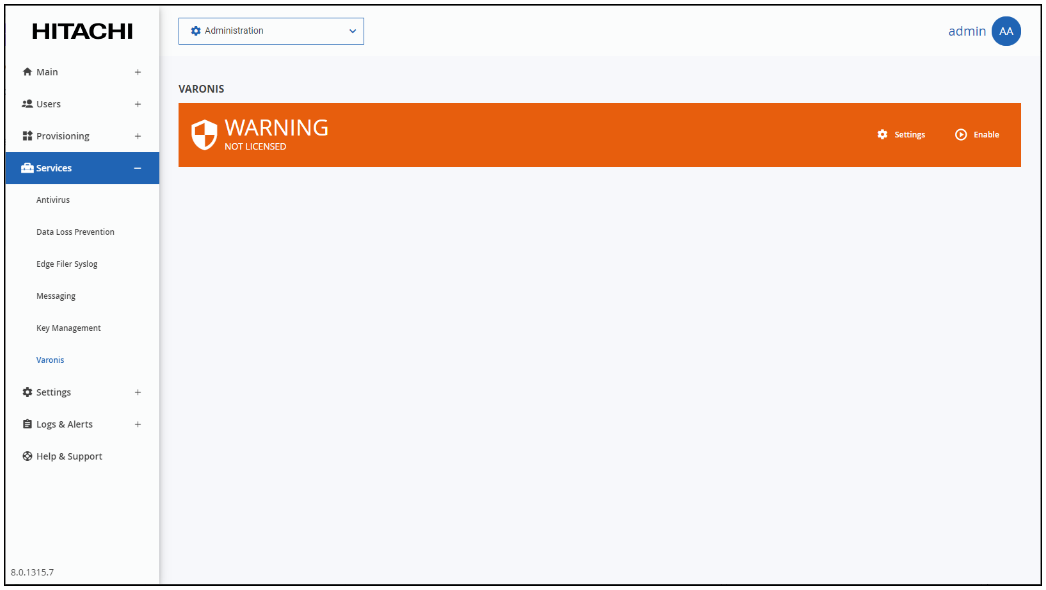
1. In the global administration view, select **Services > Varonis** in the navigation pane.
   The **VARONIS** page is displayed.



VARONIS

NOT CONFIGURED
VARONIS SETTINGS ARE NOT CONIFGURED

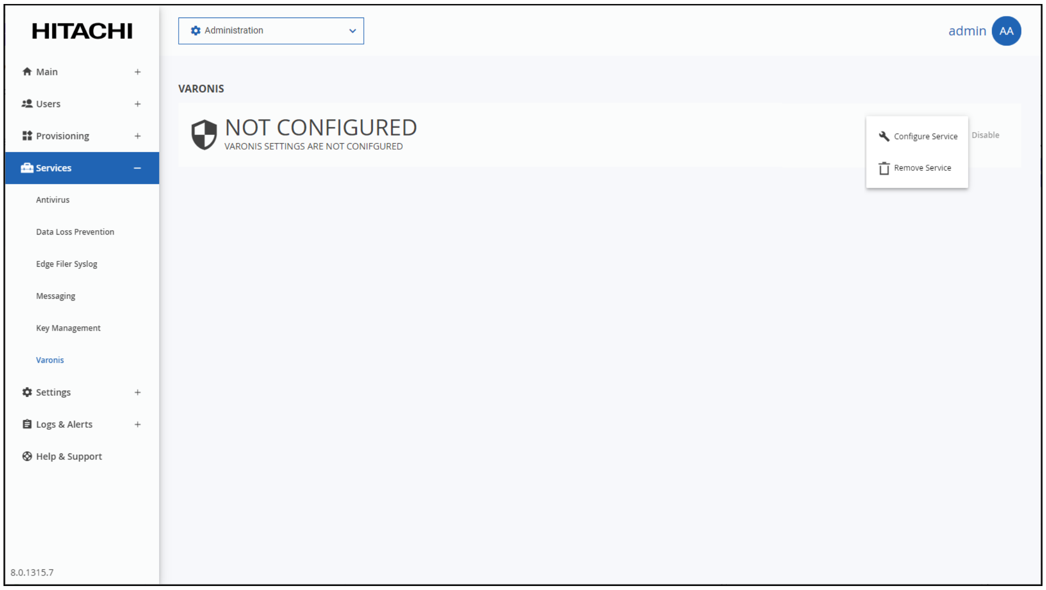
Note: You require a license to integrate Varoinis. If you do not have a license, after accessing the **VARONIS** page in HCP Anywhere Enterprise Portal, a warning status is displayed.



VARONIS

WARNING
NOT LICENSED

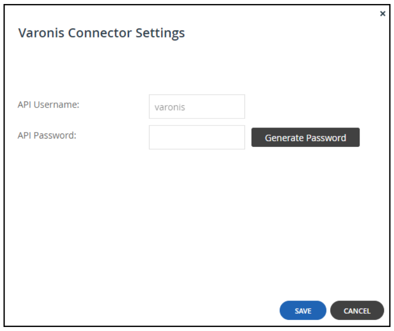
2. Click **Settings** in the status bar to configure the Varonis service.



NOT CONFIGURED
VARONIS SETTINGS ARE NOT CONIFGURED

3. Click **Configure Service**.

   The **Varonis Connector Settings** window is displayed.



Varonis Connector Settings

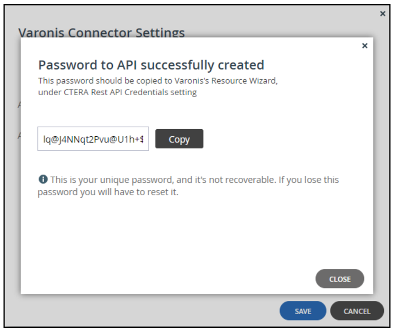
API Username: varonis

API Password:

Note: The API Username is fixed.

4. Click **Generate Password**.

   A password is generated. You use this password to configure the Varonis-HCP Anywhere Enterprise connection within Varonis.



Varonis Connector Settings

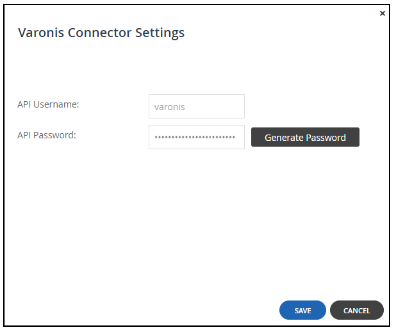
Password to API successfully created

This password should be copied to Varonis's Resource Wizard, under CTERA Rest API Credentials setting

lq@J4NNqt2Pvu@U1h+$

This is your unique password, and it's not recoverable. If you lose this password you will have to reset it.

5. Click **Copy** to copy the generated password and then click **CLOSE**.



Varonis Connector Settings

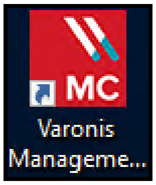
API Username: varonis

API Password: ••••••••••••••••••••••

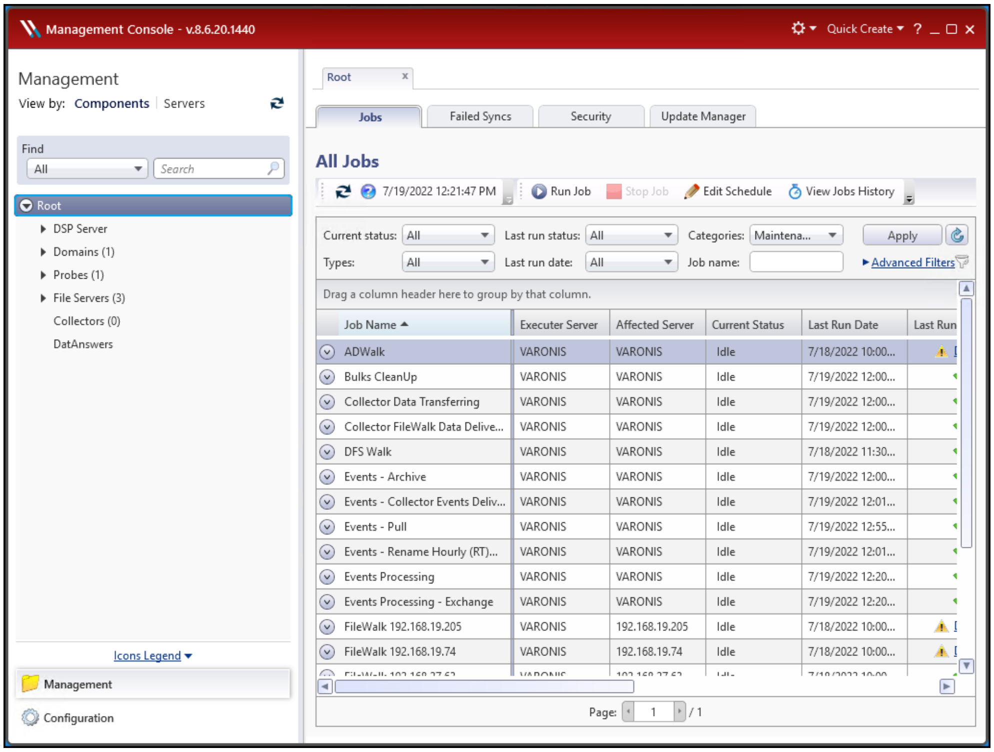
6. Click **SAVE**.
7. Save the **API Password** to use when configuring the Varonis Data Security Platform. The status changes to **WAITING**.

This status does not change until the Varonis Data Security Platform is configured.

To configure the Varonis Data Security Platform:

1. Access the Varonis Management Console, 

The **Management Console** opens.



All Jobs

7/19/2022 12:21:47 PM

Current status: All | Last run status: All | Categories: Maintena...

Types: All | Last run date: All | Job name:

Drag a column header here to group by that column.

Job Name	Executer Server	Affected Server	Current Status	Last Run Date	Last Run
ADWalk	VARONIS	VARONIS	Idle	7/18/2022 10:00...	⚠
Bulks CleanUp	VARONIS	VARONIS	Idle	7/19/2022 12:00...	
Collector Data Transferring	VARONIS	VARONIS	Idle	7/19/2022 12:00...	
Collector FileWalk Data Delive...	VARONIS	VARONIS	Idle	7/19/2022 12:00...	
DFS Walk	VARONIS	VARONIS	Idle	7/18/2022 11:30...	
Events - Archive	VARONIS	VARONIS	Idle	7/19/2022 12:00...	
Events - Collector Events Deliv...	VARONIS	VARONIS	Idle	7/19/2022 12:01...	
Events - Pull	VARONIS	VARONIS	Idle	7/19/2022 12:55...	
Events - Rename Hourly (RT)...	VARONIS	VARONIS	Idle	7/19/2022 12:01...	
Events Processing	VARONIS	VARONIS	Idle	7/19/2022 12:20...	
Events Processing - Exchange	VARONIS	VARONIS	Idle	7/19/2022 12:20...	
FileWalk 192.168.19.205	VARONIS	192.168.19.205	Idle	7/18/2022 10:00...	⚠
FileWalk 192.168.19.74	VARONIS	192.168.19.74	Idle	7/18/2022 10:00...	⚠

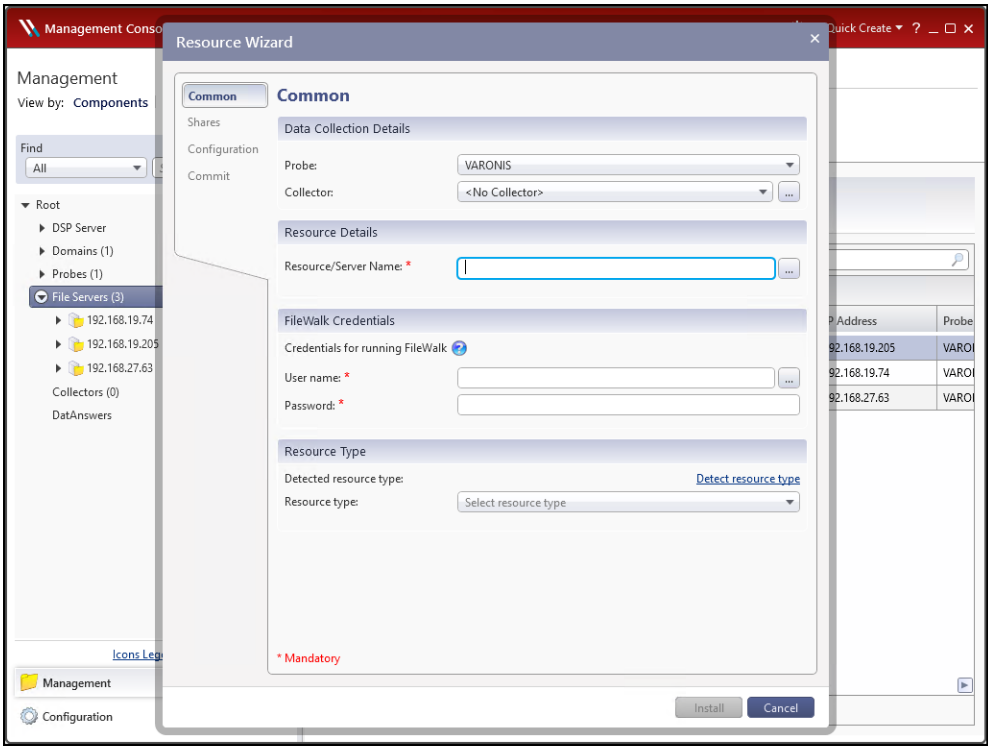
Page: 1 / 1

2. Click **File Servers**, under **Components > Root**.

The **File Servers** page is displayed.

3. Click **Add** in the resources toolbar.

   The **Resource Wizard** is displayed.



Probe: VARONIS

Collector: <No Collector>

Resource/Server Name: *

User name: *

Password: *

Detected resource type:

Resource type: Select resource type

4. Make sure that the **Common** menu option is selected and specify the following values.

   Data Collection Details

   Probe – Select the Probe to be used with the file server from the list.

   Collector – If a Collector has been defined, select the required Collector from the list. For example, when Collectors are defined for different regions.

   Note: If you have configured a Collector to interface with a Probe, you must select the same Collector, a Collector that is not yet connected to a Probe, or `No Collector`. If no Collector is used with the Probe, select `No Collector`.

   Resource Details

   Resource/Server Name – The DNS name or IP address of an edge filer.

   FileWalk Credentials

   User name – The name of the user account defined in the HCP Anywhere Enterprise Edge Filer **Backup-Operators** group from Active Directory, as part of the integration requirements, described in Varonis Integration Requirements.

   Password – The account password.

   Note: The **FileWalk Credentials** are cached, so that they are automatically entered when the next HCP Anywhere Enterprise Edge Filer is added during the same session.

   Resource Type

   Resource type – After adding the **FileWalk Credentials**, The **Hitachi Vantara** resource type should automatically be displayed.

   After specifying the **Resource Type** the **REST API Credentials** item is displayed.

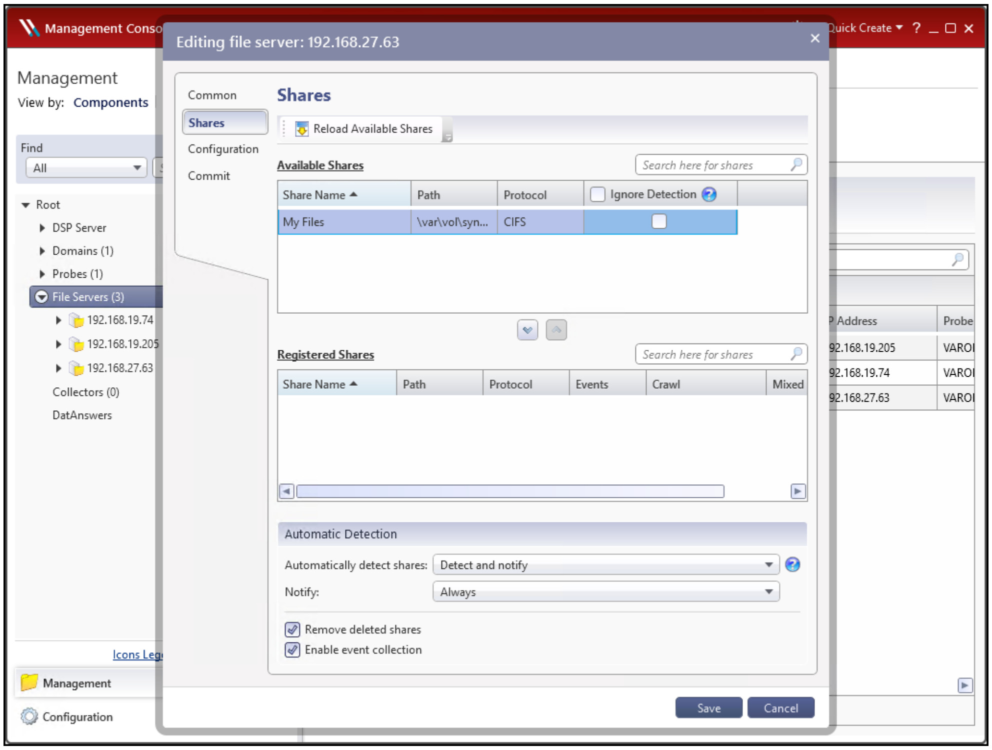
   Virtual Portal DNS Name – The DNS name of the HCP Anywhere Enterprise Portal, for example portal.HCP Anywhere Enterprise.com.

The IP address cannot be specified.

User name – The API Username from setting up the Varonis service in the HCP Anywhere Enterprise Portal. The value is `varonis`.

Password – The API Password generated when setting up the Varonis service in the HCP Anywhere Enterprise Portal.

5. Click **Connect and verify** to verify the credentials that were entered. Nothing is displayed if the connection is verified.
6. Select the **Shares** menu option.



Editing file server: 192.168.27.63

Shares

Available Shares

Share Name ▲	Path	Protocol	□ Ignore Detection
My Files	\var\vol\syn...	CIFS	□

Registered Shares

Share Name ▲	Path	Protocol	Events	Crawl	Mixed

Automatic Detection

Automatically detect shares: Detect and notify

Notify: Always

☑ Remove deleted shares

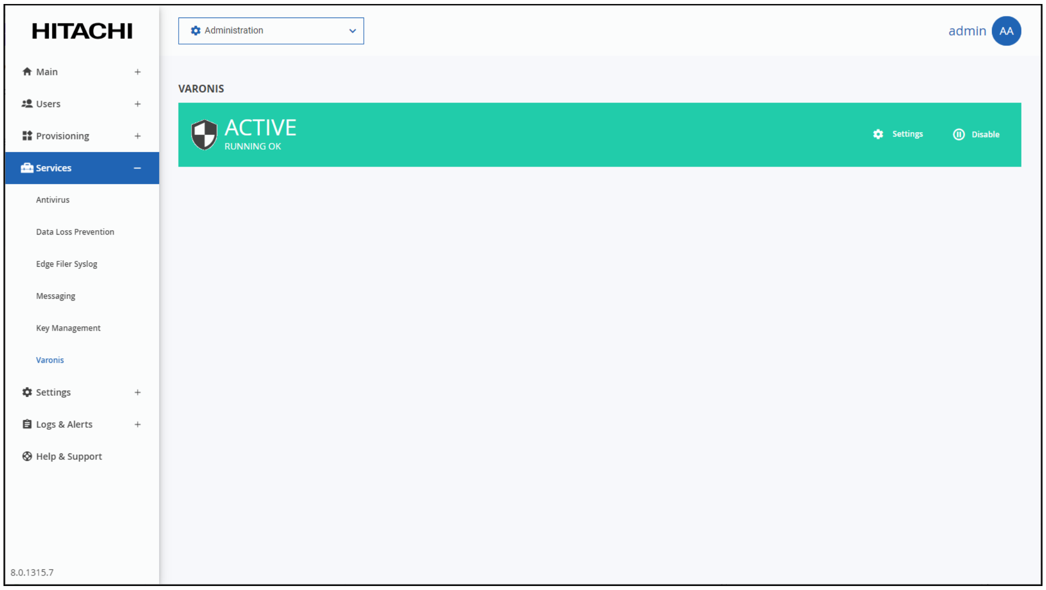
☑ Enable event collection

7. For each share on the edge filer that you want monitored by the Varonis Data Security Platform, select the share and use the down arrow to move it from the **Available Shares** list to the **Registered Shares** list.
8. Click **Save**.

   The HCP Anywhere Enterprise Edge Filer details are added to the Varonis Data Security Platform. This can take a few minutes.

   Note: Click the down arrow next to an edge filer to display the edge filer shares that are being monitored by the Varonis Data Security Platform.
9. Repeat this procedure for every HCP Anywhere Enterprise Edge Filer that you want integrated with Varonis.

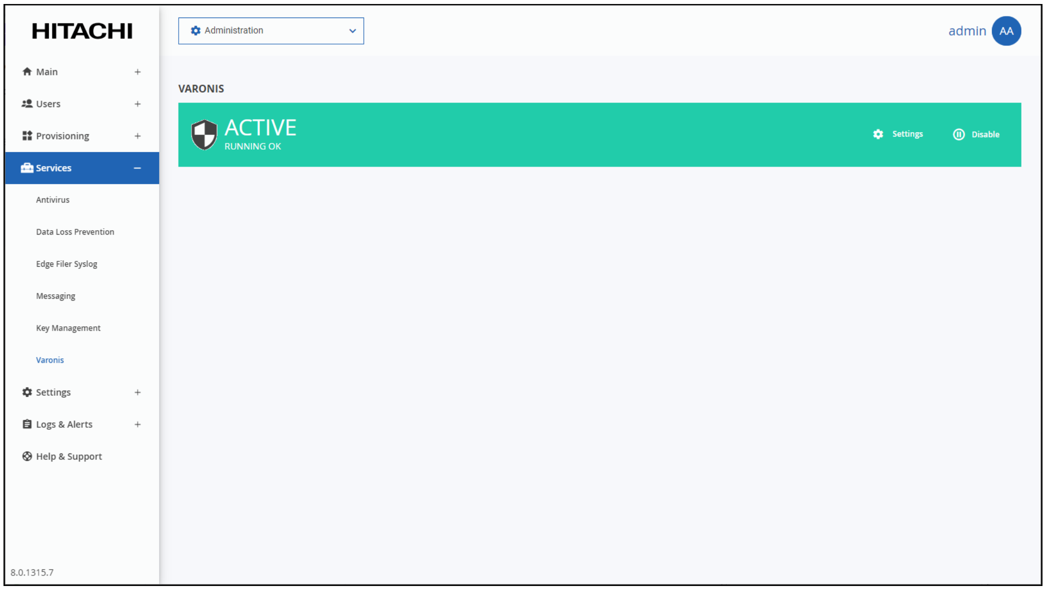
Once the integration has been finalized, the Varonis service in the HCP Anywhere Enterprise Portal status changes to **ACTIVE**.



Enabling or Disabling the Varonis Service

To enable or disable the Varonis service:

1. In the global administration view, select **Services > Varonis** in the navigation pane.
   The **VARONIS** page is displayed.



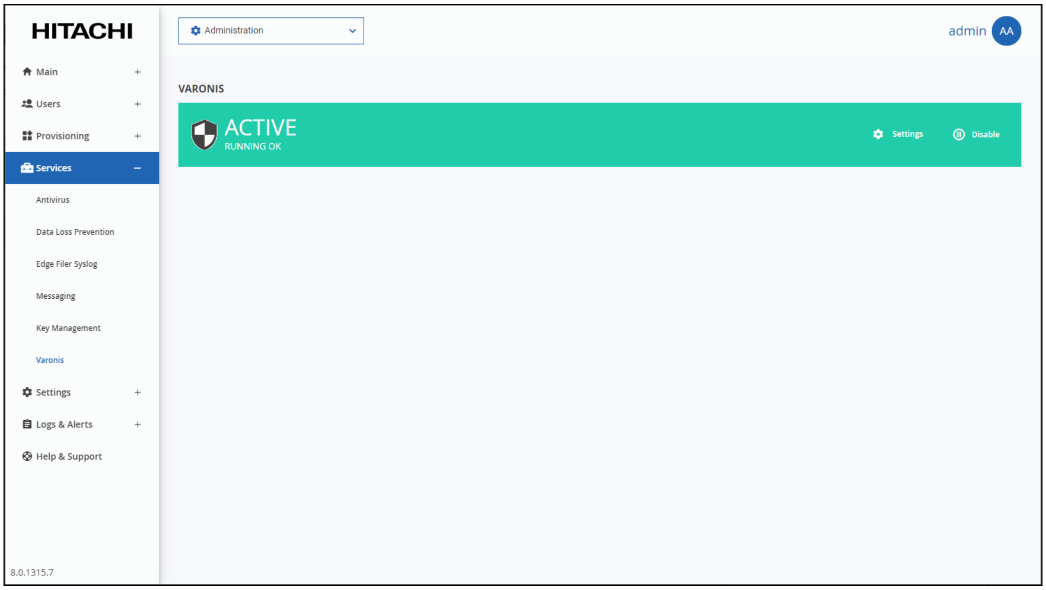
2. Click **Disable** to disable the Varonis service or **Enable** to resume the Varonis service.

Removing the Varonis Service from HCP Anywhere Enterprise Portal

You can remove the connection to the Varonis Data Security Platform within the HCP Anywhere Enterprise Portal, even if you do not remove the HCP Anywhere Enterprise configuration in the Varonis Data Security Platform.

Note: Hitachi Vantara recommends removing the HCP Anywhere Enterprise configuration in the Varonis Data Security Platform before you remove the configuration in the HCP Anywhere Enterprise Portal.

1. In the global administration view, select **Services > Varonis** in the navigation pane.
   The **VARONIS** page is displayed.



2. Click **Settings** in the status bar and then click **Remove Service**.

   A confirmation window is displayed.
3. Click **YES, REMOVE IT**.

The Varonis service is removed.

Chapter 22. HCP Anywhere Enterprise Portal Logs

The portal **Log Viewer** includes the following logs:

Log	Content
System	Events that do not belong in other log categories.
Access	User access to the HCP Anywhere Enterprise Portal events.
Audit	Changes to the HCP Anywhere Enterprise Portal configuration.

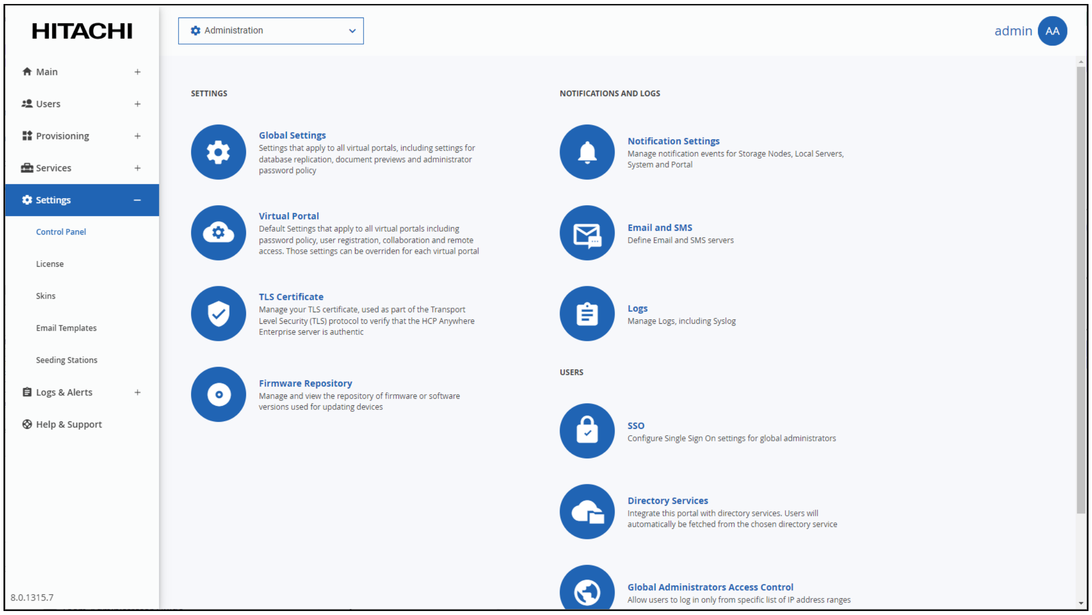
Viewing logs for the HCP Anywhere Enterprise Portal system is available in the Global Administration View. Logs for team portals can be viewed in each team portal's view.

In this chapter

Configuring Log Settings

To configure log settings:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

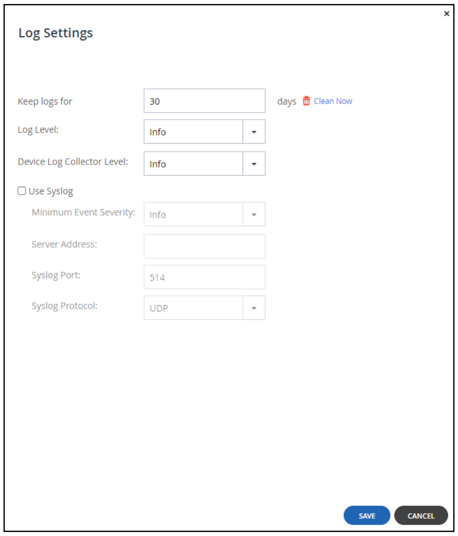
Logs
Manage Logs, including Syslog

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Logs**, under **NOTIFICATIONS AND LOGS** in the **Control Panel** content page.
   The **Log Settings** window is displayed.



Log Settings

Keep logs for: 30 days

Log Level: Info

Device Log Collector Level: Info

☐ Use Syslog

Minimum Event Severity: Info

Server Address:

Syslog Port: 514

Syslog Protocol: UDP

3. Complete the fields.

   Keep logs for – The number of days that the HCP Anywhere Enterprise Portal should store logs. The default value is 30 days.
   Log Level – The minimum log level to display in the HCP Anywhere Enterprise Portal. For example, if you select `Critical`, then only *Emergency*, *Alert*, and *Critical* logs entries are displayed in the HCP Anywhere Enterprise Portal log pages. The default value is `Info`.
   Device Log Collector Level – The minimum log level to collect from each device. For example, if you select `Critical`, then only *Emergency*, *Alert*, and *Critical* log events are collected from devices. The default value is `Info`.
4. Check **Use Syslog** if you want to configure the HCP Anywhere Enterprise Portal to send logs to a Syslog server located on your network or in the cloud.

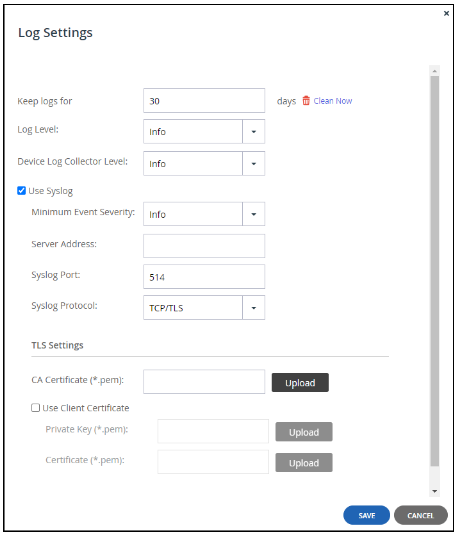
   Note: You can obtain free Syslog servers online, such as Kiwi Syslog Daemon (http://www.kiwisyslog.com/).

   The following logs are sent:

   - Server (Tomcat) logs – catalina.out.*
   - Portal logs – portal.*
   - Database logs
   - Audit logs
   - Journal logs

   Minimum Event Severity – The minimum log level to send to the Syslog server. For example, if you select `Critical`, then only *Emergency*, *Alert*, and *Critical* log events are sent to the Syslog server. The default value is `Info`.
   Server Address – The Syslog server IP address.
   Syslog Port – The Syslog server's port number. The default value is 514.
   Syslog Protocol – The protocol to use to send logs. The default is **UDP**.
   To send logs securely using TLS:

a) Change the **Syslog Protocol** to **TCP/TLS**.



Log Settings

Keep logs for 30 days

Log Level: Info

Device Log Collector Level: Info

☑ Use Syslog

Minimum Event Severity: Info

Server Address:

Syslog Port: 514

Syslog Protocol: TCP/TLS

TLS Settings

CA Certificate (*.pem):

☐ Use Client Certificate

Private Key (*.pem):

Certificate (*.pem):

b) Click **Upload** for **CA Certificate (*.pem)** and browse to your valid CA certificate, select it and click **Open**. The certificate must be in PEM format. If the certificate is valid, **CA Certificate (*.pem)** displays the certificate distinguished name.

c) Optionally, check **Use Client Certificate** if you want authentication on both the client and server sides. If client side authentication is enabled:

Click Upload for **Private Key (*.pem)**, browse to your private key, select it and click **Open**. The private key must be in PEM format.

Click **Upload** for **Certificate (*.pem)** and browse to your valid certificate, select it and click **Open**. The certificate must be in PEM format.

If the private key is valid, `Valid` is displayed for **Private Key (*.pem)**. If the certificate is valid, **Certificate (*.pem)** displays the certificate distinguished name.

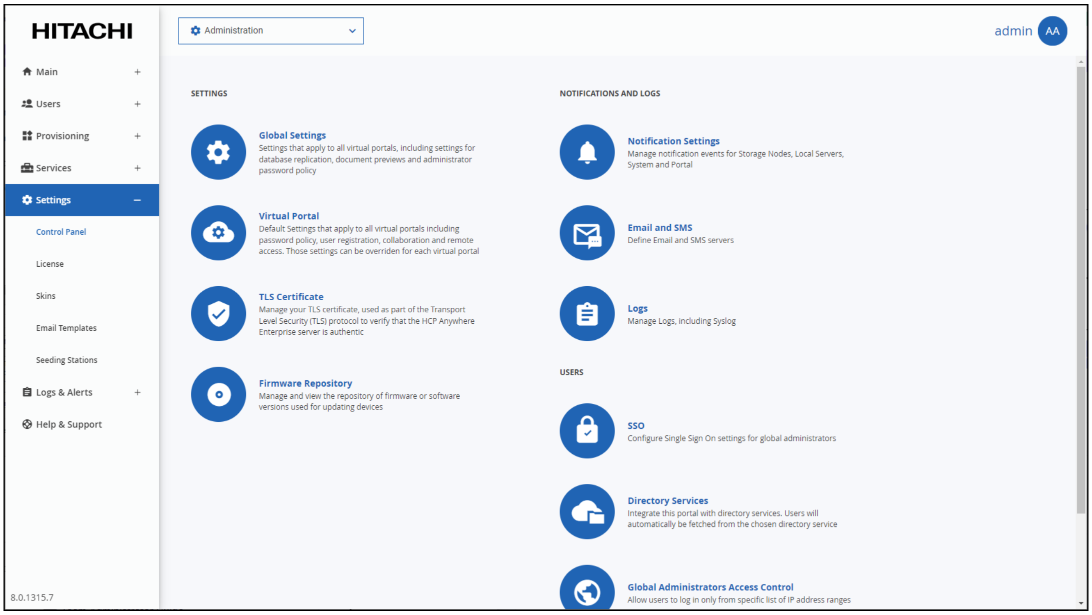
5. Click **SAVE**.

Clearing Logs

You can clear the logs of all virtual portals.

To clear all logs:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

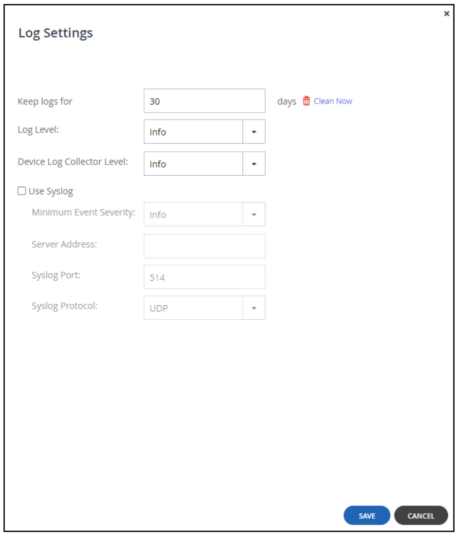
USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Logs**, under **NOTIFICATIONS AND LOGS** in the **Control Panel** content page.
   The **Log Settings** window is displayed.



Log Settings

Keep logs for: 30 days

Log Level: Info

Device Log Collector Level: Info

☐ Use Syslog

Minimum Event Severity: Info

Server Address:

Syslog Port: 514

Syslog Protocol: UDP

3. Click **Clean Now**.

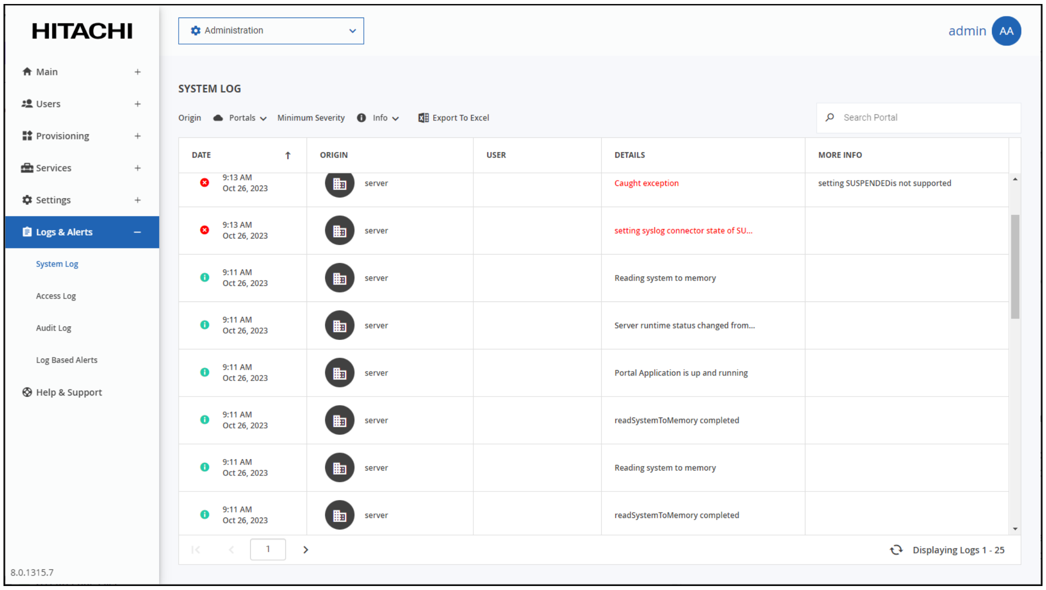
Logs are cleared in all portals.

Viewing Logs

The System Log

To view the system log:

- In the global administration view, select **Logs & Alerts > System Log** in the navigation pane. The **SYSTEM LOG** page opens, displaying the system log for the HCP Anywhere Enterprise Portals.



DATE	ORIGIN	USER	DETAILS	MORE INFO
9:13 AM Oct 26, 2023	server		Caught exception	setting SUSPENDEDis not supported
9:13 AM Oct 26, 2023	server		setting syslog connector state of SU...	
9:11 AM Oct 26, 2023	server		Reading system to memory	
9:11 AM Oct 26, 2023	server		Server runtime status changed from...	
9:11 AM Oct 26, 2023	server		Portal Application is up and running	
9:11 AM Oct 26, 2023	server		readSystemToMemory completed	
9:11 AM Oct 26, 2023	server		Reading system to memory	
9:11 AM Oct 26, 2023	server		readSystemToMemory completed	

The system log information can be filtered by:

- The log origin: portal, device or both portal and device.
- The minimum severity: Debug, Info, Warning, Error.

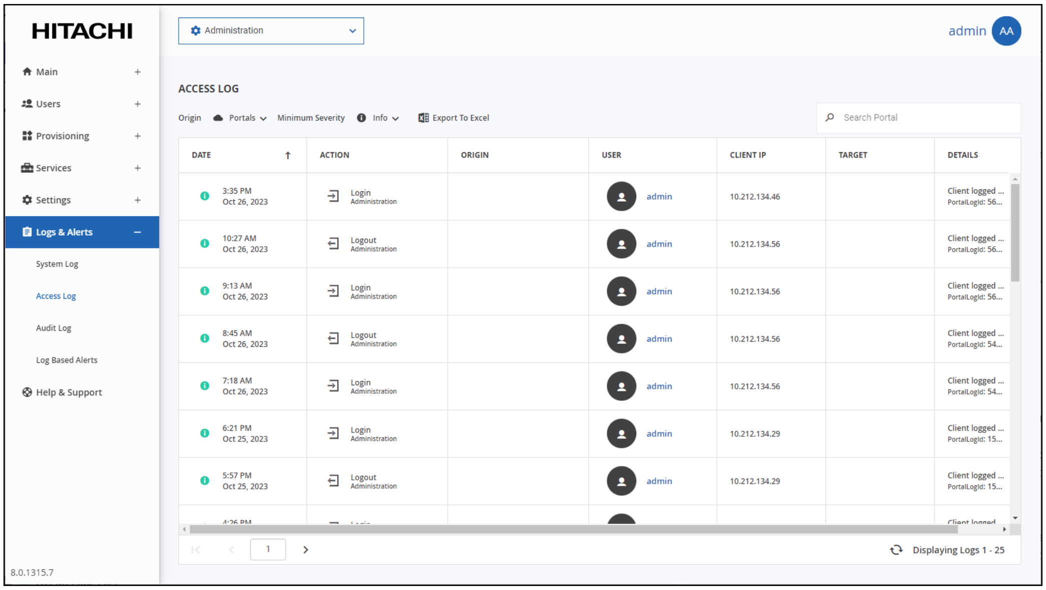
The page includes the following columns:

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.

The Access Log

To view the access log:

- In the global administration view, select **Logs & Alerts > Access Log** in the navigation pane. The **ACCESS LOG** page opens, displaying the access to the portals.



ACCESS LOG

DATE	ACTION	ORIGIN	USER	CLIENT IP	TARGET	DETAILS
3:35 PM Oct 26, 2023	Login Administration		admin	10.212.134.46		Client logged ... PortalLogId: 56...
10:27 AM Oct 26, 2023	Logout Administration		admin	10.212.134.56		Client logged ... PortalLogId: 56...
9:13 AM Oct 26, 2023	Login Administration		admin	10.212.134.56		Client logged ... PortalLogId: 56...
8:45 AM Oct 26, 2023	Logout Administration		admin	10.212.134.56		Client logged ... PortalLogId: 54...
7:18 AM Oct 26, 2023	Login Administration		admin	10.212.134.56		Client logged ... PortalLogId: 54...
6:21 PM Oct 25, 2023	Login Administration		admin	10.212.134.29		Client logged ... PortalLogId: 15...
5:57 PM Oct 25, 2023	Logout Administration		admin	10.212.134.29		Client logged ... PortalLogId: 15...
4:26 PM	Login					Client logged

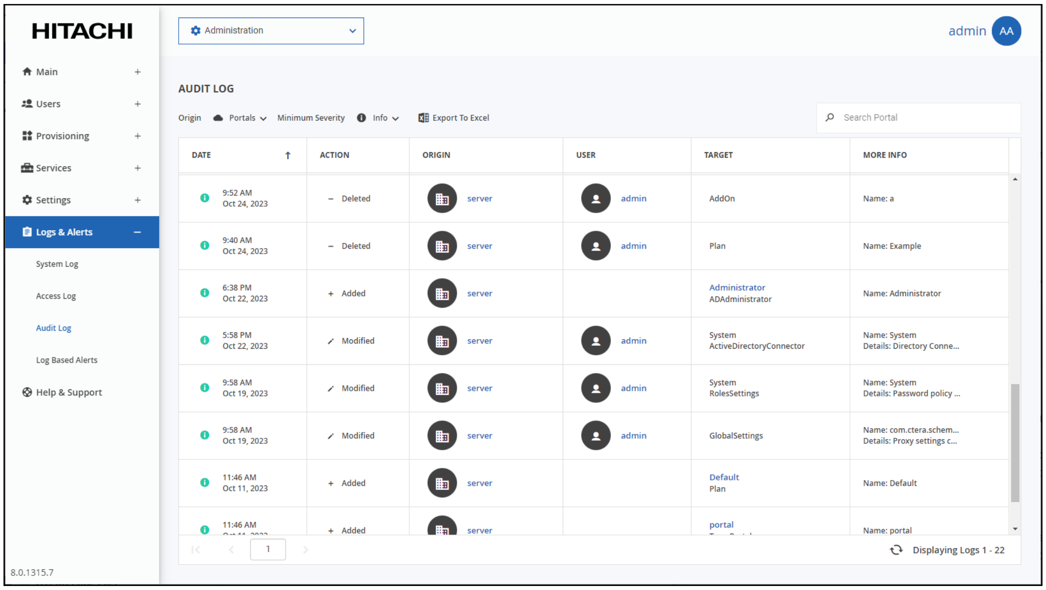
The page includes the following columns:

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. If the user is an external user, without a portal account, added as a collaborator with an email address, the email address of the user is displayed. To view details about the user, if the user is not an external 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 or logged in or a file was shared for collaboration.

The Audit Log

To view the audit log

- In the global administration view, select **Logs & Alerts > Audit Log** in the navigation pane.
  The **AUDIT LOG** page opens, displaying the audits to the portals.



DATE	ACTION	ORIGIN	USER	TARGET	MORE INFO
9:52 AM Oct 24, 2023	– Deleted	server	admin	AddOn	Name: a
9:40 AM Oct 24, 2023	– Deleted	server	admin	Plan	Name: Example
6:38 PM Oct 22, 2023	+ Added	server		Administrator ADAdministrator	Name: Administrator
5:58 PM Oct 22, 2023	Modified	server	admin	System ActiveDirectoryConnector	Name: System Details: Directory Conne...
9:58 AM Oct 19, 2023	Modified	server	admin	System RolesSettings	Name: System Details: Password policy ...
9:58 AM Oct 19, 2023	Modified	server	admin	GlobalSettings	Name: com.ctera.schem... Details: Proxy settings c...
11:46 AM Oct 11, 2023	+ Added	server		Default Plan	Name: Default
11:46 AM	+ Added	server		portal	Name: portal

The page includes the following columns:

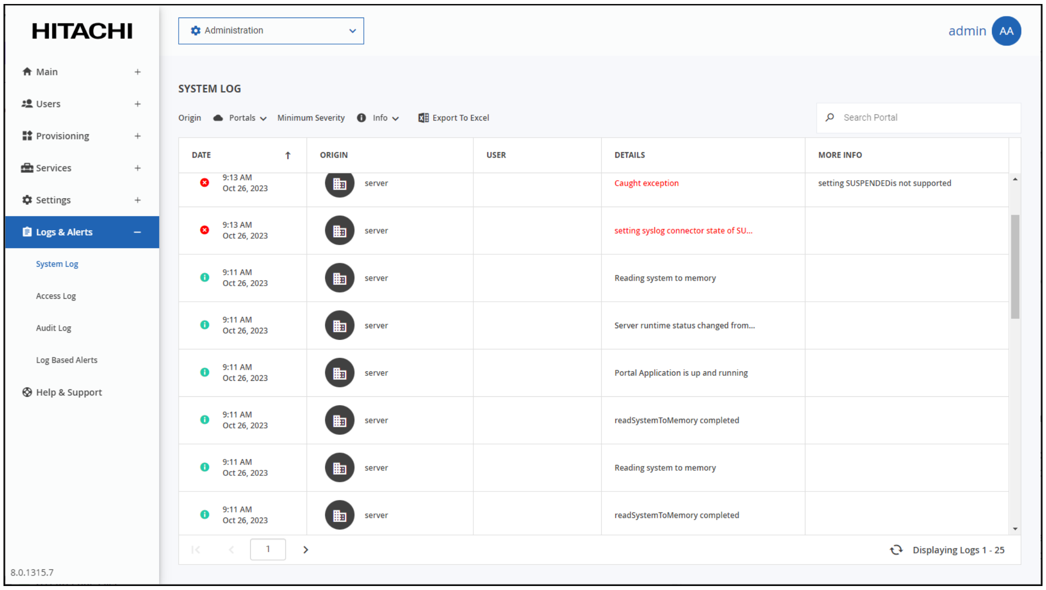
Field	Display
DATE	The date and time at which the event occurred.
ACTION	The action performed: Added, Modified or Deleted.
ORIGIN	The entity that sent the log entry. To view details about the entity, click the entity name.
USER	The user who triggered the event. To view details about the user, click the 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.

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. In the global administration view, select the log to export under **Logs & Alerts** in the navigation pane.
   The log page is displayed.



DATE	ORIGIN	USER	DETAILS	MORE INFO
9:13 AM Oct 26, 2023	server		Caught exception	setting SUSPENDEDis not supported
9:13 AM Oct 26, 2023	server		setting syslog connector state of SU...	
9:11 AM Oct 26, 2023	server		Reading system to memory	
9:11 AM Oct 26, 2023	server		Server runtime status changed from...	
9:11 AM Oct 26, 2023	server		Portal Application is up and running	
9:11 AM Oct 26, 2023	server		readSystemToMemory completed	
9:11 AM Oct 26, 2023	server		Reading system to memory	
9:11 AM Oct 26, 2023	server		readSystemToMemory completed	

2. Select the log you want to export: **System Log**, **Access Log**, or **Audit Log**.
3. Click **Export to Excel**.

The logs in the current log category are exported to your computer.

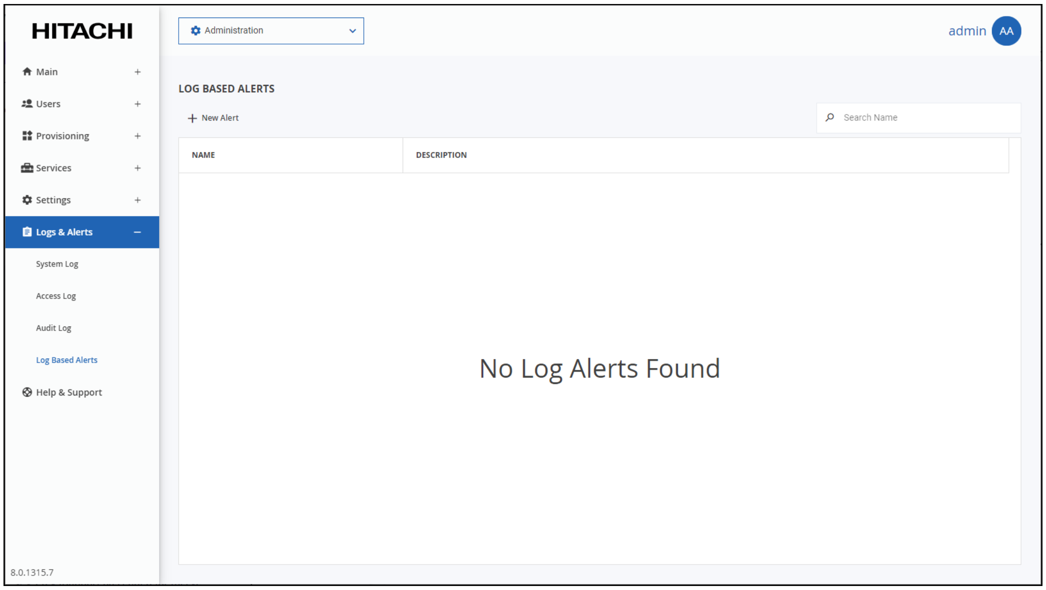
Managing Alerts Based on Log Events

You can configure the HCP Anywhere Enterprise Portal to automatically send email alerts to end users and administrators upon certain HCP Anywhere Enterprise Portal log messages.

Viewing Log Based Alerts

To view all log based alerts:

- In the global administration view, select **Logs & Alerts > Log Based Alerts** in the navigation pane.
  The **LOG BASED ALERTS** page opens, displaying all the log-based alerts.



No Log Alerts Found

The page includes the following columns:

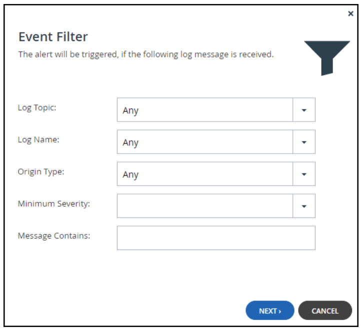
Field	Display
Name	The alert name. To edit the alert, click the alert name.
Description	A description of the alert.

Adding and Editing Alerts

To add or edit an alert:

1. In the global administration view, 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's name**.**
   The **Event Filter** window is displayed.



Event Filter

The alert will be triggered, if the following log message is received.

Log Topic: Any

Log Name: Any

Origin Type: Any

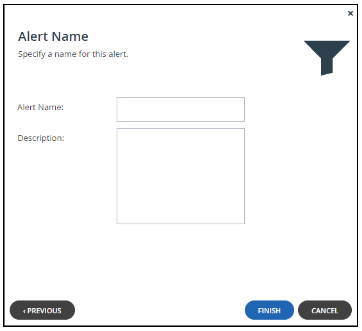
Minimum Severity:

Message Contains:

3. Complete the fields.

   Log Topic – The category to trigger the alert. Select **Any** to specify that any log category can trigger the alert.
   Log Name – The name of the log event to trigger the alert. Select **Any** to specify that any log event can trigger the email alert.
   Origin Type – The entity from which a log must originate to trigger the alert. Select **Any** to specify that any log can originate from any entity in order to trigger the alert.
   Minimum Severity – The minimum severity a log must have 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.



Alert Name

Specify a name for this alert.

Alert Name:

Description:

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. In the global administration view, 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.

Understanding HCP Anywhere Enterprise Log Messages

Log Message Levels

HCP Anywhere Enterprise products generate log messages upon various events. The log messages are divided into the 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.

Log Message Topics

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 and messages from a HCP Anywhere Enterprise Drive Share (Agent) are included in the *agent* topic.

Log messages are divided by one of the following topics:

- access
- accounting
- agent
- allTopics
- antivirus
- audit
- cloudsync
- files
- sync
- system

Log Message Examples

Example 1

Assume the following HCP Anywhere Enterprise Portal log message is received:

```
info,Login,Portal,,2023-05-06T01:32:05,,CTTP,Administration,Client
logged in to portal,192.168.1.15,,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 HCP Anywhere Enterprise Portal.

The attributes values are:
action – `Login`
protocol – `CTTP`
Message – `Client logged in to portal`
clientAddr – `192.168.1.15`
topic – `access`

The message is also timestamped (`2023-05-06T01:32:05`).

Example 2

Assume the following HCP Anywhere Enterprise Portal log message is received:

```
error,Login,Portal,,2023-05-06T13:10:00,,,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 HCP Anywhere Enterprise Portal.

The attribute values are:
action – `Login`
protocol – `CTTP`
Message – `Client login to portal failed`
failedPortal – `portal.myportal.com`
reason – `Login failed: Portal portal.myportal.com does not exist`
failedDevice – `IT`
topic – `access`

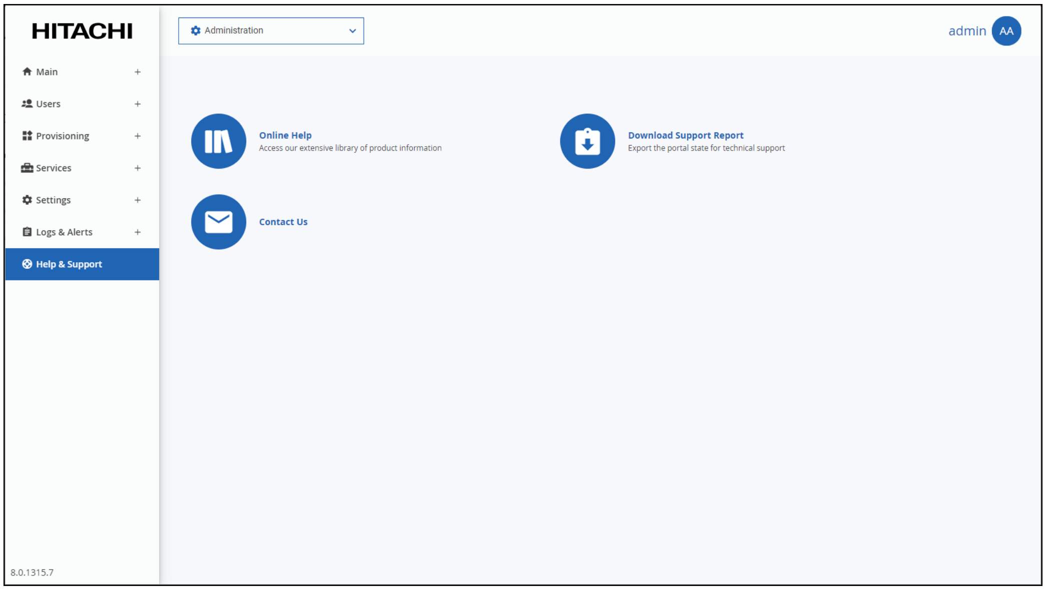
The message is also timestamped (`2023-05-06T13:10:00`).

Chapter 23. Getting Help and Support for the HCP Anywhere Enterprise Portal

If you require help with the HCP Anywhere Enterprise Portal, you can access the online help and if this is not sufficient open a support case with Hitachi Vantara support. If you are having an issue, you can generate a report which collects information that Hitachi Vantara support can then use to resolve the issue.

To get online help and support for the HCP Anywhere Enterprise Portal:

1. In the global administration view, select **Help & Support** in the navigation pane.



2. Options are displayed.

Online Help – Opens the online help in a separate tab. This is equivalent to clicking the avatar next to the name in the top right of the user interface and then clicking **HELP** to display access to the online help.

Download Support Report – If a problem arises with your portal, you can generate a report for Hitachi Vantara support to use to identify and resolve the problem. The report is generated in an encrypted ZIP file in your computer's download folder. The report includes the following information:

Portal status:

Environment details such as: versions, DB size, and server details.
Relevant sync and backup information such as the total number of devices, failures, and configuration changes.
Data related errors such as the missing blocks, incomplete file.
Infrastructure issues such as a DB corruption and DB maintenance task issues.
Sync failures.

Device status:

Critical errors.
Sync problems.
The general status of the device.

Contact – Log in to your support account directly from your portal.

Note: You require a support account to contact HCP Anywhere Enterprise support.

To generate a support report:

1. In the global administration view, select **Help & Support** in the navigation pane and click **Download Support Report**.
   The **Generate Support Report** window is displayed and the report is generated. After the report is generated, you can download it or run the procedure again to generate a new report.
2. click **CLOSE** to finish.

While the report is being generated, 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**.

Chapter 24. Managing Reports

The HCP Anywhere Enterprise Portal provides the global administration reports about the virtual portals and storage nodes.

In this chapter

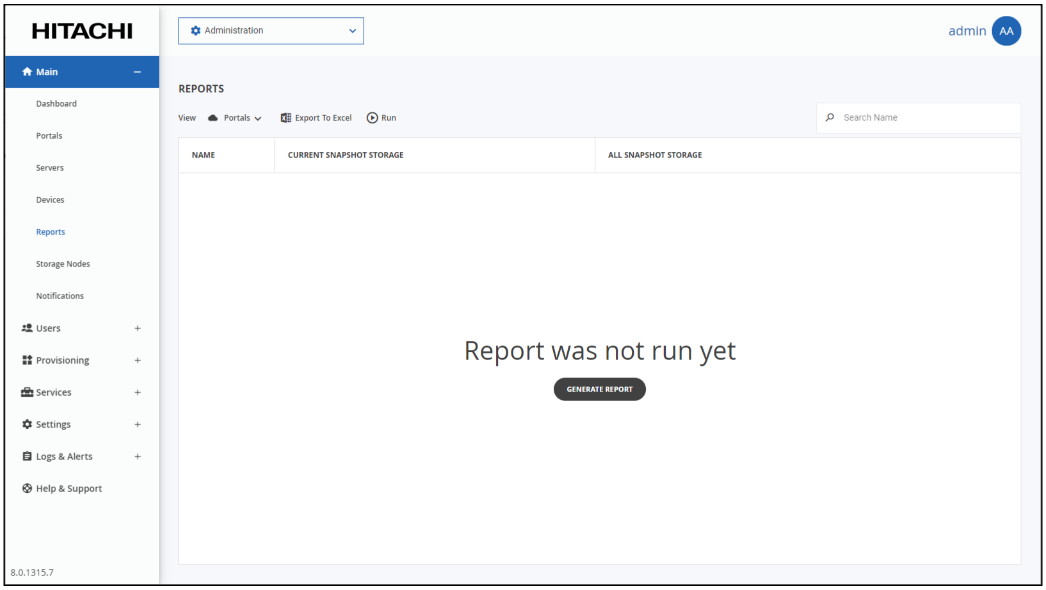
- Viewing the Portals Report
- Viewing the Storage Report
- Exporting Reports to Excel

Viewing the Portals Report

Global administrators can view information about all virtual portals.

To view the Portals Report:

- In the global administration view, select **Main > Reports** in the navigation pane.
  The **REPORTS** page opens, displaying the reports run for portals.



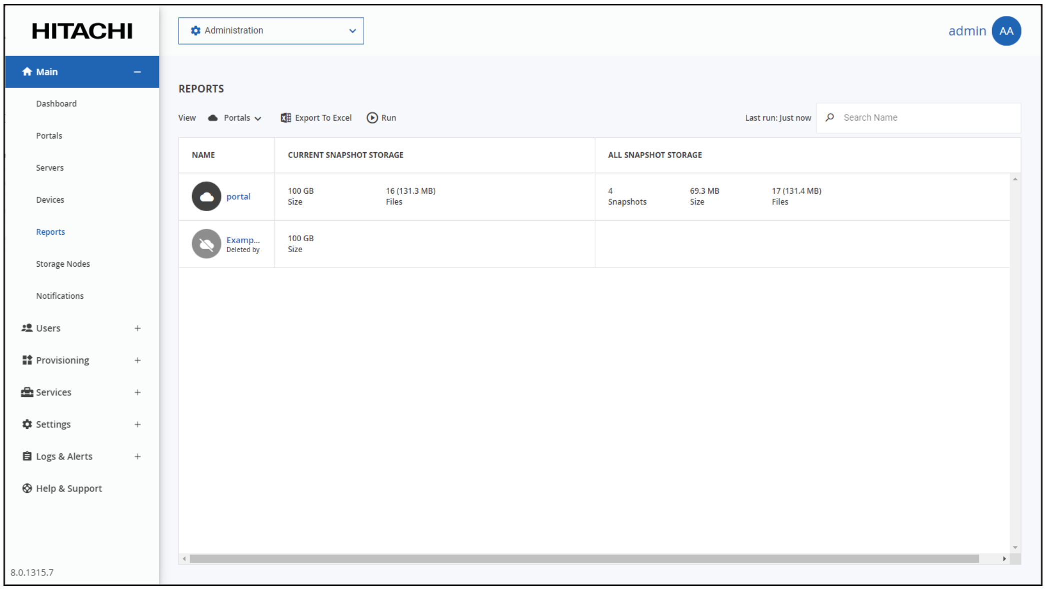
NAME	CURRENT SNAPSHOT STORAGE	ALL SNAPSHOT STORAGE

Report was not run yet

The **REPORTS** page shows the last time the report was generated. You can generate an up-to-date report.

To generate a Portals report:

- Click **Run**, or for the first report generated, you can also click **GENERATE REPORT**. The report is generated for every team portal.



NAME	CURRENT SNAPSHOT STORAGE		ALL SNAPSHOT STORAGE		
portal	100 GB Size	16 (131.3 MB) Files	4 Snapshots	69.3 MB Size	17 (131.4 MB) Files
Examp... Deleted by	100 GB Size				

The following information is displayed.

Field	Display
NAME	The team portal name. To view details about the portal and the subscription plan and add-ons defined for the portal, click the portal name.

Field	Display
CURRENT SNAPSHOT STORAGE	Details about the latest snapshot: • The storage quota allocated to this team portal in the plan, if set. If the quota is unlimited, this value is empty. The value is the logical storage before any deduplication, versioning and compression. • The amount of storage currently used in this team portal. 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 (HCP Anywhere Enterprise Edge Filers and Agents): • The total number of snapshots that are currently maintained by the HCP Anywhere Enterprise Portal. The value depends on the retention policy. For details about the retention policy, see The Snapshot Retention Policy. • The size of the storage for this virtual portal in the storage node for all the snapshots after deduplication and compression. • The total number of files in all the snapshots and the amount of storage required by these files before deduplication and compression. • 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.

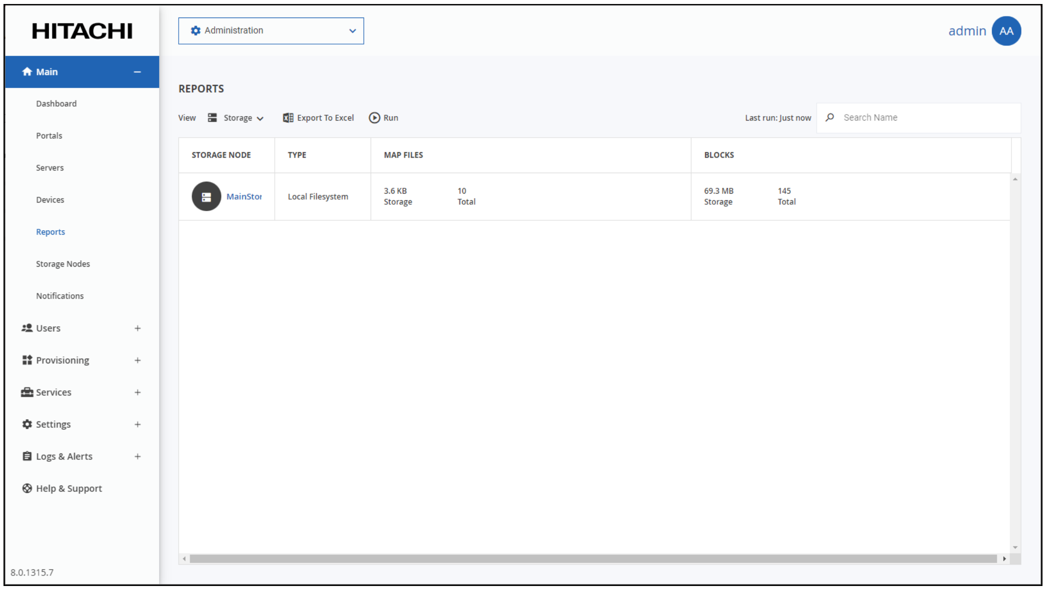
Viewing the Storage Report

Global administrators can view information about the HCP Anywhere Enterprise Portal storage nodes.

To view the Storage Report:

1. In the global administration view, select **Main > Reports** in the navigation pane and select **Storage** from the **View** drop-down list.
2. Click **Run**, or for the first report generated, you can also click **GENERATE REPORT**.

   The report is generated for every storage node.



STORAGE NODE	TYPE	MAP FILES	BLOCKS
MainStor	Local Filesystem	3.6 KB Storage 10 Total	69.3 MB Storage 145 Total

The following information is displayed.

Field	Display
STORAGE NODE	The name of the storage node. To view details about the storage node and its status, click the storage node name.
TYPE	The storage node type.
MAP FILES	Details about the storage node: • The amount of space consumed by the mapfiles for this storage node. • The total number of mapfiles in this storage node. • The number of mapfiles currently being uploaded to the storage node. • The number of missing mapfiles in this storage node.
BLOCKS	Details about the storage node: • The amount of space consumed by the blocks for this storage node after deduplication and compression. • The total number of blocks in this storage node. • The number of blocks currently being uploaded to the storage node. • The number of missing blocks in this storage node.

Exporting Reports to Excel

You can export a report to a comma separated values (*.csv) Microsoft Excel file on your computer.

The report is exported to your computer. The report includes more detailed than the details displayed in the **REPORTS** page.

To export a report to Microsoft Excel:

1. In the global administration view, select **Main > Reports** in the navigation pane.
   The **REPORTS** page is displayed.
2. Select the report to export, **Portal** or **Storage**, from the **View** drop-down list.
3. Click **Export to Excel**.

For the **Portals** report the following information is displayed.

Column	Description
Name	The team portal name.
Quota	The storage quota allocated to this virtual portal in bytes in the plan, if set. This is logical storage, before any deduplication, versioning, or compression.
Allocated	The amount of logical storage that is currently used by this portal in bytes before any deduplication, versioning or compression. It is limited by **Quota**.
Current Snapshot Files	The count size of files that are in the current snapshot, the *live* file system, not including previous versions or deleted files.
Current Snapshot Size	The amount of storage currently used in this team portal. The value is the logical storage before any deduplication, versioning and compression.
Snapshots	The total number of snapshots.
Physical	The size of the storage required for all the snapshots in bytes, in the object storage, after deduplication and compression.
All Snapshot Files	The total number of files in all the snapshots.
All Snapshot Size	The size of the storage for this virtual portal in the storage node for all the snapshots after deduplication and compression.
Files In Upload	The number of files currently being uploaded.
Files In Upload (Size)	The size of files currently being uploaded.
In Trashcan	The number of deleted files in the trashcan in the team portal. These files can be restored
Deleted on	The date the files were deleted.
Deleted by	The user who deleted the files.

For the **Storage** report the following information is displayed.

Column	Description
Name	The name of the storage node.
Type	The storage node type.
Mapfile Overhead	The total space consumed by the mapfiles for this storage node.
Total Mapfiles	The total number of mapfiles in this storage node.
In Upload Mapfiles	The number of mapfiles of files that are currently in upload, or files that have been partially uploaded and are incomplete.
Missing Mapfiles	The number of missing mapfiles in this storage node.
Blocks Storage Space	The total space consumed by blocks and file maps in this storage node, in TB. In normal situations this is expected to be equal to the storage space reported as used by the storage node. In case of discrepancy, contact Hitachi Vantara support.
Uploaded Blocks	The total number of blocks in this storage node.
In Upload Blocks	The total size of blocks that are currently being uploaded, or belonging to incomplete files that have been partially uploaded.
Missing Blocks	The number of missing blocks in this storage node.
Read Only	Whether the storage node is read only or not.

Chapter 25. Managing Servers

As a global administrator, you can manage the servers on which HCP Anywhere Enterprise Portal is installed.

HCP Anywhere Enterprise Portal servers are Tomcat servers (Apace Tomcat) running on CentOS Linux machines. The database used by the HCP Anywhere Enterprise Portal is a PostgreSQL database.

You can use third-party tools to monitor the tomcat servers and HCP Anywhere Enterprise Portal database. For example, Nagios, www.nagios.com, provides complete monitoring of CentOS Linux operating systems, including operating system metrics, service state, process state, and file system usage. To monitor the database you can use a tool such as Open PostgreSQL Monitoring (OPM).

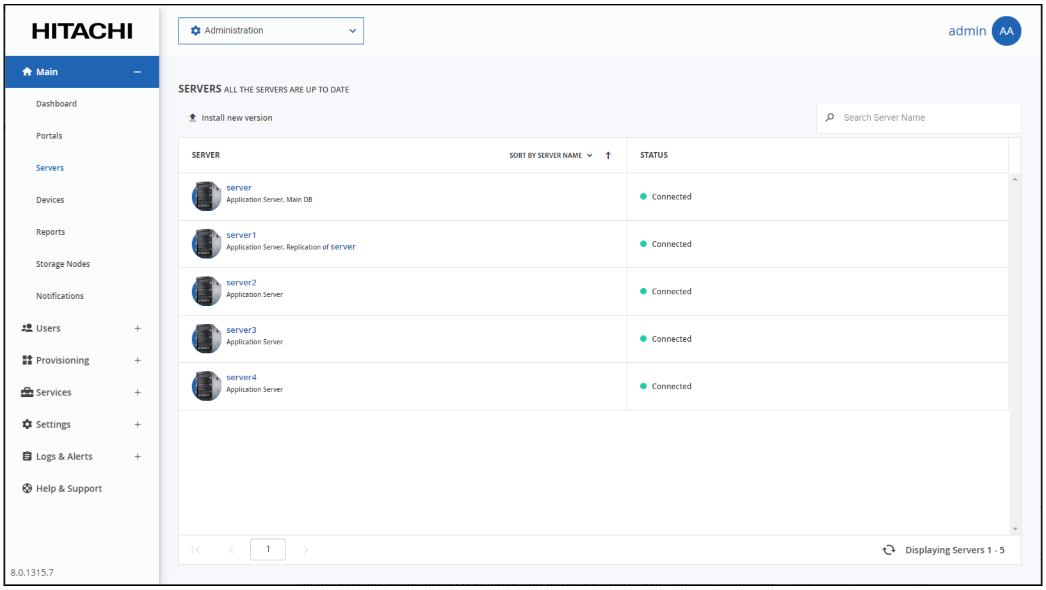
Note: For details about adding servers, refer to the installation documentation for your environment. HCP Anywhere Enterprise monitoring is available using external tools. Hitachi Vantara officially supports Datadog and Nagios monitoring systems.

In this chapter

Viewing Servers

To view the HCP Anywhere Enterprise Portal servers:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

2. To view server settings, click the server name.

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

For details refer to Editing Server Settings.

Editing Server Settings

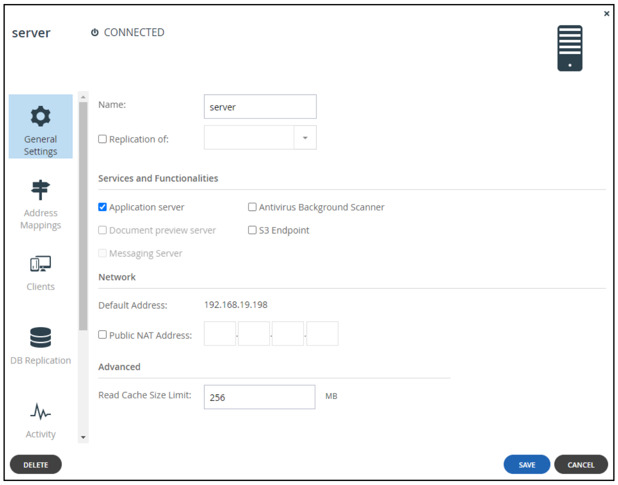
To edit server settings:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed, listing all the servers for the HCP Anywhere Enterprise Portal.
2. Click the server to edit.

   The server window is displayed with the server name as the window title.
3. Edit and monitor the following settings:
   - General Settings
   - Address Mappings
   - Clients
   - DB Replication – This option is only available for the main database and database replication servers.
   - Activity
   - Tasks
   - Status
4. Click **SAVE**.

General Settings

You can edit server settings, including configuring a server as an application server, setting the public IP address of the server, and the IP address to which each virtual portal's DNS should resolve. This allows you to restrict specific portals to be accessible only from a specific network interface.



server ⏻ CONNECTED

Name: server

□ Replication of:

Services and Functionalities

☑ Application server
□ Antivirus Background Scanner
□ Document preview server
□ S3 Endpoint
□ Messaging Server

Network

Default Address: 192.168.19.198

□ Public NAT Address: . . .

Advanced

Read Cache Size Limit: 256 MB

Note: The **DB Replication** option is only available for the main database and database replication servers.

- In the **General Settings** option, you can edit the following settings:

  Name – The unique name of the server.

  Replication of – The server is a replication server of the specified server. Replication is configured when the server is installed.

  Services and Functionalities

  Application server – The server is an application server. An application server accepts CTTP connections from HCP Anywhere Enterprise Edge Filers and Agents and HTTPS connections from end users. If unchecked, this server does not allow any client logins. Hitachi Vantara recommends designating at least two servers to act as application servers, for high availability.

  Antivirus Background Scanner – An antivirus background scan runs on this server.

  Document preview server – The server is a document preview server. HCP Anywhere Enterprise recommends designating at least two servers for generating document previews, for high availability. When a server is defined as a document preview server, the other server type options are disabled. Document previews are requested in the end user portal's Web interface, the Cloud Drive. When a user clicks on a file’s name or icon in one of these locations, the file is displayed in the online viewer.

  You have to uncheck **Application server** before you can check **Document preview server**. After checking **Document preview server**, you need to restart the server.

  S3 Endpoint – The server supports access to cloud drive folders from an S3 browser. Checking the S3 Endpoint is required on only one server. For high availability, you can set the S3 Endpoint on more than one server.

  Messaging Server – The server will also act as a messaging server. For details about the Hitachi Vantara Messaging service and server requirements, see Managing the HCP Anywhere Enterprise Messaging Service.

  Network

Default Address – The default IP address of the server.
Public NAT Address – The default IP address has a public Network Address Translation (NAT). Specify the public IP address. This controls the default IP address of this server that is exposed using DNS.

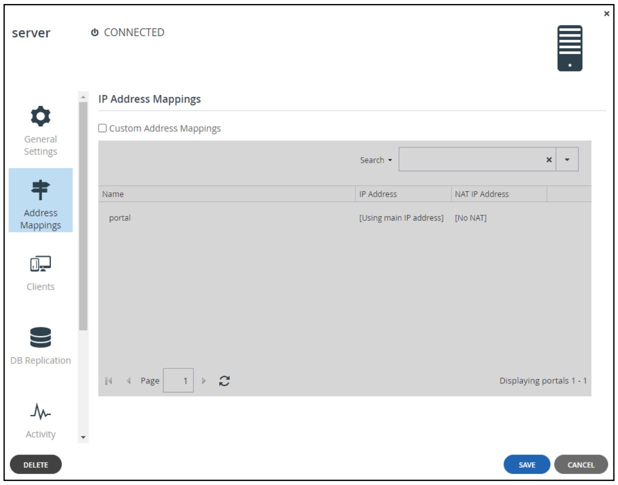
Advanced

Read Cache Size Limit – The maximum amount of server RAM to allocate to the read cache that is used to accelerate reads from the storage nodes. Recently read blocks are kept in the cache to avoid repetitive requests from the storage node. When the cache fills up, the blocks that have been in the cache the longest are removed.

5. Click **SAVE**.

Address Mappings

By default, HCP Anywhere Enterprise Portal listens to virtual portals on the default address. You can optionally bind specific virtual portals to other interfaces (specified by IP address) of the server, which will cause this IP address to be published by the DNS server, and will prevent access to the specified portal via other IP addresses of the server.



IP Address Mappings

□ Custom Address Mappings

Name	IP Address	NAT IP Address
portal	[Using main IP address]	[No NAT]

Displaying portals 1 - 1

Note: The **DB Replication** option is only available for the main database and database replication servers.

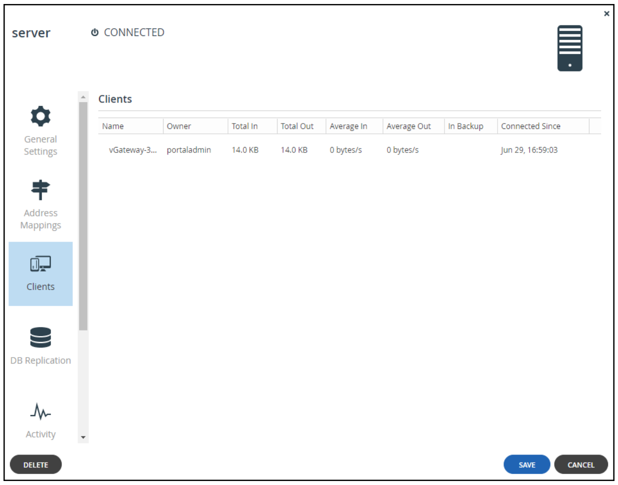
To set custom address mappings:

- Check **Custom Address Mappings**.
  You can edit the following settings:
  IP Address – The IP address for the virtual portal bound to an IP address of the server. If the virtual portal uses the default IP address, `Using main IP address` is displayed. You can change this to an IP address of the local interface to accept connections for clients.
  NAT IP Address – If NAT is used, and the public IP address of the interface differs from the private IP address, specify the IP address to which the original IP address should be translated. This public address will be published by the HCP Anywhere Enterprise Portal DNS server. To bind this team portal to the default IP address, do not enter a value in this field. To specify that the public IP address is equal to the private IP address, do not enter a value in this field.

Clients

You can view information about a server's currently connected devices.

Note: The **DB Replication** option is only available for the main database and database replication servers.



Clients

Name	Owner	Total In	Total Out	Average In	Average Out	In Backup	Connected Since
vGateway-3...	portaladmin	14.0 KB	14.0 KB	0 bytes/s	0 bytes/s		Jun 29, 16:59:03

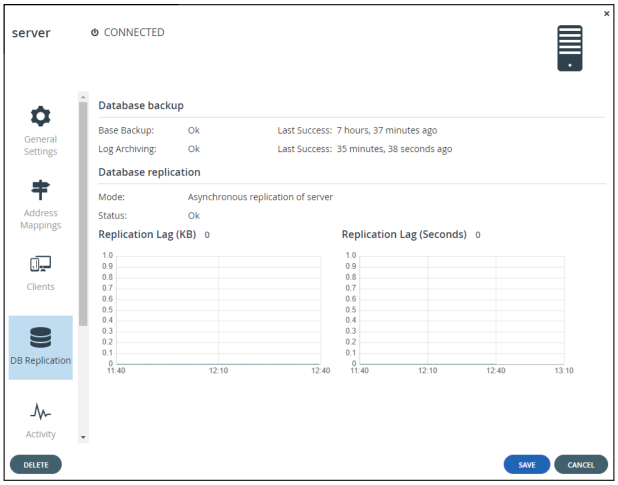
To view a server's currently connected devices:

- In the **Clients** option, you can view the following settings:
  Name – The name of the client device.
  Owner – The name of the client device's owner.
  Total In – The total CTTP traffic sent from the client device to the virtual portal.
  Total Out – The total CTTP traffic sent from the virtual portal to the client device.
  Average In – The average speed, throughput, of traffic sent from the client device to the team portal in bytes/second.
  Average Out – The average speed, throughput, of traffic sent from the team portal to the client device in bytes/second.
  Connected Since – The date and time when the connection started.

DB Replication

Note: This option is only available for the main database and database replication servers.

You can monitor the performance of the replication server by selecting the **DB Replication** tab in the server window.



Database backup

Base Backup: Ok Last Success: 7 hours, 37 minutes ago

Log Archiving: Ok Last Success: 35 minutes, 38 seconds ago

Database replication

Mode: Asynchronous replication of server

Status: Ok

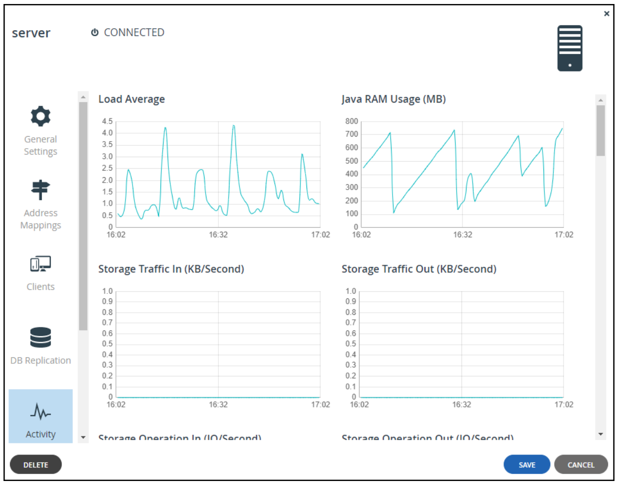
Replication Lag (KB) 0

Replication Lag (Seconds) 0

The portal reports the status of its scheduled base backups and transaction log archiving process, as well as additional metrics to help detect when database replication falls behind due to lags in the process. In the event that replication falls behind, portal administrators are notified via email. The relevant email templates are *Replication setup failed* and *Replication has errors*.

Activity

You can view charts displaying a server's activity data.



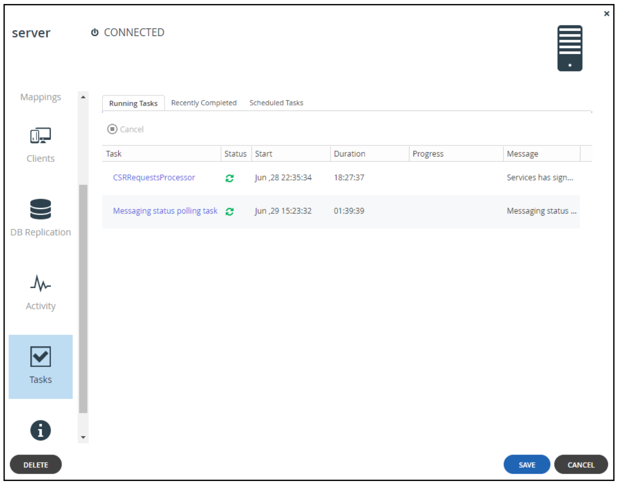
Note: The **DB Replication** option is only available for the main database and database replication servers.

To view server activity:

- In the **Activity** option, you can view the following:
  Load Average – The server's average load over time. A server's *load* is the number of currently running processes that are using, or waiting to use, the CPU.
  Java RAM Usage (MB) – The server's Java RAM usage in MB over time.
  Storage Traffic In (KB/Second) – The incoming storage traffic over time.
  Storage Traffic Out (KB/Second) – The outgoing storage traffic over time.
  Storage Operation In (IO/Second) – The number of read operations performed by the HCP Anywhere Enterprise Portal on cloud storage nodes.
  Storage Operation Out (IO/Second) – The number of store operations performed by the HCP Anywhere Enterprise Portal on cloud storage nodes.
  CTTP Traffic In (KB/Second) – The incoming CTTP traffic over time.
  CTTP Traffic Out (KB/Second) – The outgoing CTTP traffic over time.
  Blocks Cleaned (Blocks/Second) – The number of blocks cleaned per second, as part of system maintenance.
  Blocks Reclaimed (Blocks/Second) – The number of blocks deleted per second, as part of system maintenance.
  AV Throughput (KB/Second) – The amount of throughput by Cloud Drive antivirus.
  AV Files Scanned - On Demand (File/Second) – The number of files scanned by Cloud Drive antivirus.
  AV Files Scanned - Background (File/Second) – The number of files scanned by the background scan.
  DLP Throughput (KB/Second) – This feature is currently not supported.
  DLP Files Scanned - On Demand (File/Second) – This feature is currently not supported.
  Block Verifications (Per Minute) – The number of block verifications per minute. Block verifications are executed when the portal is executing a consistency check as part of system maintenance.
  Commit Threads – The number of threads running and waiting.
  File Previews (Per Minute) – The number of files previewed per minute.
  Storage Migration Traffic (KB/Second) – The amount of storage node migration traffic.
  Blocks Migrated (Blocks/Second) – The number of blocks migrated in storage node migration.
  Mapfile Blocks Cleaned (Blocks/Second) – The number of mapfile blocks cleaned per second, as part of system maintenance.
  Outbound Database Connections – The number of outbound database connections over time.
  Inbound Database Connections – The number of inbound database connections over time.
  Database Transactions (Per Minute) – Database transactions per minute.
  Logged In Users – The number of HCP Anywhere Enterprise Portal administrators logged in over time.
  Connected Devices – The number of connected client devices over time.

Tasks

You can view the server's currently running, completed, and scheduled tasks. These tasks run in background.

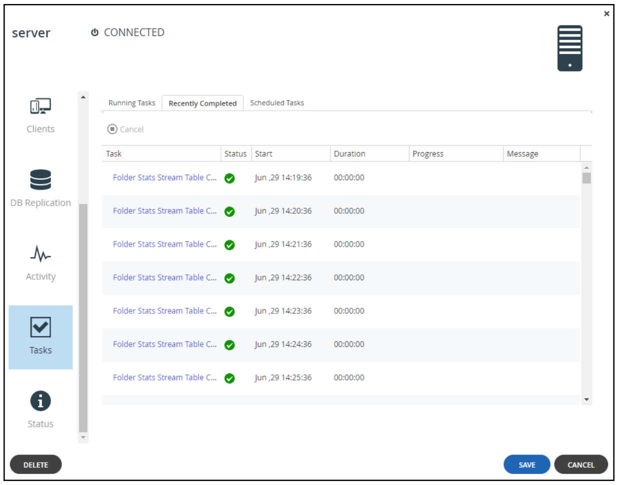


Task	Status	Start	Duration	Progress	Message
CSRRequestsProcessor	⟳	Jun ,28 22:35:34	18:27:37		Services has sign...
Messaging status polling task	⟳	Jun ,29 15:23:32	01:39:39		Messaging status ...

Note: The **DB Replication** option is only available for the main database and database replication servers.

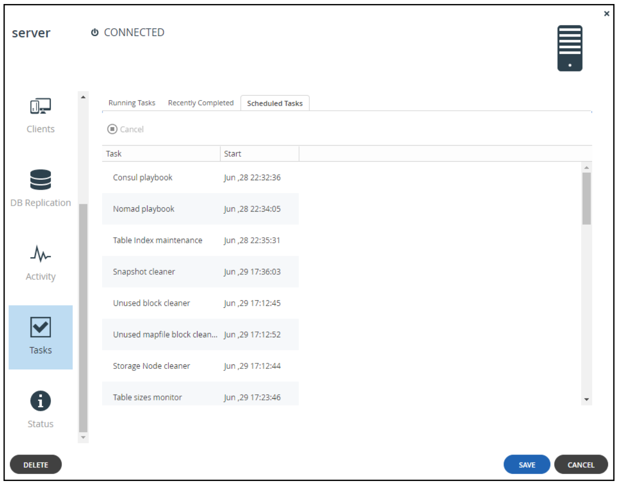
To view a server's tasks:

- In the **Tasks** option, view the following:
  Running Tasks tab **–** The currently running tasks.
  Recently Completed tab **–** The tasks completed since the beginning of the day.



Task	Status	Start	Duration	Progress	Message
Folder Stats Stream Table C...	✓	Jun ,29 14:19:36	00:00:00		
Folder Stats Stream Table C...	✓	Jun ,29 14:20:36	00:00:00		
Folder Stats Stream Table C...	✓	Jun ,29 14:21:36	00:00:00		
Folder Stats Stream Table C...	✓	Jun ,29 14:22:36	00:00:00		
Folder Stats Stream Table C...	✓	Jun ,29 14:23:36	00:00:00		
Folder Stats Stream Table C...	✓	Jun ,29 14:24:36	00:00:00		
Folder Stats Stream Table C...	✓	Jun ,29 14:25:36	00:00:00		

  Scheduled Tasks tab **–** The scheduled tasks that have not started. The information displayed includes the date and time at which the task is scheduled to start.



Task	Start
Consul playbook	Jun ,28 22:32:36
Nomad playbook	Jun ,28 22:34:05
Table Index maintenance	Jun ,28 22:35:31
Snapshot cleaner	Jun ,29 17:36:03
Unused block cleaner	Jun ,29 17:12:45
Unused mapfile block clean...	Jun ,29 17:12:52
Storage Node cleaner	Jun ,29 17:12:44
Table sizes monitor	Jun ,29 17:23:46

The following information is displayed for a task:

Task – The name of the task that is running, completed, or scheduled.

Status – The following icons are used for the task status of a running or completed task:

↻ – In progress.

✓ – Completed successfully.

❗ – Failed.

Start – The date and time at which the task started or will start for a scheduled task.

Duration – The amount of time the task took, or has taken so far for a running or completed task.

Progress – The task's progress for a running or completed task.

Message – Additional information about the task for a running or completed task.

List of Tasks

Task	Description	Server	Default Frequency
ACL Repair Tool			
Administrator report generator	Generates administrator reports.	Application	Daily
Agent licensing refresh	Refreshes HCP Anywhere Enterprise Drive Share (Agent) licensing.	Application	Ongoing
Alert sender	Generate and send emails, such as backup completed emails and log alerts.	Application	Every 60 seconds
Antivirus background scanning	Scan recently uploaded files for viruses in background.	—	Ongoing: After files are uploaded. If no files are uploaded, the scan stops for 30 seconds before checking again. Or, on demand
Antivirus re-scanning server	If a background scan has a file to scan when a rescan is initiated, the background scan completes before the rescan proceeds and files scanned during the background scan are not rescanned. Renaming a folder is treated as if the folder and the files in the folder are new. During a background scan the files in the folder are scanned first.	—	On demand
Apply Templates	Downloads templates to the connected devices.	Application	Every 600 seconds
Attachments Cleaner	Deletes expired folders of email attachments.	Application	Daily
Block Health Task			
Catalog Synchronizer			
Certificate and licenses update			
Clear Sensitive			
Cloud-DD	Tool for storage node reader/writer thread count optimization.	—	On demand
Containers cleaner			
Copy			
CSRRequestsProcessor			

Task	Description	Server	Default Frequency
Db activator and initiator			
DB Backup			
db-faulty-handler-task			
db-updater-task			
Delete			
Delete conflict files			
Delete from quarantine	Delete quarantined files.		On demand.
Delete Infected file	Delete infected files not in quarantine.		
Deleted Share Cleaner			
Disconnect devices of disabled accounts	Disconnects devices of disabled users.	Application	Daily
Entities Version Cleaner			
Expired invitations cleaner	Check for expired invitations and delete.	Main Database	Daily
Export folder			
Folder Group Key Manager Adaptor			
Frequent Contacts Cleaner	Cleans recently used contacts.	Application	Daily
FSCK	Runs file system check on the blocks in the system.	Main Database	On demand
FSCK Missing FolderGroup Cleaner			
Generate Support Report	Support report generator for administrator.	Application	On demand
Generate user notifications			
Get Mapfiles From CSV Task			
Import folder			

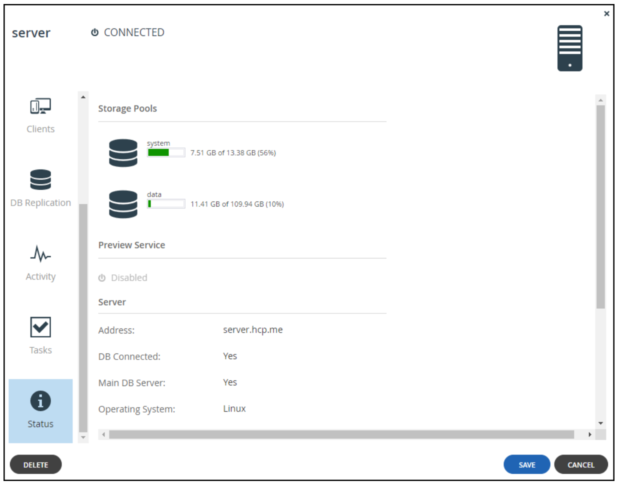
Task	Description	Server	Default Frequency
Inactive account cleaner	Does the following: • Deletes old *changing mail* pending requests from the database. • Deletes *recover password* pending requests from the database. • Deletes old inactive users and devices from the database. • Deletes old *invite to register* pending requests from the database. • Deletes old transient devices. • Permanently deletes already deleted devices.	Application	Daily
Key Manager Monitoring			
List Map File Blocks Task			
Logs Cleaner	Deletes old logs.	Application	Daily
Match auto-assignment rule	Matches templates for devices.	Application	Daily
Move			
New	Re-enables sending emails for notifications that were already sent.	Application	Daily
New Stub Files Repair Task			
Notification suppress cleaner			
Office Online Locks Cleaner	Clean office locked files.		
Orphan Scanner	Find blocks that exist in the portal but not in the storage node.	Main Database	On demand
Portal Notifications Background Mail Sender	Enters new notifications to a queue.	Application	Every hour.
Portal notifications mailing queue			
Portals Trashcan Cleaner	Checks and empties a deleted portal trashcan.	Main Database	Daily
Process ACL Parser			
Purge Storage Exceptions	Remove old storage exceptions.		

Task	Description	Server	Default Frequency
Quota Changes Notifier			
Replication Monitoring			
Report generator	Generates users reports.	Application	Once a day and on demand. Sends the report only when needed. For each end-user once a month.
Rescan			
Restore			
Scan folder			
Set ACL			
Set ACLOwner			
Shared as team sync Synchronizer	Fixes domains of shared resources when a sharing problem occurs writing to a database.	Main Database	Daily
Slave archive synchronization			
Snapshot cleaner	Deletes old temporary snapshots.	Main Database	Every 30 minutes
Snapshot closer	Closes uncompleted snapshots and inactive snapshots open more than 2 days.	Main Database	Every 300 seconds
Snapshot consolidator	consolidate snapshots to reduce the saved snapshots.	Main Database	Every hour
Snapshots simulator			
Start Replication			
Storage license quota			
Storage Node cleaner	Cleans deleted blocks from storage nodes.	Main Database	Every 60 seconds
Storage node migration			
Storage Usage Calculator	Recalculates storage usage for each user and portal.	Application	Daily
Storage Usage Cleaner	Deletes records from the storage usage table for old users and portals (not the actual data).	Application	Daily
Table Index maintenance			
Table sizes monitor	Trace for table size.		

Task	Description	Server	Default Frequency
Task update antivirus status	Antivirus monitor status.		
Undelete	Restore deleted files in retention range.		On demand
Unquarantine	Remove files from quarantine.		On demand
Unused block cleaner	Deletes unused blocks.	Main Database	Every 60 seconds
Unused mapfile block cleaner			
Update accounts	Updates users and groups from active directory, including deleting and adding users. Updates also user plans if needed.	Application	Daily
Update storage status	Monitors and updates storage status.		
Verify files			
Zones Synchronizer	Updates zones according to recent changes.		

Status

You can view the current status of servers.



system 7.51 GB of 13.38 GB (56%)

data 11.41 GB of 109.94 GB (10%)

Disabled

Address: server.hcp.me

DB Connected: Yes

Main DB Server: Yes

Operating System: Linux

To view server statuses:

- In the **Status** option, you can view the following:
  Load Average – The server's average load over time. A server's *load* is the number of currently running processes that are using, or waiting to use, the CPU.
  The following information is available.
  Storage Pools – The status and amount of free storage on each server storage pool.
  Preview Service – Disabled if not a document preview server. For a server configured as

document preview server, the status of the preview service. Click **Restart** to restart the preview server.

Server – Details about the server:

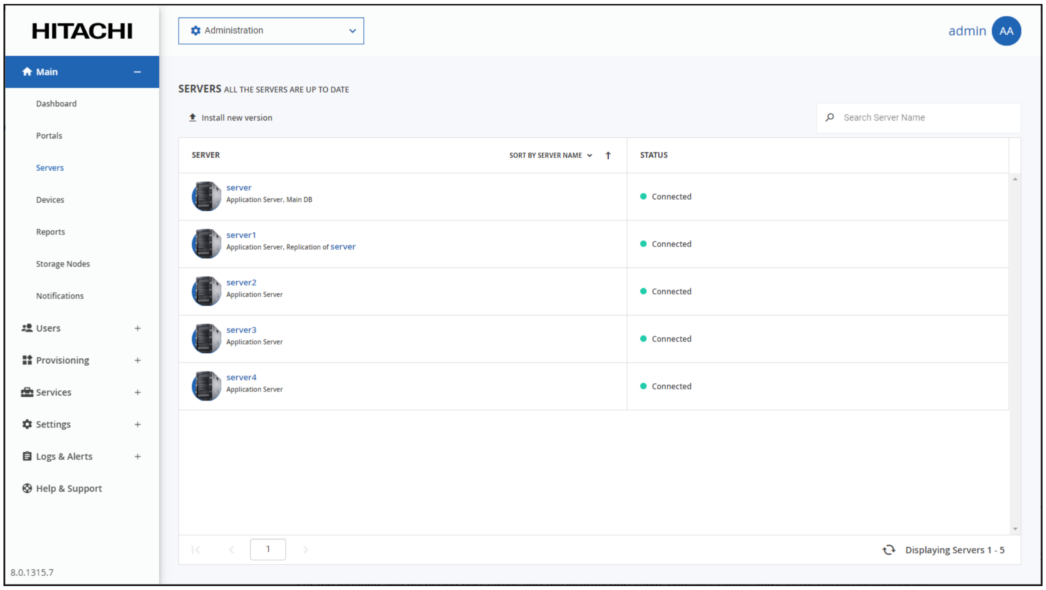
- **Address –** The server's domain name.
- **DB Connected –** Whether the DB is connected to the HCP Anywhere Enterprise Portal application.
- **Main DB Server –** Whether the server is the main DB server.
- **Operating System –** The server's operating system.
- **RAM –** The server's RAM and the amount of free RAM.
- **Number of CPUs –** The number of CPUs.
- **Portal Version –** The HCP Anywhere Enterprise Portal version.
- **Platform –** The platform on which the HCP Anywhere Enterprise Portal is installed.
- **Image Version –** The version number of the server image.
- **Uptime –** The time that the server has been up.
- **Tomcat Uptime –** The time that the Tomcat application server has been up.

Restarting and Shutting Down a Server

HCP Anywhere Enterprise Portal servers can be restarted and shut down from the global administration view.

To restart a server:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

Displaying Servers 1 - 5

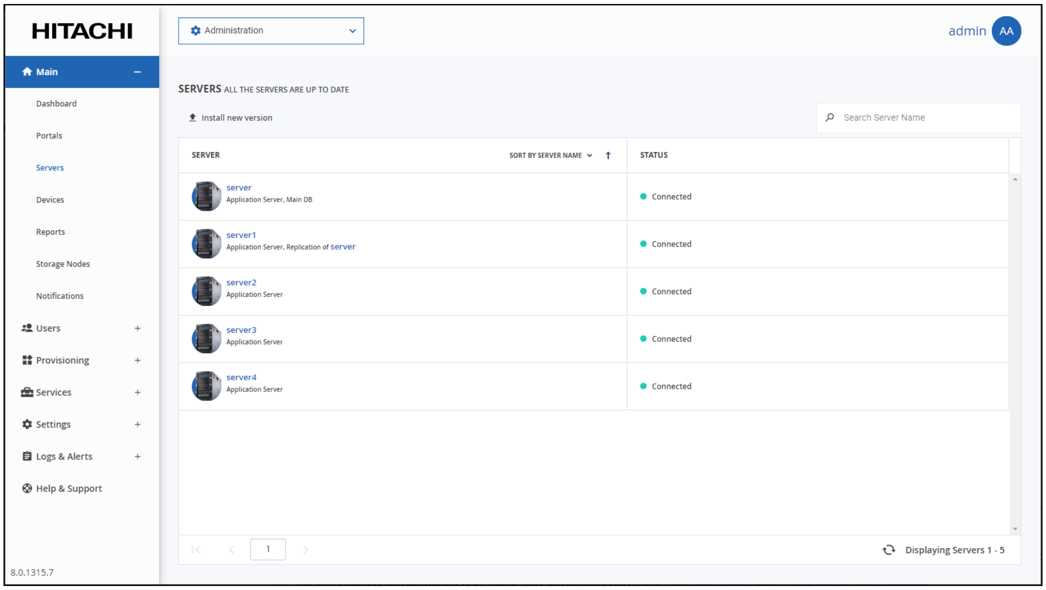
2. Select the server to restart and click **Restart**.

   A confirmation window is displayed.
3. Click **RESTART** to confirm.

The server is restarted.

To shut down a server:

1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

2. Select the server to restart and click **Shutdown**.

   A confirmation window is displayed.
3. Click **SHUTDOWN** to confirm.

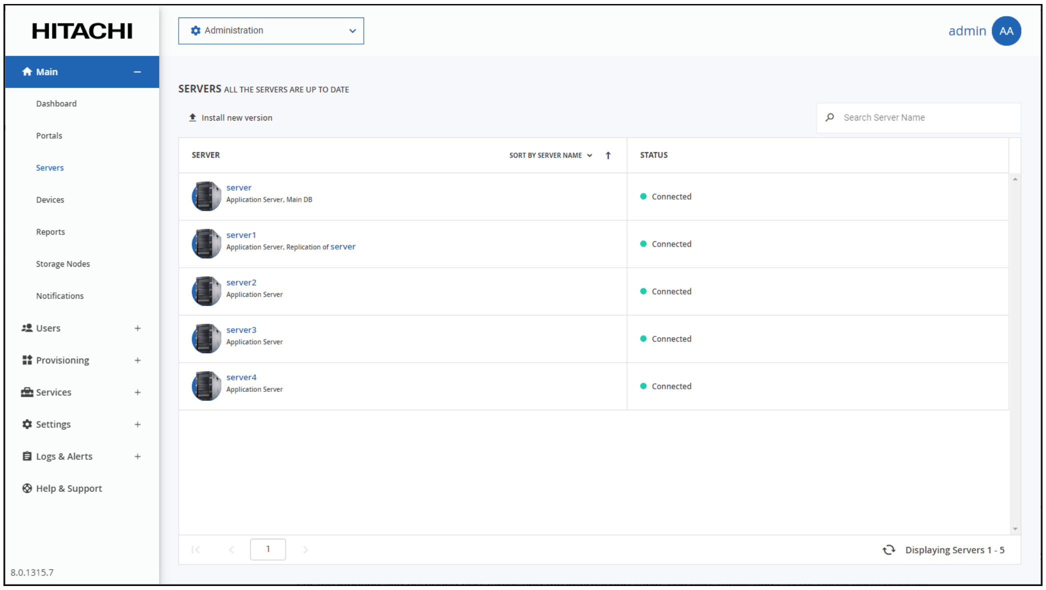
The server is shut down.

Deleting a Server

HCP Anywhere Enterprise Portal servers can be deleted from the global administration view.

To delete a server:

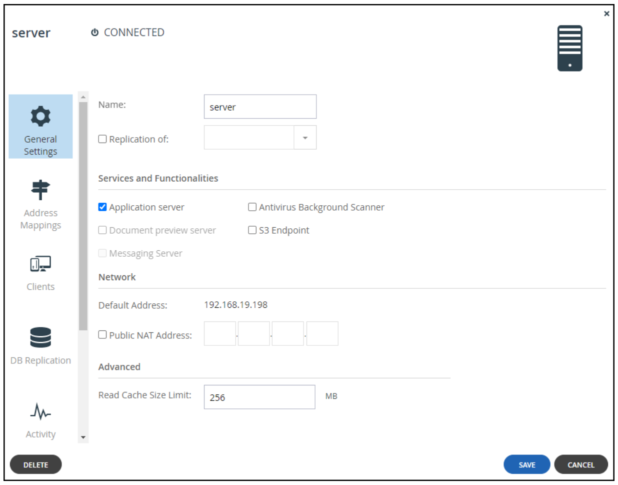
1. In the global administration view, select **Main > Servers** in the navigation pane.
   The **SERVERS** page is displayed.



SERVERS ALL THE SERVERS ARE UP TO DATE

SERVER	STATUS
server Application Server, Main DB	Connected
server1 Application Server, Replication of server	Connected
server2 Application Server	Connected
server3 Application Server	Connected
server4 Application Server	Connected

2. Either,
   a) Select the server to delete and click **Delete**.
   A confirmation window is displayed.
   b) Click **DELETE** to confirm.
   Or,
   a) Click the server name.
   The server window is displayed with the server name as the window title.



Name: server

□ Replication of:

Services and Functionalities

☑ Application server
□ Antivirus Background Scanner
□ Document preview server
□ S3 Endpoint
□ Messaging Server

Network

Default Address: 192.168.19.198

□ Public NAT Address:

Advanced

Read Cache Size Limit: 256 MB

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

c) Click **YES** to confirm.

The server is deleted.

Note: If you attempt to delete the Main DB server, Replication server, or a Messaging server, an **ERROR** window is displayed, informing you that the server cannot be deleted.

Upgrading a Server to a Newer Version

A new version of a HCP Anywhere Enterprise Portal server can be installed from the global administration view.

You should only install new software with the help of Hitachi Vantara Support.

Chapter 26. Managing Firmware Images

Each HCP Anywhere Enterprise Edge Filer or HCP Anywhere Enterprise Drive Share (Agent) in the HCP Anywhere Enterprise Portal system is installed with an image that suits the device platform.

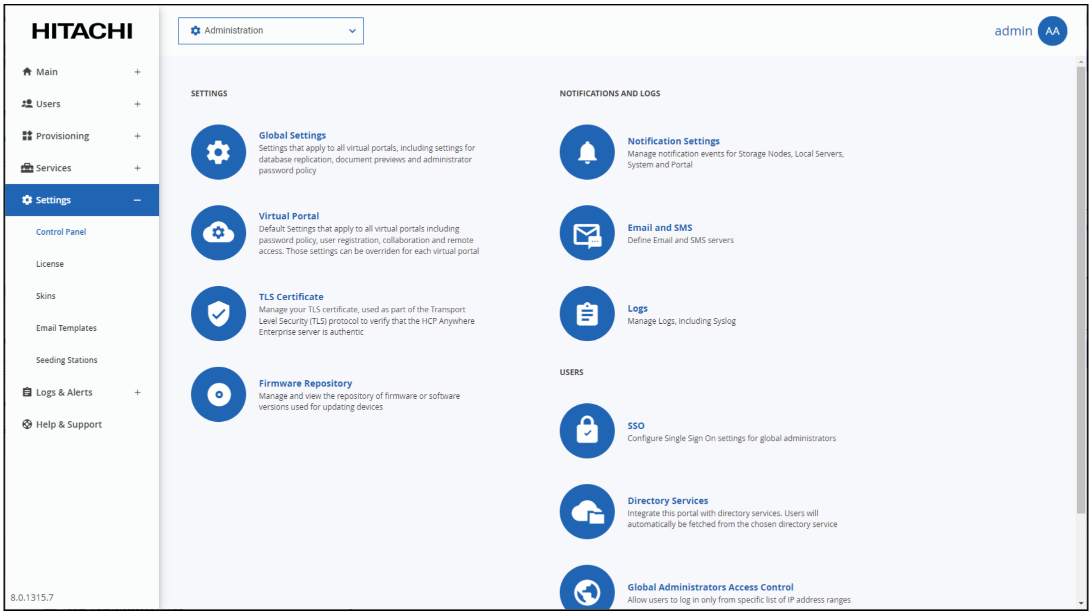
Note: Both the software, such as the HCP Anywhere Enterprise Drive Share (Agent) software packages, and firmware images are referred to as *firmware*.

In this chapter

Viewing Firmware Images

To view all firmware images in the system:

1. In the global administration view, select **Settings** in the navigation pane. The **Control Panel** page is displayed.



Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

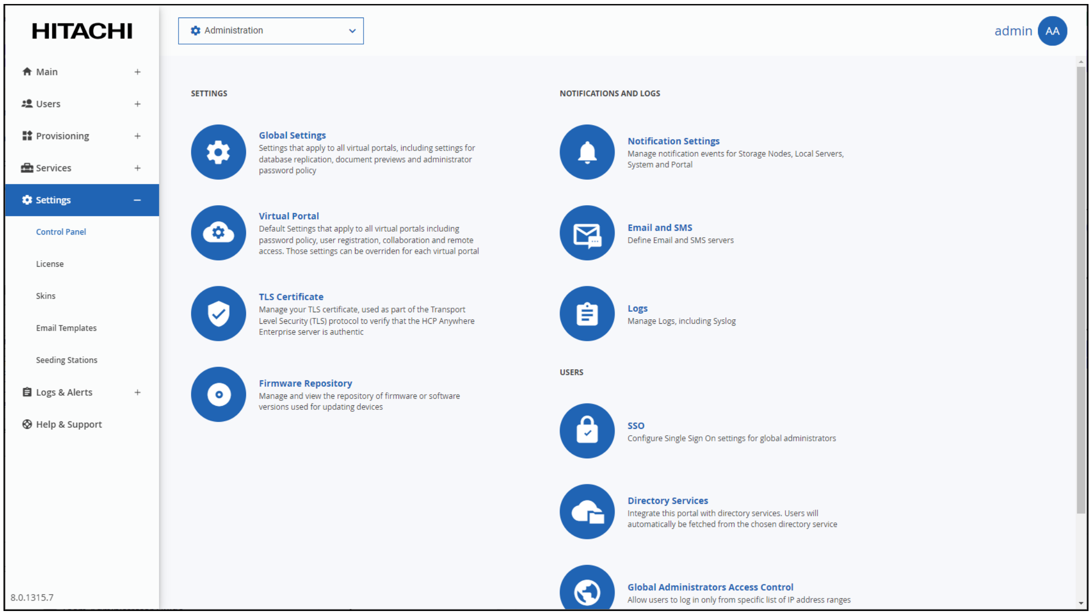
   The **Firmware Repository** window is displayed. The window shows the firmware available in the portal firmware repository.

   The current firmware in the repository is marked with .

Uploading Firmware Images

To upload a firmware image:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

USERS

SSO
Configure Single Sign On settings for global administrators

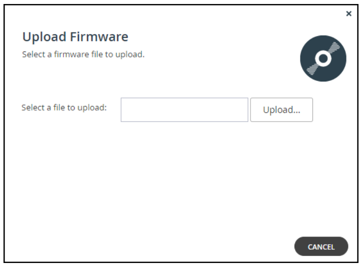
Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

   The **Firmware Repository** window is displayed.
3. Click **Upload**.

   The **Upload Firmware Wizard** opens displaying the **Upload Firmware** window.



Upload Firmware

Select a firmware file to upload.

4. Click **Upload** and browse to the file to upload.
5. Click **Open**.

   The firmware image is uploaded to the relevant device platform category and a completed window is displayed.
6. Click **FINISH**.

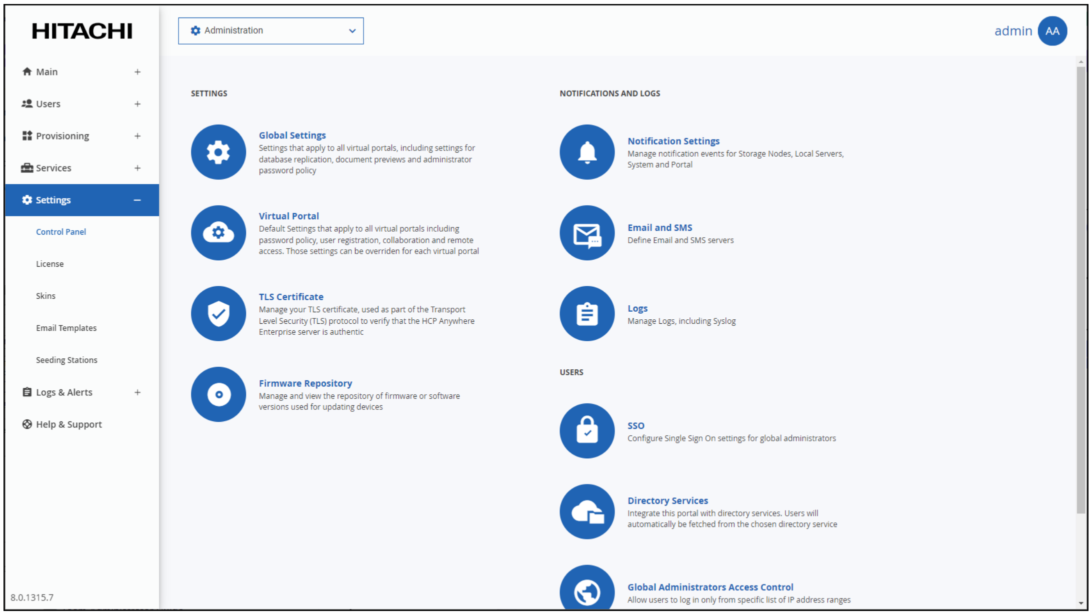
Marking a Firmware Image as the Current Firmware Image

When you mark a firmware image as the current firmware image, all devices of the relevant device platform that are 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 global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

   The **Firmware Repository** window is displayed showing the firmware available in the repository.
3. Select the firmware to make current.
4. Click **Mark as Current**.

The selected firmware image becomes the current firmware image and is marked with ⚙.

To mark a firmware image as not current:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.
2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

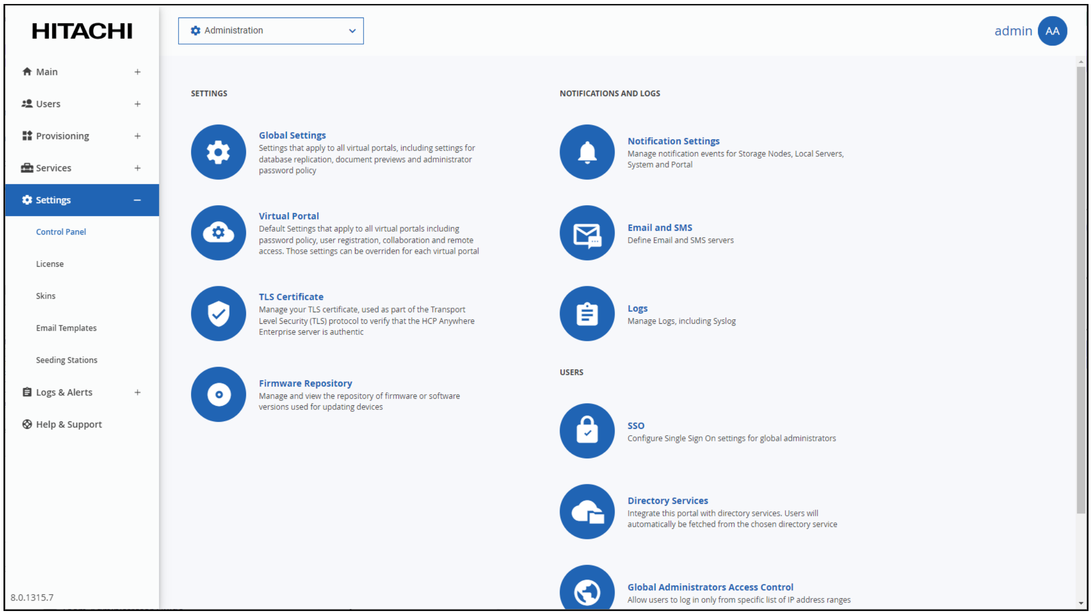
   The **Firmware Repository** window is displayed showing the firmware available in the repository.
3. Select the desired firmware image's row.
4. Click **Remove Current**.

Viewing Devices that Use a Specific Firmware Image

You can view all devices that are connected to the portal that are configured to use a specific firmware.

To view devices with a specific firmware configured:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

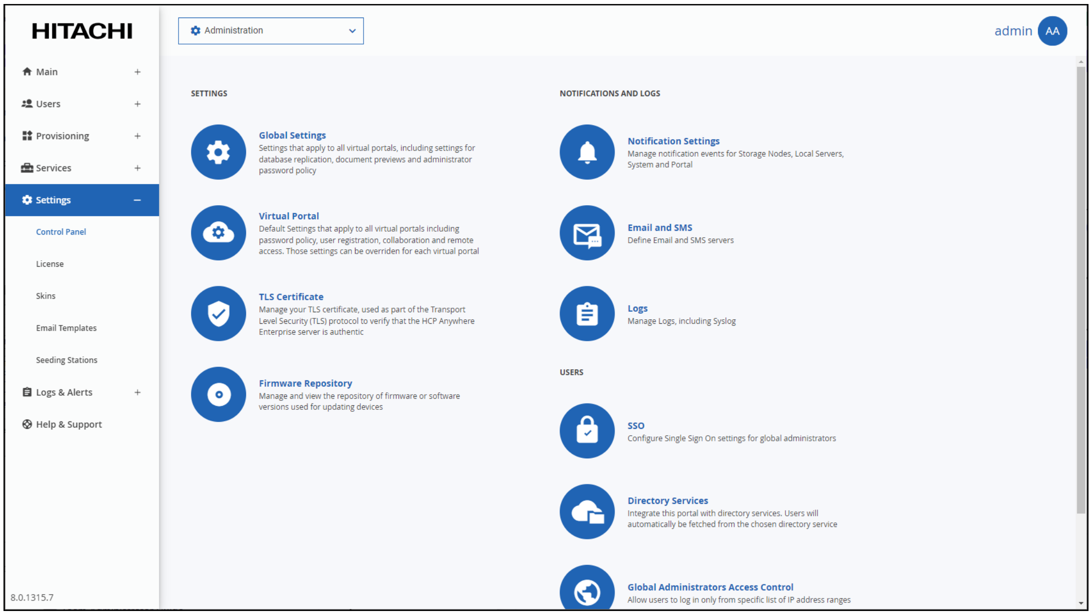
2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

   The **Firmware Repository** window is displayed showing the firmware available in the repository.
3. Click the firmware image for which you want to view the devices with this image.
4. Click **Show devices**.

Deleting Firmware Images

To delete a firmware image:

1. In the global administration view, select **Settings** in the navigation pane.
   The **Control Panel** page is displayed.



SETTINGS

Global Settings
Settings that apply to all virtual portals, including settings for database replication, document previews and administrator password policy

Virtual Portal
Default Settings that apply to all virtual portals including password policy, user registration, collaboration and remote access. Those settings can be overriden for each virtual portal

TLS Certificate
Manage your TLS certificate, used as part of the Transport Level Security (TLS) protocol to verify that the HCP Anywhere Enterprise server is authentic

Firmware Repository
Manage and view the repository of firmware or software versions used for updating devices

NOTIFICATIONS AND LOGS

Notification Settings
Manage notification events for Storage Nodes, Local Servers, System and Portal

Email and SMS
Define Email and SMS servers

Logs
Manage Logs, including Syslog

USERS

SSO
Configure Single Sign On settings for global administrators

Directory Services
Integrate this portal with directory services. Users will automatically be fetched from the chosen directory service

Global Administrators Access Control
Allow users to log in only from specific list of IP address ranges

2. Select **Firmware Repository**, under **SETTINGS** in the **Control Panel** page.

   The **Firmware Repository** window is displayed showing the firmware available in the repository.
3. Select the firmware image to remove from the repository.
4. Click **Delete.**

   A confirmation window is displayed.
5. Click **YES**.

The firmware image is deleted.

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