Hitachi Content Platform Anywhere Enterprise

v7.8

Edge Filer Installation Guide for Nutanix AHV

This book describes how to install and configure HCP Anywhere Enterprise Edge Filer on a Nutanix AHV platform.

MK-HCPAE019-01
September 2024

© 2023, 2024 Hitachi Vantara. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2) Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.
Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at https://www.hitachivantara.com/en-us/company/legal.html.

Contents

Preface 4

Chapter 1. The HCP Anywhere Enterprise Edge Filer 5

Technical Specifications 6
Port Requirements 6
Browser Requirements 7
License Types 8

Chapter 2. HCP Anywhere Enterprise Edge Filer Planning 9

Chapter 3. Installing the HCP Anywhere Enterprise Edge Filer in a Nutanix AHV environment 10

Chapter 4. First-Time Setup 15

Configuring the HCP Anywhere Enterprise Portal as a Precondition to Setting Up the HCP Anywhere Enterprise Edge Filer 15
Initial HCP Anywhere Enterprise Edge Filer Setup 18
Loading a Certificate to a HCP Anywhere Enterprise Edge Filer 24
Managing TLS Certificates 25
Additionally Trusted Certificate Authorities 27

Chapter 5. Migrating a File Server 29

Discovering Shares 31
The Dashboard After a Discovery Run 35
The Discovery Report 36
Migrating Shares 38
Preparing the HCP Anywhere Enterprise Portal to Migrate WORM Compliant Shares 38
Commands to Run Before and After the Migration 39
Migration Procedure 39
Completing a Migration and Performing a Delta Migration 47

Preface

About this document

Hitachi Content Platform Anywhere Enterprise Edge Filers (HCP Anywhere Enterprise Edge Filers) seamlessly combine collaboration capabilities, local storage, cloud storage, and data protection functionality in a single, cost-effective package. This document describes how to install and perform the initial setup of HCP Anywhere Enterprise Edge Filer on a Nutanix AHV platform.

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 users from a Windows or 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. The HCP Anywhere Enterprise Edge Filer

HCP Anywhere Enterprise Edge Filers seamlessly combine collaboration capabilities, local storage, cloud storage, and data protection functionality in a single, cost-effective package. HCP Anywhere Enterprise Edge Filers are available as virtual appliances: V Series HCP Anywhere Enterprise Edge Filers are software-based gateways running on a hypervisor, such as ESXi or KVM, or in a cloud, such as AWS.

HCP Anywhere Enterprise Edge Filers replace file servers and other traditional file storage solutions with a single, cloud-integrated and cost-effective solution.

HCP Anywhere Enterprise Edge Filers:

- Incorporate Intelligent caching technology.
  Dynamically cache files from a secure HCP Anywhere Enterprise Portal to the HCP Anywhere Enterprise Edge Filer.
- Deliver unlimited file access to office users, with visibility to all organizational files centralized in the cloud, either private or public.
- Share files across your network and provide users with collaboration across offices and endpoints with no local storage restraints.
- Synchronize folders across your network and the cloud, including keeping the main storage on the cloud with stubs saved on the HCP Anywhere Enterprise Edge Filer. A stub is a file with a tiny footprint that contains the metadata about the file, such as the file name, size, and modification date. Only the folder and file metadata and not the actual file content is saved locally.

The HCP Anywhere Enterprise Edge Filer is managed using a web-based interface or centrally through the HCP Anywhere Enterprise Portal. The HCP Anywhere Enterprise Portal also allows users to sync content between the HCP Anywhere Enterprise Portal and the HCP Anywhere Enterprise Edge Filer, as well as between HCP Anywhere Enterprise Edge Filers located in different branch offices.

The HCP Anywhere Enterprise Edge Filer connects to a HCP Anywhere Enterprise Portal to provide users with LAN speed access to all their home folders and shared folders on the HCP Anywhere Enterprise Portal. Local user accounts are mapped to the equivalent user accounts in the cloud so that each user sees only his or her personal view of the cloud files. Users can access locally stored, synced copies of the folders they are allowed to access on the HCP Anywhere Enterprise Portal.

The main storage is on the HCP Anywhere Enterprise Portal in the cloud with stubs saved on the HCP Anywhere Enterprise Edge Filer. A stub is a file with a tiny footprint that contains the metadata about the file, such as the file name, size, and modification date. Only the folder and file metadata and not the actual file content is saved locally. This results in the cost of storage being significantly lower. Also, systems with many file changes, where only some of the files are required locally, don't over use bandwidth between the cloud and HCP Anywhere Enterprise Edge Filer. Only the required files are passed across the wire.

When a user accesses a file stub, the file is downloaded and opened without delay, and where possible, large files are streamed from the cloud so they can be accessed faster. After the download has completed, the file is *unstubbed*. Any changes to the file are synced back to the HCP Anywhere

Enterprise Portal. Folders that are always required can be pinned, in which case the files in the folders, and not the stubs, are stored on the HCP Anywhere Enterprise Edge Filer.

Technical Specifications

Port Requirements

- Firewall ports opened for LAN communication and managing the HCP Anywhere Enterprise Edge Filer user interface:

Port	Protocol	Direction	Notes
443	TCP	Inbound	HTTPS. This port should be behind the firewall.

- Firewall ports opened to the HCP Anywhere Enterprise Portal:

Port	Protocol	Direction	Notes
443	TCP	Inbound	HTTPS. This port should only be open to the specific HCP Anywhere Enterprise Portal IP addresses.
995	TCP	outbound	CTTP. Communications with HCP Anywhere Enterprise Portals.
8443	TCP	outbound	—

- Firewall ports opened to the HCP Anywhere Enterprise Portal backend storage when **Direct Mode** is set for the storage node in the HCP Anywhere Enterprise Portal:

Port	Protocol	Direction	Notes
443	TCP	Outbound	HTTPS

- Firewall ports opened for Active Directory:

Port	Protocol	Direction	Notes
88	TCP/UDP	Outbound	If Kerberos is used
389/3268	TCP/UDP	Outbound	LDAP protocol/LDAP GC (Global Catalog) protocol
445	TCP	Outbound	SMB when joining to a domain as a Computer account

- Firewall ports opened for antivirus updates:

Port	Protocol	Direction	Notes
80	TCP	Outbound	HTTP

- Firewall ports opened for SMTP:

Port	Protocol	Direction	Notes
25	TCP	Outbound	The port is configurable in the HCP Anywhere Enterprise Edge Filer user interface (in the **Configuration** view, select **Alerts > Mail Server** in the navigation pane).

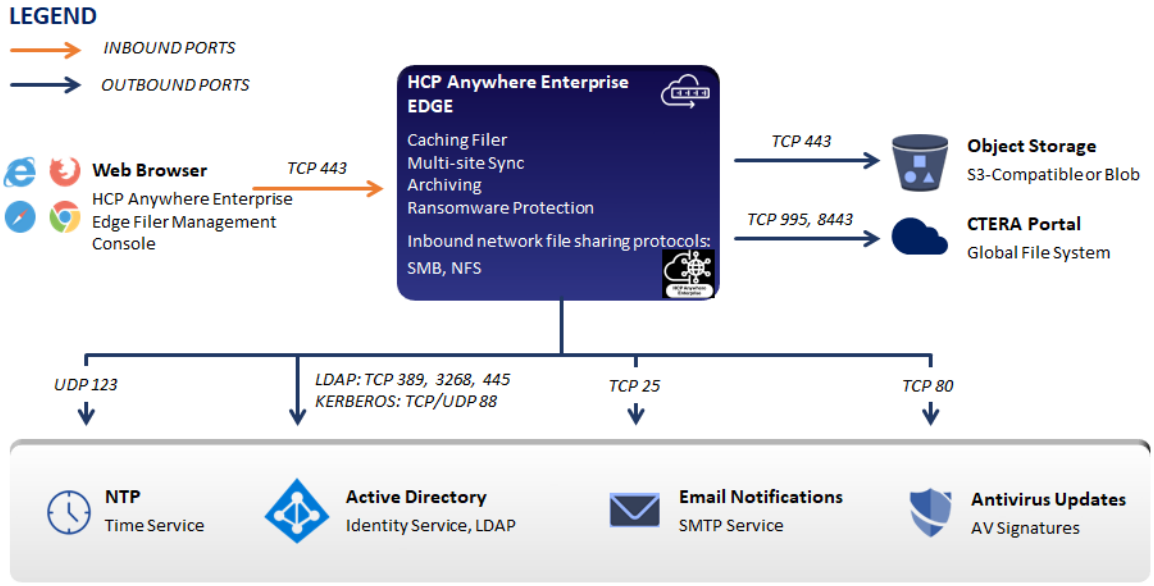
- Firewall ports opened for NTP updates:

Port	Protocol	Direction	Notes
123	UDP	Outbound	—

Warning: HCP Anywhere Enterprise Edge Filers operate behind a firewall, and it is important to leave all other ports closed.

- Internal network file sharing protocols (not requiring any port configuration):

Port	Protocol	Direction	Notes
111, 2049	TCP	Inbound	NFS
445	TCP	Inbound	SMB



Browser Requirements

The latest two releases of:

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

License Types

License	Maximum Storage
EV16	16TB
EV32	32TB
EV64	64TB
EV128	128TB
EV256	256TB

Note: The normal HCP Anywhere Enterprise Edge Filer usage is memory and network intensive and not CPU intensive. The HCP Anywhere Enterprise Edge Filer is installed with 4 vCPUs. Increasing the number of vCPUs allocated for the HCP Anywhere Enterprise Edge Filer should take the usage in to account.

Software Features

Feature	Description
Supported File Sharing Protocols	SMB 2.x/3.x (Windows File Sharing), NFS, FTP, WebDAV
Monitoring	SNMP

Cloud Service Features

Feature	Description
Protocol Security	TLS (Transport Level Security), including TLS 1.3, using cryptographic libraries certified with FIPS 140-2. HCP Anywhere Enterprise Edge Filers are FIPS 140-2 certified and FIPS 140-3 compliant.
Efficiency	Incremental updates, data compression, block level deduplication, simultaneous synchronization.
Versioning	Retention of previous file versions.
Additional Services	Centralized management, centralized monitoring, Cloud Drive caching and synchronization, reporting, logging, remote access.

Chapter 2. HCP Anywhere Enterprise Edge Filer Planning

During the planning stage for the HCP Anywhere Enterprise Edge Filer, contact support regardless of whether the installation is a new installation or an upgrade from an existing installation.

End users who are familiar with a given folder structure and shares, as well as a given permission scheme, continue to see the same folder structure, shares, and permission scheme after migration to the HCP Anywhere Enterprise Edge Filer. This enables the migration from a current file system to a HCP Anywhere Enterprise Edge Filer without the need to apply any structural changes such as flattening the folder structure or simplifying the permissions scheme. For details, see Migrating a File Server.

File and folder access continue to be available following the migration in the same way they were in the original file system. Access, after the migration, is through SMB, provided by the HCP Anywhere Enterprise Edge Filer. Users continue to access the files and folders through standard client computers; for example, using Windows File Explorer or macOS Finder.

The following file server features are fully supported by HCP Anywhere Enterprise Edge Filer and are copied to HCP Anywhere Enterprise Edge Filer as part of the migration:

- ACL files/folder share permissions.
- Nested sharing.
- ACL emulation to allow files and folders management via standard SMB protocol.
- Shares can be mounted to users via standard administrator tools:
  - DFS Management
  - Group Policy (GPO)
  - Other tools based on Net use

Use HCP Anywhere Enterprise Migrate, which is accessed from the HCP Anywhere Enterprise Edge Filer user interface, to create the corresponding shares in the HCP Anywhere Enterprise Portal and sync them down to the HCP Anywhere Enterprise Edge Filer.

Chapter 3. Installing the HCP Anywhere Enterprise Edge Filer in a Nutanix AHV environment

Installing the HCP Anywhere Enterprise Edge Filer involves creating and configuring a virtual machine and then performing an initial configuration, described in First-Time Setup.

The HCP Anywhere Enterprise Edge Filer can be installed in a Nutanix AHV environment.

Contact Hitachi Vantara, and request the latest `qcow2` HCP Anywhere Enterprise Edge Filer disk image. Add this image to the machine where you run the Nutanix Prism Central console.

Warning: The HCP Anywhere Enterprise Edge Filer installation must be done using the qcow2 file and not by cloning an existing HCP Anywhere Enterprise Edge Filer.

To install the HCP Anywhere Enterprise Edge Filer in a Nutanix AHV environment:

1. Log in to the Nutanix Prism Central console.
   The dashboard is displayed.
2. Click **Home > Settings** in the top bar.
   The **Settings** page is displayed.
3. Click **Image Configuration** in the navigation pane.
   The **Image Configuration** page is displayed.
4. Click **Upload Image**.
   The **Create Image** window is displayed.
5. Specify the details for the edge filer image.
   Name – A unique name to identify the image.
   Annotation – An optional description of the image.
   Image Type – Set to **DISK**.
   Storage Container – Set the storage container to **SelfServiceContainer**.
6. Choose the **Upload a file** option and browse to the qcow2 image file from Hitachi Vantara support.
7. Click **Save**.
   The progress of the image creation is displayed in the page under the top bar.
8. Click **Settings > VM** in the top bar.
   The **VM** page is displayed.
9. If necessary, change the view from **Overview** to **Table**, to list all the VMs.
10. Click **Create VM**.
    The **Create VM** window is displayed.
11. Specify the details for the VM.
    Name – A unique name to identify the edge filer.
    Description – An optional description of the edge filer.
    Timezone – The timezone for the VM. The default is the local timezone.
    Use this VM as an agent VM – Leave unchecked.
    vCPU(s) – The number of vCPUs.
    Number Of Cores Per vCPU – The number of cores per vCPU. Leave the default value.
12. Scroll down to complete the details for the VM.
    Memory – The memory usage. The minimum RAM requirement is 2GB (2048MB).

Disks – Add a disk for the HCP Anywhere Enterprise Edge Filer software. The minimum recommended disk size is 16GB.

a) Click **Add New Disk**.
The **Add Disk** window is displayed.

b) Specify the details for the disk.
Type – The type of disk. Select **DISK**.
Operation – Select the **Clone from Image Service** from the drop-down list.

- **Image** – Select the HCP Anywhere Enterprise Edge Filer image from the drop-down list.

c) Leave the other fields with the default values and click **Add**.

13. Under **Boot Configuration**, choose the **Legacy BIOS** option and select the added disk to be the boot device in the **Set Boot Priority** text box.

14. Add a second disk for the HCP Anywhere Enterprise Edge Filer data.

a) Click **Add New Disk**.
The **Add Disk** window is displayed.

b) Specify the details for the disk.
Type – The type of disk. Select **DISK**.
Operation – Select the **Allocate from Storage Container** from the drop-down list.
Storage Container – Select the storage container from the drop-down list.
Size (GiB) – The disk size. Hitachi Vantara recommends storage of at least 20% of the HCP Anywhere Enterprise Portal Global Name Space. The maximum storage is dependent on the license.
For an EV16 license, the maximum is 16TB.
For an EV32 license, the maximum is 32TB.
For an EV64 license, the maximum is 64TB.
For an EV128 license, the maximum is 128TB.
For an EV256 license, the maximum is 256TB.

c) Leave the other fields with the default values and click **Add**.

15. Optionally, follow your site best practices to ensure optimal performance of the VM on the cluster, in cases of node failure.

The **Set VM Host Affinity** window is displayed.

a) Under **VM Host Affinity**, click **Set Affinity** to enable the VM to another host in the cluster.

b) Select the hosts under which the VM will run in the case of a node failure.

c) Click **Save**.

16. Click **Save**.

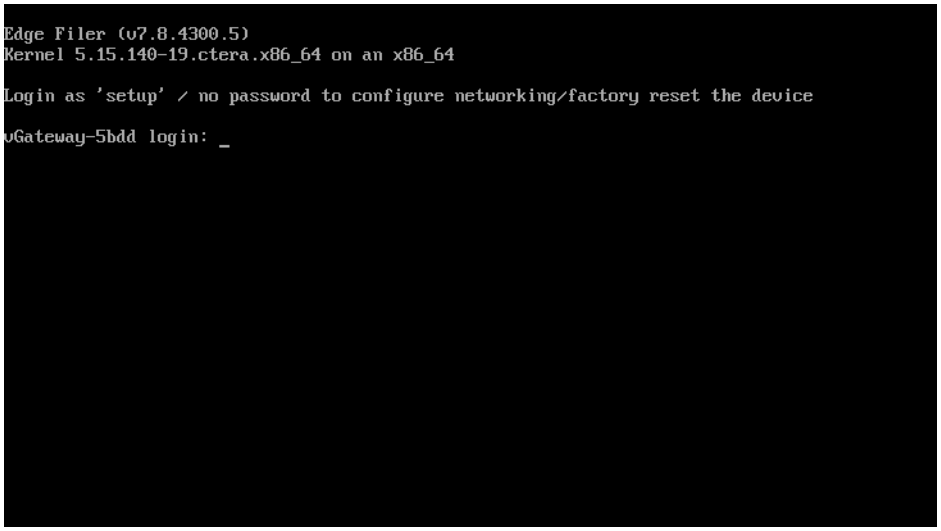
The VM is created.

17. From the list of virtual machines (**Table** view), select the new virtual machine and scroll down to display details of the VM.

18. Click **Power On**.

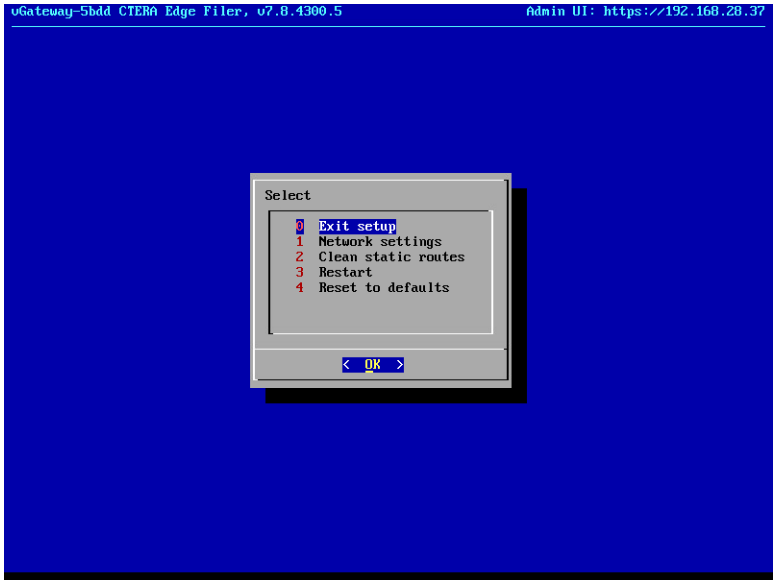
The VM is powered on and the **Launch Console** option is enabled.

19. Click **Launch Console** to open the console to get the IP address for the HCP Anywhere Enterprise Edge Filer.



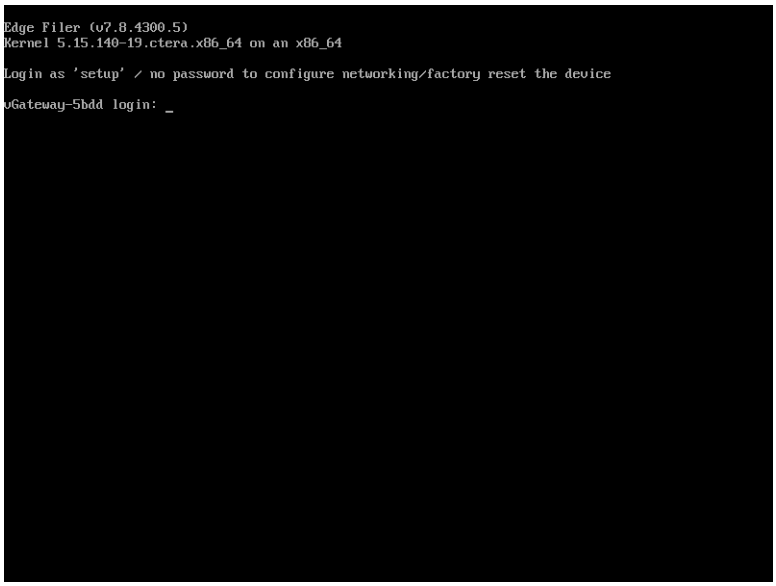
20. Login in with the username `setup` and no password, as instructed.

Using DHCP, after a few seconds the IP address to access the HCP Anywhere Enterprise Edge Filer in a browser is displayed in the top right of the console.

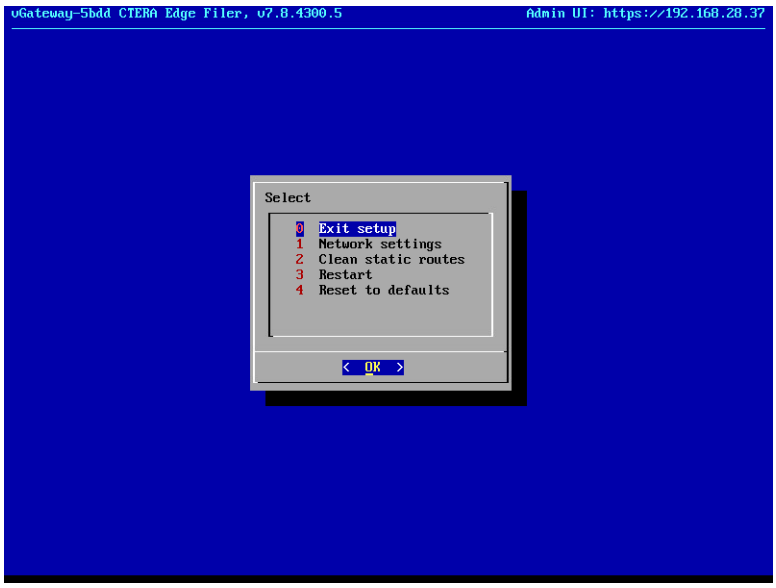


To set the virtual machine static IP address:

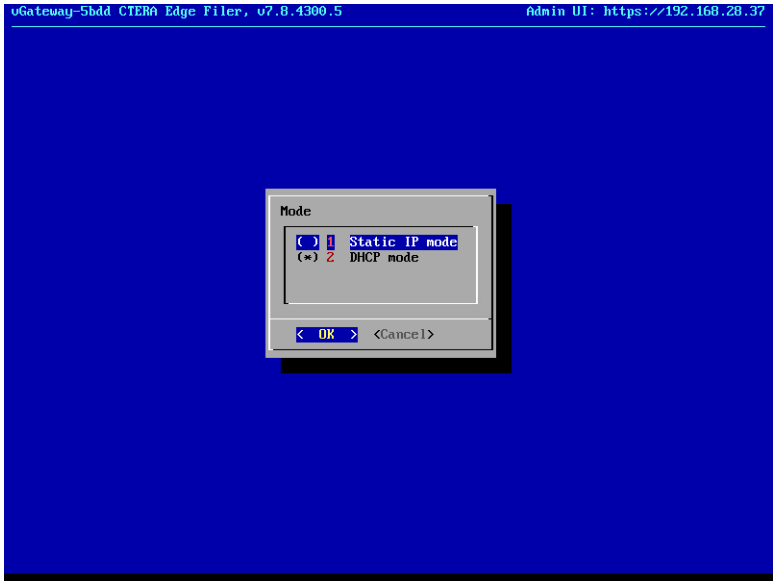
1. Access the virtual machine.
   The following login screen is displayed:



2. Login in with the username `setup` and no password, as instructed.
   The console is displayed.



3. Click in the console to transfer the keyboard control to the console and, if necessary, use the arrow keys to scroll to **Network settings**.
4. Press **Enter**.



5. Select **Static IP mode** and press **OK**.
6. Complete the configuration for static mode by entering the static IP, netmask, default HCP Anywhere Enterprise Edge Filer IP and the primary and secondary DNS server IPs.
7. Press **OK**.

Chapter 4. First-Time Setup

After installing the HCP Anywhere Enterprise Edge Filer you perform an initial configuration.

In this chapter

- Configuring the HCP Anywhere Enterprise Portal as a Precondition to Setting Up the HCP Anywhere Enterprise Edge Filer
- Initial HCP Anywhere Enterprise Edge Filer Setup
- Loading a Certificate to a HCP Anywhere Enterprise Edge Filer

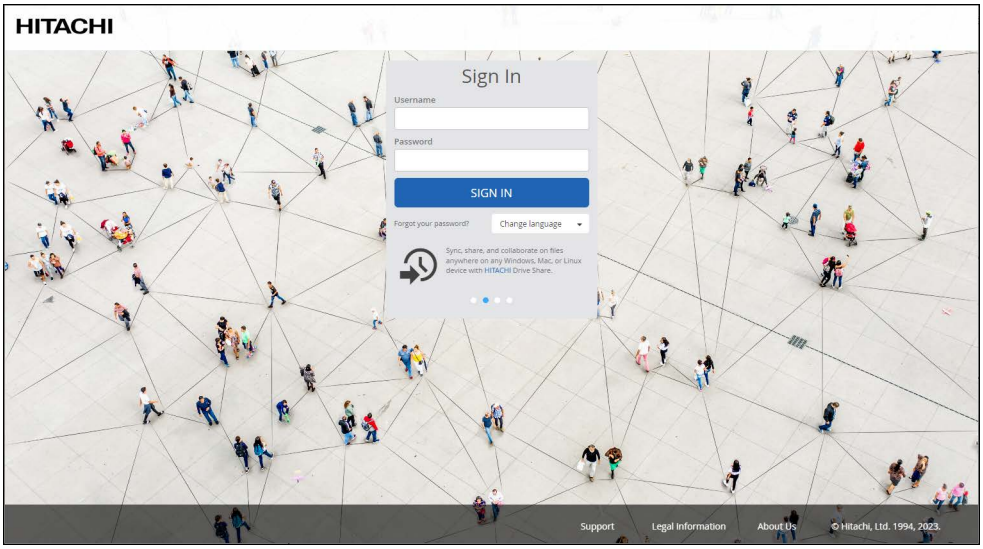
Configuring the HCP Anywhere Enterprise Portal as a Precondition to Setting Up the HCP Anywhere Enterprise Edge Filer

Before setting up the HCP Anywhere Enterprise Edge Filer, the HCP Anywhere Enterprise Portal administrator has to configure the HCP Anywhere Enterprise Portal to which the HCP Anywhere Enterprise Edge Filer will connect.

To configure the HCP Anywhere Enterprise Portal:

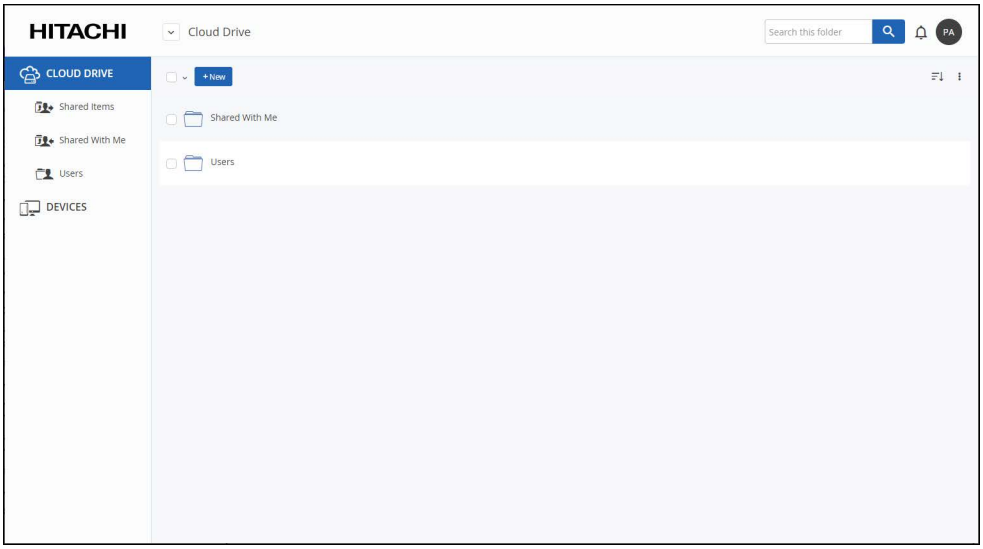
1. Sign in to the HCP Anywhere Enterprise Portal as a team administrator.
   a) In a Web browser open `http://<virtualportal_name>.<DNS_Suffix>/ServicesPortal`.
   where, `<virtualportal_name>` is the name of the HCP Anywhere Enterprise Portal, and `<DNS_Suffix>` is the DNS suffix for the HCP Anywhere Enterprise Portal installation.
   This opens the interface to the HCP Anywhere Enterprise Portal.

   Note: If the HCP Anywhere Enterprise Portal is set to redirect HTTP requests to HTTPS, HCP Anywhere Enterprise Portal redirects the browser to the HTTPS page. It is also possible to set the HTTPS access port to be different from the standard 443. In this case, the address is:
   `https://<virtualportal_name>.<DNS_Suffix>:<HTTPS_port>/ServicesPortal`, where `<HTTPS_port>` is a customized port.
   For example, to connect to Acme's administration HCP Anywhere Enterprise Portal using HTTPS port 2222, use the following address:
   `https://acme.example.com:2222/ServicesPortal`.
   The HCP Anywhere Enterprise Portal opens, displaying the sign in page.

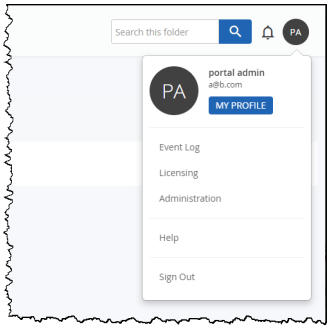


Note: If SAML Single Sign On (SSO) is enabled, you are redirected to the SAML identity provider's login page. If CAC, Common Access Card, is implemented at the site, the login page is skipped if the card access is authorized.

b) 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 end user interface is displayed.



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



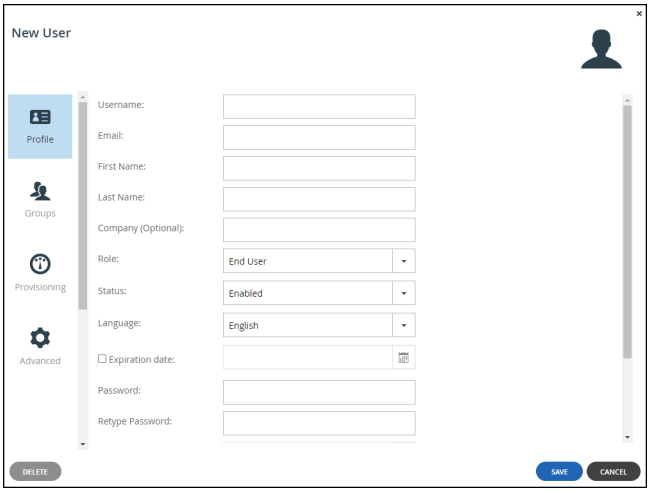
The administration interface opens in a new tab.

2. Create a designated user as an owner of the cloud folders and data. Hitachi Vantara recommends creating the owner as a local service account with administrator read/write privileges and not a real user. This account must have read and write administrator permissions to enable syncing folders between the HCP Anywhere Enterprise Edge Filer and the HCP Anywhere Enterprise Portal global file system.

   Once the data is uploaded to the HCP Anywhere Enterprise Portal global file system there is an owner for the data who can get elevated rights.

   a) Select **Users > Users** in the navigation pane.
   The **USERS** page is displayed.

   b) Click **New User**.
   The **New User** window is displayed.



   c) Complete the following fields in the **Profile** option.
   Username – A name for the user's HCP Anywhere Enterprise Portal account.
   Email – An email address.
   First Name – A first name for the service account.
   Last Name – A last name for the service account.
   Role – Select **Read/Write Administrator**.
   Password/Retype Password – A password for the account.

   d) Click **SAVE**.

3. Select **Settings > User Roles** in the navigation pane.

   The **Roles** window is displayed.

4. Click **Read/Write Administrator** and in the **Edit Roles** window make sure that **Access End**

User Folders is granted.

Initial HCP Anywhere Enterprise Edge Filer Setup

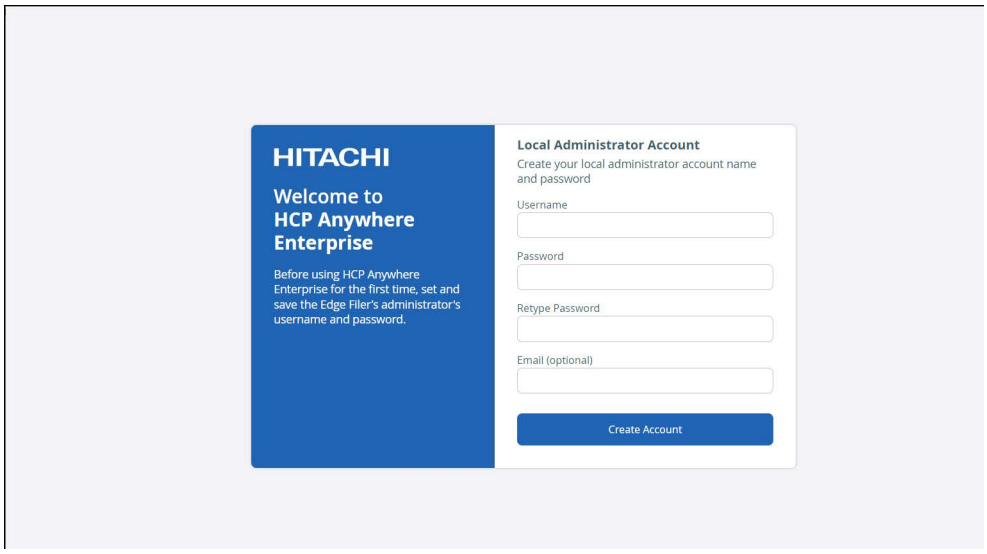
Before setting up the HCP Anywhere Enterprise Edge Filer, you have to configure the HCP Anywhere Enterprise Portal to which the HCP Anywhere Enterprise Edge Filer will connect, as described in Configuring the HCP Anywhere Enterprise Portal as a Precondition to Setting Up the HCP Anywhere Enterprise Edge Filer. After configuring the HCP Anywhere Enterprise Portal and installing the HCP Anywhere Enterprise Edge Filer, you need to perform an initial HCP Anywhere Enterprise Edge Filer setup. On first access to the HCP Anywhere Enterprise Edge Filer, you set up a HCP Anywhere Enterprise Edge Filer administrator and then a wizard guides you through connecting to a HCP Anywhere Enterprise Portal and storage and user setup. You can skip any of the wizard steps and perform them later, as described in the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.

After this initial HCP Anywhere Enterprise Edge Filer setup, the file server structure is synced from the HCP Anywhere Enterprise Portal to the HCP Anywhere Enterprise Edge Filer.

To access the HCP Anywhere Enterprise Edge Filer and initial setup:

1. Open any web browser.
2. Enter the HCP Anywhere Enterprise Edge Filer's IP address to navigate to the device.

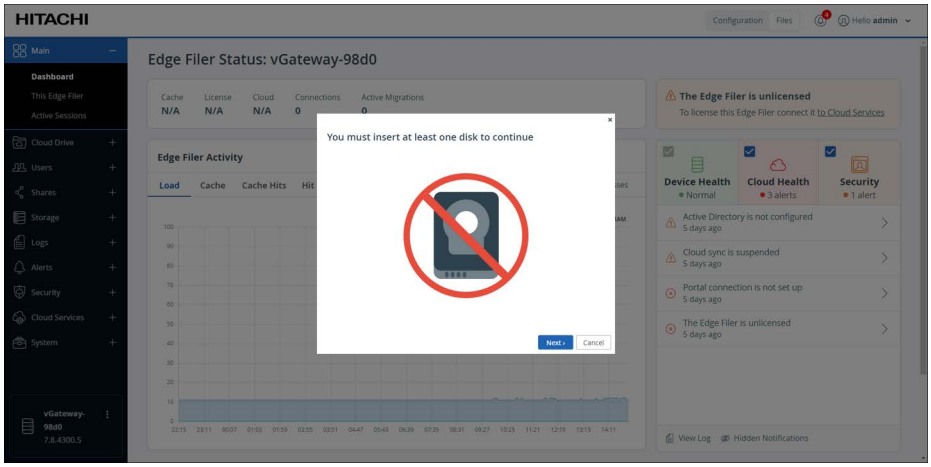
   When you connect to the web interface for the first time, your browser displays the **Welcome to HCP Anywhere Enterprise** page.



3. Choose a user name and password for the administrator. The password must be at least eight characters and must include at least a letter, digit and special character, such as ~, @, #, $, %, ^, & , (.

   Note: You can keep the default user name, `admin`. Other administrators are defined in the HCP Anywhere Enterprise Edge Filer from Active Directory.
4. Optionally, enter an email for receiving notifications regarding the HCP Anywhere Enterprise Edge Filer.
5. Click **Create Account**.

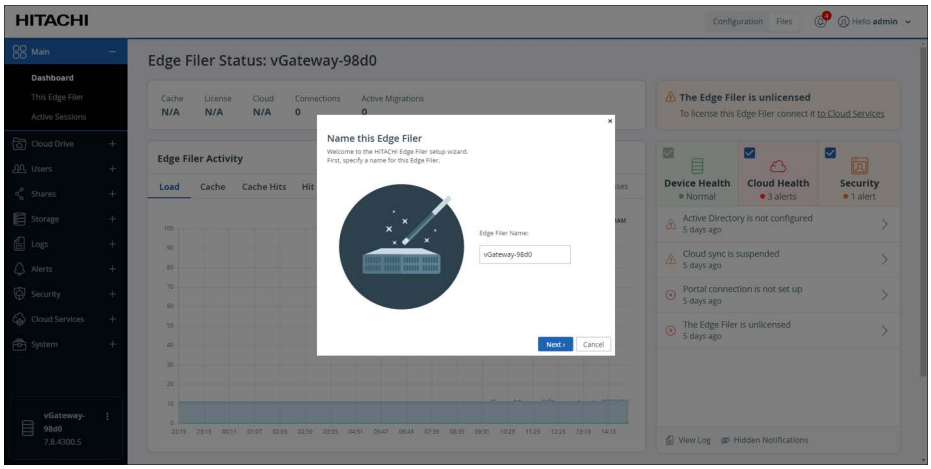
If the HCP Anywhere Enterprise Edge Filer does not have a disk, the following message window is displayed.



Click **Cancel** to close the wizard and then **Yes** to run the wizard after adding a disk to HCP Anywhere Enterprise Edge Filer virtual machine. Add a disk to the HCP Anywhere Enterprise Edge Filer virtual machine.

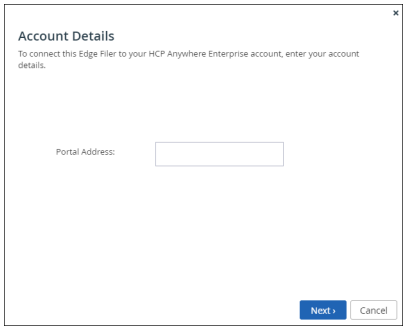
If you logged out of the HCP Anywhere Enterprise Edge Filer, the setup wizard starts when you log back in. If you did not log out, in the HCP Anywhere Enterprise Edge Filer **Dashboard** page run **Setup Wizard**.

The **Name this Edge Filer** window is displayed.



6. Either keep the HCP Anywhere Enterprise Edge Filer default name or enter a new name to identify the HCP Anywhere Enterprise Edge Filer and click **Next**.

   The administration user interface is displayed to set up the HCP Anywhere Enterprise Edge Filer, starting with the **Account Details** window.

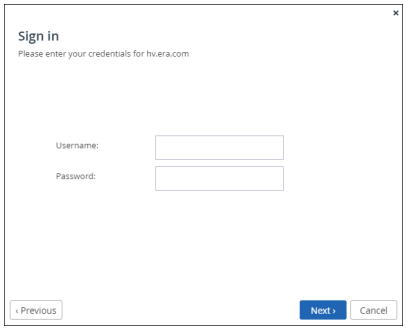


Note: You can also change the HCP Anywhere Enterprise Edge Filer name after the initial setup, as described in the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.

7. Enter the DNS name of the HCP Anywhere Enterprise Portal to which you have an account and want to connect the HCP Anywhere Enterprise Edge Filer to, in the **Portal Address** field and click **Next**.

   Note: If the HCP Anywhere Enterprise Portal does not have a valid certificate installed, a warning is displayed to the end user when logging a HCP Anywhere Enterprise Edge Filer into the HCP Anywhere Enterprise Portal, offering the option to proceed anyway. This warning is presented every time a user connects a HCP Anywhere Enterprise Edge Filer to the HCP Anywhere Enterprise Portal, until a valid certificate is installed.

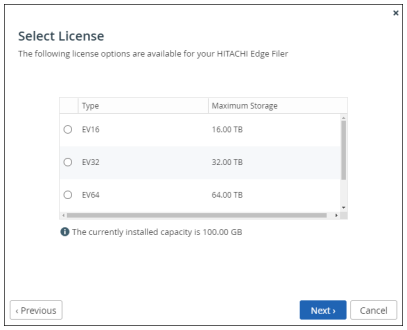
   The **Sign in** window is displayed.



   Note: If single sign-on has been set up to the HCP Anywhere Enterprise Portal, click **Sign In** and then **Allow** in a new browser window that is displayed, when prompted. The **Select License** screen is displayed with the available licenses and the available storage and RAM. Go to step **9**.

8. Enter the HCP Anywhere Enterprise Portal designated user username and password, set in Configuring the HCP Anywhere Enterprise Portal as a Precondition to Setting Up the HCP Anywhere Enterprise Edge Filer to access the HCP Anywhere Enterprise Portal and click **Next**.

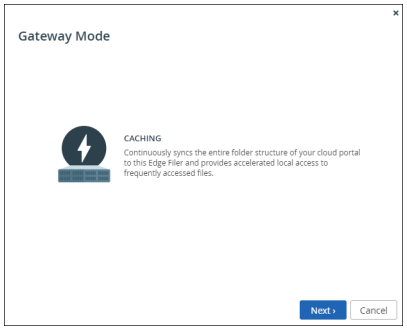
   The **Select License** window is displayed with the available licenses.



The available storage and RAM are displayed.

9. Select the license for the HCP Anywhere Enterprise Edge Filer and click **Next**.

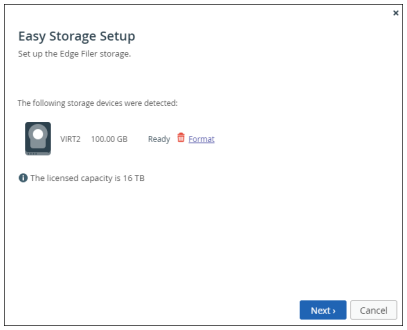
   The **Gateway Mode** window is displayed.



CACHING – Provides users with LAN speed access to all the shared cloud folders on the HCP Anywhere Enterprise Portal. Shared storage is on the HCP Anywhere Enterprise Portal with stubs saved on the HCP Anywhere Enterprise Edge Filer. A stub is a file with a tiny footprint that contains the metadata about the file, such as the file name, size, and modification date. Only the folder and file metadata and not the actual file content is saved locally. Thus, the HCP Anywhere Enterprise Edge Filer can have much less physical storage than is made available to users, who have access to both the local HCP Anywhere Enterprise Edge Filer storage and the HCP Anywhere Enterprise Portal storage. Systems with many file changes, where only some of the files are required locally, don't over use bandwidth between the cloud and HCP Anywhere Enterprise Edge Filer. Only the required files are passed across the wire. When a user accesses a file stub, the file is opened without delay, by streaming the file content from the cloud. After the download has completed, the file is *unstubbed*. Any changes to the file are synced back to the HCP Anywhere Enterprise Portal. Folders that are always required can be pinned, in which case the files in the folders, and not the stubs, are stored on the HCP Anywhere Enterprise Edge Filer.

10. Click **Next**.

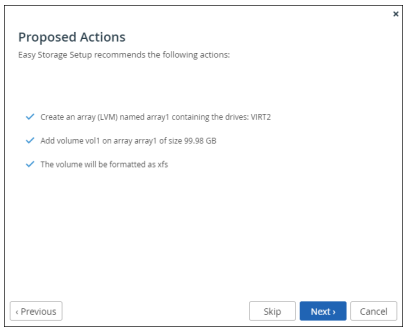
    The **Easy Storage Setup** window is displayed, showing the number of virtual disks.



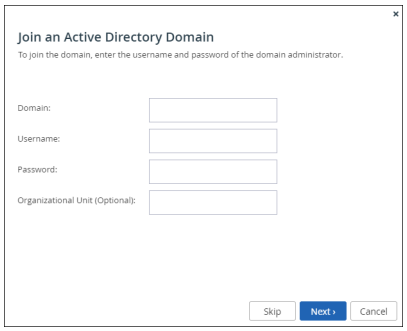
The maximum storage allowed for the selected HCP Anywhere Enterprise Edge Filer license is also displayed.

11. Click **Next**.

    Either:
    A **Proposed Actions** window is displayed with the recommended configuration.



    Hitachi Vantara recommends accepting the proposed actions and clicking **Next** and **not** clicking **Skip**.
    Or:
    The **Join an Active Directory Domain** window is displayed.



12. Specify the domain details so that the HCP Anywhere Enterprise Edge Filer is populated with the users from your Active Directory domain and click **Next** or, if you want to set up Active Directory later, click **Skip**.

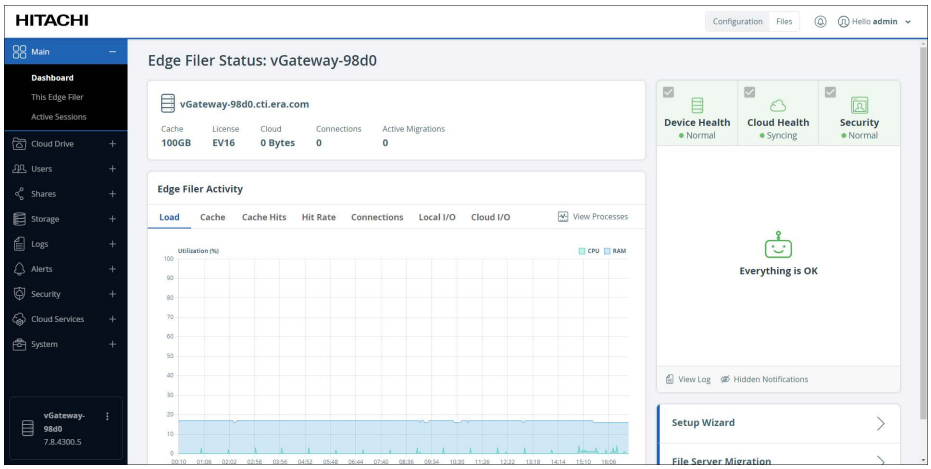
    Note: Until Active Directory is configured, there is a security alert.
    In the **Username** and **Password** fields, type the domain administrator's username and password.
    The Active Directory domain controller must be read/write and not read-only.
    Optionally, in the **Organizational Unit** field, type the name of the organizational unit

within the Active Directory domain. The format is a path and can contain the following:
CN=Fully qualified domain name, such as gatewayName.portalName.portalSuffix
L=Locality Name, for example, London
ST=State or Province Name, for example, London
O=Organization Name, for example, Hitachi Vantara Networks
OU=Organizational Unit Name, for example, Sales
C=Country Name, for example, GB
STREET=Street Address
DC=Domain Component, for example com
UID=Userid

The **Wizard Completed** window is displayed.

13. Click **Finish**.

    The **Configuration** view **Main > Dashboard** page is displayed.



An LVM array, *array1*, which includes all the virtual disks, and a single volume, *vol1*, are created.

Note: You can rerun the wizard by selecting **Main > Dashboard** and click **Setup Wizard**.

You can migrate a file server to HCP Anywhere Enterprise Edge Filer so that end users who are familiar with a given folder structure and share, while using the file server, continue to see the same folder structure and shares after migration to the HCP Anywhere Enterprise Edge Filer. If you are replacing an existing file server with the HCP Anywhere Enterprise Edge Filer, continue with Migrating a File Server.

When more than one DNS server is in use at the site, you can define the primary and secondary DNS servers, described in the *HCP Anywhere Enterprise Edge Filer Administration Guide*, under *Managing Network Settings*.

For full details about managing the HCP Anywhere Enterprise Edge Filer, see the *Hitachi Content Platform Anywhere Enterprise Edge Filer Administration Guide*.

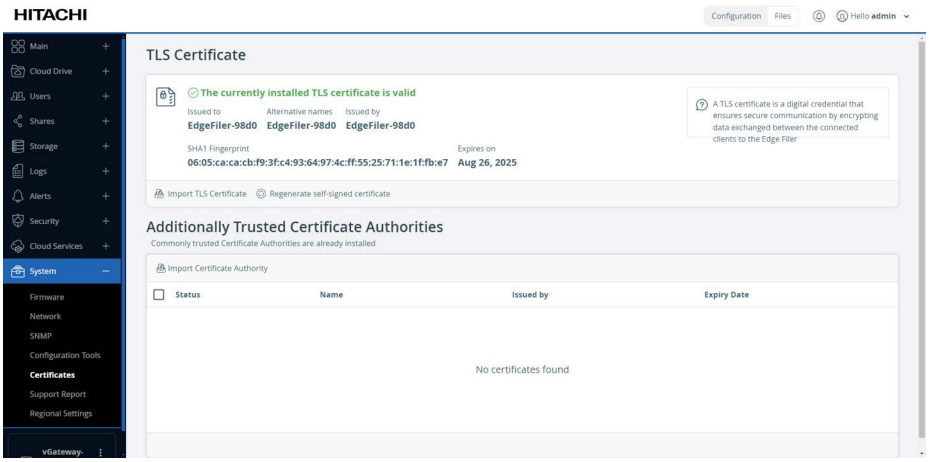
Loading a Certificate to a HCP Anywhere Enterprise Edge Filer

A TLS certificate is a digital credential that ensures secure communication by encrypting data exchanged between the connected clients to the HCP Anywhere Enterprise Edge Filer.

A customer that uses a privately issued certificate on the HCP Anywhere Enterprise Portal is required to upload the root CA to the HCP Anywhere Enterprise Edge Filer so that the HCP Anywhere Enterprise Edge Filer is trusted by the HCP Anywhere Enterprise Portal. The certificate covers the following:

- The connection between the HCP Anywhere Enterprise Edge Filer and the portal.
- When the object storage used by the HCP Anywhere Enterprise Portal is accessed by Direct Mode and uses a X.509 Certificate signed by a private Certification Authority (a self-signed certificate) and not a public trusted certificate.
- The connection between the HCP Anywhere Enterprise Edge Filer and a Syslog server.

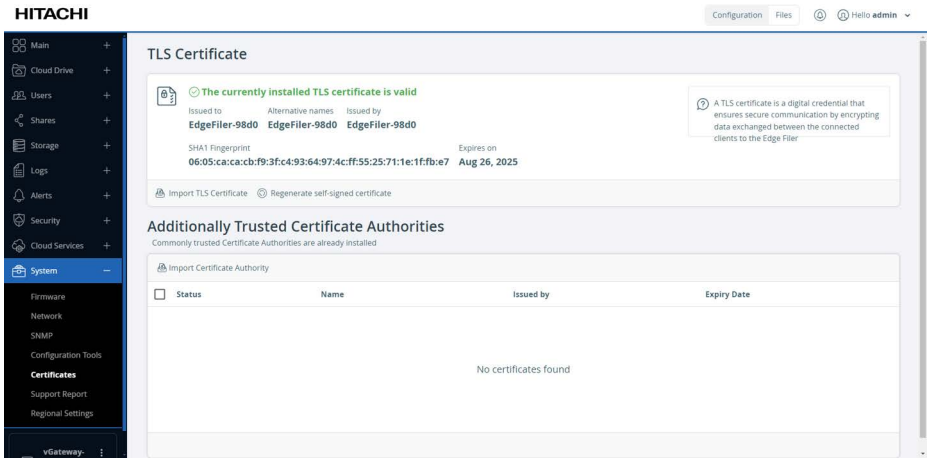
The HCP Anywhere Enterprise Edge Filer includes a self-signed certificate. Details of this certificate are displayed by accessing System > Certificates in the navigation pane.



Managing TLS Certificates

To import a TLS certificate to the HCP Anywhere Enterprise Edge Filer:

1. In the **Configuration** view, select **System > Certificates** in the navigation pane.

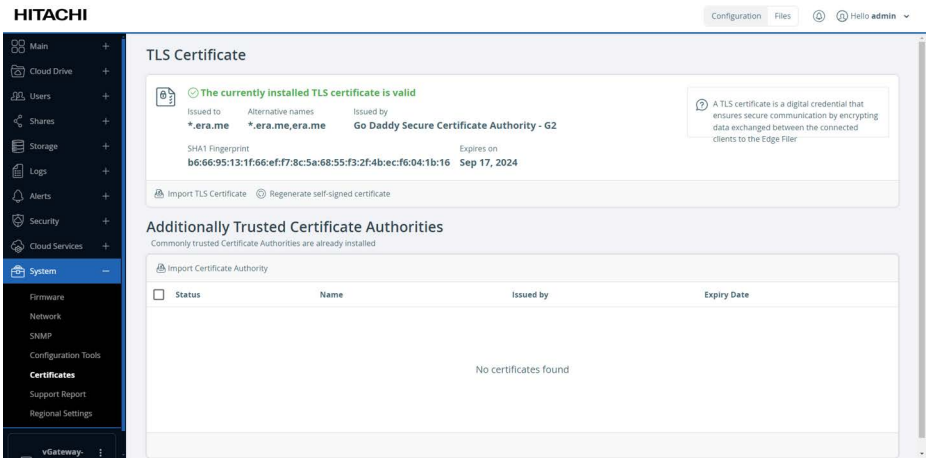


2. Under **TLS Certificate** click **Import TLS Certificate**.
   The **TLS Certificate Import** window is displayed.

3. Paste the private key for the certificate in the top text box.
4. Paste the TLS certificate in .pem format in the bottom text box.
   The TLS certificate should be similar to the following example.

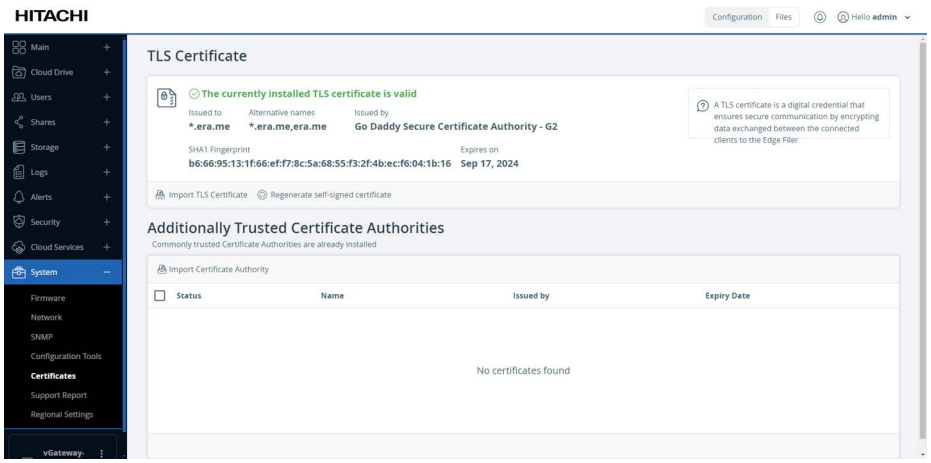
5. Click **Save**.

The certificate is imported to the HCP Anywhere Enterprise Edge Filer.



To restore the original the HCP Anywhere Enterprise Edge Filer TLS certificate:

1. In the **Configuration** view, select **System > Certificates** in the navigation pane.



2. Under **TLS Certificate** click **Regenerate self-signed certificate**.
3. Click **OK** in the confirmation window.

Any certificate that was installed to replace the self-signed certificate supplied by Hitachi Vantara is overwritten with the original self-signed certificate supplied with the HCP Anywhere Enterprise Edge Filer by Hitachi Vantara.

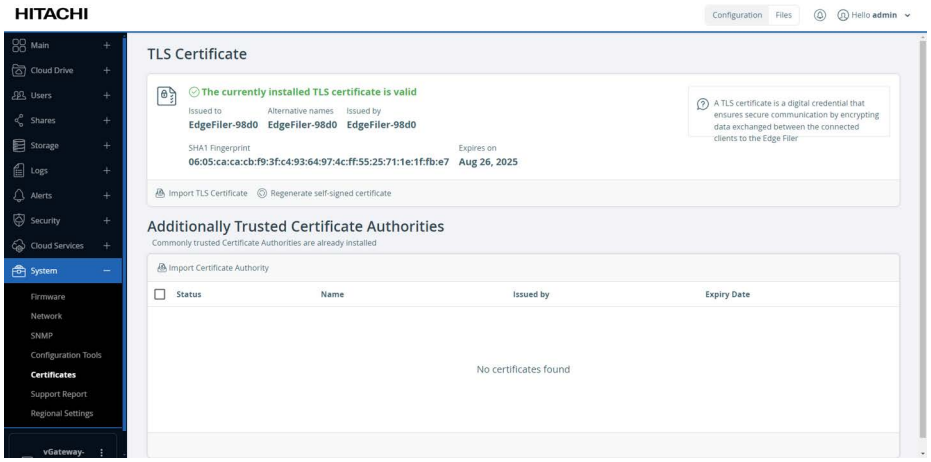
Additionally Trusted Certificate Authorities

Hitachi Vantara recognizes the most commonly trusted certificate authorities, such as DigiCert, GoDaddy, Thawte, and Verisign.

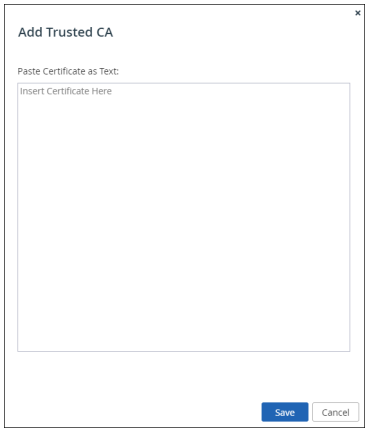
If you want to add a certificate authority that you trust, you can import the certificate authority to the HCP Anywhere Enterprise Edge Filer list and all certificates from that authority will be trusted.

To add a trusted CA to the HCP Anywhere Enterprise Edge Filer:

1. In the **Configuration** view, select **System > Certificates** in the navigation pane.

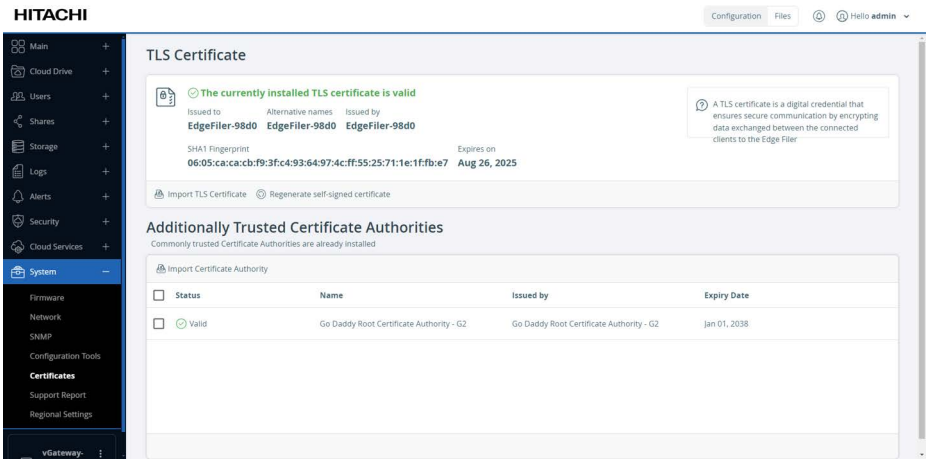


2. Under **Additionally Trusted Certificate Authorities** click **Import Certificate Authority**. The **Add Trusted CA** window is displayed.



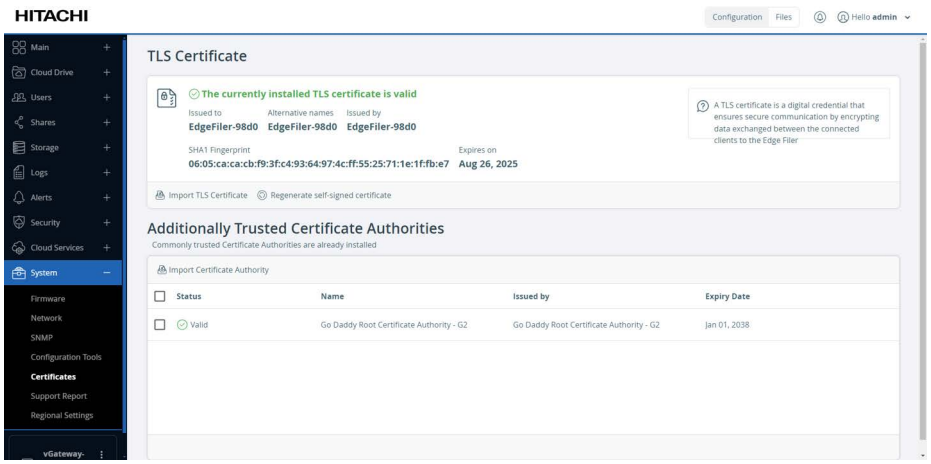
3. Paste the trusted root certificate.
4. Click **Save**.

The CA is added.

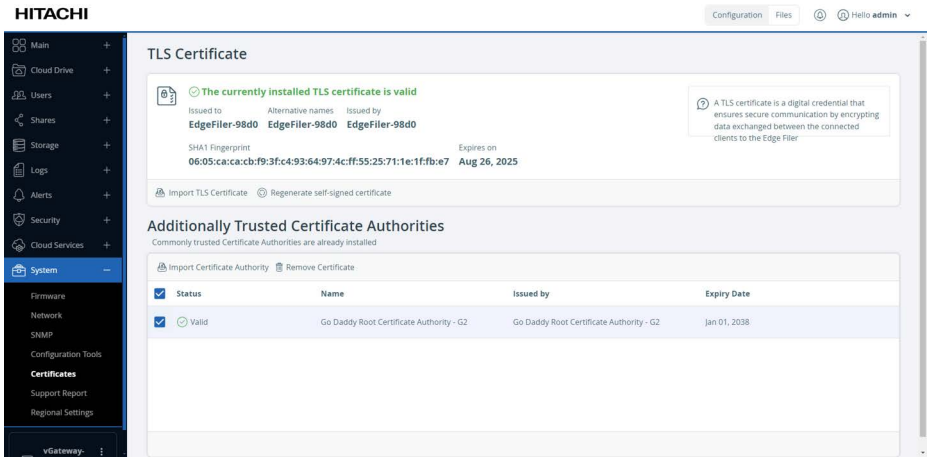


To remove a trusted CA to the HCP Anywhere Enterprise Edge Filer:

1. In the **Configuration** view, select **System > Certificates** in the navigation pane.



2. Select the CA to remove from the HCP Anywhere Enterprise Edge Filer trusted list.



3. Click **Remove Certificate**.

Chapter 5. Migrating a File Server

With HCP Anywhere Enterprise Migrate, you can migrate a file server to the HCP Anywhere Enterprise Edge Filer. After the migration has been completed, end users who are familiar with a given folder structure and shares, as well as a given permission scheme, continue to see the same folder structure, shares, and permission scheme. This enables the migration from a current file system to the HCP Anywhere Enterprise Edge Filer without the need to apply any structural changes such as flattening the folder structure or simplifying the permissions scheme.

You can from the following migrate file servers:

- Azure StorSimple
- HCP Gateway
- Hitachi Data Ingestor
- Isilon OneFS
- Microsoft Azure Files
- Nasuni Edge Appliance
- NetApp ONTAP
- NetAPP StorageGRID 9 (SMB)
- NetAPP StorageGRID 11 (SMB)
- Panzura Freedom Filer
- Windows Server

Another option, **Other**, is available to attempt to migrate from a file server that is not listed.

In addition you can discover all the shares on the current HCP Anywhere Enterprise Edge Filer by specifying the source as **This Edge Filer**.

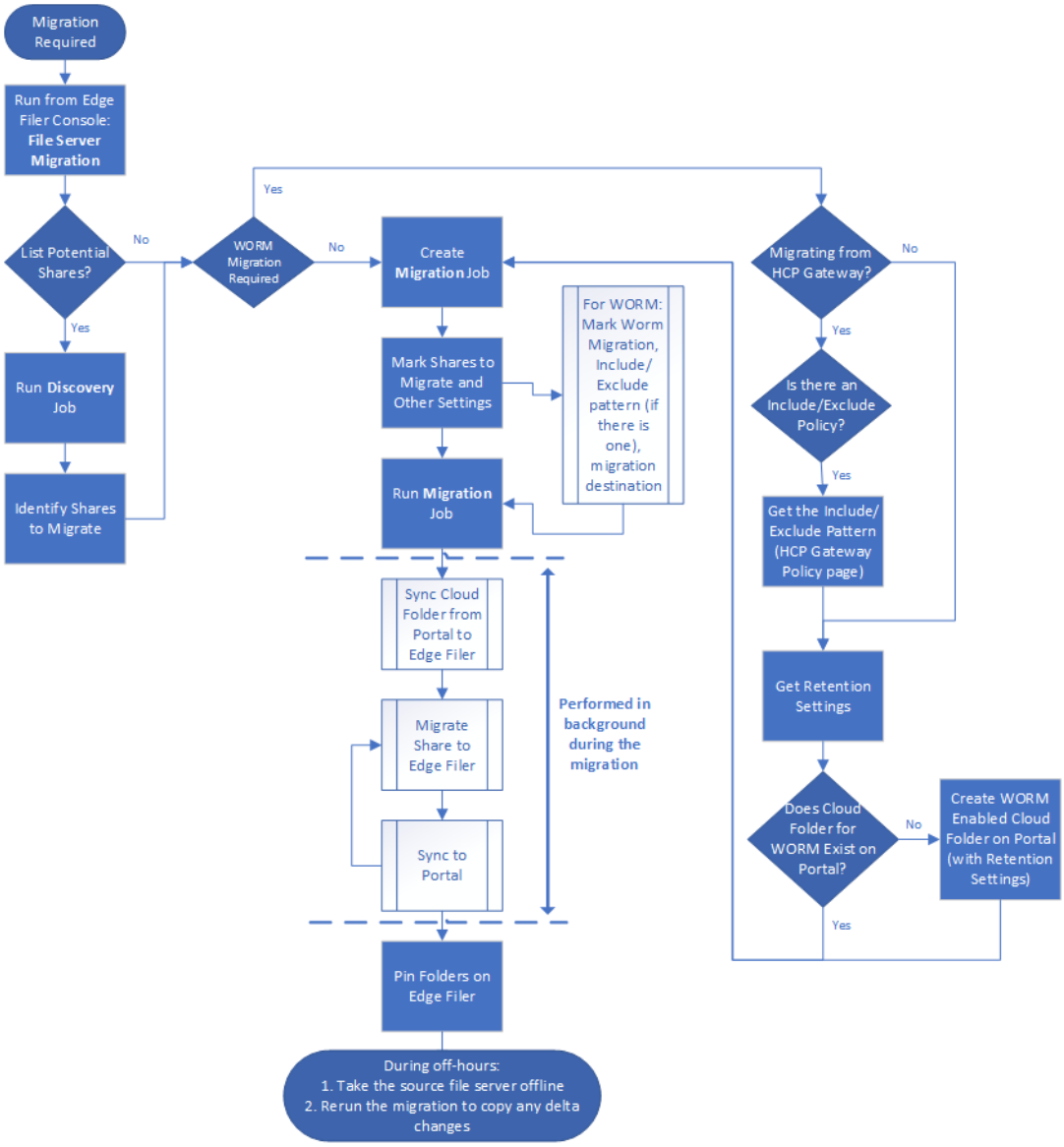
Access to files and folders after the migration is through SMB provided by the HCP Anywhere Enterprise Edge Filer so that users continue to access the files and folders in the same way as with the old system. You can migrate more storage than is physically available on the HCP Anywhere Enterprise Edge Filer, and the user has access to the global namespace, even when this is much larger than the storage available on the HCP Anywhere Enterprise Edge Filer.

You can migrate files that are defined as WORM compliant. The files are migrated with the source compliance settings, including the time remaining that they are WORM compliant.

Note: To migrate WORM compliant files, you have to prepare the HCP Anywhere Enterprise Portal before starting the migration.

Migrating a file server to a HCP Anywhere Enterprise Edge Filer can be performed while the current file server remains in production.

The flow when performing a migration is as follows:



[???

Before migrating the file server to the HCP Anywhere Enterprise Edge Filer, the HCP Anywhere Enterprise Edge Filer must be connected to the HCP Anywhere Enterprise Portal. After finishing the initial setup, make sure that syncing between the HCP Anywhere Enterprise Edge Filer and HCP Anywhere Enterprise Portal is not suspended.

To migrate a single file server to the HCP Anywhere Enterprise Edge Filer involves the following procedures:

- Discovering Shares – Optionally, survey the current file server to discover which shares to migrate.
- Migrating Shares – Migrate shares to the HCP Anywhere Enterprise Edge Filer.

After the migration, the cloud folder will start with the C: path as it represents a single server with all the shares/nested shares as cloud folders under this cloud folder. You can change the cloud folder under which all the shares are migrated as part of the migration job specification.

The shares are not created at the root cloud folder level but at the subfolder level because ACL permissions cannot be managed at the root cloud folder level, only at the subfolder level.

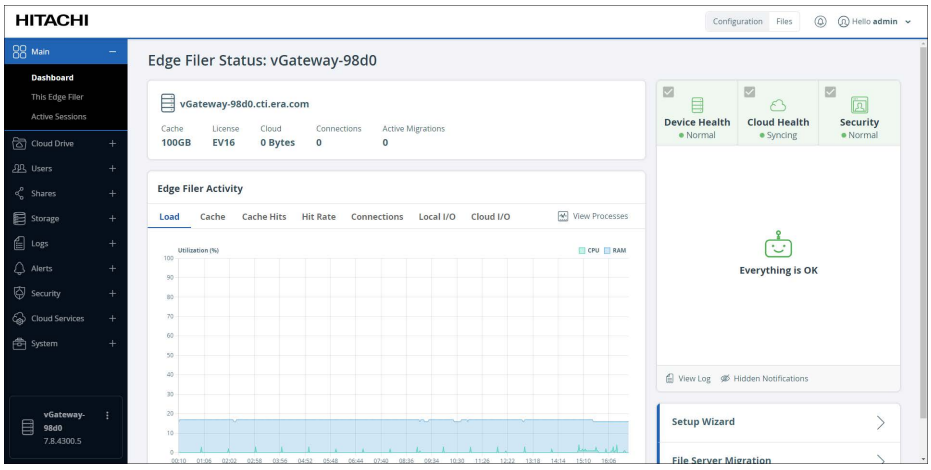
Note: Special characters in share names, % < > * ? | / \ + = ; : " , , are not supported by the HCP Anywhere Enterprise Migrate. When such characters are used, the share contents are not migrated. This condition is reported, and the job is *completed with errors*. Share names that are over 80 characters in length and include the % [ ] characters will not be accessible from Windows clients and should also not be used in share names.

Discovering Shares

Optionally, survey the current file server to discover which shares to migrate.

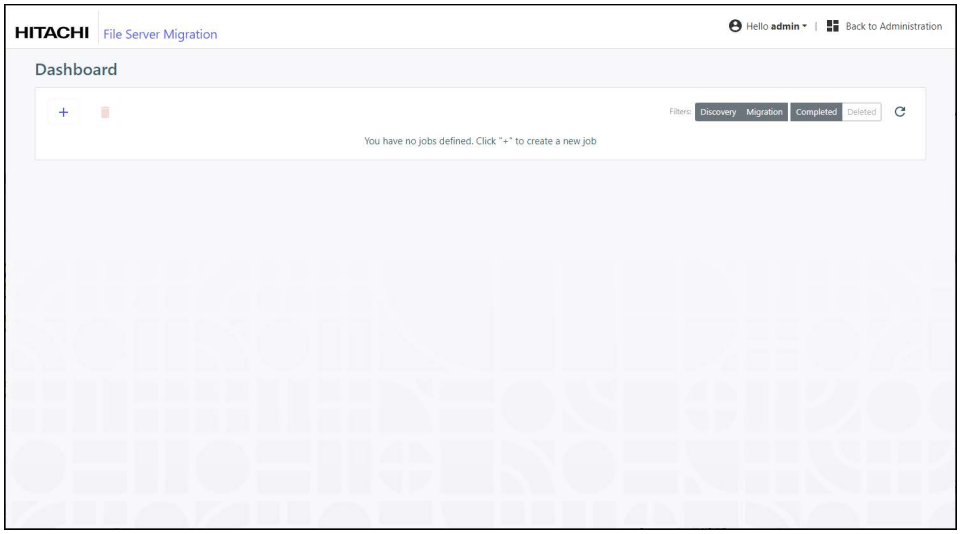
To discover the shares to migrate:

1. In the **Configuration view**, select **Main > Dashboard** in the navigation pane. The **Dashboard** page is displayed.



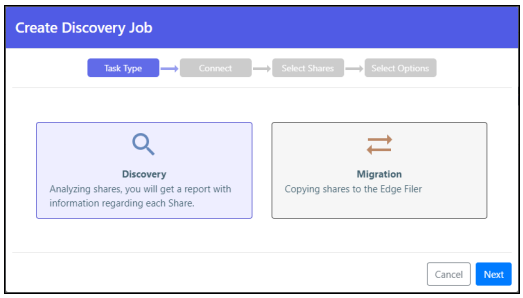
2. Click **File Server Migration**.

   The **File Server Migration** page is displayed.



3. Click **+** to create a new job.

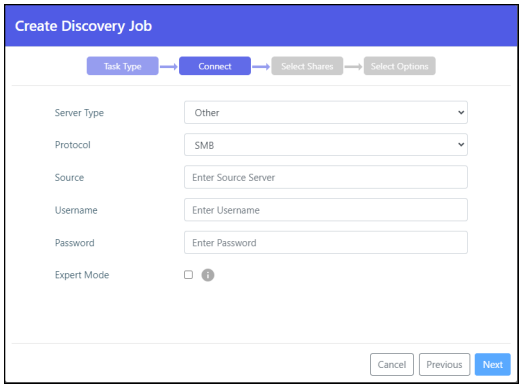
   The **Create Discovery Job** wizard is displayed showing the **Task Type** step.



   The default job is a **Discovery** job. This job analyzes the file server that is being replaced to identify what data should be migrated.

4. Click **Next**.

   The **Connect** step is displayed.

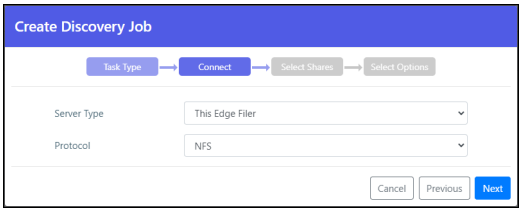


5. Select the server type to connect to from the drop-down box. You can connect to one of the following:
   - Azure StorSimple
   - HCP Gateway

- Hitachi Data Ingestor
- Isilon OneFS
- Microsoft Azure Files
- Nasuni Edge Appliance
- NetApp ONTAP
- NetAPP StorageGRID 9 (SMB)
- NetAPP StorageGRID 11 (SMB)
- Panzura Freedom Filer
- Windows Server

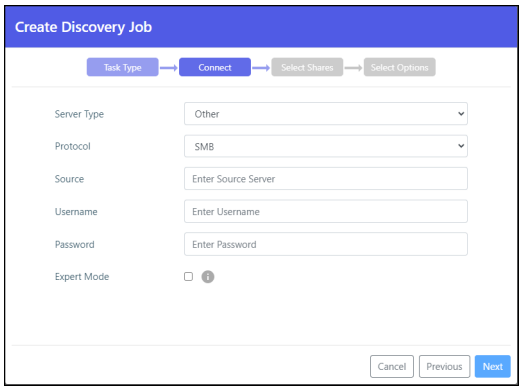
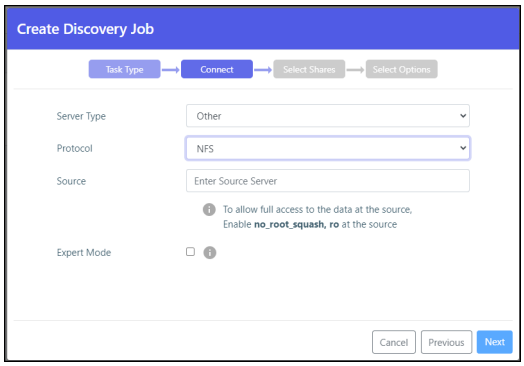
Another option, **Other**, is available to attempt to migrate from a file server that is not listed.

Note: You can run discovery on the HCP Anywhere Enterprise Edge Filer itself, by selecting **This Edge Filer** for **Server Type**. When **This Edge Filer** is selected, the only other parameter that is displayed is the **Protocol** parameter; either **SMB** or **NFS.**



6. Select the protocol to use for the migration: **SMB** or **NFS**.

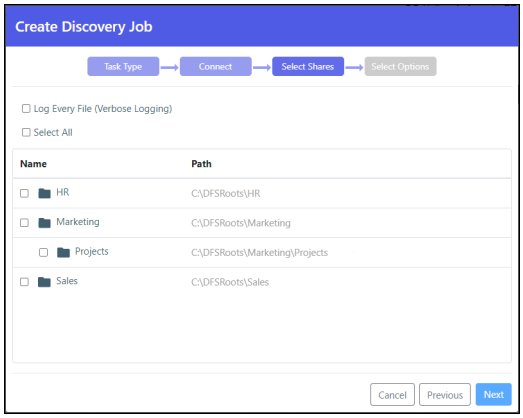
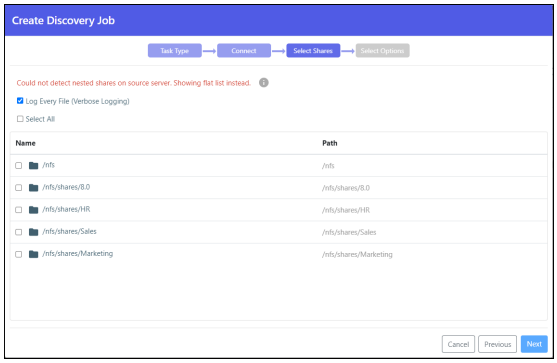
   Both NFS versions 3 and 4 are supported.
   The wizard window changes depending on the protocol selected.

SMB	NFS
	

7. For all server types except **This Edge Filer**, enter the IP address or DNS name for the source file server.
8. When **Protocol** is **SMB**, enter an administrator user name and password to access the server.

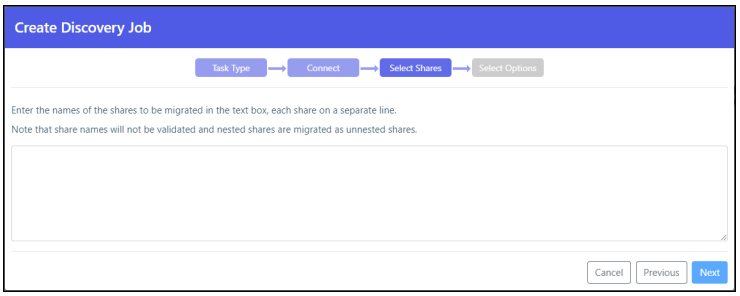
   Note: The administrator used must have access to the files to migrate.
9. For **Microsoft Azure Files**, the shares cannot be presented and have to be added manually. **Expert Mode** is automatically selected to enable specifying the shares in the next step.
10. Click **Next**.

The **Select Shares** step is displayed.

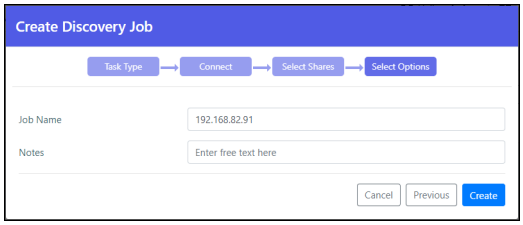
SMB	NFS
	

The shares on the file server are displayed, and you can select the shares that you want to migrate to the HCP Anywhere Enterprise Edge Filer.

Note: When **Expert Mode** was selected, the following window is displayed where you enter the shares to migrate.



11. Select the shares to migrate and click **Next**.



12. Optionally, provide a different name for the job and any specific notes about the job.
13. Click **Create**.

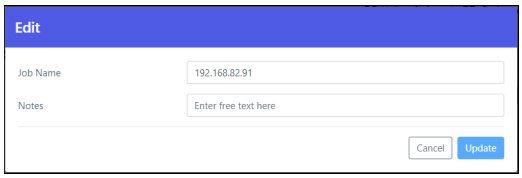
The discovery job runs and the results are displayed in the Dashboard.

The Dashboard After a Discovery Run

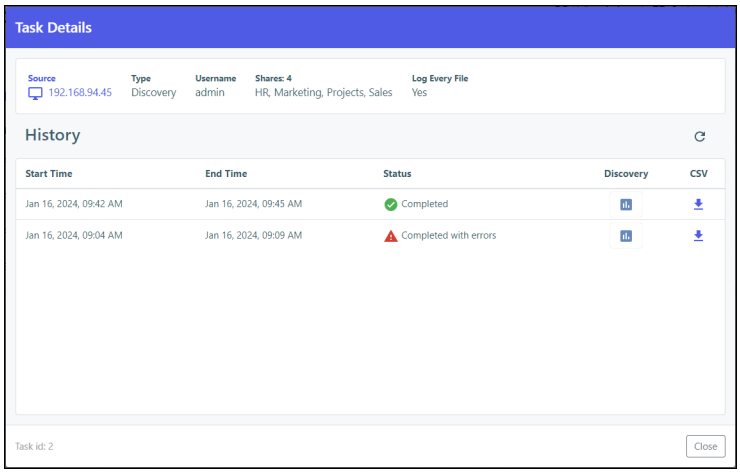
After analyzing the file server, the job completes and you get a report as well as a full analysis of each share in the filer server that you selected.

Log files and discovery file lists generated by the migration are compressed if they are greater than 100MB.

- Click the icon to edit the discovery job name and notes.

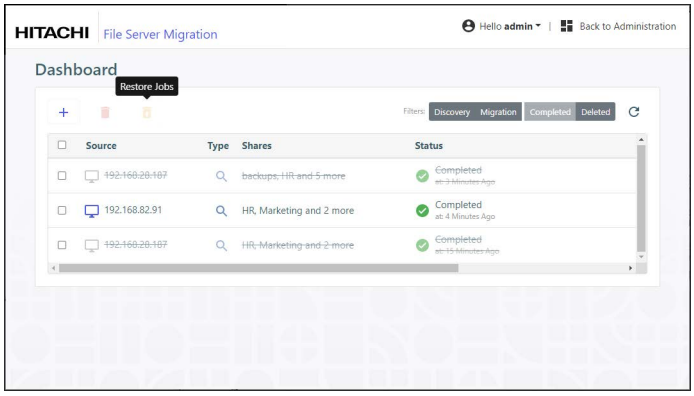


- Click the report icon to display the The Discovery Report.
- Click the icon to display the list of every time this job was run and rerun with the results of each run. The **Task Details** can also be accessed by clicking **Details** in The Discovery Report.



- Click the icon to rerun the discovery.
  The discovery job reruns.
- Optionally, in the dashboard, you can select a job and click the icon to delete the job. After deleting a job, you can display all the jobs, including the deleted jobs, by clicking the

Deleted filter in the dashboard.

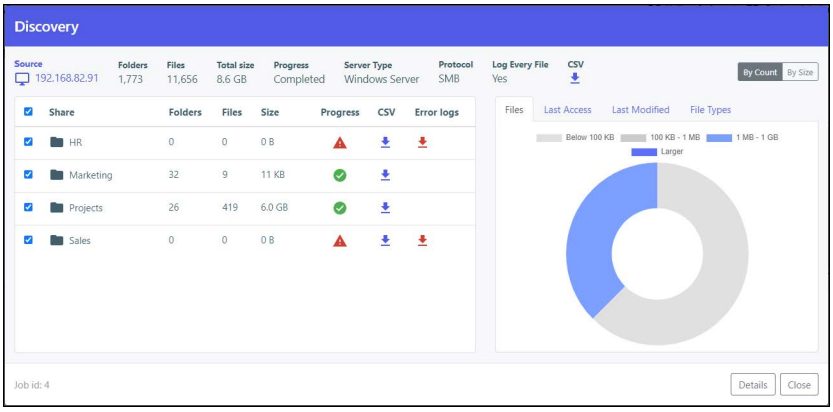


You can restore deleted jobs by selecting the deleted jobs to restore and clicking the icon.

The Discovery Report

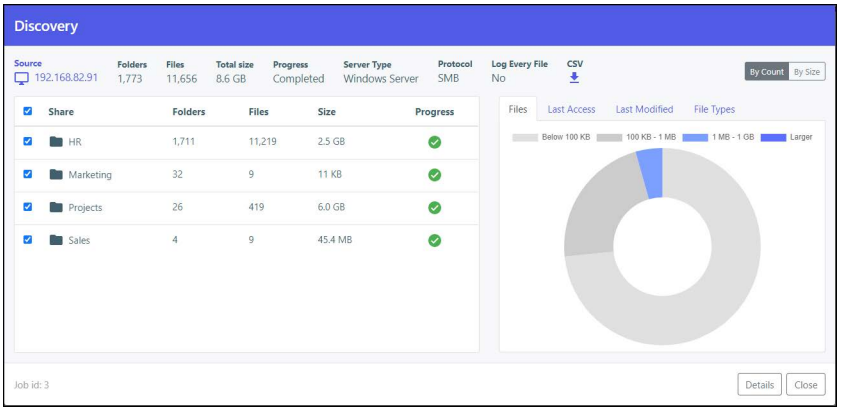
Clicking the icon displays the discovery report.

A report when **Log Every File (Verbose Logging)** was checked (the default):



If there are no errors, the **Error Logs** column is not displayed.

A report when **Log Every File (Verbose Logging)** was not checked.



At the top of the report the sum of the information for the migrated shares is displayed. Optionally, click the CSV icon to download the discovery report as a .csv file.

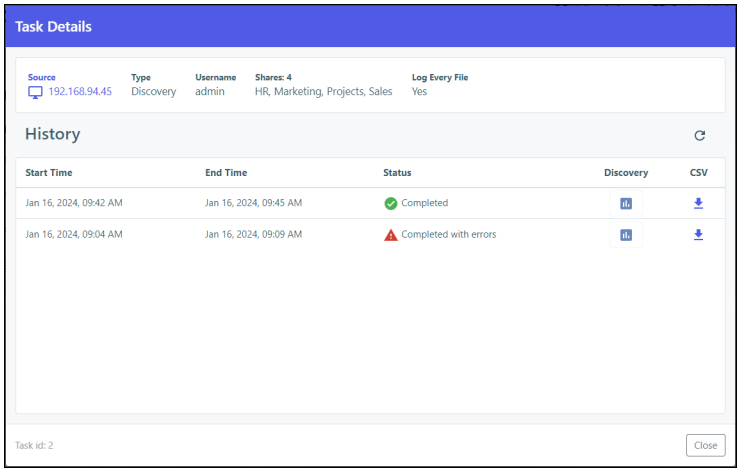
The first pane in the discovery report shows the list of shares with details of each share:

- The number of folders in the selected shares.
- The number of files in the selected shares.
- The size of the selected shares.
- The status of the migration for the selected shares.

- If **Log Every File (Verbose Logging)** was checked, optionally for each share, click the CSV icon to download the discovery report for the share as a .csv file.
- Any errors in the discovery job are written to a separate log, under `/errorlog`. Each share with an error has a separate log file. Clicking the icon downloads the log file as a .csv file.

The second pane in the discovery report has tabs showing the following:

- **Files** – A pie chart with the sizes of the files in the selected shares.
- **Last Access** – A bar chart showing when the files in the selected shares were last accessed.
- **Last Modified** – A bar chart showing when the files in the selected shares were last modified.
- **File Types** – The list of the file types in the selected shares.
  You can display this information either **By Count**, for example, the number of each file type, or **By Size**, for example, the size of each file type.
- Click **Details** to display the list of every time this job was run and rerun with the results of each run.



- Click **Close** to return to the **Dashboard**.

Migrating Shares

Migrate shares to the HCP Anywhere Enterprise Edge Filer. The shares are created on the HCP Anywhere Enterprise Edge Filer and the HCP Anywhere Enterprise Portal. The shares are not created at the root cloud folder level but at the subfolder level because ACL permissions cannot be managed at the root cloud folder level, only at the subfolder level.

Note: Before starting a migration, all non-essential features like local deduplication, antivirus, and HCP Anywhere Enterprise Ransom Protect should be disabled.

Preparing the HCP Anywhere Enterprise Portal to Migrate WORM Compliant Shares

When migrating a WORM compliant share, there must be a WORM Compliant Cloud Folder on the HCP Anywhere Enterprise Portal for the files to be synced from the HCP Anywhere Enterprise Edge Filer. This cloud folder must, therefore, be created before the migration is performed. Use the retention settings from the source file system when defining the WORM Compliance settings for the cloud folder. For details about creating a WORM Compliant cloud folder, see the section *Folder (WORM) Compliance: HCP Anywhere Enterprise Vault* in the *Managing Folders and Folder Groups* chapter in the *HCP Anywhere Enterprise Portal Team Administration Guide*.

The cloud folder is specified in the migration job as the destination for the WORM compliant share from the source file system. You define a separate WORM compliant cloud folder for every WORM compliant share on the source file system and run the migration for each share, one share at a time.

When migrating a WORM compliant share together with non-WORM compliant shares, you have to run a migration job that migrates the WORM compliant share and a separate migration job that migrates the non-WORM complaint shares.

If you are migrating from Hitachi Content Platform Gateway (HCP Gateway), in the HCP Gateway Policy page note any include and exclude policies that you will specify when setting up the migration job.

Commands to Run Before and After the Migration

Before starting a migration of a WORM compliant share you must run the following command on the HCP Anywhere Enterprise Portal: `calculateRetentionFromCreationTime portals/<portal_name>/cloudDrives/Users/<owner_name>/<cloudfolder_name> BACK_DATE_BIT`

where:

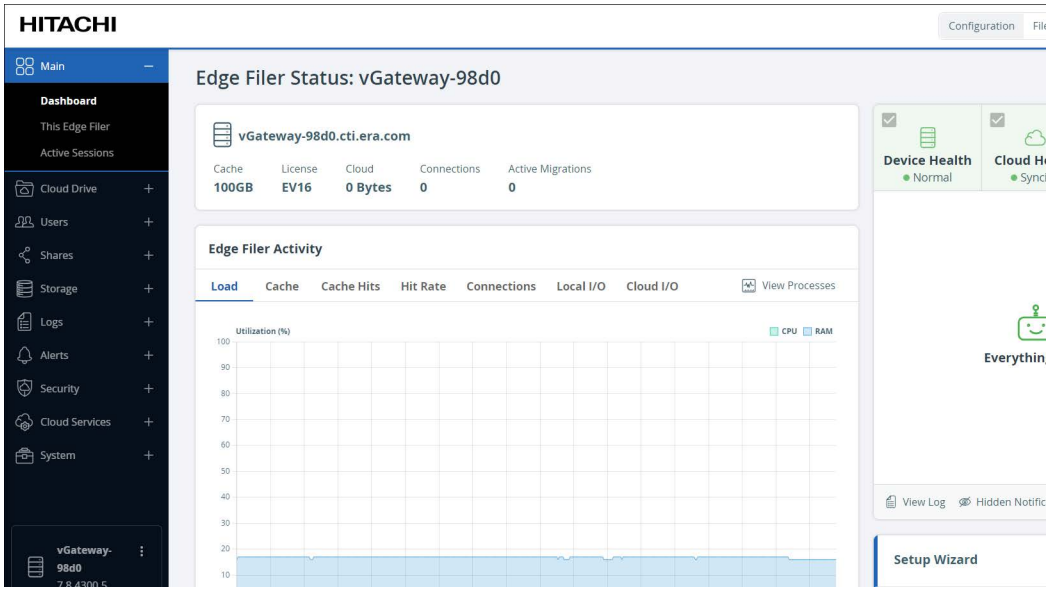
portal_name – The name of the team HCP Anywhere Enterprise Portal where the WORM compliant cloud folder is defined.
owner_name – The name of the team HCP Anywhere Enterprise Portal admin user who owns the WORM compliant cloud folder.
cloudfolder_name – The name of the WORM compliant cloud folder.

After the migration of the WORM compliant share completes, you must run the following command on the HCP Anywhere Enterprise Portal: `calculateRetentionFromCreationTime portals/ <portal_name>/cloudDrives/Users/<owner_name>/<cloudfolder_name> NONE`

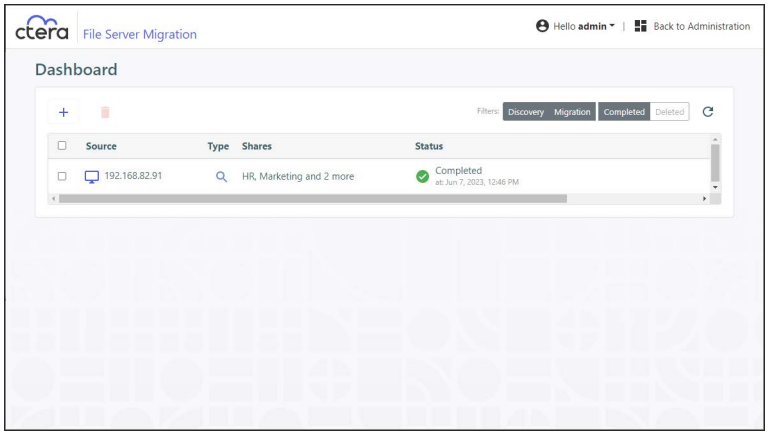
Migration Procedure

To migrate shares to the HCP Anywhere Enterprise Edge Filer:

1. In the **Configuration view**, select **Main > Dashboard** in the navigation pane.
   The **Dashboard** page is displayed.

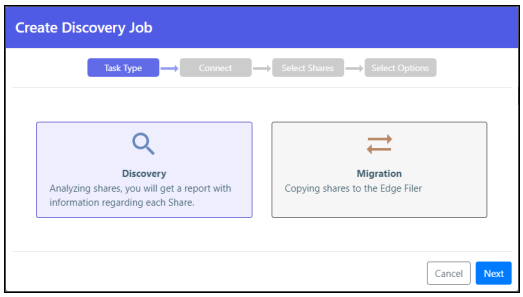


2. Click **File Server Migration**.
   The **File Server Migration** page is displayed.



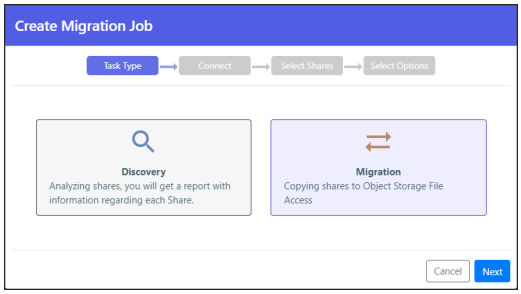
3. Click **+** to create a new job.

   The **Create Discovery Job** wizard is displayed, showing the **Task Type** step.



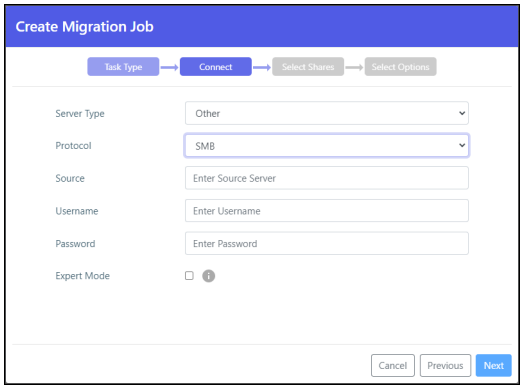
   The default job is a discovery job.

4. Click the **Migration** job to change the job to migrate a file server.



5. Click **Next**.

   The **Connect** step is displayed.

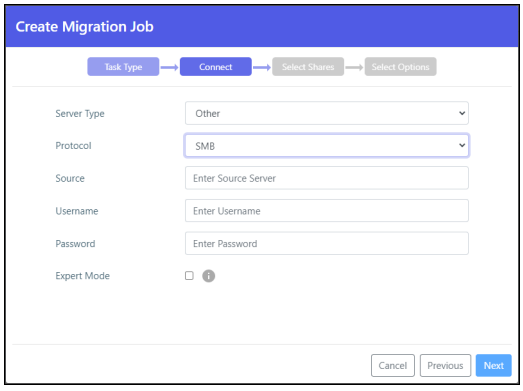


6. Select the server type to connect to from the drop-down box. You can connect to one of the following:
   - Azure StorSimple
   - HCP Gateway
   - Hitachi Data Ingestor
   - Isilon OneFS
   - Microsoft Azure Files
   - Nasuni Edge Appliance
   - NetApp ONTAP
   - NetAPP StorageGRID 9 (SMB)
   - NetAPP StorageGRID 11 (SMB)
   - Panzura Freedom Filer
   - Windows Server

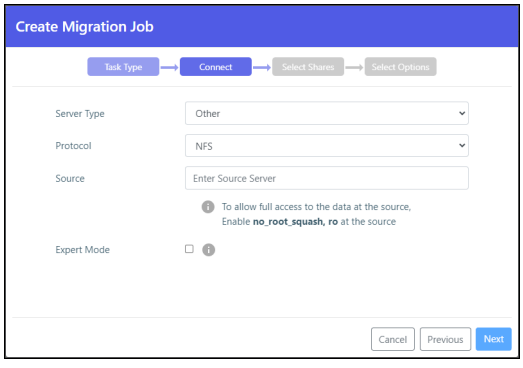
   Another option, **Other**, is available to attempt to migrate from a file server that is not listed.
7. Select the protocol to use for the migration: **SMB** or **NFS**.

   Both NFS versions 3 and 4 are supported.
   The wizard window changes depending on the protocol selected.

SMB



NFS

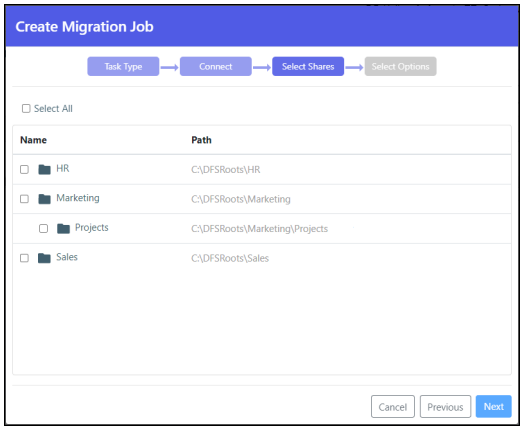
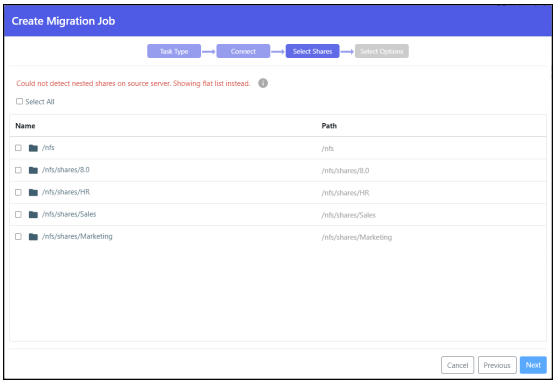


8. Enter the IP address or DNS name for the source file server.
9. When **Protocol** is **SMB**, enter an administrator user name and password to access the server.

   Note: The administrator used must have access to the files to migrate.
10. For **Microsoft Azure Files**, the shares cannot be presented and have to be added manually. **Expert Mode** is automatically selected to enable specifying the shares in the next step.

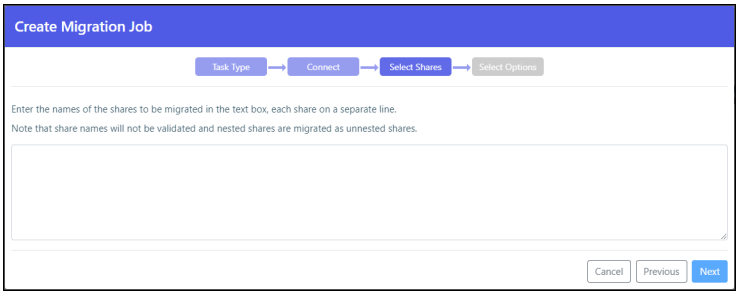
11. Click **Next**.

    The **Select Shares** step is displayed. For example:

SMB	NFS
	

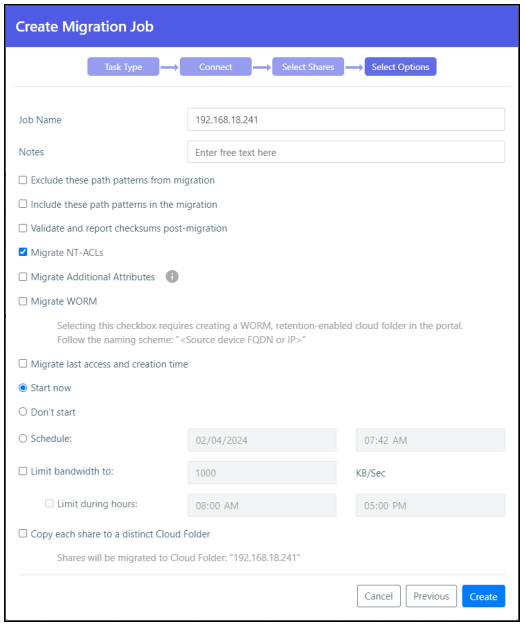
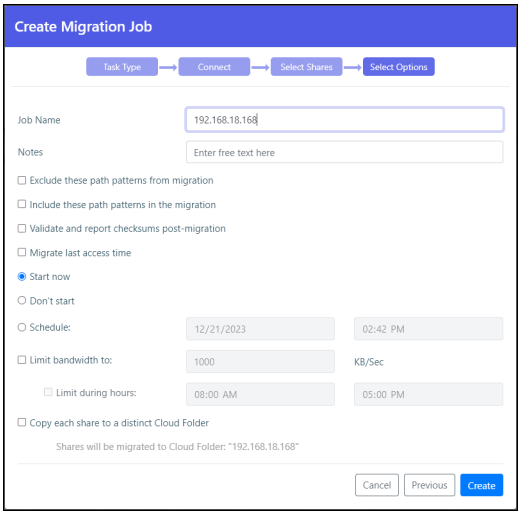
When migrating WORM compliant shares, select the relevant shares. You also check **Migrate WORM**.

Note: When **Expert Mode** is selected, the following window is displayed where you enter the shares to migrate.

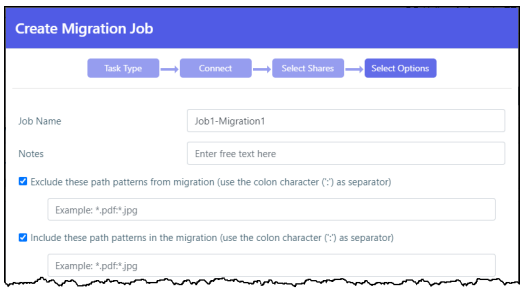


12. Select the shares to migrate and click **Next**.

The **Select Options** step is displayed.

SMB	NFS
	

13. Optionally, provide a different name for the job and any specific notes about the job.
14. You can specify patterns that you do not want to migrate, or that you do want to migrate, separating each pattern with a colon (:). You can include the asterisk (*) as a wildcard in the pattern. To specify the pattern, check the relevant box.
    - Exclude these path patterns from the migration (use the colon character (':') as a separator)
    - Include these path patterns in the migration (use the colon character (':') as a separator)



When the migration protocol is SMB:
To include only WORM compliant folders in a share to migrate, and exclude all the other folders in the share:

- If you are migrating from HCP Gateway, specify the shares to include and the shares to exclude that you noted in the HCP Gateway policy page. You also check **Migrate WORM**.

Note: Using the option to migrate specific folders can cause a migration to fail, depending on the size of the folders being migrated and the amount of RAM available to the HCP Anywhere Enterprise Edge Filer.

15. Check **Validate and report checksums post-migration** to include an MD5 hash checksum for every file being migrated to verify that the migration was successful when the hash is compared with the checksum of the file in the source file server.

Note: The checksum validation is performed after all the files are migrated. Depending on the number of files to check, the validation can take some time. You should not allow users to access the migrated files until the actual migration job finishes, after the validation completes, in case there is a checksum discrepancy for one or more of the migrated files that needs resolving.

16. **When the migration protocol is SMB**: Check **Migrate NT-ACLs** to migrate the data from the file server with the ACLs.

    Note: If **Migrate Additional Attributes** is checked, then **Migrate NT-ACLs** is also checked and cannot be unchecked.
    Alternate data streams (ADS), including macOS tags, cannot be migrated. POSIX ACLs are migrated when **Migrate NT-ACLs** is checked.
    When the migration protocol is NFS: Alternate data streams (ADS), including macOS tags, and POSIX ACLs, cannot be migrated.

17. Check **Migrate Additional Attributes** to migrate supported extended attributes. The supported extended attributes are listed in the cloud drive folder created on the HCP Anywhere Enterprise Portal.

    Note: If **Migrate Additional Attributes** is checked, then **Migrate NT-ACLs** is also checked and cannot be unchecked.

    Warning: Only check Migrate Additional Attributes when the HCP Anywhere Enterprise Edge Filer is connected to a HCP Anywhere Enterprise Portal version 8.1.x and higher.

18. **When the migration protocol is SMB**: Check **Migrate WORM** to migrate WORM data from the file server.

    Note: When **Migrate WORM** is checked, **Migrate NT-ACLs** is also checked and cannot be unchecked.

19. Check **Migrate last access and creation time** to include in the migration the last access time and the creation time for each item being migrated.

    Note: When **Migrate WORM** is checked, **Migrate last access and creation time** is checked by default and cannot be unchecked. These times are used to calculate the remaining retention period for each file in the share. If the retention time was changed in the source file system, this is not reflected in the destination and the migration calculated the remaining retention for all the files in the share based on the last retention defined for the source file server and used in the definition of the WORM compliant cloud folder on the HCP Anywhere Enterprise Portal.

20. You can specify when to start the migration:
    - **Start now** to start the migration immediately.
    - **Don't start** to save the job configuration for later use.
    - **Schedule** to schedule the date and time to start the migration.

21. Check **Limit bandwidth** to throttle the bandwidth used for the migration to apply this throttling so as not to adversely impact ongoing work.
    - Check **Limit during hours** to throttle the time range to apply this throttling so as not to adversely impact ongoing work.

22. Check **Copy each share to a distinct Cloud Folder** if you want to specify that each share is migrated to a distinct cloud folder.

    Note: When migrating WORM compliant shares, **Migrate WORM** is checked, specify the name of the cloud folder that was defined as WORM compliant on the HCP Anywhere Enterprise Portal as the destination.

    The cloud folder where the cloud folders are migrated is displayed under the **Copy each share to a distinct Cloud Folder** checkbox.

When **Copy each share to a distinct Cloud Folder** is checked:

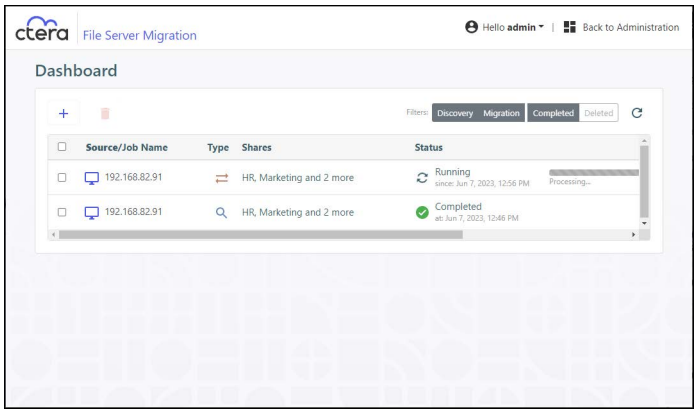
- Jobs that were created in a previous version will continue to migrate into the cloud folder root directory.
- New jobs will create a redundant directory with the name of the source share into the cloud folder root directory, and migrate into it instead.

When **Copy each share to a distinct Cloud Folder** is not checked:

- Depending on the source exposing the data, either the full path in the original server is recreated and no files are migrated into the cloud folder root, or the share name is used under the cloud folder root as was the case in previous versions.

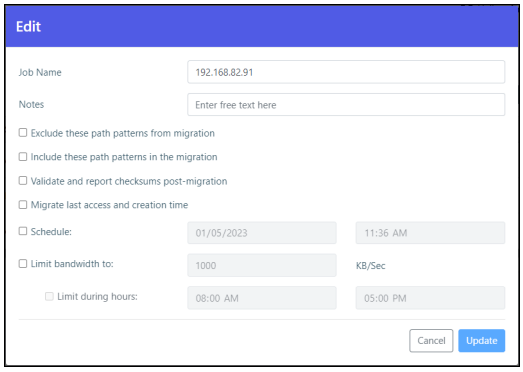
23. Click **Create**.

During the migration, the progress bar in the **Dashboard** shows the percentage completed and what is currently being processed.

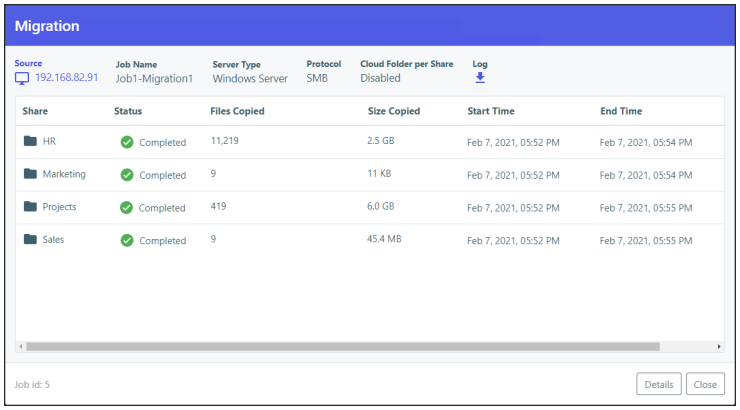


After migrating all the shares, the job completes and an email alert is sent with the job summary.

24. Click the icon to edit the migration job name, notes, include and exclude paths, migration checksum, whether to migrate access and creation times, schedule and throttling.



25. Click the icon to display the migration report.

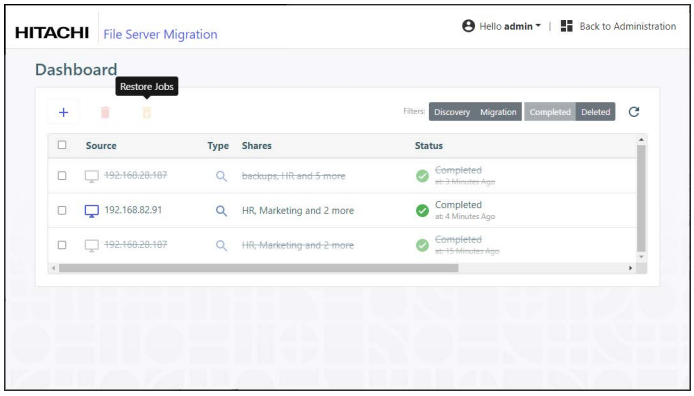


26. Optionally, click the Log icon to download the migration log file to a .log text file.

27. Click the ⓘ icon to display the list of every time this job was run with the results of each run, including the start and end times for the job, the number of files migrated and the total size of the migration, access to the report and the ability to download the log, which provides information about the migration and any errors that occurred during the migration.

28. Optionally, in the dashboard, you can select a job and click the 🗑 icon to delete the job.

After deleting a job, you can display all the jobs including the deleted jobs by clicking the **Deleted** filter in the dashboard.



You can restore deleted jobs by selecting the deleted jobs to restore and clicking the 🗑 icon.

The share structure from the source is recreated on the HCP Anywhere Enterprise Edge Filer, including nested shares and their permissions. If there are any recoverable errors during the copy process, retry the migration for the failed shares.

Note: Only ACLs are migrated with the files. Windows extended attributes are not migrated. In the HCP Anywhere Enterprise Edge Filer, the shares are defined with Windows ACL Emulation Mode.

Direct all the users to the HCP Anywhere Enterprise Edge Filer.

Users can now access and work on the HCP Anywhere Enterprise Edge Filer.

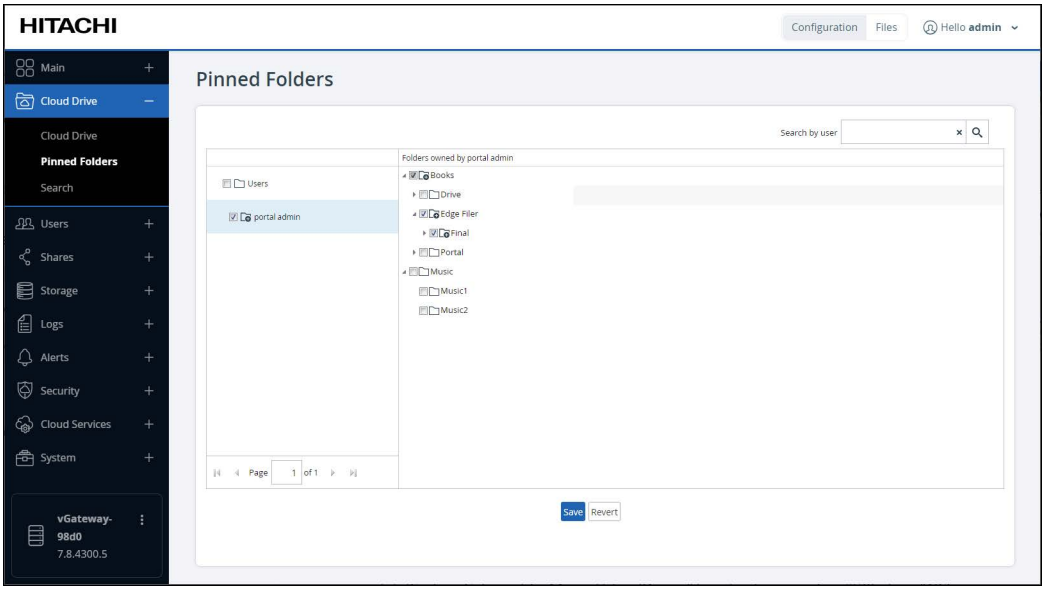
Note: If you enabled **deduplication** and then run a migration, the file system is automatically re-indexed. You must **not** restart the HCP Anywhere Enterprise Edge Filer while the re-indexing is being performed. If the HCP Anywhere Enterprise Edge Filer is restarted while re-indexing is being performed, any file that was not re-indexed when the HCP Anywhere Enterprise Edge Filer was restarted, is never evicted from the HCP Anywhere Enterprise Edge Filer.

Completing a Migration and Performing a Delta Migration

After completing the migration, there may well be a number of new or changed files on the original file server that require migrating. Complete the migration process using the following procedure.

To complete a migration:

1. During off-peak hours, disconnect the filer server.
2. In the HCP Anywhere Enterprise Edge Filer user interface, pin the folders that you want to remain local to the HCP Anywhere Enterprise Edge Filer.
   a) In the **Configuration** view, select **Cloud Drive > Pinned Folders** in the navigation pane. The **Pinned Folders** page is displayed.



   The **Pinned Folders** area is separated into a users pane and folders pane, with paging in the users pane. This makes it easier to page through the users and select the folders to pin.
   b) Select a user to display the folders owned by the user and then select the folders that you want pinned for this user, so that the folder content is always available on the HCP Anywhere Enterprise Edge Filer.
   In addition, you can use the search field to jump to a specific user.
   Note: You can select a a user to select all the folders and subfolders owned by the user. You can also select a higher level folder to select all the subfolders under it and then uncheck specific folders to unpin them. If you check a cloud folder, all the subfolders under the cloud folder are pinned, and any folders added later under the cloud folder will be pinned automatically.
   c) Click **Save**.

The checked folders are pinned.

3. In the **Configuration** view's **Main > Dashboard** page, click **File Server Migration**.

   The **File Server Migration** page is displayed, showing the discover and migration jobs previously run.

4. Select the migration job to rerun and click the ▶ icon.

The migration job reruns, migrating the deltas from the last migration.

Note: If you enabled **deduplication** and then re-run the migration, the file system is automatically re-indexed. You must **not** restart the HCP Anywhere Enterprise Edge Filer while the re-indexing is being performed. If the HCP Anywhere Enterprise Edge Filer is restarted while re-indexing is being performed, any file that was not re-indexed when the HCP Anywhere Enterprise Edge Filer was restarted, is never evicted from the HCP Anywhere Enterprise Edge Filer.

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